



Infrastructure Assurance for Mobile Telephony

The rugged quest for a policy baseline

Master Thesis

Nelson H. Enano, Jr.
Engineering and Policy Analysis

August 2008

*“Harmonizing Infrastructure Assurance Initiatives in Telecommunications through
Adaptive Policy Baseline Benchmarking”*

Faculty of
Technology, Policy and Management
Information and Communication Technology
Policy, Organization, Law and Gaming

 **TU**Delft

Infrastructure Assurance for Mobile Telephony

The rugged quest for a policy baseline

Name	Nelson H. Enano, Jr.
Student Number	1330268
Course Number	EPA 2941
Email	n_enano_jr@yahoo.com
Date	August 2008
University	Technische Universiteit Delft
Faculty	Faculty of Technology, Policy and Management
Sections	Information and Communication Technology Policy, Organization, Law and Gaming

Graduation Committee

Dr. ir. Jan van den Berg	Section Professor	TU Delft
Dr. Tineke Egyedi	First Supervisor	TU Delft
Dr. Mark de Bruijne	Second Supervisor	TU Delft
Eric Luijff, MSc	External Supervisor	TNO Defence, Security and Safety

*“Harmonizing Infrastructure Assurance Initiatives in Telecommunications through
Adaptive Policy Baseline Benchmarking”*

Preface

Mobile telephony has never failed to amaze us. Since its inception more than two decades ago, it has continued to connect people worldwide becoming one of the prime global means of long-distance communication. Its penetration in developing countries is phenomenal -- the fastest rate of diffusion ever as compared to other high-end technologies introduced in this generation. In countries where fixed-line is barely available, mobile telephony practically defines the meaning of telecommunications. Aside from its traditional multimodal functionality of voice and data, this infrastructure has become the backbone of a multitude of financial transactions, an indispensable means of information dissemination, a significant source of livelihood and an important facilitator in abating the great societal divide. Its impact to the economy, education, politics and governance, social cohesion and coordination, more especially in developing countries, is truly undisputable.

The risk factors to the continuity of quality and efficient mobile telephony products and services are, however, increasing in number. Their sources are countless, but those that prevail to get attention include: nature of technology architecture, shifts in the trends of business and governance models, pressures due to the fragmentation of its ecosystem, globalization and other international systems change. The purpose of this study is to provide a means to assure mobile telephony, in the global setting, amidst all the risk factors surrounding it. And such is, by experience, indeed a daunting task! This report never comes to its present form without the assistance, push and inspiration of the following well-valued people and organizations:

- International Telecommunication Union, Christine, Robert, Tim, Martin, Xiaoya, Georges and Sarah;
- GSM Association, Tom and Jeanine;
- Ministry of Economic Affairs, The Netherlands, Hans, Simon and Jacqueline;
- Federal Office for Information Security, Germany, Dirk, Tom, and Susanne;
- Federal Department of Defense, Civil Protection and Sport, Switzerland, Stefan;
- Federal Office of Police, Switzerland, Marc;
- National Economic and Development Agency, The Philippines, Kenneth, and Grace;
- TNO-Defence, Security and Safety, The Netherlands, Eric;
- TUDelft, The Netherlands, Jan, Tineke, Mark, Michel, Jean-François, Toke Hoek, Martin, Jos, Jo-Ann;
- Royal KPN N.V., Michael, Cindy, and Christel;
- ETSI Rapporteur on 3GPP work item on PWS, T-Mobile, Mark;
- ETSI Rapporteur on 3GPP work item on ETWS, NTTDoCoMo, Inc., Ryo;
- Globe Telecom, Jenny and Benjie;
- Michelle L.A. Mendoza;
- My parents and siblings, relatives; and
- Classmates and friends

This paper involves a number of people and organizations. A careful editing was provided; nevertheless, I hold responsible for any inaccuracies that may have arisen.

“Bedankt voor uw interesse en moge dit stuk van waarde voor u zijn”
(Thank you for your interest and hope you find a value out from this humble piece of work.)

Nelson H. Enano, Jr.
Delft, The Netherlands
August 2008

Executive Summary

GENERAL

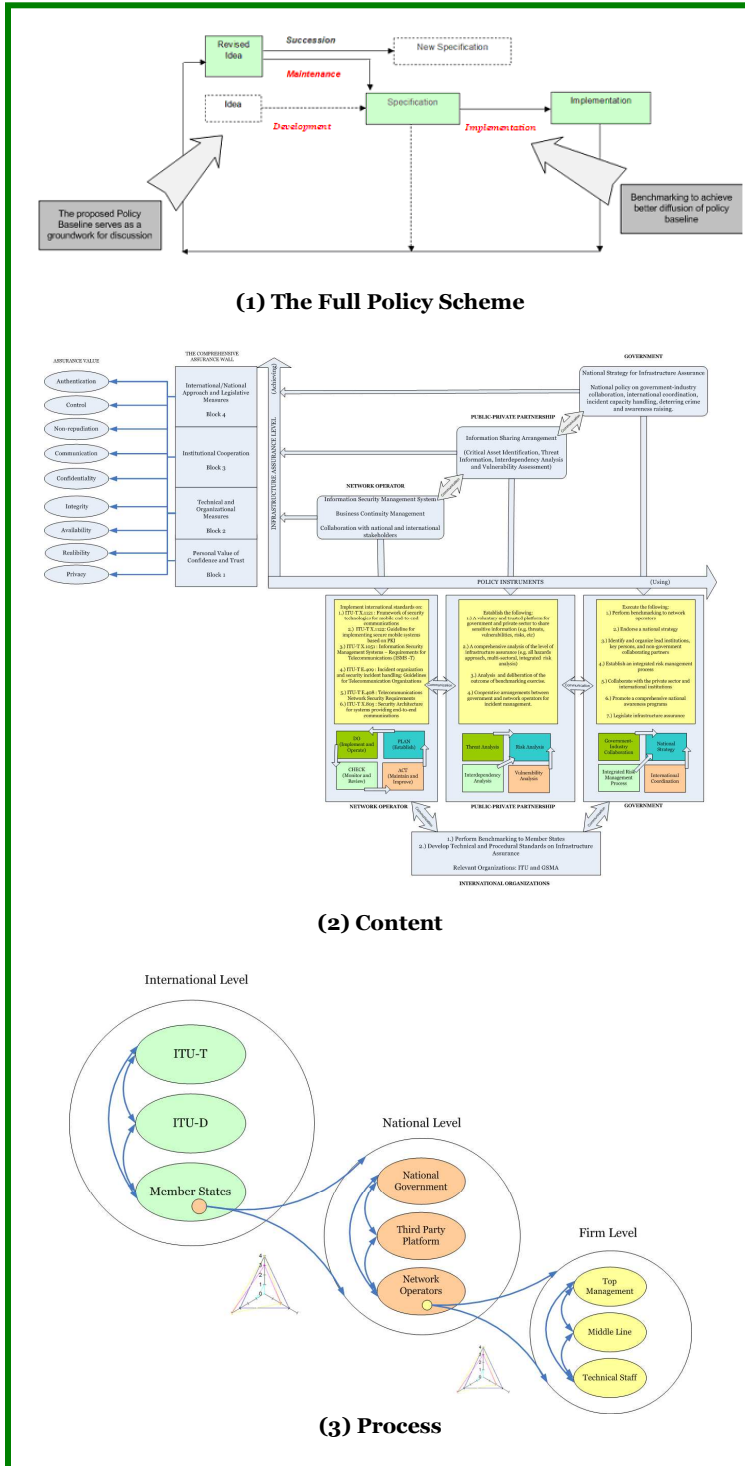
The International Telecommunication Union (ITU) has been mandated by its membership to take concrete steps to curb the threats and vulnerabilities of the global telecommunications infrastructure. One of the strategies being pushed forward in ITU Resolutions 130 (Rev. Antalya, 2006) is the harmonization of infrastructure assurance policy initiatives to its member states to address the call for international, national and regional coordinated and collaborative action to this issue. This strategy, in particular, is a response to the clear need of developing countries for assistance as they create national capacities to ensure the assurance of their telecommunication infrastructure that plays an indisputable important role in the efficient functioning of their society. The task of global harmonization can be very difficult to implement and fragmented because of the differing mandates of national governments and the innate technical and political complexities of the issue of infrastructure assurance. The study has found that the mechanism to be employed should not be intrusive, in the sense that it is non-regulatory and does not detract the infrastructure from achieving its innovative capacity. The focus infrastructure of this study is the mobile telephony infrastructure, a global telecommunication infrastructure considered to be critical by most of the countries in the world.

OBJECTIVE

The main objective of this study is to provide the relevant international organization, which is the ITU as this study advocates, a full policy scheme on how to harmonize initiatives through adaptive policy baseline benchmarking to improve the global infrastructure assurance of mobile telephony (shown in fig. 1 in the left). This study strives to put forward the infrastructure assurance case of mobile telephony into the international discussion to achieve substantive explication of the issue. The study mainly endeavors to answer the inquiry as stated as follows:

“How to ensure infrastructure assurance for mobile telephony in the global setting?”

This main research question is tackled through answering the sub-research questions. These sub-research questions are individually answered in each of the subsequent chapters. This study is a qualitative study that aims to present the encompassing issue of infrastructure assurance with a focus on mobile telephony though defining a policy baseline that sets the reference policies needed to ensure infrastructure assurance.



** Legible illustrations are provided in the chapters where they are thoroughly explained.

A benchmarking process will be employed afterwards to attain greater diffusion of the policy baseline. The “effectiveness” of the policy baseline will be evaluated through two analyses done ex-ante, namely SWOT Analysis and Policy Transplantation Assessment.

APPROACH

There are various research methods employed in this study to achieve a more substantive report. Various literatures ranging from magazine articles to ITU reports were used in this study. Literature review was conducted especially on the inquiry on how the Standardization Process and Policy Benchmarking can lead to greater harmonization of initiatives. Comparative analysis was done to identify essential policy lessons from three model countries, namely the Netherlands, Germany and Switzerland. The policy transplantation assessment uses the contextual setting of a developing country, namely the Philippines, to provide a hint on the suitability of the policy lessons identified. In addition, expert discussion was conducted to get a general perception of the perspectives of relevant experts/stakeholders on the issue. The views of selected international organizations, national governments and network operators were obtained. Invited experts from the academia also contributed to the clarification of the issue. The rationale on the choice of respondents will be provided.

POLICY GOALS

The main policy goal of the study, as has been expressed above, is to improve mobile telephony infrastructure assurance done through harmonization of initiatives with adaptive policy baseline international benchmarking as the policy instrument. This scheme leads to better awareness of stakeholders in the international, national and firm level frames. This helps in assessing the present level of assurance of relevant stakeholders in reference to the developed policy baseline. It casts roles and responsibilities to actors clarifying the inquiry on “who is responsible for what?”. More importantly, this policy scheme is beneficial to developing countries as their weaknesses are identified and are being aided by partners to achieve greater national capacity. These could be in the area of legal, technical and procedural measures, organizational structures and international cooperation. Identifying “good” practices abroad is found to be resource intensive if individually done by developing countries themselves.

PROPOSED PRELIMINARY POLICY BASELINE

The main output of this study is summarized as follows.

Policy Baseline (shown in fig. 2 above)

The policy baseline for mobile telephony consists of the following:

Assurance Levels:

Assurance Level 1: Building personal value of trust and confidence

Assurance Level 2: Implementing organizational and technical assurance measures

Assurance Level 3: Engaging into institutional cooperation

Assurance Level 4: Creating a national strategy with an international perspective

Casting Roles:

Network Operators:

1. Implement Information Security Management System
2. Create Business Continuity Planning and Management
3. Collaborate with other institutions in a public-private partnership setting

Government:

1. Create a coherent national strategy with emphasis on integrated risk analysis and management, government-industry collaboration and international coordination.
2. Collaborate with the market players
3. Perform a benchmarking exercise to network operators

Public-Private Partnership:

1. Create a trusted third party platform to perform a comprehensive risk analysis based on vulnerability, threats and dependency information.

Coordination Mechanism: International Benchmarking (shown in fig. 3 above)

ITU: 1. Define the policy baseline employing standardization process

2. Perform international benchmarking to member states using the adaptive policy baseline

Member States: Perform benchmarking to network operators using the adaptive policy baseline

Further recommendation on the proposed scheme and specific policy advice for relevant stakeholders will be provided. A reflection on the result and conclusion of the study is also presented.

Table of Contents

Preface.....	i
Executive Summary.....	ii
Glossary	
Country Codes	x
Definitions of Key Concepts	x
Acronyms.....	xii
Table of Contents.....	v
List of Figures and Tables.....	viii

CHAPTER 1: INTRODUCTION

1.1 Background	1
1.2 Problem Description	2
1.2.1 Intricacy in Harmonizing Initiatives.....	3
1.2.2 Lack of Capacity and Resource in Developing Countries	3
1.2.3 Marketplace Insufficiency	4
1.2.4 Inefficacy of Regulation.....	4
1.2.5 Absence of Public-Private Partnership	4
1.2.6 Complexity and Sensitivity of the Issue.....	5
1.3 Research Objective	5
1.4 Research Questions	5
1.4.1 Main Research Question	5
1.4.2 Sub-research Questions.....	5
1.5 Scope of Research Questions	6
1.5.1 Domain Description	6
1.5.2 Conceptual Framework	6
1.5.3 Formulation of the Preliminary Policy Baseline	6
1.5.4 Evaluation of the Solution Space	7
1.5.5 Recommendations	7
1.6 Research Approach.....	7
1.6.1 Inception Phase	7
1.6.2 Analysis and Design Phase.....	8
1.6.3 Evaluation Phase.....	9
1.6.4 Reflection Phase.....	9
1.7 Outline of the Report	11

CHAPTER 2: DOMAIN DESCRIPTION

2.1 Aim of the Chapter	12
2.2 Institutional Fragmentation.....	13
2.3 Vulnerabilities	14
2.4 Hazards and Threats.....	19
2.5 Risk Factors	21
2.6 Dependencies in Mobile Telephony.....	22
2.7 Impact and Criticality of Mobile Telephony to Developing Countries.....	23
2.8 Adaptive Policy Baseline as a Possible Solution Space	24
2.9 Integration.....	25
2.10 Key Messages of Chapter 2.....	26

CHAPTER 3: CONCEPTUAL FRAMEWORK

3.1 Aim of the Chapter	27
3.2 Infrastructure Assurance Delineated	27
3.3 Standardization and Policy Harmonization	28
3.4 Benchmarking and Policy Harmonization	30
3.4.1 Benchmarking Defined	31
3.4.2 Benchmarking as a Public Policy Tool	33
3.4.3 Harmonization Process	36
3.5 Filling up the Gap	39
3.6 Key Messages of Chapter 3	39

CHAPTER 4: FORMULATION OF THE PRELIMINARY POLICY BASELINE

4.1 Aim of the Chapter	41
4.2 What can be learned from the national arrangement of the model countries?	41
4.2.1 The Netherlands	41
4.2.2 Germany	47
4.2.3 Switzerland	51
4.2.4 Comparative Analysis of the Model Countries	54
4.2.5 Philippines	55
4.2.6 Integration of the Policy Lessons Identified	58
4.2.7 Sample Benchmarking Exercise	60
4.2.8 Defining Levels of Assurance	62
4.2.9 International Benchmarking Exercise	63
4.3 What are the present initiatives of the selected international organizations?	66
4.3.1 International Telecommunication Union	66
4.3.2 GSM Association	68
4.4 Policy Baseline and the International Organizations	68
4.5 What can be learned from experts?	69
4.5.1 Discussion of the Perspectives of Selected Experts/Stakeholders	70
4.6 Insights Identified from Selected Stakeholders' Perspectives	73
4.7 The Design of the Policy Baseline	74
4.8 Key Messages of Chapter 4	80

CHAPTER 5: EVALUATION OF THE PROPOSED POLICY BASELINE

5.1 Aim of the Chapter	81
5.2 SWOT Analysis	81
5.2.1 Strengths of the Proposed Policy Baseline	82
5.2.2 Weaknesses of the Proposed Policy Baseline	82
5.2.3 Opportunities of the Proposed Policy Baseline	83
5.2.4 Threats of the Proposed Policy Baseline	84
5.3 Policy Transplantation Assessment	85
5.3.1 Proposition 1: Imposition versus Adoption	86
5.3.2 Proposition 2: "Xeroxing" versus Adaptation	86
5.3.3 Proposition 3: Single Model versus Multiple Models	87
5.3.4 Proposition 4: Endogamy versus Exogamy	87
5.3.5 Proposition 5: Concrete Procedures versus Guiding Principles	87
5.3.6 Proposition 6: Performance crisis versus protracted sense of dissatisfaction	87
5.4 Performance of the Proposed Policy Baseline	88
5.4.1 Based on SWOT Analysis	88
5.4.2 Based on Policy Transplantation Assessment	89
5.5 Key Messages of Chapter 5	89

CHAPTER 6: CONCLUSION AND RECOMMENDATIONS

6.1 Conclusions.....	91
6.2 Recommendations	95
6.2.1 Recommendations in Response to the Evaluation of the Policy Baseline.....	95
6.4 Recommendations to the Standardization Process.....	97
6.5 Recommendations to the Benchmarking exercise.....	98
6.6 Recommendations to Specific Stakeholders.....	98
6.6.1 Recommendation to ITU.....	98
6.6.2 Recommendation to Member States.....	99
6.6.3 Recommendation to GSMA.....	99
6.6.4 Recommendation to Network Operators.....	99
6.6.5 Recommendation for End-Users.....	99
6.6.6 Recommendation to the Philippine Government.....	99
6.7 Further Research Recommendations.....	100

CHAPTER 7: REFLECTION.....	101
----------------------------	-----

APPENDICES

A. Respondents and Inquiries.....	103
B. Electronic Communications Vulnerabilities	112
C. Description of GSM Family	114
D. Ecosystem for Infrastructure Assurance with ITU as the facilitating organization	118
E. Mobile Telecommunications Market in the Philippines	12020
F. Relevant Statistics.....	1222
G. ITU-T Telecommunications Security Standards	122
H. ITU and its Infrastructure Assurance Initiatives in Telecommunications	123
I. References	1244

PERSONAL NOTES.....	128
---------------------	-----

CURRICULUM VITAE.....	130
-----------------------	-----

List of Figures and Tables

FIGURES

Figure 1: The Inception Phase.....	7
Figure 2: Analysis and Design Phase.....	8
Figure 3: Evaluation Phase.....	9
Figure 4: Reflection Phase.....	9
Figure 5: Research Approach Framework.....	10
Figure 6: The Four Subsystems of GSM-based Mobile Telephony.....	16
Figure 7: The GSM Network and its Main Elements.....	17
Figure 8: General model of mobile end-to-end data communication.....	19
Figure 9: Security function required for each entity and relation between entities.....	20
Figure 10: Integrated Risk Analysis.....	21
Figure 11: Convergence of fixed-line and mobile telephony.....	23
Figure 12: Policy Baseline and the Standardization Process.....	30
Figure 13: Fields of Benchmarking.....	32
Figure 14: General Process of the Policy Baseline.....	34
Figure 15: Harmonization through Standardization and Benchmarking.....	37
Figure 16: Harmonization through Standardization and Benchmarking.....	37
Figure 17: Levels of Harmonization.....	39
Figure 18: Netherlands National Arrangement.....	44
Figure 19: Benchmarking Matrix.....	64
Figure 20: International Coordination Mechanism.....	65
Figure 21: Study Group 17 Inquiries.....	66
Figure 22: Infrastructure Assurance Level.....	75
Figure 23: Casting Roles for Stakeholders.....	77
Figure 24: Recommended Policy Instruments for Each of the Stakeholder.....	78
Figure 26: GSM Timeline.....	116
Figure 27: 3G Timeline.....	116

TABLES

Table 1: Some of the Issues in Infrastructure Assurance.....	12
Table 2: Some reasons of disintegration of institutions.....	13
Table 3: Vulnerabilities of Mobile Telephony.....	15
Table 4: GSM Family of Wireless Technology Platforms.....	18
Table 5: Threats in mobile end-to-end communications.....	19
Table 6: General Threats and Hazards.....	20
Table 7: Perceived Risk Factors in Mobile Telephony.....	21
Table 8: (Inter)-dependencies with other sectors.....	22
Table 9: Common GSM Services.....	23
Table 10: Utility of Mobile Telephony.....	23
Table 11: Factors of Diffusion.....	24
Table 12: Levels of governmental influence.....	25
Table 13: The need for harmonization of initiatives.....	25
Table 14: Problems in Implementing Standards.....	31
Table 15: Types of Benchmarks.....	32
Table 16: Pros and Cons of Externally Imposed Benchmarking.....	33
Table 17: Possible Complexities of Using Benchmarking in the Public Sector.....	36
Table 18: Integration.....	38
Table 19: Some Early CIP and CIIP Efforts.....	43

Table 20: Dutch Government Agencies involved in CIP	44
Table 21: Laws and Legislations relevant to CIP in the Netherlands	45
Table 22: PPP Initiatives	46
Table 23: Lessons Identified from the Activities of the Netherlands	46
Table 24: Initiatives for Situational Analysis	48
Table 25: Government Initiatives in Infrastructure Assurance	49
Table 26: Ministries and Agencies in Germany involved in Infrastructure Assurance	49
Table 27: Laws relevant to Assurance of Telecommunications	49
Table 28: Public-Private Partnership Initiatives	50
Table 29: Lessons Identified from the Activities of Germany	50
Table 30: Information Assurance Initiatives in Switzerland	52
Table 31: Swiss Chronology of Infrastructure Assurance Initiatives	52
Table 32: Government Agencies Involved.....	52
Table 33: Relevant Legislations	53
Table 34: PPP Initiatives	53
Table 35: Lessons Identified from the Activities of Switzerland.....	54
Table 36: Comparative Analysis Table	54
Table 37: National Arrangement in the Philippines	56
Table 38: Philippines Laws and Legislations dealing with Telecommunications/CIIP	56
Table 39: Public-Private Partnership in the Philippines	57
Table 40: Observation on Philippines National Arrangement.....	57
Table 41: Infrastructure Assurance Arrangements in Four Selected Countries	58
Table 42: Level of Infrastructure Assurance Measured through Initiatives Instituted.....	62
Table 43: Sample Benchmarking Exercise Table.....	63
Table 44: Initiatives Compared.....	64
Table 45: SG 17 Inquiries.....	67
Table 46: Standards presently available and the assurance value they provide	67
Table 47: GSMA Perspectives on Regulation	68
Table 48: Policy Baseline and the International Organizations.....	68
Table 49: Perception Test Results	69
Table 50: Insights from Experts/Stakeholders Interviewed.....	73
Table 51: Integration of Insights Derived from Results	74
Table 52: Definition of Assurance Values.....	76
Table 53: Infrastructure Assurance Defined	76
Table 54: Policy Transplantation Propositions	85
Table 55: Result of the Policy Transplantation Assessment	86
Table 56: SWOT Analysis Result	88
Table 57: Policy Transplantation Assessment Result	88
Table 58: Strategies Derived from SWOT Analysis	95

Country Codes

CH	Switzerland
DH	Germany
NL	Netherlands
PH	Philippines

Definitions of Key Concepts

(Adaptive) Policy Baseline	<p>A policy baseline is a set of reference policies agreed to be necessary to achieve a common goal [1]. A policy baseline is “adaptive” when its provisions can be framed unto a particular environment where it will be deployed [2].</p> <p>[1] adapted from the definition of reference standard, (Sherif, 1999) [2] adapted from the definition of adaptive policy, (Walker et al., 2001)</p>
(International) Benchmarking	<p>Benchmarking is the systematic process of comparing, measuring, analyzing and improving performance in terms of products/services/processes/initiatives of an entity against a reference entity (or entities) (E. Luijff et al., 2006).</p> <p>Benchmarking is often performed to attain a superior performance or to evaluate one’s performance relative to one’s (economic) effort (E. Luijff et al., 2006).</p> <p>Benchmarking becomes international when the sought reference entity (or entities) is (are) located abroad because the reference entities are simply not found within the home country or the number of entities is just too few to arrive to a valid result (E. Luijff et al., 2006).</p>
Infrastructure	<p>Infrastructure is a set of interconnected elements that provide the framework supporting an entire structure (Firth et al., 2006).</p>
(Critical) Infrastructure	<p>Critical Infrastructures (CI) are those assets and parts thereof which are essential for the maintenance of critical societal functions, including the supply chain, health, safety, security, economy or social well-being of people (Commission, 2006)</p>
Infrastructure Assurance	<p>Infrastructure Assurance is the set of planned and systematic actions necessary to provide confidence that the infrastructure is secure and reliable (Motteff & Parfomak, 2004).</p>
(Inter)-dependency	<p>Dependency is the relationship between two (or more) entities in which one entity is required for the operation of the other (E. Luijff et al., 2008).</p>

	An interdependency is a mutual dependency among the involved entities (ACIPconsortium, 2003).
Harmonization	<p>Harmonization is the process of coordinating different provisions by eliminating major differences and creating minimum requirements or reference standards. It is designed to incorporate different systems under a basic framework. It takes into account local factors and yet applies general principles to make a consistent framework (Menski, 2005).</p> <p>Said in another way: harmonization is the process of adjustment, of differences and inconsistencies among different measurements, methods, procedures, measures, schedules, or systems to make them uniform or mutually compatible. Harmonization of socio-technical systems can result in a baseline (set of minimum requirements) or a reference standard.</p>
Integrated Risk Management	Integrated risk management is a continuous, proactive and systematic process to understand, manage and communicate risk factors (Borodzicz, 2005) .
Public Good	<p>A public good is good that is non-rivalled and non-excludable (Block, 1983).</p> <p>The security and reliability of a public good, which is supplied by private operator(s) may demand government intervention in the market.</p>
Public-Private Partnership (PPP)	PPP is a cooperative venture between the public and private sectors aimed to meet the agreed public goal executed through the appropriate allocation of expertise, resources, risk and rewards (Spackman, 2002).
Risk	Risk refers to the uncertainty that surrounds future events and outcomes. It is the expression of the likelihood and impact of an event with the potential to influence the achievement of an objective (Stoneburner et al., 2002).
Risk Management	Risk management is a systematic approach to identify, assess, understand, reduce risk factors, accept and communicate the residual risk.
Standardization	<p>Standardization is the process of developing and agreeing upon a (set of) requirement(s) to be established. It is done through a consensus of involved experts [1].</p> <p>[1] adapted from the definitions of ISO/IEC and NNI</p>
Threat	Threat is a potential occurrence that can have an undesirable effect on the system's asset, resources, and its functioning (Dunn & Mauer, 2006).
Vulnerability	Vulnerability is a system's weakness that makes it possible for threat to occur (Chambers, 2004).

Acronyms

ARECI	Availability and Robustness of Electronic Communications Infrastructure
ASP	Application Service Provider
ASPR	Agreements, Standards, Policies and Regulations
BBK	Federal Office for Civil Protection and Disaster Response
BKA	Federal Criminal Police Agency
BMI	Bundesministerium des Innern (Federal Ministry of the Interior)
BPOL	Federal Police
BS	Base Stations
BSI	Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security)
BSC	Base Stations Controller
BSS	Base Station Subsystem
BTS	Base Transceiver Station
CEN	Comité Européen de Normalisation (European Committee for Standardization)
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection
DoS	Denial of Service
ECP.NL	Platform for Electronic Commerce in the Netherlands
EDGE	Enhanced Data Rates for GSM Evolution
ETSI	European Telecommunications Standards Institute
EU	European Union
GCA	Global Cybersecurity Agenda
GPRS	General Packet Radio Service
GPS	General Positioning System
GSM	Global System for Mobile Communications
GSMA	GSM Association
HLR	Home Location Register
HSPA	High Speed Packet Access
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IMT-2000	International Mobile Telecommunications-2000
ISB	Federal Strategy Unit for Information Technology
ISO	International Organization for Standardization
ISDN	Integrated Services Digital Network
ITU	International Telecommunication Union
ITU-D	International Telecommunication Union-Development Sector
ITU-R	International Telecommunication Union- Radiocommunication Sector
ITU-T	International Telecommunication Union- Standardization Sector
KPN	Koninklijke PTT Nederland (Royal PTT Netherlands)
LDC	Least Developed Countries
LTS	Large Technical System
MELANI	Reporting and Analysis Centre for Information Assurance
MS	Mobile Station
NACOTEL	National Telecommunications Continuity Plan
NAVI	Nationaal Adviescentrum Vitale Infrastructuur
NBI	National Bureau of Investigation
NCO-T	National Continuity Consultation Platform Telecommunication

NEDA	National Economic and Development Authority
NICC	National Infrastructure against Cyber Crime
NMS	Network Management System
NSS	Network and Switching Subsystem
OECD	Organisation for Economic Co-operation and Development
PCCIP	President's Commission on Critical Infrastructure Protection
PKI	Public Key Infrastructure
PPP	Public-Private Partnership
PSTN	Public Switched Telephone Network
SIM	Subscriber Identity Module
SG 17	Study Group 17
SMS	Short Message Service
SONIA	Special Task Force for Information Assurance
SWOT	Strength, Weaknesses, Opportunities, Threats
TCP/IP	Transmission Control Protocol/Internet Protocol
TDMS	Time Division Multiple Access
UMTS	Universal Mobile Telecommunications System
UN	United Nations
VLR	Visitor Location Register
WAP	Wireless Application Protocol
WCDMA	Wideband Code Division Multiple Access

1 Introduction

Privatization and liberalization of infrastructures have become the global trend in the governance of large-scale infrastructures since the latter half of the last century. These shifts in the model of governance are aimed to make infrastructures more efficient in their provision of products and services. As a consequence, in many cases, these economic policies improve financial and operating performance of infrastructure, yield fiscal and macroeconomic benefits and improve overall welfare in a multi-stakeholder setting (Nellis & Kikeri, 2002).

The greater welfare, as the gain of privatization and liberalization of infrastructures, is exhaustively illustrated in many literature entries (Treheux, 1992). Such economic model becomes like a readily available template, executing the concept in all means one can (De Vries, 2004). Privatization and liberalization-- implemented in all areas possible (Megginson & Netter, 2001). This research takes the risk of venturing to study the area where privatization and liberalization becomes the major source of the dilemma. This is when the government is traditionally expected to perform the leading role but hindered due to its close to nothing control on the infrastructure. Infrastructure assurance¹ is one of the public policy areas where a dilemma on casting responsibility arises (Abele-Wigert, 2006). Who should be tasked to assure the infrastructure and what roles have to be played?

1.1 Background

“Why the interest on global infrastructure assurance for mobile telephony?”

Mobile telephony is the focus infrastructure of the study. More than 90% of network providers in the world are owned and managed by private individuals and organizations (FEMA, 2007). The assurance of these networks has become an issue of increasing importance to society today. More and more networks are connected to the mobile telephony system, which widens its scope and functions, along with that is the growing number of players at stake to its security and reliability. Mobile telephony has radically become a critical infrastructure demanding assurance (Gow, 2005), most especially in developing countries where fixed-line telephone system fails to connect the many to the network. Criticality, in these places, becomes a question of alternatives available, in which developing countries more often than not fail by default.

85% of the world mobile communications are GSM-based networks (GSMA, 2007). This is then to say that GSM-based mobile telephony system is an infrastructure that anchors a global reach. One GSM network shares connection with other GSM networks (within a country or abroad) which utilizes radio-links from transmitters to satellite, uses the facility of fixed-line telephony (PSTN/ISDN) which are, as well, connected by wires and fiber optic cables either on land and under the sea, connects to the internet grid (TCP/IP) which are also dependent on data communications and satellite systems. The physical infrastructure itself is dependent on the facility provided by electricity and to some extent on other energy resources, water and transportation. Its network of manufacturers for equipment and materials needed for infrastructure installations and operations are scattered around the globe. Although most networks are operating nationally, there are growing markets that attained international in scope

¹ For definition, refer to the table for Definitions of Key Concepts

due to increasing mobility of subscribers, globalization, etc. (e.g. “diaspora”², greater chance to travel abroad). Content providers of mobile applications could virtually come from anywhere, and the linkages and list of (inter)-dependencies to this infrastructure seem to never end. For almost 15 years, the GSM standard was deliberated at the international level starting from European countries until it reached the platform of ITU in the form of IMT-2000 (GSMA, 2007). With its design to make the network as wide as possible, the infrastructure has the capacity to provide greater scales of services and, with that, become more efficient in its operation attributed to economics of scale and scope. The infrastructure is taking advantage of the network effect, which makes the network more useable as the more are connected to the end nodes (Birke & Swann, 2005). Becoming a global network, indeed, offers greater welfare, however, this, as well, paves to limitless arrays of vulnerabilities, threats from any source, and because of that, risks that undermine assurance become strikingly enormous. A network of networks has been proven to be favorable in many respects, but this, as well, goes without saying that the whole network is facing a myriad of vulnerabilities by just being such (De Bruijne, 2006). This justifies the grounds of this study that infrastructure assurance for mobile telephony is a global concern demanding a concerted effort from all its stakeholders. This goes in consonance to the need of telecommunications sector to be assured from being insecure and unreliable (ITU GCA, 2008), including those of other telecommunication technologies such as the cyberspace, fixed telecommunication network services, radio communication and navigation, satellite communication and General Positioning System (GPS), broadcast services, and postal and courier services (E. Luijff et al., Sept. 2003). The level of assurance differs in each of these telecommunications technologies depending on the maturity of the technology and degree of their importance to mainstream application. As observed, the more mature the technology, the greater is the assurance effort put into it (e.g. legislations, policies, international coordination, etc.). If the technology is relatively novel but its service is highly demanded in the mainstream, the support for assurance is in the process (Hughes, 1987). This is the case of mobile telephony, which is relatively unsecured and unreliable at present as compared to the century-aged fixed-telephone because the latter has already achieved its height, and is even now superseded.

1.2 Problem Description

As explained above, mobile telephony is a global infrastructure. The ITU³, through the mandate of its membership, expresses the need of harmonized initiatives in the area of assuring global infrastructures. At present, global infrastructures⁴ in the ITU level are more or less defined by internet and mobile telephony. Since the Antalya Resolution 130⁵ in 2006, ITU has been the platform for global discussion about the appropriate cyber-governance. Infrastructure assurance for mobile telephony is expressed to be part of its Global Cyber-security Agenda (GCA) since convergence and (inter)-dependencies of IP technologies to mobile telephony, and vice versa, has been occurring this time and will continue to merge more closely in the future (ITU GCA, 2008). Mobile internet has been a buzzword of today (ITU Internet Report, 2002). However, in the context of whole GCA efforts, assurance for mobile telephony is relatively novel and has not yet come with a strong appeal in the ITU level. Mobile telephony is admitted part of the GCA agenda but its niche in the whole picture is yet to be defined. This is the underlying rationale of this research-- that is to put forward the issue of mobile telephony assurance in the international agenda so it can be deliberated and global solutions can be discussed. This has much implication due to the critical application of mobile telephony in developing countries (Forlin et al., 2008). In these countries, residents have more access on the mobile phone than on the internet (ITU Report, 2002).

² Diaspora is the dispersal of any population sharing common ethnic identity to leave their settled territory, and become residents in areas often far removed from the former.

³ ITU – International Telecommunication Union

⁴ Global infrastructures are those infrastructures that have global scope

⁵ ITU Resolutions Relating to Cybersecurity/CIIP, ITU Cybersecurity Work Programme to Assist Developing Countries, 2007-2009

1.2.1 Intricacy in Harmonizing Initiatives

Through the mandate of its membership formalized in 2006 Plenipotentiary Conference, the ITU is tasked to take concrete steps towards curbing the threats and insecurities of global telecommunication and information infrastructure. The need for a global harmonization of initiatives is the greatest obstacle to hurdle since vulnerabilities and threats of telecommunication networks do not respect national boundaries (Assaf, 2008). Legislations and policies in assuring the infrastructure seriously vary in level across the globe (Moteff & Parfomak, 2004). In 2000, the Philippines, for example, was once disconnected from the rest of the information world due to the infamous I LOVE YOU virus (also known as VBS Loveletter or Love Bug worm), which originated from the country that had just an authorship from an amateur university student. Its effect spread to Hong Kong then traveled through Europe and then to the United States, infecting 10% of all computers connected to the internet and causing more than 5 billion dollars of damages⁶. As there were no laws in the Philippines about cybercrime, the prosecutors dropped all the charges against the perpetrator. The same case happened to Pakistan (“Brain Virus in 1986”) and Syria who were a number of times debarred from the information community due to the various cybercrimes that originated from these countries (ITU Facilitation Meeting, 2008). In a number of times Nigeria, Ethiopia and other African countries were marked disgrace in the international community because of being known as havens of cyber-syndicates (ITU Facilitation Meeting, 2008). There are other countless cases showing that being a network of networks is its weakness as much as its strength. This, as well, applies to the case of mobile telephony, which possesses myriad of threats and vulnerabilities. Its functionality is already not confined within just voice-and-data telephony. In many countries, financial transactions can already be done though the convenience of mobile phone (GSMA, 2008). The mobile phone identification number almost already classifies individuals, which in a number of cases lead to privacy transgressions due to its lack of assurance mechanism. Most of the threats (and vulnerabilities) come from the countries who lack or void of legislations, policies and initiatives in infrastructure assurance (Goertz & Sheno, 2008) and most of these countries are developing countries who are short of capacity and resource to put up a comprehensive, effective and updated means of assuring the infrastructure. By such a situation, international cooperation is demanded in this respect to nearly level off initiatives. Harmonization then becomes an indispensable instrument to provide mitigations to the weak points in the network through international collaboration. Differing national mandates and priorities, together with the political and commercial sensitivity of the matter, makes harmonization difficult to achieve, more especially if the mechanism employed is inappropriate or, the worst, if none at all.

1.2.2 Lack of Capacity and Resource in Developing Countries

As expressed above, developing countries are in struggle to protect their infrastructure. There are many cases that attacks to the infrastructure originate from developing countries, but this does not necessarily mean that the perpetrators of these attacks are nationals of these developing countries (Dunn, 2004). As discussed in the ITU C5 Facilitation Meeting (2008), most of the attackers are those who have high-end knowledge of the technology, those who have the facility to perform massive attacks, who have connections to intelligence organizations, who have the power to abuse the incapacitated and the powerless, who have greater understanding of world affairs, who have vested interests to becoming a world power and so on. Developing countries are always found the victim of these international system change and shifts and tireless dragging of power and interests (Dunn, 2004). Assisting developing countries as they build their national infrastructure assurance capacity is a sustainable solution in reducing vulnerabilities in the infrastructure, thus, increasing confidence to its usage and, therefore, a greater welfare for all (ITU GCA, 2008). At present, according to the WSIS C5⁷ Facilitation Meeting (2008), there is one problem solved for the global assurance of mobile telephony, and that is: there is ITU-- an

⁶ http://en.wikipedia.org/wiki/I_Love_YOu_virus, Accessed: July 1, 2008

⁷ WSIS C5 is the ITU Action Line in Building Confidence and Security in the Use of ICTs

intergovernmental organization (a UN agency) that can provide a platform for deliberation on how this international coordination in infrastructure assurance for mobile telephony can be implemented. Identifying concrete actors to perform the role is, indeed, a great leap forward in the effort of assuring the infrastructure (ITU Facilitation Meeting, 2008).

1.2.3 Marketplace Insufficiency

A report of the 2005 Rueschlikon Conference expressed that the market alone is insufficient because it lacks the proper incentives to provide greater assurance than what the individual companies will voluntarily provide (Cukier, 2005). “Free-riders” never fail to exist in a public good such as national security or infrastructure assurance (Hummel, 1990). Initiatives that do not offer direct economic benefits most of the time face aversion attitude from market players. The technology for protection that the market implements does not provide a comprehensive societal infrastructure assurance (Cukier, 2005). Threats and vulnerabilities are dynamic, making it difficult to solely depend on what technical security solutions can offer (Dunn, 2006). In developing countries, infrastructure assurance is provided lesser priority because network operators are more inclined to invest on building or installing infrastructure in new locations or remote places to afford universal access in view of its economic returns. Infrastructure assurance is considered not part of the business cost (Dynes et al., 2008).

1.2.4 Inefficacy of Regulation

Government regulation has the reputation of being interventionist and sterile for innovation (Cukier, 2005). It does not produce optimal results because it is inflexible to technical change and place emphasis on compliance rather than assurance (Cukier, 2005). A government might have information about threats from its intelligence agency, but it does not have sufficient knowledge and capacity to reduce vulnerabilities. The private players are the experts in this area (Ghosh & Del Rosso, 1998). Since they are the ones who manage the infrastructure, the government has less or close to no jurisdictions in the operation of the infrastructure.

1.2.5 Absence of Public-Private Partnership

In the first part of this chapter, it was expressed that privatization and liberalization changed the setting of power and control in the large-scale technical infrastructure. Stakes now come both from the government and private sectors (Ghosh & Del Rosso, 1998). The government is at stake on the continuity of the infrastructure’s operation because such is necessary for the functioning of its society (Ghosh & Del Rosso, 1998). Both the people and the government itself are dependent on the services provided by mobile telephony. The private sectors, on the other hand, also view continuity important for business reasons (Ghosh & Del Rosso, 1998). The trust, however, to build partnership is yet the missing element in the picture (BSI, 2005). The case is aggravated in developing countries where institutional trust is not “yet” found in the culture. Or maybe defined in another way according to their context. Government agencies are fragmented from one another. Overall coordination is lacking (ITU Facilitation Meeting, 2008). Overlapping of initiatives exists, often without clear and strong linkages between the government and other institutions (ITU Facilitation Meeting, 2008). The private sector, on the other hand, does not trust the government for a multitude of reasons: reputation of corruption, bureaucratic, inefficient, slow, incapacitated, oblivious, etc. and what it only knows is its traditional top-down style of approach (Ghosh & Del Rosso, 1998). Collaborations in the past with the government frustrate private sectors to perform other collaborations in the future. Absence of trust deters cooperation, and this is, indeed, evident in the realities of most of the developing countries and emerging economies in the world. Information sharing, essential for the provision of greater societal assurance, is believed to be effectively implemented through public-private participation (Goertz & Sheno, 2008). Public-private partnership is the way to move forward to assure the infrastructure (Andersson & Malm, 2006).

1.2.6 Complexity and Sensitivity of the Issue

Infrastructure assurance bears with it materials that are relatively complex and sensitive to tackle. Its complexity roots from the largeness of its scope (Boin & McConnell, 2007)-- involving stakeholders from a number of sectors (e.g. telecom, electricity, content provision, spare parts manufacturing, etc.) and multi-level (e.g. national, regional and international). It is a unique problem in that it involves such a wide array of assets and sectors, and as a result no one approach or even discipline is adequate for addressing it (Gorman, 2005). Since it is a global infrastructure, thus, threats and vulnerabilities extend beyond national boundaries (Assaf, 2008), with countries differing in national mandates. The issue is sensitive because it involves the essential stakes of parties. The government possesses high stake in the safety and security of its citizen for that reasons many of the data from its intelligence bodies about threats (e.g. attacks, terrorism, etc.) could not be readily available for the public (Ghosh & Del Rosso, 1998). The private sector, on the other hand, is reluctant to reveal information due to economic interests (e.g. competition with other network operators) and apprehensive for its legal liability (e.g. in case their vulnerabilities will be known) (Cukier, 2005). Network operators do not easily share problems and information to their competitors and to the government because such could be the source of strategic behavior that places their market position in jeopardy (ITU Facilitation Meeting, 2008).

1.3 Research Objective

This study aspires to provide a working document for the development and implementation of a policy baseline for mobile telephony infrastructure assurance.

To restate the output of the study, these are the following:

- A working document specifying elements of policy baseline; and
- Provisions of its further development and implementation

The policy baseline for infrastructure assurance has a tripartite purpose, which are well correlated to one another.

- Harmonization of Initiatives
- Information Dissemination/Sharing or Learning Facilitation (Awareness Raising)
- A Benchmark (Performance Measurement in the process of implementation)

1.4 Research Questions

1.4.1 Main Research Question

“How to ensure infrastructure assurance for mobile telephony in the global setting?”

1.4.2 Sub-research Questions

This section lists the sub-research questions for each of the succeeding chapters that are essential to fully answer the main research question stated above.

Problem Analysis

“Why does the existing situation demand harmonization of initiatives to improve infrastructure assurance for mobile telephony?”

Theory

“Based on theoretical concepts, how can the harmonization of initiatives be achieved in an efficient and effective way?”

Formulation of the Preliminary Policy Baseline

“In considerations to the results of various research methods conducted, what policy scheme (both content and process) is needed to ensure the assurance of mobile telephony in the global setting?”

Evaluation of the Solution Space

“Based on the two evaluative (ex-ante) analyses conducted, what hints can be provided on the effectiveness and suitability of the policy scheme proposed to ensure the assurance of mobile telephony?”

Recommendations

“In response to the results of the study, which decisions are needed to be made and what additional information is required to implement the proposed policy scheme?”

1.5 Scope of Research Questions

This provides brief delineations on how each of the above sub-research questions can be answered. The answers of the sub-research questions provide elucidation to the solution of the main research problem.

1.5.1 Domain Description

This part aspires to elucidate the problem and advocates the need for international coordination. Harmonization of initiatives through international coordination is believed to ensure the assurance of the infrastructure. Key concepts discussed are the following:

- Institutional Fragmentation in Mobile Telephony Sector
- Vulnerabilities of the Mobile Telephony Infrastructure
- Hazards and Threats Confronting Mobile Telephony Infrastructure
- Risk Factors Surrounding Mobile Telephony Infrastructure
- Dependencies in Mobile Telephony
- Criticality of Mobile Telephony in Developing Countries
- Benchmarking an Adaptive Policy Baseline as Possible Solution

1.5.2 Conceptual Framework

This part aims to provide theoretical concepts that aid the further development and diffusion of the policy baseline. Support and adjustment to the forwarded coordination mechanism elicits harmonization believed to ensure the assurance of the infrastructure. Support and adjustment can be deduced from the process of standardization and benchmarking, respectively. The following key concepts are discussed.

- Definition of Infrastructure Assurance
- Principles of Standardization
- Principles of Benchmarking
- Integration of Principles

1.5.3 Formulation of the Preliminary Policy Baseline

This part discusses what are available in the pipeline derived from various methods conducted. From the analysis of the results of the research methods, the preliminary policy baseline and the provision of its further development and implementation will be provided. The section is sequenced as follows.

- What can be learned from theories?
- What can be learned from the model countries?
- What are the initiatives of ITU?
- What are the initiatives of GSMA?
- What can be learned from the experts interviewed?
- From the lessons identified, how can the preliminary policy baseline be defined?

1.5.4 Evaluation of the Solution Space

This part assesses the extent of the perceived efficacy of the developed preliminary policy baseline. The evaluation is done ex-ante based on the perspectives of experts interviewed and supported by literature reviews and analysis of the author. Evaluative methods used are the following:

- SWOT Analysis
- Policy Transplantation Assessment

1.5.5 Recommendations

Based on the discussions of the need and possible solution, recommendations are provided to the proposed method and relevant stakeholders.

1.6 Research Approach

The research framework is divided into four main phases, namely: the inception phase, analysis and design phase, evaluation space and reflection phase based on the chronological sequence of the research. Each of these phases is provided a brief description as shown below.

1.6.1 Inception Phase

In this phase, the inquiry about infrastructure assurance arose. Issues from various levels (critical infrastructure, telecommunication sector, mobile telephony sector) were considered. The need for infrastructure assurance for each of this level was identified and related to one another. Possible solution was then thought out. Since mobile telephony is considered a global infrastructure, a global approach was perceived to be appropriate. The need for harmonization and international coordination was then acknowledged. The inquiry expended in this phase has brought out the problem definition as the phase deliverable. This is further illustrated below.

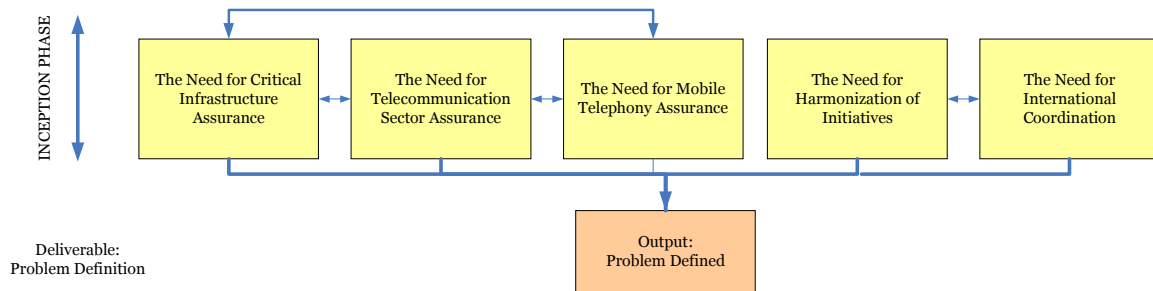


Figure 1: The Inception Phase

The research approaches used for this phase are: literature survey, mainly journals, reports and press releases and discussion from experts in the academe and study supervisors.

1.6.2 Analysis and Design Phase

In this phase, the study detailed its inquiry. The infrastructure assurance issue in the area of mobile telephony was provided a closer look. In this stage, various views of the stakeholders provided light on how should a policy baseline be developed and implemented. The perspectives of representatives of national governments were asked (NL, DE, CH and PH), a number of network operators representatives participated, ITU and GSMA also provided their stance on the issue. The rationale of the choice of respondents was based on the aim of arriving to a representative policy baseline derived from a comprehensive search for perspective. It was then decided that stakeholders from international, national and firm level frames would be considered. The most relevant international organizations for this issue are believed to be the ITU, a UN agency for telecommunication, and GSMA, an industry-initiated organization for GSM operators. In the national level, the governments of NL, CH and DE were chosen because they are the three leading nations in the area of infrastructure assurance based on literature reviews and conferences attended. To illustrate the idea of harmonization and policy transplantation, a developing country was chosen. PH is one of the developing countries where mobile telephony finds its plethora. In this country, mobile telephony is a critical infrastructure⁸ and there is increasing number of important transactions being done through mobile telephony. Detailed description of the choice of respondents, questions raised, and how the data were processed is placed in Appendix A. A description of the Philippines mobile telephony market is provided in Appendix E.

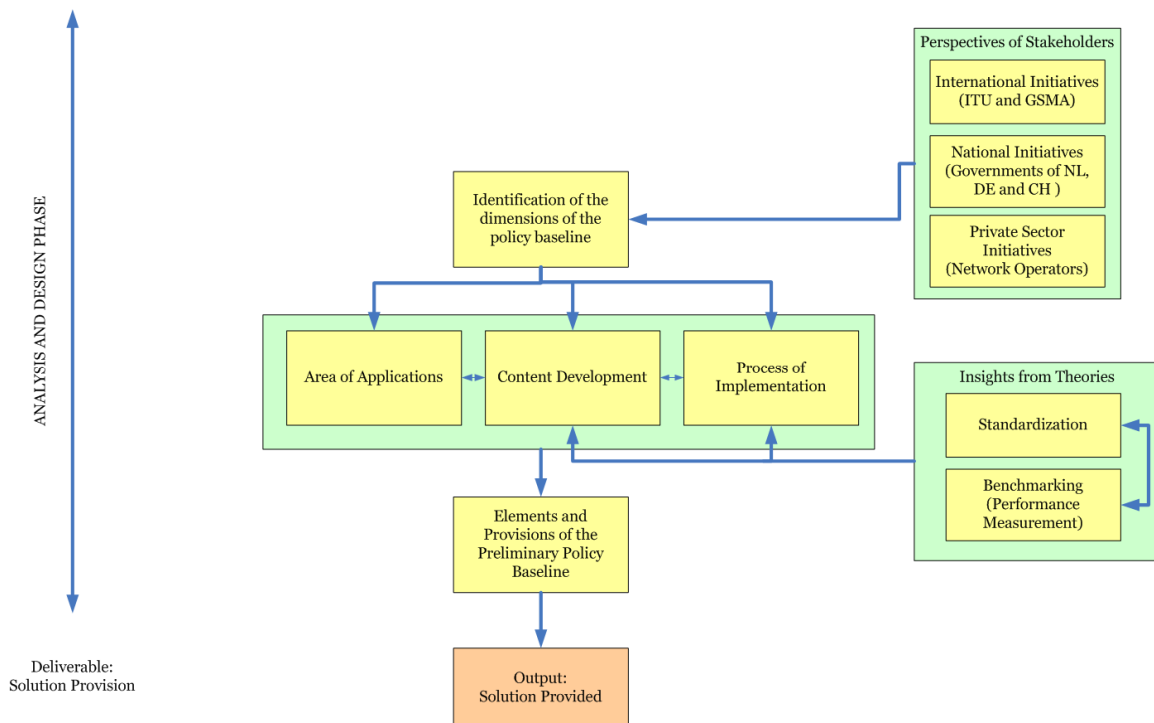


Figure 2: Analysis and Design Phase

The research approaches used for this phase were: analysis of relevant theories (Standardization and Benchmarking Principles), comparative analysis of national arrangements, and discussions with stakeholders and experts from the government, industry (specifically network operators), ITU, and GSMA.

⁸ For definition, refer to the table for Definitions of Key Concepts

1.6.3 Evaluation Phase

After defining the policy baseline and its provisions for further development and implementation, the extent of its efficacy was evaluated through two analyses, namely: SWOT Analysis and Policy Transplantation Assessment. SWOT Analysis aims to provide a description of the Strength, Weaknesses, Opportunities and Threats of the developed policy baseline. The Policy Transplantation Assessment provides a glimpse of its suitability and practicability as applied to the realities of a developing country. In this case, the Philippines, renowned as the “SMS capital of the world” where a mobile phone is a well-valued lifeline, will be the contextual setting in which the policy baseline will be assessed. The framework of this phase is shown below.

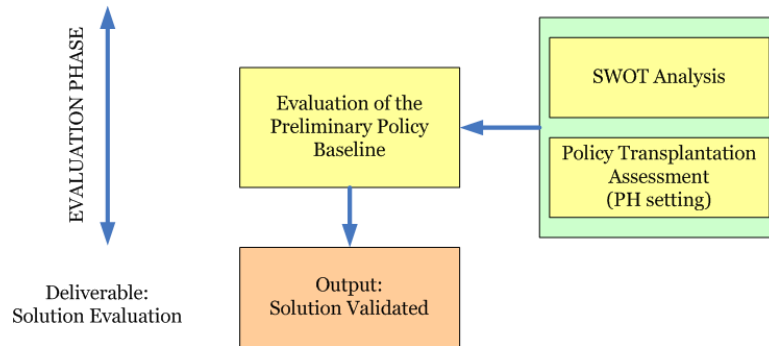


Figure 3: Evaluation Phase

The research approaches used in this phase were: the qualitative analyses mentioned above and expert discussion also provided insight in this part of the research.

1.6.4 Reflection Phase

After the policy baseline is defined and evaluated, conclusion, recommendations and reflection on the results of the study are provided. Conclusion and recommendations were grounded from the results derived problem definition, solution provision and solution evaluation. Reflection was based on the results and conclusion of the whole study. This is illustrated below.

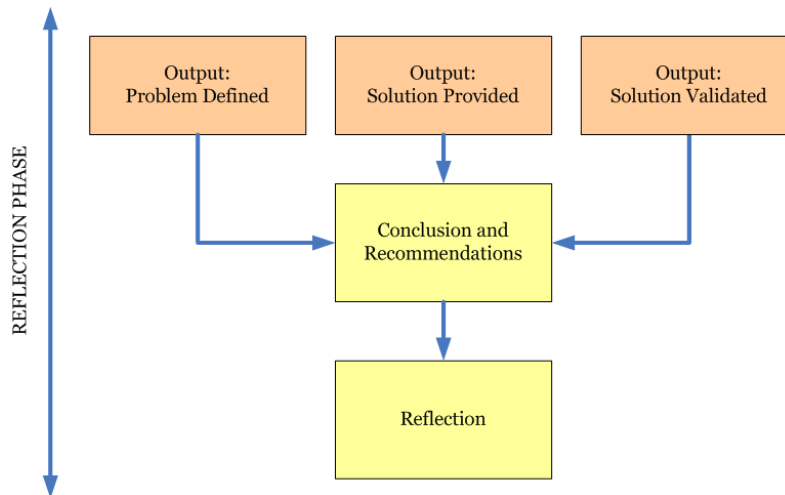


Figure 4: Reflection Phase

The complete research approach of the study is shown through the illustration below.

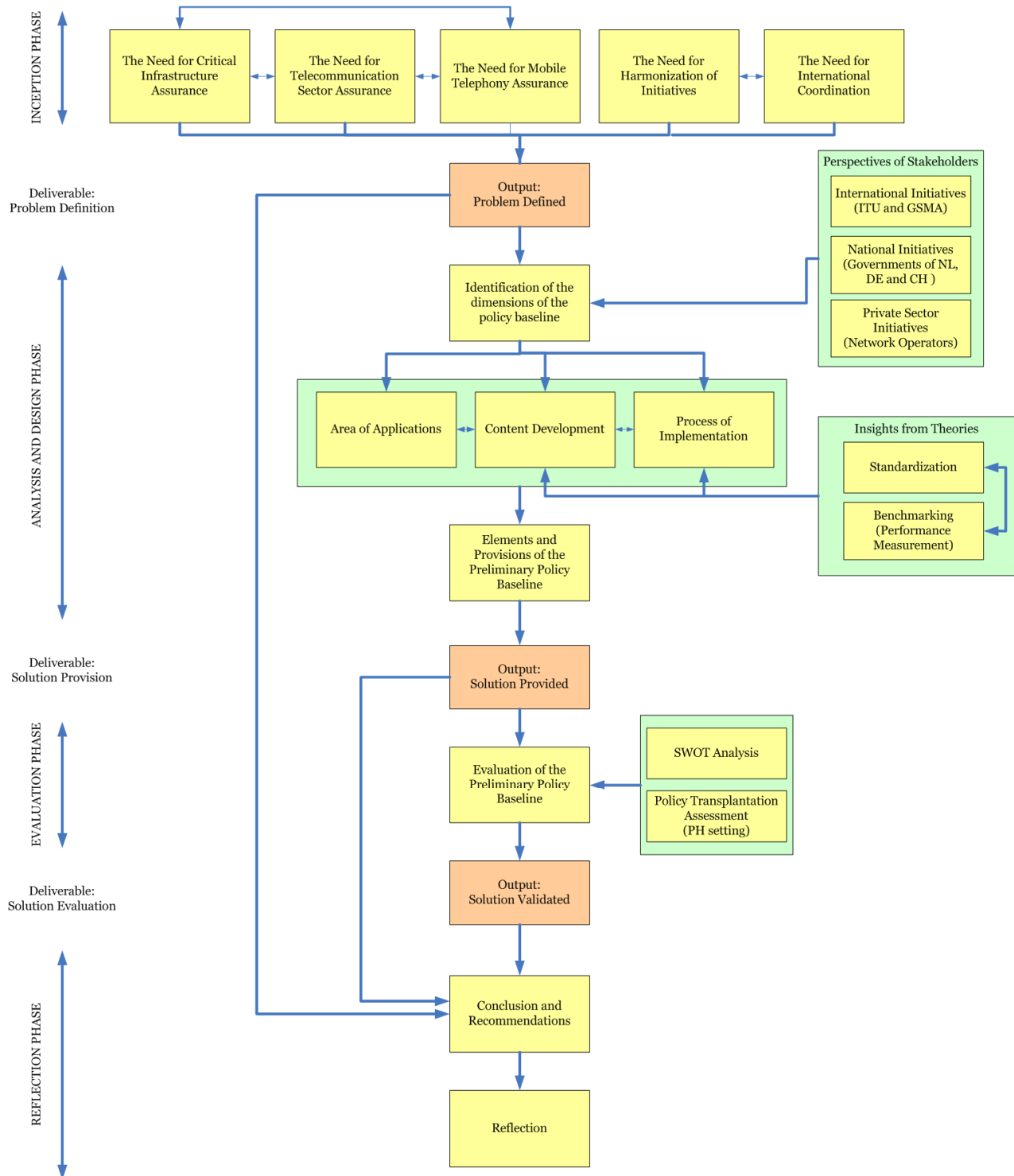


Figure 5: Research Approach Framework

1.7 Outline of the Report

Chapter 1 provides the introduction of the study, delineating problem description, the main research question, its sub-research questions, and the whole research framework.

Chapter 2 provides the detailed analysis of the problem and brings in the underlying rationale for the need of international coordination.

Chapter 3 provides the theoretical framework of the research, specifying the needed concepts to understand the process of developing and implementing a policy baseline for infrastructure assurance. The harmonization process brought down through standardization and benchmarking process is emphasized.

Chapter 4 provides the various initiatives and “good”⁹ practices of different stakeholders, and the policy baseline will be defined out from this information.

Chapter 5 provides the result of the qualitative (ex-ante) assessments of the “effectiveness” or suitability of the policy baseline in the setting of a developing country.

Chapter 6 provides the conclusion and recommendations of the study. The conclusion part wraps up the salient points of the study. The recommendations part presents mitigations for the weak areas of the policy baseline and policy advices to relevant stakeholders. Further research areas are also recommended.

Chapter 7 provides the reflection of the whole study and extends its insights to other possible applications of the findings.

⁹ The term “good” as opposed to “best” for practices is a politically appropriate word to use in this context of application.

2 Domain Description

The International Telecommunication Union, being a UN¹⁰ Agency for telecommunications, has been mandated by its membership, through Resolution 130 of Plenipotentiary Conference¹¹(Antalya 2006), to build confidence and security in the telecommunications sector. Plenipotentiary Conference, being the highest policy making body of ITU, has recognized the crucial importance of the applications of telecommunications infrastructure to practically all forms of social and economic activity, and in the same manner, aware of the various threats and vulnerabilities that undermine its reputation of being a secure and reliable infrastructure. One of the main resolutions placed affront is the need to engage the member states and sectors to an international coordination strategy for a more sustainable and comprehensive approach to assuring the infrastructure by reducing its vulnerabilities and identifying various risks and threats confronting the infrastructure. This study takes perspective from this frame of advancing international coordination for the greater harmonization of infrastructure assurance initiatives. A policy baseline, which sets the minimum required policies, is perceived by this study as the instrument of coordination that leads to the goal of global harmonization of initiatives.

This chapter elucidates the problem of infrastructure assurance in the case of mobile telephony¹². Due to the various system shifts (e.g. both in technology and regimes) and the increasing threats on its operation, the mobile telephony becomes a critical infrastructure in many parts of the world. Its high rate of diffusion to mainstream market and increasing number of essential transactions being done through the mobile phone (e.g. financial, internet, etc.) are indications of the infrastructure's growing importance to the normal functioning of society. In the latter part of this chapter, the adaptive policy baseline as a possible solution space is briefly discussed.

2.1 Aim of the Chapter

The chapter, as a whole, strives to answer the following sub-research question:

“Why does the existing situation demand harmonization of initiatives for infrastructure assurance?”

The various salient issues on infrastructure assurance mentioned in the introduction chapter are listed in the table below. The difficulty to harmonize initiatives is the great hindrance in the effort of increasing the assurance level of a global infrastructure (e.g. mobile telephony, internet, etc.).

Table 1: Some of the Issues in Infrastructure Assurance

Main Issues in Infrastructure Assurance
Intricacy in the harmonizing initiatives
Lack of capacity and resource in developing countries
Marketplace insufficiency
Inefficacy of regulation
Absence of public-private partnership
Complexity and sensitivity of the issue

There is a serious gap between the initiatives of the developed and the less developed countries. The lack of capacity of developing countries (both in the capacity and resource) is seen to be a

¹⁰ UN- United Nations

¹¹ Resolution130 (Rev. Antalya, 2006): Strengthening the Role of ITU in Building Confidence and Security in the use of ICT

¹² Mobile Telephony is a short wave analog or digital telecommunication in which a subscriber has a wireless connection from a mobile telephone to nearby transmitter. Detailed description of mobile telephony and GSM family is placed in Appendix C.

weak link in the assurance chain and, thereby, should be addressed through international cooperation (Aviram & Tor, 2004). Both the marketplace and the government have insufficient incentives to appropriately respond to the issue, which result to the lack of public-private collaborations (Cukier, 2005). This issue is more aggravated by the complexity of the infrastructure itself and the sensitivity of the issue on infrastructure assurance that seriously impede information sharing and other collaborative undertaking (Aviram & Tor, 2004). The rest of the chapter presents the analysis of the underlying causes of the issues and, in the last part, provides insight on how this dilemma can be mitigated.

2.2 Institutional Fragmentation

Institutions are social machineries (Farrell & Knight, 2003). Culture of assurance is strongly defined by the manner institutions link among one another for a common goal of improving confidence (Nannestad & Svendsen, 2005). If the atmosphere of trust is not yet established, cooperation can be hardly achieved (Cohen, 1985). Mismatched or incoherent institutional arrangement is one of the main reasons of difficulty in forming public-private partnerships (Cukier, 2005). This case is more evident in developing countries, where economic ascendancy prevails more and trust among institutions is scarce to find (Efendioglu et al., 2001). This concern is raised in Resolution 45¹³ of the 2006 ITU Plenipotentiary Conference that the colossal challenges faced by institutions in the developing countries should be taken into account in forming international strategy. Institutionally, developing countries do not have the capacity and resource to build its own national strategy. There is a real gap to deal with in harmonizing initiatives in developing countries due to the reason of national institutions fragmentation. Institutions are inappropriately arranged and countries have differing mandates and priorities (ITU Facilitation Meeting, 2008). The following areas, at least, are the common failing points of developing countries.

- Human and institutional capacity building
- Enforcement (capacity building domain)
- National policies and strategies in infrastructure assurance
- Establishment of national focal points
- Exchange of information between countries and relevant stakeholders
- Building basic awareness

Table 2: Some reasons of disintegration of institutions

Fragmentation of Institutions	
Government	Disintegration of Policies Unclear Goals Oblivious Incapacitated
Public-Private Partnerships	Unfounded Trust Expensive/Risky Initiative Uncertain Output Adverse legal issues/laws ¹⁴
Industry	Reluctant to Share Information Averse to Liability Strategic Behavior Disoriented with regulations

¹³ Resolution 45 (Geneva): Report of the Meeting on Mechanisms for Cooperation on Cybersecurity and Combating Spam, August 31 to September 1, 2006

¹⁴ E.g. Anti-trust laws disallowing sharing of information and collaboration

The table above shows the various causes of not responding to the appeal for infrastructure assurance. Although roughly said that each of the countries have programs on national security, there is an off-putting ambiguity if infrastructure assurance is a part of it. More than 90%¹⁵ of the world's important infrastructures are owned and managed now by the private sector, and the government has been having a 'hands-off' approach in this present setup (Cukier, 2005). These lead to unclear agreements, standards, policies and regulations (ASPR) (ARECI, 2007). The obliviousness of the national government and its incapacitation corrupt its pivotal response to the need of infrastructure assurance. The industry, on the other hand, does not have the incentive to increase the assurance it has been providing because such does not provide him added economic return (Assaf, 2008). As with any other public good, a greater infrastructure assurance (or national security) for all brings in "free-riders" who are benefiting but not contributing (Block, 1983). The security and reliability of a public good, a good/service that is non-rival and non-excludable, which is supplied by private operator(s) may demand government intervention in the market. Although business continuity in difficult times is a stake of the operator, additional assurance provisions that are out of traditional market feature do often than not face reluctance (Cukier, 2005). The industry sees that infrastructure assurance should be a market-oriented initiative and government intervention is found to be irrelevant (Dynes et al., 2008). For industry, collaboration with the government consumes resources with uncertain results. The sector is generally averse to collaborate and share information due to the risk of liability and strategic behavior from rival players, which have far implications to the continuity of their business (Andersson & Malm, 2006). Trust, that facilitates cooperation, is missing in the picture. This situation is more in developing countries, where the culture of distrust rather pervades the atmosphere.

Key Contribution: Institutional fragmentation detracts the effort of collaboration to ensure infrastructure assurance. Institutions (e.g. government, private sector, etc.) are individually providing their own assurance measures without the appropriate coordination with others to provide greater societal assurance. Developing countries, more especially, are presently experiencing this colossal fragmentation among institutions. International collaboration is needed to assist less developed countries as they form their national capacities for infrastructure assurance.

2.3 Vulnerabilities

As with other global infrastructure, the vulnerabilities of mobile telephony are myriad. Since mobile telephony is also a network of networks, its vulnerabilities are spread among the networks in which it is connected (ARECI, 2007). With such an argument, vulnerabilities have to be dealt with by stakeholders in an international frame. Vulnerability¹⁶ is the susceptibility of mobile telephony to threats¹⁷ that cause possible disruption of its normal operation (BMI, 2008b). It is a system's weakness that makes it possible for threat to occur (Chambers, 2004). The ARECI¹⁸ study (2007) conducted vulnerability analysis on electronic communications infrastructures and identified eight dimensions where vulnerabilities mostly reside. The dimensions provided are comprehensive and have been used extensively by key industry-government and academe forums¹⁹. Mobile telephony is an electronics communications infrastructure by itself; thereby, these vulnerabilities identified by the ARECI study are very relevant also for this case of mobile telephony. The vulnerabilities are summarized in table placed below.

¹⁵ FEMA 2007

¹⁶ For Definition, refer to the Table of Definitions of Key Concepts

¹⁷ For Definition, refer to the Table of Definitions of Key Concepts

¹⁸ Availability and Robustness of Electronic Communications Infrastructure – A study of PSC Europe

¹⁹ The 8 Ingredient Framework was first used by the IEEE Technical Committee on Communications Quality and Reliability (CQR) to anticipate the challenges of emerging technologies. It has also been used by the FCC Network Reliability and Interoperability Council (NRIC) toward the development of vulnerability-based best practices, by the ATIS Network Reliability Steering Committee (NRSC) to identify possible influencing factors driving observed improvements, and by the President's National Security Telecommunications Advisory Committee (NSTAC) to prepare for next-generation networks.

Table 3: Vulnerabilities of Mobile Telephony (ARECI, 2007)

Vulnerabilities of Electronic Communications Infrastructure	
Policy	Lack of ASPR (agreements, standards, policies, regulations), conflicting ASPR, outdated ASPR, unimplemented ASPR, interpretation of ASPR, inability to implement ASPR, enforcement limitations, boundary limitations, pace of development, information leakage from ASPR processes, inflexible regulation, excessive regulation, predictable behavior due to ASPR, ASPR dependence on misinformed guidance, ASPR ability to stress vulnerabilities, ASPR ability to infuse vulnerabilities, inappropriate interest influence in ASPR
Human	Physical, cognitive, ethical, user environment, human-user environment interaction
Hardware	Chemical, physical, electromagnetic energy, environment, life cycle, logical
Software	Ability to control, accessibility, interception, developer loyalties, errors in coding logic, complexity of programs
Networks	Capacity limits, points or modes of failure, congestion, complexity, dependence on synchronization, interconnection, need for upgrades and new technology, automated control, accessibility and border crossing control
Environment	Accessible, exposed to elements, dependence on other infrastructures, contaminate-able, subject to surveillance, continuously being altered, identifiable, remotely managed, non-compliance with established protocols and procedures
Payload	Unpredictable variation, extremes in load, corruption, interception, emulation, encapsulation of malicious content, authentication, insufficient inventory of critical components, encryption
Power	Uncontrolled fuel combustion, fuel contamination, fuel dependency, battery combustion, battery limitations, battery duration, Maintenance dependency, require manual operation, power limitations, frequency limitations, susceptibility to spikes, physical destruction

The policy dimension includes behavior between entities. These could be standards, policies and regulations (ASPR) that have national and international scopes (ARECI, 2007). These could, as well, be legislations, industry cooperation and arrangements between entities. Policy vulnerabilities of mobile telephony have to be coordinated internationally. At present, this is a problem due to the differing and conflicting mandates in the national level (ITU Facilitation Meeting, 2008). Most of the Telecommunications Policy Acts in the world are just requiring for coverage and quality as part of securing permits. This means that only in the concern of universal access and competition are catered by the Acts, but insurance of reliability and security of the infrastructure is out of the scope. This is in the belief that such is an industry initiative, and including it in the provision of these Acts would detriment other essential concern such as innovation and economic efficiency. There is a need of passing anti-liability legislations to provide a trusted environment, bonded by law, to allow stakeholders sensitive infrastructure assurance information. There are some specific aspects of anti-trust laws and freedom-of-information acts that have to be lifted to provide stronger ground for the establishment of a trusted environment. This dilemma on laws and policies has to be raised to the international platform for a more representative deliberation of the issue and achieve greater harmonization (ITU Facilitation Meeting, 2008).

Human vulnerability in mobile telephony is usually described as the weakest link in the security chain (Riguidel, 2006). The human power, as said, is a real asset and at, the same time, a real liability. The personnel can be motivated by a number of factors to breach the security policy, such as: vested interest, malicious intent, corporate culture, etc (ARECI, 2007). Since the personnel is involved in the entire operation of providing a service of mobile telephony, such as from design, implementation, operation, maintenance, and to de-commissioning, the personnel has a great role to play in maintaining reliability and security of the infrastructure (ARECI, 2007). The international need for this is the assistance for developing “good” practices in training personnel and overall management that an international platform and bodies can sufficiently provide (ITU Facilitation Meeting, 2008). Recommendations (e.g. standards, guidelines, etc.) developed by international bodies will be found invaluable in this respect.

Hardware and software are buzzwords in electronics and communications. The hardware in mobile telephony includes frames, system of antennas (for base and mobile station subsystems), circuit packs, metallic and fiber optic transmission cables, semiconductor chips, etc (ARECI, 2007). Software, on the other hand, defines the physical storage of software releases, development and test loads, version control and management and software delivery controls (ARECI, 2007). International cooperation is done through sharing information about technical standards and standard operating procedures. The network dimensions, as shown in the table above, includes the configuration of nodes and their interconnection, network topologies and architectures, various types of networks, technology, synchronization, redundancy, physical and logical diversity, network design, operation and maintenance. The environment refers to buildings, trenches where cables are buried, space where satellites orbit, location of microwave towers and cell sites, and the ocean where submarine cables reside (ARECI, 2007). The payload includes the information transported across the infrastructure, traffic patterns and statistics, information interception, and information corruption. It includes both normal and signaling and control traffic. Lastly, the power refers to the internal power infrastructure, batteries, grounding, high voltage and other cabling, fuses, back-up emergency generators and fuel (ARECI, 2007). The figure below shows the subsystems of GSM-based mobile telephony. Except for mobile station (MS), the other three are critical assets of internal network that are essential to maintain normal operation. This network will be connected to other networks. The greater is the network, the more indispensable it is. The three critical assets are: Base Station Subsystem (BSS), Network Switching Subsystem (NSS) and Network Management Subsystem (NMS).

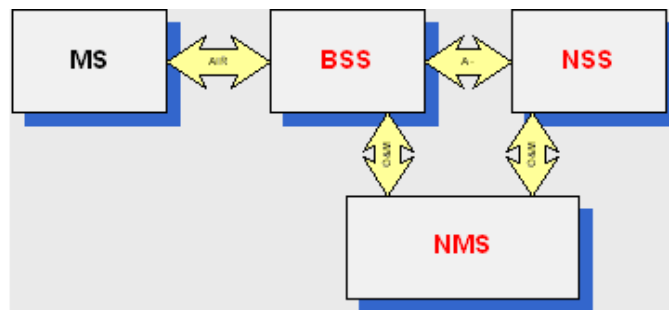


Figure 6: The Four Subsystems of GSM-based Mobile Telephony

Key Contribution: Being a network of networks is a strength as much as a weakness. Vulnerabilities are myriad and extend national boundaries and operators. Mobile telephony products and services have reached international, so do its vulnerabilities. Network operators can reduce vulnerabilities through employing “good” practices available in the international platform. Government, on the other hand can reduce the vulnerability through the establishment of national capacity for mobile telephony infrastructure assurance with international perspective.

TECHNICAL DESCRIPTION

Cellular Mobile Telephone System (or GSM-Based Mobile Telephone) is a system in which each geographic area is covered by a base station and is called a cell. If the phone moves to another cell, the call is automatically transferred to the base station in the new cell. The critical technical facilities of GSM-Based network are shown below. The Base Station Subsystem (BSS) is responsible for radio path control and every call is connected through the BSS. The Network Switching System (NSS) takes care of call control functions. Calls are always connected by and through the NSS. The Network Management System (NMS) is the operation and maintenance related part of the network and it is needed for the control of whole GSM network. The network operator observes and maintains network quality and service offered through NMS. (Source: Nokia, GSM Architecture)

The BSS consists of Base Station Controller (BSC), Base Transceiver Station (BTS) and Transcoder (TC). The NSS consists of Mobile services Switching Centre (MSC), Visitor Location Register (VLR), Home Location Register (HLR), Authentication Centre (AC) and Equipment Identity Register (EIR). The NMS has sections for fault management, configuration management, and performance management. (Source: Nokia, GSM Architecture)

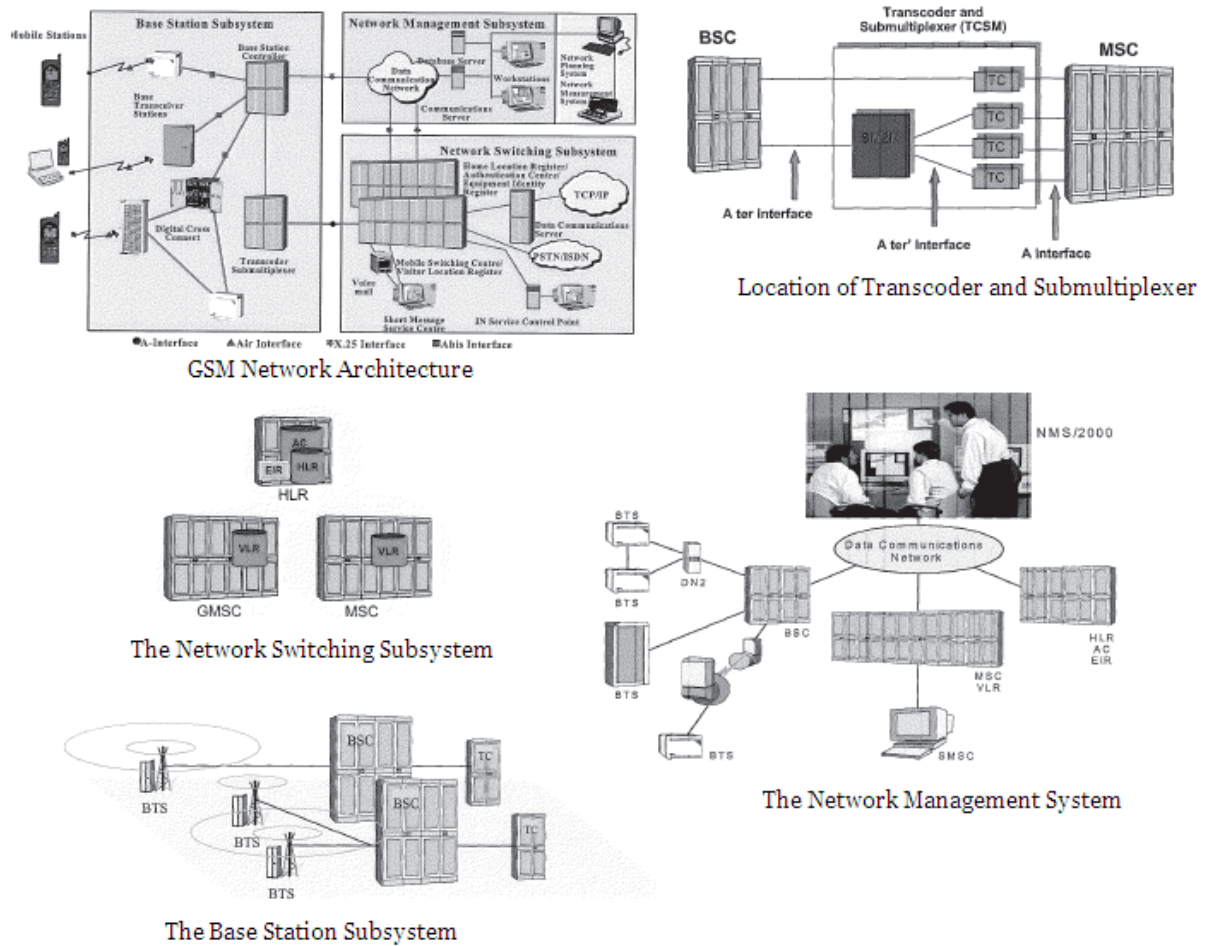


Figure 7: The GSM Network and its Main Elements (Photo Source: Nokia)

TECHNOLOGY EVOLUTION: From GSM to IMT-2000

As shown in the table below, enhancements upon second-generation (2G) GSM systems include HSCSD, GPRS and EDGE – all of which allows higher data transmission rates and new features are added. The goal of GSM migration is to reach UMTS, which is part of the ITU IMT-2000’s vision of a global family of third-generation (3G) mobile communications systems. (Source: ITU)

GSM-Based networks are global infrastructures. Majority of mobile telephony in the world is GSM base. As seen from the table below, GSM is a living and evolving standard. (Source: GSMA)

The description of each of the technologies in GSM family is placed in Appendix C1. The timeline of the evolution of both GSM and 3G technologies is affixed in Appendix C2.

Table 4: GSM Family of Wireless Technology Platforms (Source: Forrester Research)

		Technology	Bandwidth (kbps)	Features
First Generation Mobile	AMPS/ NMT	Advanced Mobile Phone System Nordic Mobile Telephony	9.6	<ul style="list-style-type: none"> ■ Analog voice service ■ No data capabilities
Second Generation Mobile	GSM	Global System for Mobile Communication	9.6 to 14.4	<ul style="list-style-type: none"> ■ Digital voice service ■ Advanced messaging ■ Global roaming ■ Circuit-switched data
	HSCSD	High-Speed Circuit Switched Data	9.6 to 57.6	<ul style="list-style-type: none"> ■ Extension of GSM ■ Higher data speeds
	GPRS	General Packet Radio Service	9.6 to 115	<ul style="list-style-type: none"> ■ Extension of GSM ■ Always-on connectivity ■ Packet-switched data
	EDGE	Enhanced Data Rate for GSM Evolution	64 to 384	<ul style="list-style-type: none"> ■ Extension of GSM ■ Always-on connectivity ■ Faster than GPRS
Third Generation Mobile	IMT-2000/ UMTS	International Mobile Telecommunications 2000 / Universal Mobile Telecommunications System	64 to 2,048	<ul style="list-style-type: none"> ■ Always-on connectivity ■ Global roaming ■ IP-enabled

2.4 Hazards and Threats

Being a network of networks, the hazards and threats of mobile telephony are also in multitude and can come from anywhere of the 85% present world GSM coverage (GSMA, 2008). The threats can interrupt the system because of the vulnerable link between the open and the mobile network to the application server provider (ASP). The general model of mobile end-to-end data communication is shown in the figure below. Most of the insecurities occur in the convergence of the mobile network and the open network. GSMA maintains that GSM-based mobile telephony is still a secure infrastructure due to various encryption technologies. Amidst such assertion, technical means is believed to be not the full solution for critical infrastructure such as mobile telephony. The perception that mobile telephony is a secure and dependable infrastructure is not yet established as compared to other mature critical infrastructures such as fixed-line telephone, banking and finance, etc. This is because of the various institutional supports that they receives, the infrastructure is backed up by policies and legislations, for example, and it has organized coordination schemes with other institutions in case its security and reliability are jeopardized. This is evident in the hesitance of the end-users and businesses to use mobile application to conduct sensitive transactions (e.g. m-banking, m-commerce, international roaming, etc.). The infrastructure can only exploit the opportunities it can potentially provide to the end-users through technical and institutional assurance that ensures its security and reliability.

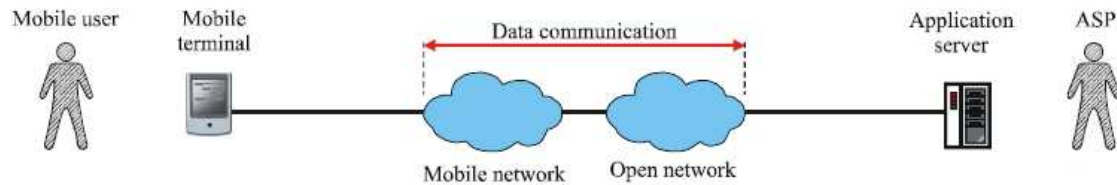


Figure 8: General model of mobile end-to-end data communication (Photo Source: ITU, 2004)

The table below provides some of the known threats in each of the mobile entity. Due to the various threats and vulnerabilities of mobile telephony, together with the high importance of its functionality with limited alternatives in many countries in the world, the infrastructure has become a critical infrastructure whose assets and parts become essential for the maintenance of critical social functions.

Table 5: Threats in mobile end-to-end communications

Mobile Entity	Threats
Mobile Terminal	Shoulder Surfing Loss of Terminal Stolen Mobile Terminal Misreading Input Error Unprepared Communication Shutdown
Open and Mobile Networks	Eavesdropping Communication Jamming Insertion or modification of data Interruption Unauthorized Access Repudiation Masquerade
Application Servers	Communication Jamming (DoS) Unprepared Communication Shutdown

The figure below provides the various security functions as identified by the ITU in 2006.

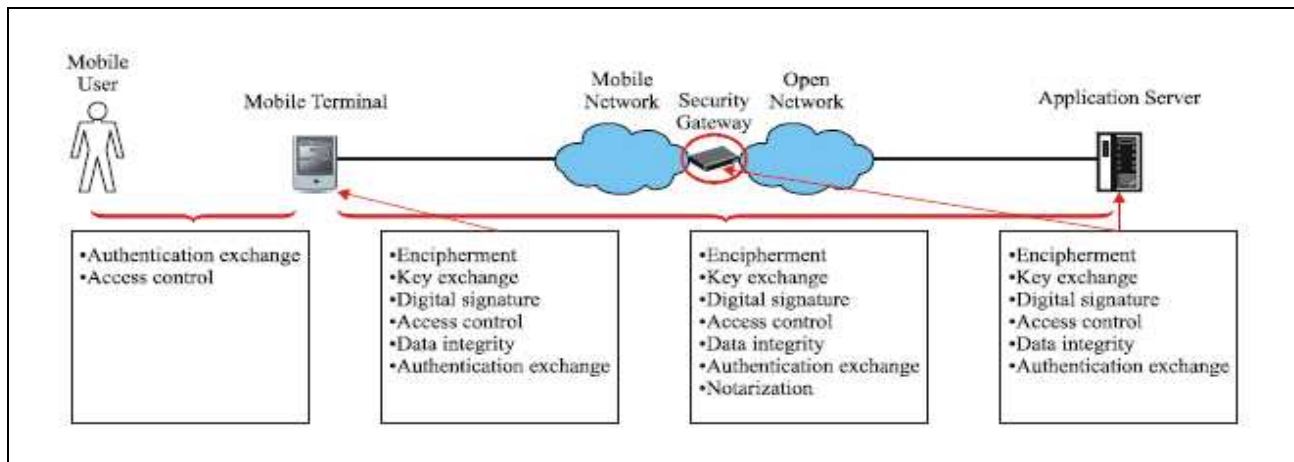


Figure 9: Security function required for each entity and relation between entities (Photo Source: ITU, 2006)

The attractiveness of mobile phones as a target for attacks and data theft is determined by at least two factors: First, the more mobile phones perform the same functions as personal computers (Internet access, storage of sensitive data, performance of financial transactions, etc.), the more they become a lucrative target for criminals. Secondly, similarly to malware targeting personal computers, it can be assumed that mobile phone malware will become more attractive as the size of the "target audience" grows. It can therefore be expected that modern mobile phones will become an increasingly attractive target as they become more widespread (MELANI, 2007). The table below provides the general hazards that confront a large-scale technical network.

Table 6: General Threats and Hazards

General Threats and Hazards
Technical/Human Failure
Natural Hazards
Pandemics
Terrorism/Sabotage/Organized Crime

The hazards and threats confronting mobile telephony range from various sources. As shown from the tables and illustrations above, the security and reliability of mobile telephony can be breached by a number of factors. The technical failure is due to the innate vulnerability of the infrastructure. There is a large threat of insecurity when information is sent from an open network to the mobile gateway and then sent again to an open network to be received by another mobile gateway of another network. Breaches can occur through interception of information in the gateways, or interception of information in the open network through employing another unauthorized receiver. Human failure can cause threats to security and reliability of mobile telephony and the reason of failure is also myriad: physical, cognitive, ethical, user environment, human-user environment interaction, and so on. Failures from personnel are reduced through appropriate training. Natural hazards and pandemics can, indeed, make the infrastructure insecure and unreliable. Storms, tectonic earthquake, fire, flooding and so on can cause interruption to the normal operation of the infrastructure. Atmospheric conditions can distort quality of reception and can make interconnection unreliable. Terrorism, sabotage, organized crime, targeted attacks, etc. may harm the infrastructure. There have been many instances in the world that these dramatic events lead to malfunctioning of the infrastructure (e.g. Sept. 11, London and Madrid attacks, etc.)

Key Contribution: The hazards and threats of mobile telephony also extend national boundaries. From the manufacturers of parts to content providers, a network of networks anchors an international scope. Service of mobile phone is international. Installation, operation and

maintenance of GSM networks are standardized. Thus, infrastructure assurance of each of the network that forms the whole global GSM network has to be ensured. GSM networks operating in different countries may find almost the same threats, vulnerabilities and risk factors undermining their infrastructure.

2.5 Risk Factors

From vulnerabilities and threats, risk factors can be determined. Risk refers to the uncertainty that surrounds future events and outcomes. It is the expression of the likelihood and impact of an event with the potential to influence the achievement of an objective (Stoneburner et al., 2002). Risk management is a systematic approach to identify, assess, understand, reduce risk factors, accept and communicate the residual risk. The table below lists down the various risk factors facing mobile telephony.

Table 7: Perceived Risk Factors in Mobile Telephony

Risk factors
Dependencies
Cutback in Redundancy
Internationalization
Mobility

The (inter)-dependency of mobile telephony with other infrastructure intensifies the risk in the assurance of infrastructure (SEMA, 2008). Mobile telephony is connected with the fixed-line, systems of satellite, radio links, internet, electricity, and so on, aside from the fact that it is dependent to another mobile network within its management and to another network provider outside its management both nationally and internationally. Cutback in redundancy poses risk to the reliability of the infrastructure. As availability defines criticality, redundancy is a very important element for the continuous operation amidst the hazards and threats. Internationalization (and globalization) paves way to multitude of risk factors. This, of course, does not mean that internationalization is damaging but the risk that it provides to the infrastructure should be, as well, be given attention. With internationalization, mobile telephony plays an important role. Its mobility features allow the people to communicate anytime, anywhere. Being open and mobile are where the risk lies, so mitigation has to be provided in this respect (ITU Facilitation Meeting, 2008). Risk analysis provides a structured overview of an organization's individual processes, possible threats to these processes and the vulnerability inherent in these processes. Combining this information yields a risk analysis for all critical processes in individual scenarios (BMI, 2008a).

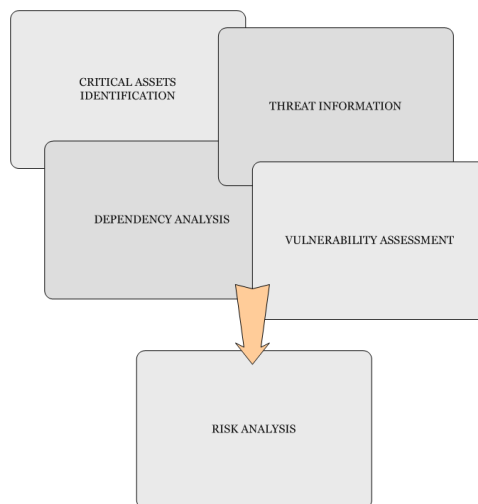


Figure 10: Integrated Risk Analysis

Management of the assurance of infrastructure should be based in risk analysis (SEMA, 2008). It is a comprehensive assessment of the areas where the infrastructure can possibly fail. This is lacking in the many approaches of the network operators and governments. Most are just done in the level of qualitative analysis. Risk analysis combines at least the result of vulnerability assessment, threat information, interdependency analysis, and critical asset identification (BMI, 2008a). It is a comprehensive and proactive approach in assuring the infrastructure.

Key Contribution: As vulnerabilities and threats are increasing and becoming international in scope and nature, so do the risk factors. Risk is the chance that innate vulnerabilities are triggered by the surrounding threats; thereby, providing imperil to the security and reliability of the infrastructure. Risk analysis is a comprehensive manner of assessing the factors that jeopardize the infrastructure. It is an analysis in consideration with the result of threats and vulnerability analyses, together with critical asset and dependency information. It is advocated that vulnerabilities have to be reduced and threats have to be identified through the comprehensive risk-based analysis and management in order to ensure infrastructure assurance.

2.6 Dependencies in Mobile Telephony

It has been said that mobile telephony has a number of (inter)-dependencies. Without the operations of other networks, its narrow scope makes a network less important. The credit of mobile telephony is hinged on the number of people being connected to the network and the quality and availability of its service. The table below lists down the inter-dependencies of the infrastructure.

Table 8: (Inter)-dependencies with other sectors

(Inter)-dependencies of Mobile Telephony
■ with other telecommunications/ICT technologies
■ with energy supply (electricity, oil, natural gas)
■ with finance and insurance
■ with operating and maintenance people (transport, health, drinking water)

Mobile telephony connects to other telecommunications infrastructure to complete its operation. The whole value chain of mobile telephony is a network of sectors that provides the infrastructure products and services essential for its operation. Energy and electricity sustains its operation. Finance and banking institutions are important to critical infrastructures. Network of operating and maintenance people performs the logistics. Mobile telephony is dependent on the normal functioning of other critical infrastructures.

Key Contribution: The global network of sectors that serve mobile telephony implies that ensuring infrastructure assurance goes beyond the peripheries of mobile telephony network. Again, being a network of networks is a strength as much as a weakness. Joints and junctions of the network, which means dependencies with other sectors, are huge sources of risk factors.

2.7 Impact and Criticality of Mobile Telephony to Developing Countries

Mobile telephony is the prime means of telecommunications in most of the developing countries (Kinkade & Verclas, 2008). In 2000, as shown by the figure below, mobile telephone subscribers in the world level off with fixed-line telephony. This dramatic increase of subscription to the infrastructure implies its increasing undeniable importance to society.

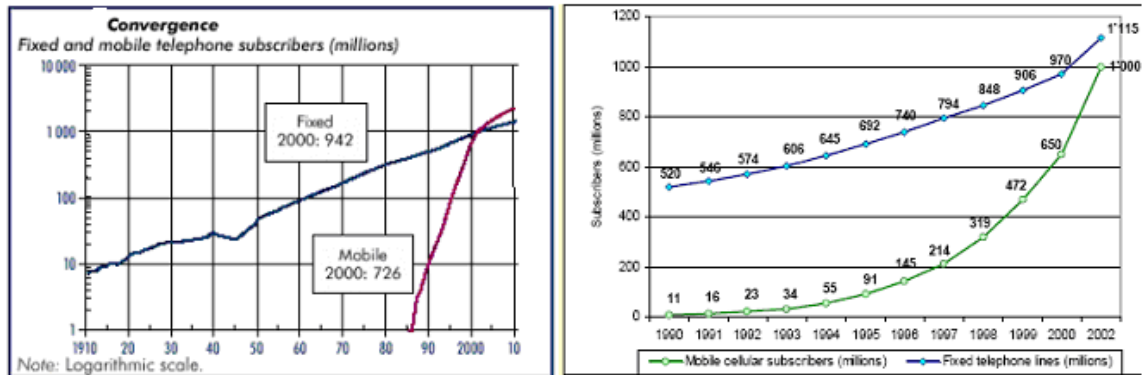


Figure 11: Convergence of fixed-line and mobile telephony (Source: ITU)

Mobile telephony has tremendous impact to the economies of developing countries. Aside from the individual benefits that one derived from its mobile service of voice and data, it extends its applications to many utilities. The table below shows some of the many functionalities of mobile telephony.

Table 9: Common GSM Services

Some Common GSM Services
Voice
Messaging
Information (e.g. internet)
Entertainment
Location-Based Service
M-Commerce (m-shopping, m-auction, etc.)
M-Banking (Money Transfer)
User Generated Content
Video Services
Services Document Download
Emergency Services (112 emergency number)

The following table lists down the utility of mobile telephony in many important sectors in the society.

Table 10: Utility of Mobile Telephony

The Value of Mobile Telephony in Developing Countries
Individual benefits
Industrial and economic growth
Sustainable socio-geographic structure (alleviates social divide)
Security
Government efficiency

Aside from the mobile-mode voice and data utility, mobile phone is a huge source of income for many people in developing countries. The infrastructure creates small business enterprises such as selling of credit load, transferring of load (“pasa”-load), accessories of mobile phone, charging booth, money transfer through texting, media voting, etc. These enterprises are the livelihood of many individuals and family living below poverty line. Moreover, the connectivity that the mobile phone provides also reduces social divide. The cohesion of people through texting, for example, leads to interaction that paves way to camaraderie. Warm (convivial) societies find this indispensable. There are a number of business models in texting that allows people to send very cheaply. GSM mobile phone helps ensure security through providing emergency services (e.g. 112 or 911). Mobile telephony also leads to government efficiency. The service has been used in elections in a number of countries worldwide. It has shown useful for electing and ousting government officials, even the highest in the rank such as the president, as in the case of the Philippines.

Table 11: Factors of Diffusion

Factors Affecting Diffusion of Mobile Phone
Geographical
Government Policy
Current Physical Infrastructure
Availability of Technology
Ease of Use
Economic Models
Culture

There are a number of factors for the fast diffusion of mobile phone to mainstream user. Difficult geographical location of the country favors the setup of mobile telephony. This is the problem of telephone in diffusing the infrastructure due to high cost and difficulty in installing infrastructures to places of difficult terrain. The government policy on the deployment of mobile telephony also adds to easier diffusion of mobile telephony. The government acts on competition, universal access, tariffs, rates, etc, are influencing factors in favoring mobile telephony market atmosphere. Availability of technology, ease of use and current physical infrastructure do affect diffusion. The culture, as well, has great influence on choosing mobile telephony. In many cultures that value close and mobile interaction, the feature of mobile telephony finds it favorable.

Key Contribution: Mobile telephony is generally regarded as a critical infrastructure by many countries in the world. This means that the infrastructure is indispensable for the functioning of the society. The criticality of this infrastructure is greater felt in developing countries where the infrastructure provides the basic means of telecommunications and access to telecommunication alternatives is limited. Its importance is growing due to the increasing number of functionalities (e.g. internet, m-banking, m-commerce, etc) it provides.

2.8 Adaptive Policy Baseline as a Possible Solution Space

Due to the various gaps in initiatives as mentioned above, ensuring infrastructure assurance through harmonization is a befitting policy goal. Harmonization leads to the leveling off of initiatives that leads to greater assurance of the infrastructure. An adaptive policy baseline is advocated by this study as instrument for harmonization. The policy baseline allows policy makers and network operators to know the needed initiatives to be instituted. The mechanisms for harmonization are discussed in the next chapter.

The table below shows the suggested arrangement for infrastructure assurance for mobile telephony. It is non-regulatory (or minimal regulation) and voluntary in response to the present setup of the infrastructure: most are owned by the private sector and little influence from the government. These mechanisms believed to ensure the mobile telephony infrastructure in the global setting will be fully described in the next chapters that follow.

Table 12: Levels of governmental influence (Adapted from BMI)

	Advantages	Disadvantages
Laws	Binding for all operators	No alternative solutions Need for control Long change cycles
Voluntary bodies of rules and regulations	Accepted by operators, Sector specific Can be adapted quickly to changes in operating environment ²⁰	Little influence of the government
Recommendations and guidelines	Cooperative approach, Voluntary	Non-binding
(Informal) talks	Allows discussion, voluntary	Non-binding, no-defined results

2.10 Integration

The table below strives to integrate the main points raised in this chapter to accentuate the problem and the need for harmonization of initiatives to ensure infrastructure assurance for mobile telephony.

Table 13: The need for harmonization of initiatives to assure the mobile telephony infrastructure

Problem Area	Description	Why harmonization of initiatives?
1. Institutional Fragmentation	Infrastructure Assurance is a collaborative undertaking. The fragmentation hinders stakeholders to collaborate.	Standardized technology (GSM) makes “ecosystem” of actors almost the same.
2. Vulnerabilities	Being a “network of networks” makes the infrastructure more vulnerable. Vulnerabilities weaken the capacity of the infrastructure.	GSM networks possess almost the same vulnerabilities.
3. Hazards and Threats	Being a “network of networks”, hazards and threats are increasing. They undermine the capacity of the infrastructure.	GSM networks face almost the same hazards and threats.
4. Risk Factors	The chance that hazard and threats can imperil the vulnerabilities is increasing.	Since GSM networks have almost the same hazards and vulnerabilities, they face almost the same risk factors.
5. Dependencies	Being a “network of networks”, mobile telephony is dependent on the operation of other infrastructures. Dependencies	Standardized technology (GSM) implies almost the same dependencies.

²⁰ Discussion with E. Luijff, 2008

	increase the number of risk factors.	
6. Criticality in developing countries	Mobile telephony is critical in developing countries. These countries have lesser capacities to assure their infrastructure.	Less capacitated can be assisted by other parts of the network who employ “good” practices.
<p><u>Analysis:</u> The standardized GSM technology makes the problem of stakeholders in the world on mobile telephony infrastructure assurance <u>almost</u> the same, both in nature and scope.</p>		
<p><u>Proposed Solution:</u> Same problem faced generally implies same solution. Harmonization of initiatives is needed to level off assurance condition in the global setting. Diffusion of “good” practices increases the assurance level of the infrastructure. Harmonization encourages learning and adjustment. The study advocates the adoption of “good” practices in the form of adaptive policy baseline deployed through voluntary schemes.</p>		

2.11 Key Messages of Chapter 2

- Mobile Telephony has been found as one of the critical infrastructures in the telecommunication sector. Its facility to the society is increasing as more and more applications and important transactions are being done through mobile phones.
- The criticality of mobile telephony is greater felt in developing countries. The infrastructure is highly valued in these countries due to the limited availability of other means of telecommunications. An increasing number of transactions is being done through it. The majority of the population is connected to the network, and the risk factors confronting the infrastructure are increasing in number.
- The vulnerabilities, threats and risk that challenge the infrastructure are global in scope. This suggests that increasing assurance for mobile telephony demands international coordination. It is advocated that vulnerabilities have to be reduced and threats have to be identified through the comprehensive risk-based analysis and management in ensuring infrastructure assurance.
- Policy baseline has the potential to internationally coordinate initiatives. It institutes the required policies to increase assurance. The mechanism to implement the policy baseline should be non-regulatory in nature due to the present arrangement of the infrastructure. The chapter then recommends the process of benchmarking for the better diffusion of the policy baseline.
- Institutional fragmentation detracts the effort of collaboration to ensure infrastructure assurance. Institutions (e.g. government, private sector, etc.) are individually providing their own assurance measures without the appropriate coordination with others to provide greater societal assurance.
- The global network of sectors that serve mobile telephony implies that ensuring infrastructure assurance goes beyond the peripheries of mobile telephony network. Joints and junctions of the network, which means dependencies with other sectors, are huge sources of risk factors.

3 Conceptual Framework

The problem analysis chapter brought us to the conclusion that policy initiatives should be harmonized to ensure infrastructure assurance of mobile telephony in the global setting. The reasons placed forward were that mobile telephony is a network of networks and its size and scope extends beyond national boundaries and operators (ARECI, 2007). Steps towards policy harmonization can focus on compliance with international covenants and codes voluntarily adhered to on a bilateral or multi-lateral basis. Unfortunately, many of those defined in the meta-platform do not find their way to local utilization of their function.

Chapter 3 provides the theoretical glimpse of the development and implementation processes of the minimum policy requirements needed to be initiated for the desired assurance level --- this study calls this set of requirements a policy baseline. Many assumptions in the construction of this chapter are based on the important principles of standardization and benchmarking. The chapter comprises of two parts: the first part explains how can standardization can harmonize initiatives, and the second part explains how benchmarking reinforces the harmonization of initiatives.

3.1 Aim of the Chapter

The chapter, as a whole, strives to answer the following sub-research question:

“Based on theoretical concepts, how can the harmonization of initiatives be achieved in an efficient and effective way?”

3.2 Infrastructure Assurance Delineated

Infrastructure assurance is an emerging policy field, which arose to open agenda due to the need for more secure and reliable infrastructures. The dependence of society to the product and services of large-scale technical infrastructures increases as more and more important applications are done using them (Haimes et al., 2006). Infrastructure assurance is an encompassing concept of building confidence and trust on the use of the infrastructure, which anchors more than the idea of security or protection. It involves pre-emptive integrated risk management designed to increase confidence and trust that disruption or failure of the operation of the infrastructure will be minimized or avoided when its critical vulnerabilities are beset by the surrounding threats (Gorman, 2005). It is the set of planned and systematic actions necessary to provide confidence that the infrastructure is secure and reliable (Moteff & Parfomak, 2004).

To ensure infrastructure assurance in the global setting, this study advocates that harmonization of policy initiatives has to be done in a comprehensive manner through multi-level and multi-lateral approaches. The process of harmonizing policies is gradual to be accomplished because of the various factors and constrictions that shape national policies (Yasin, 2002). Harmonization leads to diffusion of “good” practices defined in what this study calls a policy baseline. It is a set of reference policies agreed to be necessary to ensure infrastructure assurance²¹. A policy baseline

²¹ Adapted from the definition of reference standard, (Sherif, 1999)

becomes adaptive when its provisions can be framed unto a particular environment where it will be deployed²².

Creating a concrete and effective strategy to harmonize initiatives is indeed indispensable so that the goal of bringing the level of assurance into one accord is not far-fetched to occur. Through the perspective of an international organization, which is mandated to build confidence on a global infrastructure, harmonizing initiatives to its members or member states is an overwhelming task to do (ITU Facilitation Meeting, 2008). The mechanism should have the appropriate incentives in order for the stakeholders to be on board. The rest of the chapter will excavate more on the pertinent concepts for the achievement of greater policy harmonization to ensure the assurance of infrastructure.

3.3 Standardization and Policy Harmonization

This study builds its assumptions from the tenets of standardization process. As the policy baseline being aimed to harmonize, it is assumed that in order to be able to do so the relevant stakeholders should give support to the contents of the policy baseline and the process it goes through to achieve harmonization. “Support” is a hallowed word that only occurs when the stakeholders see their niche in the whole baseline harmonization scheme. Standardization, by its very essence, is a process towards harmonization. Standards reduce needless variety (ISO/IEC). One cannot harmonize without a standard. There must be a set of references that frames the elaboration of actions. For example, houses in a village cannot be harmonized unless there is a standardized aspect of its construction. It could be the size, the shape, or the color, etc. but how the houses are designed inside or outside is in the whims of the owner. A choir, another example, cannot sing harmoniously if one or more of its members are not in the standard pitch or standard quality of voice. As one sees, standardization is the first requirement to acquire in order to achieve harmonization. A policy baseline can be viewed as standardized policy lessons. It is a policy reference, which could be comprised with technical, procedural or encompassing policy options practiced within a firm or in a national or international frame. The common character among them is that they are all based on the agreed “good” practices. Harmonization is the process of coordinating different provisions by eliminating major differences and creating minimum requirements or reference standards. It is designed to incorporate different systems under a basic framework. It takes into account local factors and yet applies general principles to make a consistent framework (Menski, 2005). It can be viewed as the process of adjustment, of differences and inconsistencies among different measurements, methods, procedures, measures, schedules, or systems to make them uniform or mutually compatible. Harmonization of socio-technical systems can result in a baseline (set of minimum requirements) or a reference standard²³

Standardization process, as where the development of the policy baseline takes inspiration to, embody ideas, values, beliefs and assumptions that together make up the tissue of the standards ideology (Egyedi, 1996). Standardization is the process of developing and agreeing upon a (set of) requirement(s) to be established. It is done through a consensus of involved experts²⁴. Most of those “traditional” ideological elements that are relevant for this study, because they provide direct effect to harmonization, are the following:

1. The **consensus²⁵ principle** allows the policy baseline to seek into account the views of all stakeholders concerned and to reconcile conflicting arguments (Egyedi, 1996). By so doing, the stakeholders could arrive to a compromised equilibrium where at least the majority agrees or there is no sustained opposition (Egyedi, 1996). Deliberating the views and stands of stakeholders is essential to both the process of developing and implementing the policy baseline. In the development process, the principle of consensus

²² adapted from the definition of adaptive policy, (Walker et al., 2001)

²³ discussion with E. Luijff, 2008

²⁴ Adapted from the definition ISO/IEC and NNI

²⁵ General agreement or accord; An opinion or position reached by a group as a whole

paves way to the creation of a policy baseline with contents that approximately reflect the demands of the stakeholders. In this manner, the stakeholders find meaning and relevance to what the policy baseline stipulates. In the process of implementation, the principle of consensus establishes the foundational support needed for the diffusion of the policy baseline. Since stakeholders see that their demands are considered in the development of the contents, they have greater tendency to implement what they have created. When stakeholders find that they are part of the process, there is greater chance that they will take responsibility of its implementation.

2. The ***voluntary principle*** is established on the idea that the application of the policy baseline is based on the willingness of the concerned parties to participate or implement (CEN, 2007). This is the rationale of ITU-T having used the word “recommendations” rather than “standards” to emphasize the value of voluntary principle (Egyedi, 1996). Voluntariness brings with it the flexibility of applications that responds fittingly to the dynamic nature of the technology. This is in contrast to the principle of coercion through regulation or a top-down command, etc., which has binding rules that are found inappropriate for the dynamic setup of technology. The voluntary principle takes advantage of the aversion behavior experienced by coercion-oriented approach. Voluntariness is believed to be a “best” practice in a world where most of the societies are built on democracy and individual choice.
3. The ***democratic principle*** envisages the involvement of relevant stakeholders in the preparation of the policy baseline (Egyedi, 1996). This provides a balanced influence from relevant level of powers. This principle seeks for greater representation to achieve holistic output. As much as possible, perspectives of all relevant kinds and levels of stakeholders should be considered in the deliberation. Democracy is basically “already” a process of gaining support. In the development of the policy baseline, the government, the industry and international organizations work in partnership among one another to arrive to the set of necessary reference policies at least agreed by the majority.
4. The ***coherence principle*** makes sure that there is alignment in principle and value with the precedent international or regional agreements or covenants (CEN, 2007). This is to avoid inconsistencies in the implementation and brings in smoother adaptation. Overlapping policies can lead to confusion due to unnecessary complexities. Thus, in the development of the policy baseline, stakeholders have to make sure that international values (in the form of international covenants, agreements, etc.) are not being transgressed. Support to a policy or mandate is inclined to be directed to general (or international) values that have traditionally set the frame of human logic.
5. The ***rationality principle*** puts forward the importance of relevant and consolidated foundations of the policy baseline, which should be based on the findings of science, technology and experience (Egyedi, 1996). Policies that are practical or proven to be valuable have greater tendency to gain support. Obscure policy lessons will find a difficult way in convincing stakeholders for their implementation.

The important element of those principles stated above is that they are all geared to the aim of gaining support for the implementation process. The support element is the one that leads to harmonization of initiatives. The standardization process paves way to the interaction of stakeholders. And interaction means increasing the likelihood of support for the system (De Bruijn, 2007). Interaction has a number of advantages, namely: support for the trade-offs of conflicting values, stakeholders become the owner of the system, and such creates a mutual trust (De Bruijn, 2007). These principles of the standardization process, which have been tagged as “traditional” because of their stable relevance, are indispensable in the development of the need-driven policy baseline contents. The standardization process establishes the needed support for the implementation of the policy baseline invaluable for the greater level of harmonization of initiatives.

The general standardization process is shown by the figure below. As one can see that the policy baseline outputted by this research is defined during the development process. There is the idea of the need of the policy baseline for greater harmonization of initiatives and this idea will be deliberated in the development process. The output of this study is envisioned to become the “groundwork” for the further discussion of the issue, together with other relevant stakeholders. Then, in an appropriate platform, the policy baseline will be specified with relevant stakeholders gathered in one table, with due “representativeness”. At the end of the specification process, the policy baseline is available and ready for implementation. The greater harmonization in the implementation achieved through the instrument of benchmarking, which will be elaborated in the next section.

The development and implementation of the policy baseline should undergo such process for it to earn the paybacks of the principles of standardization. This process itself builds the support of its eventual application, and it is by such rationale that standardization process is found relevant in the harmonization process of policy initiatives.

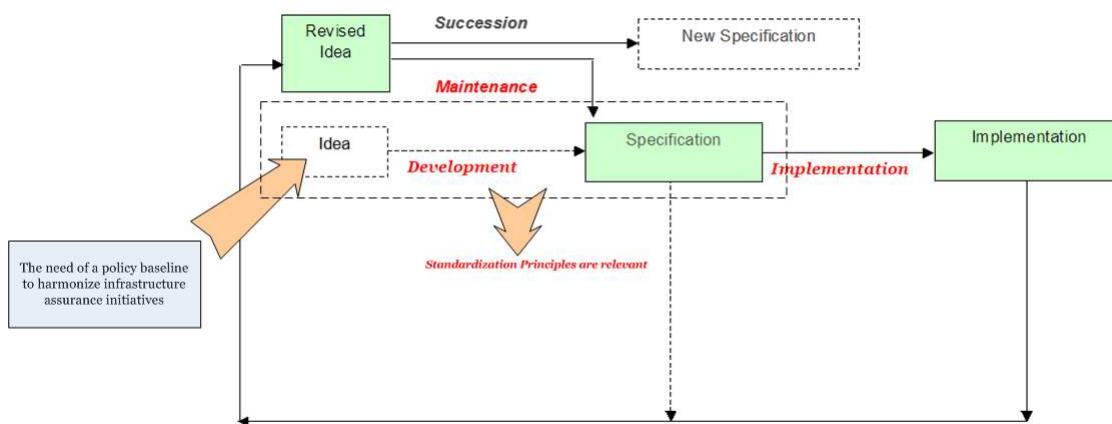


Figure 12: Policy Baseline and the Standardization Process (adapted from the framework of Egyedi, 2007)

The dotted box in the figure above signifies where the principles of standardization process are relevant. The arrow that points to the “idea” box is the idea of developing a policy baseline as a need for greater harmonization of initiatives. The idea, then, is deliberated through the inputs of the involved stakeholders. This study offers ideas for the contents of the policy baseline. This is discussed in the next chapter. Then the idea ends at the last stage of specification and becomes available for implementation. By experience, standards or policy baseline is prone to becoming dormant on the shelves or incapable of reaching its intended recipients. There are many reasons for this incapacitation to be implemented to the ground level. Some of the problems of implementation are listed in the next table. But the most important source of problem in the implementation of a policy baseline or standards is the lack of incentive for the stakeholders behind their compliance or non-compliance. Stakeholders are reluctant to implement policy baseline (or standards) if they do not see much how they can benefit from it. It has to be shown that the benefit derived, which is the source of incentive for stakeholders, is way greater than the cost of implementation. Stakeholders such as government or network players are driven by incentives. They work because they are being pushed and/or pulled by incentives (Ellingsen & Johannesson, 2007). It is even described that incentives are both strength and a weakness in the assurance chain (Wash & MacKie-Mason, 2006). To accentuate even further, humans are the weakest link in the infrastructure assurance chain (Wash & MacKie-Mason, 2006).

3.4 Benchmarking and Policy Harmonization

This section provides us concepts on how we can better respond to the problem of implementation that arises due to lack of incentives. Incentive theory in psychology tells us that it

is the environment that brings out behavior (Killen, 1982). The basic concept behind the incentive theory is goals (Killen, 1982). People are driven by their goals. When a goal is present, humans strive to attain such goal. This concept of incentives will be applied in this study to reinforce the greater level of harmonization in the implementation process of the policy baseline. As believed, any humans aspires betterment of their situation (Maskin, 2001). It could be in any respect: economic, psychological, egoistic, etc. In the same manner, the stakeholders of large-scale infrastructures, such as mobile telephony, have the goal to increase profit through increasing market share, or maintain business continuity through increasing security level, decreasing vulnerabilities, mitigating threats, etc. or provide greater welfare to the citizen through stabilizing economy, furnishing vibrant innovative atmosphere, assuring infrastructures, etc. In short, stakeholders that participate in the development and implementation of the policy baseline are incentive-driven. Now, if there is a reference standard or a policy baseline to be made, it should be designed in a manner that the goal of the stakeholders towards the “betterment” is a foundation of it. The adjustment that stakeholders do in order to respond to their respective incentives entrenched in the reference standard or policy baseline is the one that propels towards greater harmonization. The level of harmonization provided by the standardization process in the development stage through gaining the support of the stakeholders will be reinforced by the incentive-driven mechanism employed in the implementation stage. Such is the rationale of the inclusion of benchmarking in this theoretical chapter because it is the “believed” mechanism that triggers the incentive of stakeholders towards improving their situation. As they see in their environment, that there is an available “best” practice model and everybody is conforming to it, then they have high tendency to conform to it as well. May we go back to our two examples above on house and choir. If in a village, the majority of the homeowners conform to a reference standard and such standard made them look “better”, there is a great tendency that the minority will adjust the formation of their house to what they see on others with the incentive that it might look good on them too. In a choir, if almost everybody does sing well and conforms to the right notes and melody, the one who performs inadequately will adjust his behavior (e.g. practice more, go to a voice coach, etc.) with an incentive to better sound in the group. Benchmarking does the same. It harmonizes initiatives through letting the stakeholders adjust their behavior to a reference standard (in this case a policy baseline) founded by “good” practices in the field. Benchmarking is described in more detail in the next section.

Table 14: Problems in Implementing Standards

Standardization Implementation Problems (adapted Egyedi, 2008)
1. Errors, ambiguities, inconsistencies
2. Uncertainty concerning its capacity to harmonize initiatives
3. Parallel options and parameters; overlapping functionalities; alternative modeling techniques
4. Complexity; aim to be comprehensive
5. Unclear status of non-binding recommendations
6. Functional deviation and partial implementation; superfluous features, too expensive for intended users
7. Real environment where the standards have to be deployed (discussion with Luijff, 2008)

3.4.1 Benchmarking Defined

Benchmarking has long been used in the management world (E. Luijff et al., 2007). It first emerged in the private sector as an engineering tool serving as point of reference for comparative measurement. It has many applications in the private sector, and has grown and evolved to many other forms. The figure below shows the various fields of utilities of benchmarking and the consequent table lists down the most known form of benchmarking present today. This study explores the application of benchmarking in the public policy field.

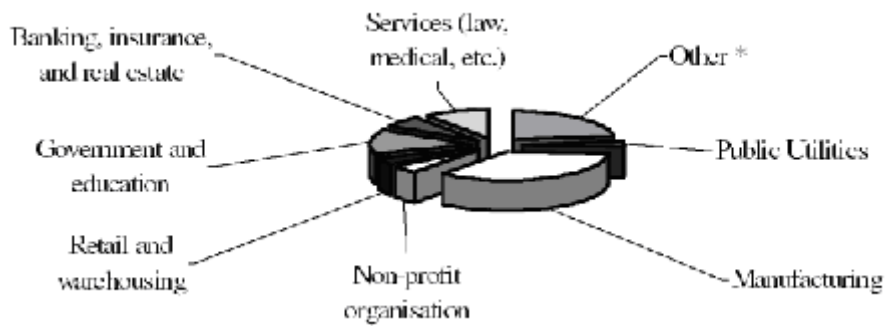


Figure 13: Fields of Benchmarking (Source: Zairi)

Benchmarking is the systematic process of comparing, measuring, analyzing and improving performance in terms of products/services/processes/initiatives of an entity against a reference entity (or entities) (E. Luijff et al., 2006). It is often performed to attain a superior performance or to evaluate one's performance relative to one's (economic) effort (E. Luijff et al., 2006). The table below lists the known types of benchmarking.

Table 15: Types of Benchmarks (Luijff et al., 2007)

Types of Benchmarks	
1.	Strategic Benchmarking
2.	Performance Benchmarking or Competitive Benchmarking
3.	Process Benchmarking
4.	Functional Benchmarking or Generic Benchmarking
5.	Internal Benchmarking
6.	External Benchmarking
7.	Financial benchmarking
8.	Product benchmarking
9.	International Benchmarking

International benchmarking, the last one in the list, will be carried on further in the discussion of this paper for it is the kind of mechanism that the study advocates to employ. It is the type of benchmarking in which partners for the exercise are sought from other countries because best practices are located elsewhere abroad and/or there are too few benchmarking partners within the same country to produce valid results (E. Luijff et al., 2006). Globalization and advances in information technology paves to an easier manner to implement this exercise. However, international benchmarking, as compared to other types of benchmarking, takes more time and resources to set up and implement and the results may need careful analysis due to national differences (E. Luijff et al., 2007). This is a resource-intensive kind of benchmarking and might be difficult to implement by less capacitated parties by themselves, such as developing countries. But because its makeup is the most relevant in the effort of harmonizing global initiatives, this kind of benchmarking is the one advocated by this paper. The international organization does it through its connections with countries employing the “good” practices (EducCom, 2004). In international benchmarking, countries can learn from the “good” practices of one another to achieve a certain goal such as greater infrastructure assurance. Developing countries and even developed countries, which have not formed their strategy, yet would find the exercise useful. Through the benchmark developed, countries can refer to it to assess their present performance in assuring their infrastructures. The pros and cons of externally imposed benchmarking, which is the case of international benchmarking, are tabulated below.

Table 16: Pros and Cons of Externally Imposed Benchmarking

International Benchmarking for Public Policy (OECD, 1997)	
Pros	Cons
<ul style="list-style-type: none"> ■ Secures participation ■ Comprehensive because experiences from many organizations in the world are studied and shared ■ Ensures a better overview on the effects of different processes on performance ■ Ensures effects of external factors to performance ■ Ensures standardization of methods 	<ul style="list-style-type: none"> ■ Lack of ownership by countries and / or organizations ■ Lack of detailed knowledge of activities of the country or organization ■ Externally imposed benchmarking may tend to oversimplify the complex issues ■ There is a risk that the results will only be used at the central level, rather than within individual organizations

3.4.2 Benchmarking as a Public Policy Tool

As shown in Fig. 12, benchmarking has already set foot in the world of public policy, although its application to this field is yet very meager as compared to its intensive use in the private sector (Papaioannou et al., 2006). There are a wide variety of applications of benchmarking but fundamentally it is a structured approach to comparison to facilitate learning (Papaioannou et al., 2006). In the case of this study, the policy baseline that is formed in an international platform will become a benchmark that will be referred to and compared by countries and network operators at stake. The policy baseline, derived from “good” practices, can be used as a reference framework. Benchmarking that is developed through the private sector and its applications may not be straightforward for public services. The competitive pressures for improvement are not the same (OECD, 1997). The objectives of the public sector are not defined by competition and consumers but through a democratic process. If benchmarking is adapted to the needs of the public sector, it is indeed an important instrument for performance improvement. In the same manner, it has a great potential to harmonize initiatives.

The benchmarking of the policy baseline becomes an instrument for harmonization because countries and organizations are able to learn from the “good” practices of others. By becoming aware of both the pros and cons of public policy benchmarking, complex and multi-faceted public issues can be better delineated.

3.4.2.1 Principles of Benchmarking

Benchmarking is defined as the systematic process of comparing, measuring, and analyzing the products, services or processes of an entity against actual experiences of other (preferably world-class) entities to attain a superior performance’ (Zairi, 1996). Its general process (OECD, 1997) is shown by the figure below. The process shows that the pressure for improvement drives the stakeholders to adjust their behavior in reference to what is available in the environment as “good” practices.

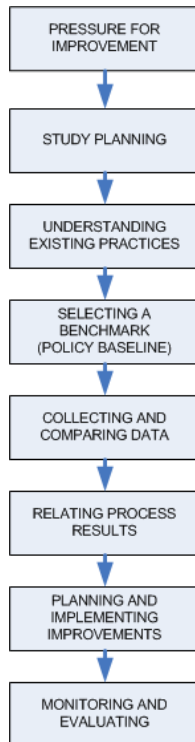


Figure 14: General Process of the Policy Baseline

Together with the principles of standardization and benchmarking, the policy baseline to be developed has the potential to become effective in harmonizing initiatives of a public concern such as infrastructure assurance. The following enumerates and describes the principles of benchmarking. Explanation on how these principles can lead to learning and adjustment is also provided.

1. The ***principle of focus*** implies the creation of systematic comparison of several support schemes with a similar focus. The tighter the definition of the core process being studied, the more valuable and focused the learning opportunities (Papaioannou et al., 2006). As applied to the case, countries might be compared through the initiatives instituted in the area of public-private partnerships, or nature of standards employed by companies, or the approach on scope, etc. By comparing initiatives with a concrete gauge would make the facilitation of learning systematic and easier.
2. The ***principle of measurement*** means that benchmarking the policy baseline requires some sort of objective indicator (Papaioannou et al., 2006). The more objective the measures, the more effective the learning becomes. In the case of the study, initiatives could be assessed by the number of initiatives, the comprehensiveness of the initiatives, the response to the initiatives, the number of attacks/insecurities to network operators, comprehensiveness of laws instituted, and so on.
3. The ***principle of differentiation*** implies that benchmarking of the policy baseline requires differentiation of performance and practice (Papaioannou et al., 2006). Benchmarking should not just be looked at as a “beauty contest” activity—the more the process or initiatives employed become like the policy baseline, the better is your system or the more assured is your system. One has to look more than conformance, more than just installing initiatives. One has to know why such an initiative is lacking, why the system cannot perform as expected and further mitigations should be provided. Understanding the process of the system is more than executing initiatives. In the case of

the study, for example in the Philippines, one should ask why not the Filipino government could not easily conduct a “trusted” public-private partnership and why other countries can just easily trust one another. Such has deeper cultural implications that lead to such a scenario.

4. The ***principle of learning*** is the very essence of benchmarking. This learning is envisioned to lead to harmonization of initiatives. Harmonization does not mean that initiatives are identical. The approaches are the same but the specifics might be different. While the framework of the policy baseline may be used to facilitate who is the “best in class”, but such is only a motivator, not an end in itself (Papaioannou et al., 2006). A learning process occurs when the benchmarking country or company adjusts its policy initiatives based on observation of the benchmarked policy baseline and thus improves its infrastructure assurance.
5. The ***principle of comparability*** implies the need to know the gaps between the benchmarking country and the benchmarked countries (Papaioannou et al., 2006). The developing Philippines cannot fully copy the initiatives of the benchmarked highly developed Netherlands, or Germany or Switzerland. But what the Philippines can take are policy lessons, and their implementations are contour fitted to the country’s capacities and realities. If the gap is seen, one must respond on how to fill in the gap in another means. The emphasis is not copying initiatives, but learning of the initiatives of others.
6. The ***principle of integration*** implies that benchmarking does not only lead to learning but as well accountability (Papaioannou et al., 2006). Policy-makers might be accountable on their position because their performance is being benchmarked. Network operators become accountable in infrastructure assurance because their initiatives are being monitored through a benchmark.
7. The ***principle of applicability*** dictates that cross-country comparisons need to be well-designed to ensure that like-to-like comparisons are being made and that the influence of external contextual factors is minimized as possible or else the difference should be justified in the interpretation (Papaioannou et al., 2006). The context of highly developed countries, for example, might be different from those of developing countries, but as has been said above that developing countries should understand the policy lesson and implement them according to their frames.

The principles above can be both applied for private and public sectors benchmarking. The analysis of a benchmark, using those above-mentioned principles, will become more complicated though when benchmarking is applied to public sector, such as the case of infrastructure assurance, due to its innate complexity--- there are more actors, many interests (political), many definitions of terms, differing mandates, no control, differing degree of powers, etc. The focus, for example, becomes a blur due to the multi-faceted nature of public sector. The indicators might become irrelevant due to complexity that assurance performance is not directly comparable. Issue on comparability and applicability might arise due to the difference in contextual settings of the countries compared, from socio-economic, political to institutional perspectives. These complexities of benchmarking when applied to a public concern are placed in the table below.

Table 17: Possible Complexities of Using Benchmarking in the Public Sector

Principles of Benchmarking	Possible complexities if applied to an issue of public concern
1. Focus	- Comparing something broad and multi-faceted like infrastructure assurance can be extremely difficult
2. Measurement	- Performance measurements are not always comparable
3. Differentiation between performance and practice	- To emphasize the practice dimension as being distinct from performance is a challenge
4. Learning	- Practices which are good in one context may not be applicable in another
5. Comparability	- Comparability is a complex issue. It depends not only on the size of organizations or countries involved but also on socio-economic, political and institutional similarities (and differences) of public sectors
6. Integration	- Releasing some policy-benchmarking information can damage public trust
7. Applicability	- Policy comparisons should be made on the grounds of historically developed socio-economic, political and institutional parallels of the countries involved

Infrastructure assurance as a public concern faces aversion of participation. Due to the various reasons explained in the previous chapter, infrastructure assurance does not have sufficient market incentives to propel market players to drive into this direction. Infrastructure assurance is usually not part of the business cost. Or if there are initiatives appropriated for it most of them are constrained just within the perimeter of the company, not extending to other rival company, and much more to the entire society. Infrastructure assurance for the whole society is a concerted effort of all stakeholders from the government to real operators of the infrastructure. Government alone is insufficient to respond, so does the private sector. As advocated by this paper the infrastructure assurance is the collaboration of both the government and the private sector, but there are hindrances for the private players to participate in the collaboration process. The reasons of liability, insufficient trust, strategic behavior, tight competition, etc. among others are the problems private sector is facing that obstruct them to participate. Liberalization and privatization takes away the concept of regulation as much as possible. Thus, to achieve assurance for a public concern, for it to gain support it has to be non-regulatory and economic-driven in nature. The principles of standardization process are very much applicable to provide stakeholders the grasp of the policy baseline that they will be implementing.

3.4.3 Harmonization Process

As has been expressed above, both the process of standardizations and benchmarking will be used to harmonize initiatives. The standardization process is more suited to harmonize initiatives through the development of the policy baseline, which is also the policy benchmark, and the benchmarking process is more on reinforcing the harmonization process in the implementation stage. The principles of standardization lead to greater support because stakeholders are involved in the process of its development. The principles of benchmarking lead to the adjustment of one's performance in infrastructure assurance as a response brought by the incentives of "good" practices seen in one's environment. A standardization process harmonizes initiatives through developing contents that increase the support of stakeholders while the benchmarking process harmonizes initiatives through providing stakeholders incentives to adjust their performance as they refer to the policy baseline. These concepts are further illustrated by the two figures below.

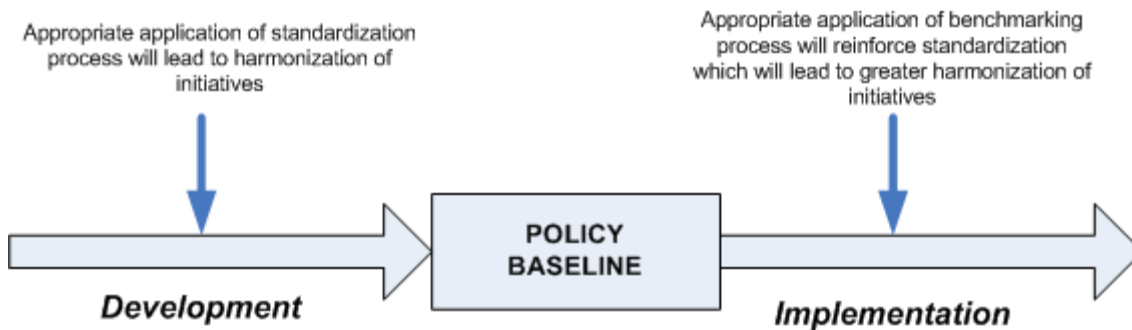


Figure 15: Harmonization through Standardization and Benchmarking

The figure below provides the full trajectory of this study. It starts from an idea of the need of a policy baseline to harmonize initiatives. This idea is further developed and specified by stakeholders in which principles of the standardization are relevant. In this stage the support for implementation has already been acquired. This support is insufficient, though, to achieve a greater level of harmonization due to the problems that occur in the implementation stage. Thus, the mechanism of benchmarking is advocated, which is incentive-driven, to reinforce the harmonization already provided by the standardization process. In this process of implementation, as shown in the figure below, principles of benchmarking are relevant that allow the stakeholders to adjust their behavior to the policy baseline.

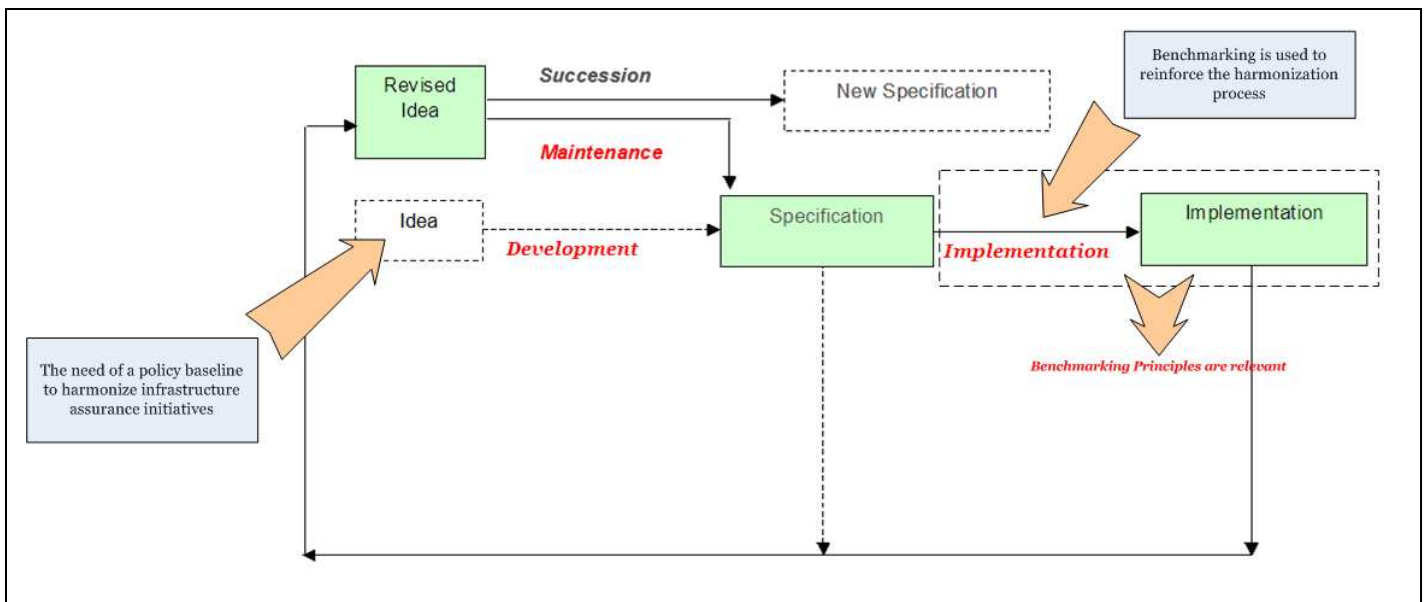


Figure 16: Harmonization through Standardization and Benchmarking (framework adapted from Egyedi, 2007)

3.4.3.1 Integration of Principles

Allow this part to integrate the concepts through placing the principles of both Standardization and Benchmarking in one table and identify how they are able to contribute to the harmonization process.

Table 18: Integration

Standardization harmonizes initiatives in the development process		Benchmarking reinforces the harmonization of initiatives in the implementation process	
Principle	Harmonization Value (Support leads to harmonization)	Principle	Harmonization Value (Adjustment leads to harmonization)
1. Consensus	-Deliberated ideas gain more support -When a compromise is made, everybody decides to support the chosen initiatives	1. Focus	-Areas acknowledged to be problematic elicits learning leading to adjustment
2. Voluntary	-Coercion induces repulsion -Those who volunteer to participate are the ones willing to implement	2. Measurement	-Specific knowledge of the problematic area elicits learning leading to adjustment
3. Democratic	-Balances representation -A more representative baseline gains more support	3. Differentiation	-Learning through the “process” than just the superficial performance leads to adjustment
4. Coherence	-Initiatives consistent to greater values gain more support	4. Learning	-Learning “best” practices leads to adjustment
5. Rationality	-Logical, scientific, and well-based initiatives gain more support	5. Comparability	-Learning differences and similarities leads to adjustment
		6. Integration	-Valuing integrity leads to adjustment
		7. Applicability	-Learning the contextual realities leads to adjustment

As implication of this theory chapter to the context of this study, an international organization is the appropriate platform to develop the policy baseline. Developing countries by themselves are incapable to develop a policy baseline that best reflects the “good” practices in the field. It is also a kind of monitoring mechanism for this international organization on the present performance of their members. For mobile telephony, the ITU is the most relevant international organization, which has the capacity, through its considerable resources and connections, to develop a policy baseline for mobile telephony and perform the international benchmarking exercise for mobile telephony infrastructure assurance. In such a manner, the structure and status of the ITU provides incentives for its member states to conform. Likewise, network operator is pulled to cooperate due to the pressure of its national government and the ITU. There is as well the pressure to respond when the rest of the others are conforming to the policy baseline.

The figure below illustrates further the levels of harmonization both standardization and benchmarking processes provide.

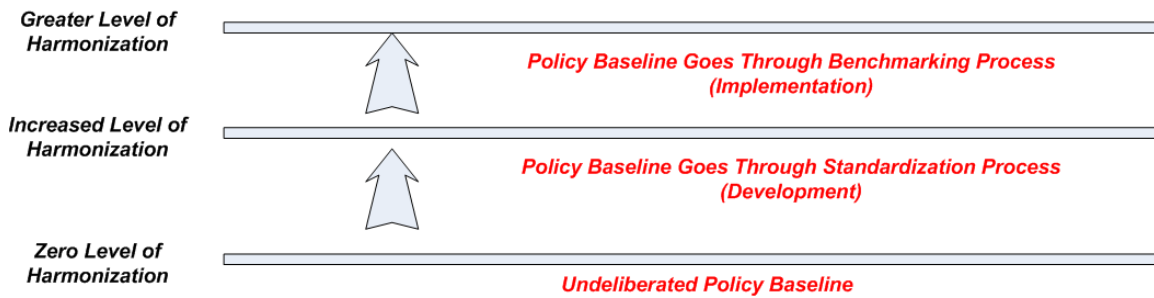


Figure 17: Levels of Harmonization

As shown, if the policy baseline is just made by one person or institution or organization and left “undeliberated”, the level of harmonization is least to occur if none. If a standardization process is employed in the development of policy baseline, support to implement is acquired which leads to harmonization. And then when the policy baseline is made, benchmarking provides the needed incentives to conform to its implementation. Those who do not support the policy baseline during the standardization stage might change their view and find it compelling to adjust their behavior to the direction of conforming to the policy baseline after understanding the value of the benchmarking process in the implementation stage. In such a manner, greater harmonization of initiatives is achieved.

3.5 Filling up the Gap

From the understanding provided by the discussion above, recommendations, such as technical or procedural standards, decision and strategy support or policy baseline as the case of this study, have greater extent of diffusion if the scheme is intentionally designed to include stakeholders’ perspectives and drives in the process—that means, stakeholders, themselves, are the ones who made it and their interests are reflected on it. In so doing, stakeholders find that the recommendations forwarded are their own social construction; thereby, they are more inclined to implement them.

3.6 Key Messages of Chapter 3

- A policy baseline is a set of reference policies agreed to be necessary to achieve a common goal. A policy baseline is adaptive when its provisions can be framed unto a particular environment where it will be deployed.
- Standardization is the process of developing and agreeing upon a (set of) requirement(s) to be established. It is done through a consensus of involved experts.
- Benchmarking is the systematic process of comparing, measuring, analyzing and improving performance in terms of products/services/processes/initiatives of an entity against a reference entity (or entities). It is performed to attain a superior performance or to evaluate one’s performance relative to one’s (economic) effort.
- Benchmarking becomes international when the sought reference entity (or entities) is (are) located abroad because the reference entities are simply not found within the home country or the number of entities is just too few to arrive to a valid result.
- The principles of standardization elicit harmonization through gaining the support of stakeholders to take responsibility of the development and implementation of the policy baseline.

- The principles of standardization relevant to harmonization are: consensus, voluntary, democratic, coherence and rationality.
- The principles of benchmarking reinforce the harmonization process provided by standardization through incentives that encourage stakeholders to implement the policy baseline. In such a manner, greater harmonization is achieved.
- The principles of standardization relevant to harmonization are: focus, measurement, differentiation, learning, comparability, integration and applicability.
- International benchmarking is the most appropriate for the case of this study. International organization is the most appropriate platform to develop the policy baseline and perform benchmarking exercise.
- Benchmarking is incentive-driven that find it suitable to encourage stakeholders to conform to the policy baseline without coercion.
- The principles of benchmarking can be relevant to the public sector as they are in the private sector. It must be acknowledged, however, that benchmarking of a public policy carries with it additional complexity that adds to the difficulty in both developing and implementing the policy baseline. Thus, a more focused approach and a more careful design of a policy baseline, for an issue of public concern, are recommended.
- Employing both processes of standardization and benchmarking will lead to the greater harmonization of policy initiatives.

4

Formulation of the Preliminary Policy Baseline

The previous theoretical chapter defined the concept of infrastructure assurance, enlightened the principles of standardization process serving as the foundation of the development of the content of the policy baseline, and then described the principles of benchmarking in which the implementation process of the policy baseline will be based. Both standardization and benchmarking processes are believed to lead to the greater harmonization of initiatives.

In this chapter, the content of the policy baseline itself will be developed. This is done through taking policy lessons from three countries exemplifying “good” practices, supplemented by expert discussion and on-going initiatives of international organizations. The chapter is divided into four parts. The first part tackles the national arrangement of selected countries (NL, DE, CH and PH) and identifies policy lessons out from their approaches. The second part looks at the initiatives of relevant international organizations (ITU and GSMA) and identifies the niche of the policy baseline in the whole arrangement. The third part presents the salient points derived from the expert discussion conducted. The fourth part constructs the policy baseline and specifies its details. An analysis on its method of implementation is also provided. The rationale of choosing the selected respondents mentioned above is explained in the introduction chapter and detailed in Appendix A2. A “To-Note” box²⁶ is shown whenever there is important policy lesson to emphasize.

4.1 Aim of the Chapter

The chapter, as a whole, strives to answer the following sub-research questions:

“In considerations to the results of various research methods conducted, what are the elements and provisions of the preliminary policy baseline that ensure the global assurance of mobile telephony infrastructure?”

4.2 What can be learned from the national arrangement of the model countries?

4.2.1 The Netherlands

Under the Dutch model, the private sector plays a particularly important role²⁷. The government performs an active role through facilitating initiatives in the protection of infrastructures. Most of the initiatives of the government are non-regulatory. Its initiatives are strongly influenced by the policies at the EU level, and there is a conscious effort to complement policies in the national level²⁸. The Netherlands defines infrastructure assurance in the context of critical infrastructure protection²⁹. Critical infrastructures are formally defined as products, services and their



²⁶ “To-Note” Box

²⁷ Interview with NL01, held June 02, 2008

²⁸ Interview with NL03, held June 02, 2008

²⁹ Interview with NL02, held June 02, 2008

accompanying processes, which society heavily depends on and in the event of disruption or failure, could cause a major disruption in society. This disruption could present itself in the form of tremendous amount of casualties, severe economic damage, or in terms of an extremely lengthy recovery period and a lack of any readily available viable alternatives³⁰ (Merkom, 2008). According to such definition, criticality is framed in the context of impact (e.g. length of time to recover, damage loss, etc.) that the disruption may cause and the availability of viable alternatives when a disruption occurs. Degree of impact and viable alternatives available as criteria would imply that not all infrastructures that are important in the society are considered critical. Mobile telephony in the Netherlands is considered a critical infrastructure³¹. A study in 2002-2003 revealed that mobile telephony is one of the vital infrastructures of telecommunications in the Netherlands (H. A. M. Luijff et al., 2003). The voice facility, however, carries more criticality than the data (SMS) facility³². The assurance of mobile telephony is part of the national strategy to protect critical infrastructures³³. It is under the assurance initiatives on telecommunications and general ICT³⁴. There have been initiatives from both the government and private sector. There have also been public-private partnership implemented, in which the private sector was greatly involved. There is not yet a CIP law in the Netherlands, and it is expressed that the country will not have such kind of law in the sooner future³⁵. The country only has general policies on the responsibilities of the network operators for a secure and reliable mobile telephony³⁶. All activities are done in voluntary manner, and no binding laws that compel stakeholders to implement CIP. But since CIP is also a stake of the private players, the government is not having a difficulty to get them on board³⁷. Various sector in the government coordinate with EU bodies in order to initiate coherent actions.



To Note: The approach in the Netherlands is private sector driven³⁸. There is a conscious effort to coordinate with international bodies and avoid overlapping of policies³⁹. The used “rule of thumb” is: never start with regulation and, by all means possible, do things in a bottom up approach⁴⁰.

4.2.1.1 Government Initiatives

The Ministry of the Interior and Kingdom Relations (BZK) carries coordination responsibility for critical infrastructure protection (CIP) as part of its mandate as the coordinating ministry for crisis management⁴¹. Every ministry is responsible for the protection of its own governed sectors. The national policy on Critical Information Infrastructure Protection (CIIP) for the private sector is under the national ICT policy responsibility of the Ministry of Economic Affairs, in which initiatives are based on policies set for CIP⁴². The areas of coordination in CIP are in the tasks of mapping out vulnerability and resistance and investigating inter-sectoral harmonization⁴³.

■ Institutional Arrangements

In the Netherlands, infrastructure assurance is carried out through several activities, supported by several organizations, which are all operating from their respective perspectives. The Ministry of Interior furnishes a step-by-step plan for mapping out vulnerability and resistance, offers help

³⁰ European Commission, Response of The Netherlands, 31 March 2008

³¹ Interview with NL01, June 02, 2008

³² Interview with NL03, held June 02, 2008

³³ Interview with NL01, held June 02, 2008

³⁴ Interview with NL01, held June 02, 2008

³⁵ Interview with NL01, held June 02, 2008

³⁶ Interview with NL01, held June 02, 2008

³⁷ Interview with NL03, held June 02, 2008

³⁸ Interview with NL02, held June 02, 2008

³⁹ Interview with NL03, held June 02, 2008

⁴⁰ Interview with NL01, held June 02, 2008

⁴¹ Critical Information Security Protection Policy in the Netherlands (ENISA Contribution)

⁴² Protection of the government ICT (of e.g. the emergency services; GOVCERT.NL, NICC) is part of the Ministry of the Interiors policy fields and some of its operational tasks.

⁴³ Critical Information Security Protection Policy in the Netherlands (ENISA Contribution)

for topics not exclusive to a sector and encourages collaboration⁴⁴. It also investigates whether protection measures have been adopted by sectors and whether harmonization is achieved or not.

Table 19: Some Early CIP and CIIP Efforts

Early Efforts to Protect Information and Communication Infrastructures
The Digital Delta ⁴⁵
Whitepaper 2000 ⁴⁶
KWINT study 2001 (vulnerability of the Dutch Internet) ⁴⁷
Protection of Dutch Critical Infrastructure

CIP/CIIP in the Netherlands is perceived increasingly as a crucial issue of national security. Since the end of the 1992, several efforts have been made to better manage CIP/CIIP. For mobile telephony in the Netherlands, its criticality will continue to increase as more and more applications are being done through the mobile phone⁴⁸. It is expressed that in the Netherlands, the EU has greater influence than UN or ITU when it comes to policy initiatives⁴⁹.

The figure below shows the whole arrangement in the Netherlands. Coordination between the different activities/projects is taking place through the steering committees at top management level in the three involved ministries⁵⁰. For national ICT policy for the private sector/citizens, the Ministry of Economic Affairs is the coordinating organization. Mobile telephony is part of the national ICT policy⁵¹. The national ICT policy initiatives are not separated from the initiatives of national infrastructure assurance. For infrastructures that are owned or controlled by public organizations, the government has full authority to execute risk analyses and implement protective measures⁵². For infrastructures owned or controlled by private organizations or companies, the government is mandated to monitor if responsible organizations/companies are initiating risk analyses and employing appropriate protective measures⁵³. This monitoring responsibility of the government depends on the extent of regulation in force to the sector. In the sector of full competition, in which only the least regulation is allowed, the government performs an advisory role for infrastructure assurance to the sector.

⁴⁴ Response of the Netherlands on Specific Elements of National Policies for Critical Infrastructure Protection in the ICT Sector, European Commission, March 31, 2008

⁴⁵ Luijff, Eric, and Marieke Klaver. In Bits and Pieces: Vulnerability of the Netherlands ICT-Infrastructure and Consequences for the Information Society (Amsterdam, March 2000); translation of the Dutch Infodrome essay 'BITBREUK', de kwetsbaarheid van de ICT-infrastructuur en de gevolgen voor de informatiemaatschappij, p. 5.

⁴⁶ Ministerie van Defensie, Defensienota 2000, (1999), p. 59.

⁴⁷ Van Till, J., Luijff, H.A.M., de Boer, J. Klaver, M.H.A., Huizenga, J.R., van de Sandt, C., *KWINT: Samen werken voor veilig Internet verkeer, een e-deltaplan*, Ministry of Transport, Public Work and Water Management, The Hague, The Netherlands, 2001

⁴⁸ Interview with NL01, held June 02, 2008

⁴⁹ Interview with NL03, held June 02, 2008

⁵⁰ Critical Information Security Protection Policy in the Netherlands (ENISA Contribution)

⁵¹ Interview with NL03, held June 02, 2008

⁵² Critical Information Security Protection Policy in the Netherlands (ENISA Contribution)

⁵³ Critical Information Security Protection Policy in the Netherlands (ENISA Contribution)

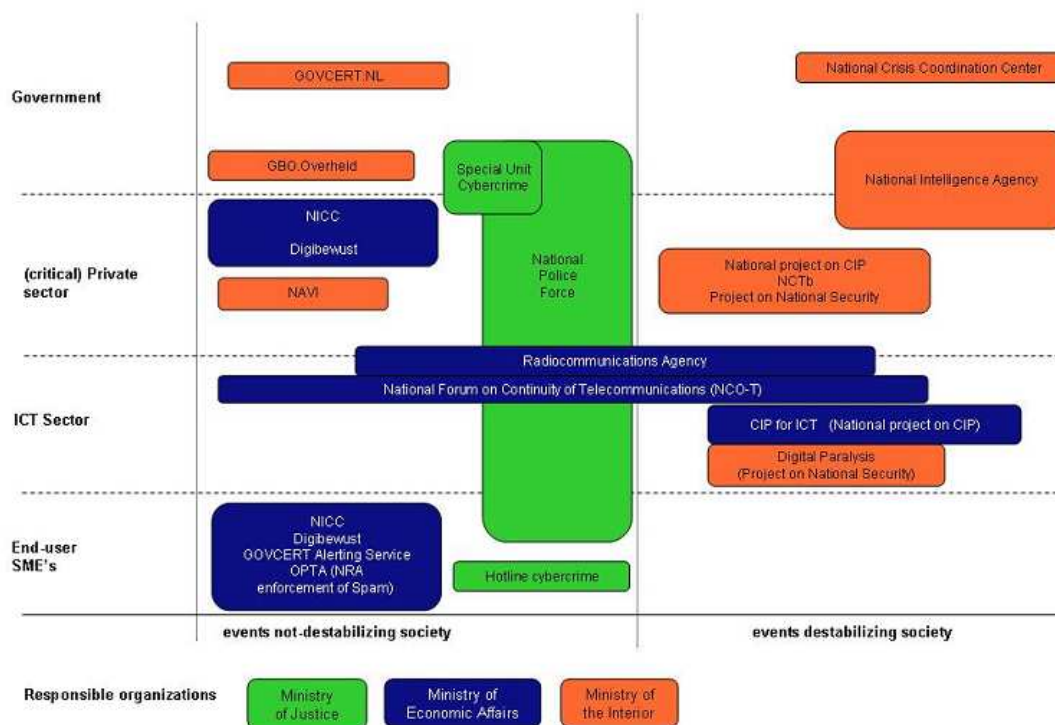


Figure 18: Netherlands National Arrangement (Source: NL CIIP provided for ENISA Quarterly)

The National Coordinator for Counterterrorism (NCTb), through the Counterterrorism Alert System, is responsible for terrorist cases on ICT provision or usage⁵⁴. Appropriate actions start in cooperation with the respective organizations most relevant to the threats. The Ministry of Interior is responsible for crisis management, the Ministry of Economic Affairs is responsible for national policy on public telecommunications service provisioning⁵⁵.

Table 20: Dutch Government Agencies involved in CIP

Important Agencies Most Involved in Critical (Information) Infrastructure Protection
Ministry of the Interior and Kingdom Relations (BZK)
Ministry of Economic Affairs (EZ)
Ministry of Transport, Public Works, and Water Management (V&W)
Ministry of Housing, Spatial Planning, and the Environment (VROM)
Ministry of Health, Welfare and Sport (VWS)
General Intelligence and Security Service (AIVD, part of the BZK)

■ **Laws and Legislations**

The following are the relevant laws in the assurance of telecommunications sector. It has to be noted that the Telecommunications Law of the Netherlands states the requirements that must be met by public telecommunications operators with regards to the capacity, quality, and other properties of the services offered (e.g. free access to the 112 emergency number), as well as regulations of with respect to safety and privacy precautions regarding their network and services (Dunn & Abele-Wigert, 2006a).

⁵⁴ Critical Information Security Protection Policy in the Netherlands (ENISA Contribution)

⁵⁵ Critical Information Security Protection Policy in the Netherlands (ENISA Contribution)

Table 21: Laws and Legislations relevant to CIP in the Netherlands

Laws and Legislations
Penal Code
Telecommunications Law ⁵⁶
Criminal Code, Articles 138a and 138b

There is no specific law for general CIP, but the Telecommunications Law itself mandates that safety and privacy in mobile telecommunications, and with the rest of other telecommunications technologies, should be upheld.



To Note: In the Netherlands, the government performs regular risk and vulnerability assessments⁵⁷. It is part of its approach to harmonize initiatives between sectors and encourages collaboration with the private sector. The government does check if private sectors are initiating risk analysis and employing appropriate measures⁵⁸. The government does act as an advisory body in the concern of infrastructure assurance. There are no laws presently instated for general critical infrastructure assurance, but the Dutch Telecommunications Law instated safety and privacy precautions in the network and its services⁵⁹.

4.2.1.2 Public-Private Partnerships

Public-Private Partnership (PPP) is a crucial element in Infrastructure Assurance. PPP is the structure to suit best the work needed in the field of CIP since the private sector is owning or controlling 70% of the critical ICT infrastructure⁶⁰. It is expressed that there have been a number of initiatives executed in the Netherlands to upgrade the level of national infrastructure assurance⁶¹. Information Security Awareness raising programs have been initiated by organizations like ECP.nl⁶², a public-private partnership to cooperate on important preconditions and breakthroughs regarding digital economy and society. For specific infrastructure protection matters, NAVI⁶³ (National Centre for Advice on Critical Infrastructures, a dedicated advisory function, was established under the coordination form the Ministry of the Interior and Kingdom Relations. The National Forum on Continuity of Telecommunications (NCO-T), chaired by the Ministry of Economic Affairs, provides a common platform for providers of public ICT services identified as critical. The National Infrastructure Cyber Crime (NICC) programme was established in 2006, modeled after UK's NISCC⁶⁴. NICC aims to bring together, in a confidential environment, public and private parties from each sector and to exchange among these parties best practices and experiences in fighting cyber crime⁶⁵. It also aims to implement information exchange points about threat or real life attacks based on the information from national intelligence or CERTs. A project on the national security strategy and its implementation, coordinated by the Ministry of Interior, carries out activities in the field of strategy towards the robustness of critical infrastructures (Dunn & Abele-Wigert, 2006b).

⁵⁶ <http://www.verkeerenwaterstaat.nl/?!c=uk>

⁵⁷ Response of the Netherlands on Specific Elements of National Policies for Critical Infrastructure Protection in the ICT Sector, European Commission, March 31, 2008

⁵⁸ Interview with NL03, held June 02, 2008

⁵⁹ Interview with NL01, June 02, 2008

⁶⁰ Response of the Netherlands on Specific Elements of National Policies for Critical Infrastructure Protection in the ICT Sector, European Commission, March 31, 2008

⁶¹ Interview with NL03, held June 02, 2008

⁶² www.ecp.nl

⁶³ NAVI – Nationaal Adviescentrum Vitale Infrastructuren


⁶⁴ Interview with NL02, held June 02, 2008

⁶⁵ Critical Information Security Protection Policy in the Netherlands (ENISA Contribution)

Table 22: PPP Initiatives in the Netherlands

Public-Private Partnership Initiatives
KWINT Program (2003-2006)
Platform for Electronic Commerce in the Netherlands (ECP.NL)
Critical Infrastructure Protection Project
Strategic Council for CIP (SOVI)
National Continuity Consultation Platform Telecommunication (NCO-T) → a successor of the earlier National Continuity Plan for Telecommunications (NACOTEL)
Nationaal Adviescentrum Vitale Infrastructuur (NAVI)
The National Infrastructure against Cyber Crime (NICC)

The activities carried out under the scope of risk management take the all-hazard approach. Mobile telephony assurance is all part in the critical infrastructure protection national strategy. At national level, information sharing is done in National Crisis Centre regular meetings, NICC, NAVI, National Continuity Platform, etc. The Ministry of Economic Affairs and the Ministry of Interior participates in several international policy settings such as EU (EPCIP, CIIP, ENISA MB, OECD (WPISP), NATO (CEP/CPC), OECD, CIIP Handbook, Meridian Conference, International Watch and Warning Network (IWWN)⁶⁶.

 To Note: The approach to acquire assurance is through public-private partnership. The partnership provides platform for information sharing of “good” practices. The partnership is an exchange point in a private and confidential setting. Activities undertaken are risk-based, all hazards, multi-stakeholders and multi-sector for overall CIP initiatives. There is an effort to collaborate with international bodies.

4.2.1.3 Lessons Identified

Table 23: Lessons Identified from the Activities of the Netherlands

Essential Policy Lessons to be Derived from the Netherlands
Private Sector Driven
Public-Private Partnership
Most of the initiatives are non-regulatory oriented
Inclusion of safety and privacy in Telecommunications Law
High level of trust
Coordination with international bodies
All hazards approach
Multi-sector approach for overall CIP initiatives

Looking at how the Netherlands arranges its initiatives to acquire assurance in the infrastructure, it can be deduced that, if there is a policy baseline to be made, sharing of information is a prerequisite. The government and the private sector have to gather in the table to discuss the issue in the atmosphere of trust. There have been various public-private partnerships conducted and support from the private sector is witnessed. The private players are participative in the undertakings because they see their stakes in the assurance of mobile telephony. The government has their stake, as well, and it is for such reason that strong collaboration among institutions exists. Providing a trusted platform is seen to be the policy baseline in the Netherlands. In their initiatives, there is a strong emphasis on being comprehensive in the approach, which means that the process should be risk based, multi-sector and all hazards. The level of trust cannot happen in a shot but various public-private partnerships can pave the way towards more cohesive institutions that assure the infrastructure. International undertakings should be included in the policy baseline because it is by such a manner, through comparison, that the government or network operators can assess the level of the assurance of their infrastructure.

⁶⁶ Critical Information Security Protection Policy in the Netherlands (ENISA Contribution)

4.2.2 Germany

In Germany, the infrastructure assurance of mobile telephony is part of its national plan for critical infrastructure protection with the government having the pivotal role to play⁶⁷. The main assumption underlying infrastructure assurance is that both the government and the citizens heavily depend on the secure and reliable operation of infrastructures⁶⁸. Germany's Constitution on Civil Protection Law states that the Federal Government is responsible for civil protection in war time, while the 16 states are responsible for disaster control during peacetime⁶⁹. All elements that comprise an infrastructure whose failure or impairment would cause dramatic consequences for large parts of the population (e.g. sustained storage of supplies, disruptions of public order, etc.) are defined as critical⁷⁰. As mandated by the German Constitution, it is the task of the government to ensure public security, order and safety and guarantee the provision of essential good to the citizen⁷¹. Infrastructure assurance is, thus, the main responsibility of the government and should provide the leading role to initiate mitigating policies and initiatives⁷².

There have been direct and indirect initiatives attributed for infrastructure assurance⁷³. The inter-ministerial initiative started with the Federal Minister of Interior provoked by the report of PCCIP⁷⁴ and events of September 11, 2001. This issue was initially framed in the context of campaign against terrorism and was expanded to other assurance activities of national scope, which also eventually led to international dialogue. There were two key documents created in 2005, which can be seen as the first milestones for establishing infrastructure assurance throughout the country. The first one is the "National Plan for Information Infrastructure Protection (NPSI), enacted by the cabinet decision of the federal government. The second one is the "Baseline Protection Concept for Critical Infrastructure Protection"⁷⁵.



To Note: The government of Germany plays a pivotal role in the assurance of infrastructures. The activities all emanate from a central body then implemented to the private sector⁷⁶. The activities were at first terrorism-focused but expanded to other kind of hazards and from nationally oriented to including international perspectives in its approaches.

4.2.2.1 Government Initiatives

Germany's strategy and approaches can be described through specifying three requirements, namely (1) defining responsibility, (2) fostering cooperation, and (3) identifying economic benefits⁷⁷. The first one clarifies the responsibility of the infrastructure operators mandating them to integrate safety and security concepts in their company's policies. It also reveals public responsibility for civil protection requiring to integrate safety and security concepts into civil protection strategy. The second strategy of the government is to foster cooperation through identifying stakeholders (operators, associations, etc.) and fostering dialogue through roundtable discussions, networking, etc. The third strategy of the government is identifying economical benefits through integrating safety and security through value-added chain (e.g. control of production and supply chains, business continuity management, cost-benefit analysis, etc.). The

⁶⁷ Interview with DE01, held June 02, 2008

⁶⁸ Interview with DE02, held June 02, 2008

⁶⁹ Federal Ministry of the Interior, German National CIP Strategy

⁷⁰ Federal Ministry of the Interior, German National CIP Strategy

⁷¹ Interview with DE01, held June 02, 2008

⁷² Draft update on the contribution for CIIP Handbook

⁷³ Interview with DE01, held June 02, 2008

⁷⁴ US President's Commission on Critical Infrastructure Protection (PCCIP)

⁷⁵ Bundesministerium des Innern. Schutz Kritischer Infrastrukturen – Basisschutzkonzept, (Berlin, August 2005).

http://www.bmi.bund.de/Internet/Content/Common/Anlagen/Broschueren/2005/Basisschutzkonzept_kritische_infrastrukturen_de,templateId=raw,property=publicationFile.pdf/Basisschutzkonzept_kritische_infrastrukturen_de.pdf
http://www.bbk.bund.de/cln_007/nn_398882/SharedDocs/Publikationen/Publikationen_20Kritis/Basisschutzkonzept__engl,templateId=raw,property=publicationFile.pdf/Basisschutzkonzept_engl

⁷⁶ Interview with DE01, held June 02, 2008

⁷⁷ Federal Ministry of the Interior, German National CIP Strategy

German government places it forward that investment into safety and security is the solution for increasing the level of infrastructure assurance⁷⁸. For the assessment of the hazards and threats confronting critical infrastructures, the following activities have been done.

Table 24: Initiatives for Situational Analysis

Initiated Activities for Situational Analysis of Threats and Hazards	
1.	Comprehensive Report on Threats and Hazards
2.	Kirchbach Report
3.	Critical Infrastructure Protection – Baseline Protection Concept
4.	Critical Infrastructure Protection – Risk and Crisis Management (Guideline for Enterprises and Government)
5.	LÜKEX
6.	Pandemic Handbook

In the “Comprehensive Report on Threats and Hazards”, the German Ministry of the Interior (BMI) published a second comprehensive threat analysis for Germany⁷⁹. The Kirchbach Commission analyzed the overall structure of the German Emergency Protection System after the disastrous Elbe flooding in 2003. It provided comprehensive analysis of the existing facilities and recommendations for future capacities to secure information and communications technology in cases of emergency, leading to a broad range of measures in several ministries and agencies⁸⁰.

The “Baseline Protection Concept for Critical Infrastructure Protection”, developed in closed coordination among national agencies, namely: Federal Ministry of the Interior (BMI)⁸¹, the Federal Office for Civil Protection and Disaster Response (BBK)⁸², the Federal Criminal Police Agency (BKA)⁸³, with the private sector. It provides guidance for the analysis of potential hazards such as terrorist attacks, criminal acts, and natural disasters, as well as recommendations for companies for adequate protective measures. The CIP baseline protection concept was complemented by a guideline: “Critical Infrastructure Protection – Risk and Crisis Management (Guideline for Enterprises and Government)”^{84,85}, which provides methods to support the implementation of risk and crisis management in enterprises and government organizations for and provides checklists and examples. The LÜKEX Series⁸⁶ (2004, 2005, and 2007) is a strategic exercise for large-scale power outage, mass events and pandemic, respectively. The Pandemic Handbook⁸⁷, published in 2007, encourages especially small and medium-sized enterprises to plan precautions for potential pandemics.

⁷⁸ Federal Ministry of the Interior, German National CIP Strategy

⁷⁹ Federal Ministry of the Interior. Zweiter Gefahrenbericht der Schutzkommission beim Bundesminister des Innern. Bericht über mögliche Gefahren für die Bevölkerung bei Grosskatastrophen und im Verteidigungsfall (Berlin, October 2001). http://www.bmi.bund.de/Internet/Content/Common/Anlagen/Broschueren/2001/Zweiter_Gefahrenbericht_der_Id_12312_de,templateId=raw,property=publicationFile.pdf/Zweiter_Gefahrenbericht_der_Id_12312_de.pdf

⁸⁰ Bericht der Unabhängigen Kommission der Sächsischen Staatsregierung. Flutkatastrophe 2002 (2nd ed., 2003). <http://home.arcor.de/schlaudi/Kirchbachbericht.pdf>.

⁸¹ Bundesministerium des Innern. <http://www.bmi.bund.de/>

⁸² Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. <http://www.bbk.bund.de>.

⁸³ Bundeskriminalamt. <http://www.bka.de>.

⁸⁴ Presented in January 2008, Press release: see http://www.bmi.bund.de/cln_028/nn_165030/Internet/Content/Themen/BevoelkerungsschutzUndKatastrophenhilfe/DatundFakten/Leitfaden_SchutzKritischerInfrastrukturen.html

⁸⁵ Available only in German: http://www.bmi.bund.de/Internet/Content/Common/Anlagen/Broschueren/2008/Leitfaden_Schutz_kritischer_Infrastrukturen,templateId=raw,property=publicationFile.pdf/Leitfaden_Schutz_kritischer_Infrastrukturen.pdf

⁸⁶ http://www.bmi.bund.de/cln_028/nn_662928/Internet/Content/Nachrichten/Pressemitteilungen/2007/11/Luekex_Uebung.html, in German

⁸⁷ See <http://www.gesundheitsamt-bw.de/servlet/PB/menu/1245313/index.html> and <http://www.gesundheitsamtbw.de/servlet/PB/show/1238642/Handbuch%20BePP%20Version%202.2B%20071220.pdf> (in German).

Table 25: Government Initiatives in Infrastructure Assurance

CIIP in Germany
CIIP at the Federal Office for Information Security
National Plan for Information Infrastructure Protection
CIP Implementation Plan
IT Security Situation in Germany
IT Security Guidelines

The overall responsibility and coordination of CIP- and CIIP-related activities rests with the Federal Ministry of the Interior (BMI)⁸⁸, together with several of its subordinated agencies, such as the Federal Office for Information Security (BSI), the Federal Agency of Civil Protection and Disaster Response (BBK), the Federal Law Enforcement Agency (BKA), and the Federal Police (BPOL). A task force for critical infrastructure protection (PG KRITIS) was established to coordinate the ministry and its subordinated agencies. Strategy development and implementation are also coordinated with other federal ministries. Furthermore, strategic partners from the private sector are consulted. In Germany, the tasks for CIP, defined as physical protection, and CIIP, defined as cyber-protection, are separated in management. This is opposite as compared to the Netherlands and Switzerland where CIP and CIIP are integrated in one strategy⁸⁹.

The following are the ministries and agencies involved in the initiatives of infrastructure assurance in Germany.

Table 26: Ministries and Agencies in Germany involved in Infrastructure Assurance

Institutional Arrangements in Germany
Federal Ministry of the Interior (BMI) ⁹⁰ ⁹¹
-- specifically its Federal Office for Information Security (BSI) ⁹²
Federal Office for Civil Protection and Disaster Response (BBK) ⁹³ ⁹⁴
The Federal Criminal Police Agency (BKA) ⁹⁵
Federal Ministry of Economics and Technology (BMW <i>i</i>) ⁹⁶
Federal Network Agency ⁹⁷
Federal Ministry of Justice (BM <i>J</i>) ⁹⁸
Federal Ministry of Defense (BM <i>Vg</i>) ⁹⁹

■ Laws and Legislations

The following laws are relevant for infrastructure assurance in telecommunications.

Table 27: Laws relevant to Assurance of Telecommunications

Laws and Legislations
Telecommunications Act ¹⁰⁰
Telecommunications and Media Act 2007 ¹⁰¹
Electronic Signature Act 2001 ¹⁰²
Penal Code ¹⁰³

⁸⁸ Interview with DE01, held June 02, 2008

⁸⁹ Interview with DE02, held June 02, 2008

⁹⁰ http://www.bmi.bund.de/Internet/Content/Ministerium/Organigramm__Neu/Referate/itstab__engl.html

⁹¹ http://www.bmi.bund.de/Internet/Content/Ministerium/Organigramm__Neu/Referate/abteilung__km__engl.html

⁹² <http://www.bsi.de/english/functions.htm>

⁹³ http://www.bbk.bund.de/cIn_007/nn_402322/EN/00__Home/homepage__node.html__nnn=true

⁹⁴ As a main CIP output, The BBK has developed the “Critical Infrastructure Protection – Baseline Protection Concept” and the “Critical Infrastructure Protection – Risk and Crisis Management (Guideline for Enterprises and Government)”, and the GMLZ has a central role in all LÜKEX exercises

⁹⁵ <http://www.bka.de>

⁹⁶ <http://www.bmwi.de/>

⁹⁷ <http://www.bundesnetzagentur.de/enid/0a888f9d9a85f3748b2d8fb635f752e7,0/xn.html>

⁹⁸ http://www.bmj.bund.de/enid/4e02aa38526e9a3069072ac5fa5dbc01,0/aktuelles_13h.htm

⁹⁹ <http://www.bmvg.de/portal/a/bmvg>



To Note: In Germany, the initiatives conducted are comprehensive in approach, such as comprehensive analysis of threats and hazards, comprehensive baseline protection for enterprises and government, comprehensive analysis of criticality of existing facilities, etc. One striking difference with the Netherlands is that the implementation process in Germany is government-centric, a top-down approach. Although there are some strategic private partners involved in assuring the infrastructure, the pivotal role to implement is heavily relied on the hands of Federal Ministry of Interior together with its subordinated agencies.

4.2.2.2 Public-Private Partnerships

In Germany, there is a common understanding that public-private partnership is the best approach to assure the infrastructure¹⁰⁴. The latest example of public-private cooperation was the development of CIP implementation plan. This is followed by a set of ongoing activities to actually implement the strategy. The “Germany secure in the Network” campaign is an initiative undertaken by the BMI and participation of private enterprises and non-profit organizations was recognized. The Initiative D21 is the largest public-private partnership in Germany that gave focus on the areas of digital integration, competence and excellence. Some other initiatives are listed below.

Table 28: Public-Private Partnership Initiatives

PPP Initiatives
CIP Implementation Plan
“Germany secure in the network” Campaign
Initiative D21
IT Situation Center
IT Crisis Response Center



To Note: Public-private partnership is an essential factor in the successful implementation of the initiatives¹⁰⁵. German government takes the lead to cooperate with the private sector to gain greater support. The government initiates activities so that private sectors (and non-profit organizations) can join the process.

4.2.2.3 Lessons Identified

Table 29: Lessons Identified from the Activities of Germany

Essential Policy Lessons to be Derived from Germany
Government-Centric Driven
Need to identify critical infrastructures
Perform comprehensive risk analysis
Establish appropriate institutional arrangements
Central coordination could be efficient
Involve the private sector
Coordinate with international bodies
All hazards approach

¹⁰⁰ http://www.gesetze-im-internet.de/tkg_2004/BJNR119000004.html

¹⁰¹ <http://bundesrecht.juris.de/tmg/BJNR017910007.html>, in German

¹⁰² Bundesministerium der Justiz. Gesetz über Rahmenbedingunge für elektronische Signaturen (Signaturgesetz – SigG). Available:http://www.gesetze-im-internet.de/sigg_2001/BJNR087610001.html.

¹⁰³ See: Cybercrimelaw. Country Survey Germany. Availabe: <http://www.cybercrimelaw.net/countries/germany.html>; and Bundesministerium der Justiz. Strafgesetzbuch. Available: <http://www.gesetze-im-internet.de/stgb/index.html>.

¹⁰⁴ Interview with DE02, held June 02, 2008

¹⁰⁵ Interview with DE02, held June 02, 2008

Germany is an example where government takes a leading role in implementing initiatives to protect infrastructures. Through its initiatives, the private sector participates. In this scheme of central coordination, the government has an active role to safeguard its citizen from threats and hazards. Although the approach is government-centric, there is still a common understanding that public-private partnership is the best strategy. The government puts forward the initiative first and allows the private sector to participate. This is done in such manner in order to achieve more coherent and more coordinated initiatives. If there is a policy baseline to be made, the initiatives should be comprehensive, which is based on risk analysis and covers all hazards. It must also be included in that policy baseline the idea that the government and private owners should coordinate internationally.

4.2.3 Switzerland

Under the Swiss model, infrastructure assurance is understood as military-political and state function¹⁰⁶. The most important organization is the Swiss Department for Defence, Civil Protection and Sport (DDPS) that looks after all the main Critical Infrastructure Protection programmes¹⁰⁷. The “Strategic Management Exercise of 1997”¹⁰⁸ resulted in the adoption of the “Strategy for Information Society Switzerland”. DDPS conducts information operations as a standard line of operations and prepares its forces to counter the challenges of the information revolution¹⁰⁹. Protection against information operations and information warfare is seen as crucial for the functioning of Swiss army, but also for Swiss society and its economy. The lessons identified from the conceptual design of the military operation capability will be used to prepare the civilian world to cope with mode of conflict and the threats it constitutes.

There are a number of incidents that led them to define a coherent national strategy for critical infrastructure protection and these are the following: breakdown of the mobile telephone network (2001), power blackout in Italy due to line breakdown in Switzerland (2003), SBB¹¹⁰ black-out which made a country-wide outage of railway infrastructure due to power failure (2005), and the closing of the Gotthard Highway A2 through the Alps in one month due to rock fall (2006)¹¹¹.



To Note: Infrastructure assurance is seen through the perspective of military operation. The Ministry of Defence of the Federal is given the highest role to protect the civil society, and included in this protection are the critical infrastructures. Mobile telephony is viewed as one of the Switzerland’s critical infrastructures.

4.2.3.1 Government Initiatives

There have been a number of initiatives since 1990 that aimed to assure infrastructure but during that time these are not yet part of a national strategy (Dunn & Abele-Wigert, 2006b). The table below lists the previous initiatives that aimed to improve the management of critical infrastructures. The Strategic Leadership Exercise in 1997 revealed that Switzerland’s critical infrastructures are facing new threats and one of the recommendations was the need for an independent organization to deal with information security issues. “The Concept of Information Assurance” in 2000 recommended the establishment of a crisis management system of a special task force on “Information Assurance”. In 2005, there was a formal mandate to create a national strategy for Critical Infrastructure Protection. This strategy is built on the tenets of the four pillars, namely: prevention, early recognition, crisis management and technical problem solution. The overall responsibility lies with Federal Strategy Unit for Information Technology (ISB), together with the participation of MELANI¹¹², SONIA¹¹³ and NES¹¹⁴.

¹⁰⁶ CIP Program in Switzerland, Federal Office for Civil Protection

¹⁰⁷ Interview with CH01, held May 28, 2008

¹⁰⁸ The SFU, which is subordinated to the Swiss Federal Chancellery, is responsible for the periodical training of federal decision-makers. [http:// www.sfa.admin.ch](http://www.sfa.admin.ch).

¹⁰⁹ Interview with CH02, held June 03, 2008

¹¹⁰ Swiss Federal Railway

¹¹¹ CIP Program in Switzerland, Federal Office for Civil Protection

¹¹² The Reporting and Analysis Center for Information Assurance

Table 30: Information Assurance Initiatives in Switzerland

CIP Initiatives
Strategic Leadership Exercise ¹¹⁵
Strategy for the Information Society Switzerland
Security Policy Report ¹¹⁶
Concept of Information Assurance

The Swiss infrastructure assurance national strategy is coordinated by the Federal Office for Civil Protection (Department of Defence, Civil Protection and Sport) and collaborated with interdepartmental working group involving more than 20 federal offices, 26 cantons¹¹⁷ and industry players¹¹⁸.

Table 31: Swiss Chronology of Infrastructure Assurance Initiatives (Source: Federal Office for Civil Protection)

Switzerland's Chronology of Infrastructure Assurance Initiatives	
1997	SFU Strategic Leadership exercise on revolution in information technology
1998	"Strategy for the Information Society Switzerland"
2000	Security Policy Report 2000 → Recognizes CIP/CIIP as a goal of its security policy
2001	Informo 2001 Strategic Leadership Training → Train new special task force on information assurance SONIA
2004	MELANI (Reporting and Analysis Center for Information Assurance) is operational
2005	Federal counsel decision to start CIP project

The government agencies involved in assuring telecommunications/ICT infrastructure in Switzerland are listed below.

Table 32: Government Agencies Involved

Institutional Arrangements in Switzerland
Federal Department of Defense, Civil Protection and Sports ¹¹⁹
Federal Office for Communication ¹²⁰
Federal Office of IT, Systems and Telecommunication ¹²¹
Federal Strategy Unit for Information Technology ¹²²

There are no binding legislations yet instated for infrastructure assurance except for the Swiss penal code. Everything is in the level of policy initiatives of the Ministry of Defence and public-private partnerships involving key industry players¹²³.

¹¹³ Special Task Force for Information Assurance

¹¹⁴ National Economic Supply

¹¹⁵ The SFU, which is subordinated to the Swiss Federal Chancellery, is responsible for the periodical training of federal decision-makers. <http://www.sfa.admin.ch>.

¹¹⁶ <http://www.vbs.admin.ch/internet/vbs/de/home/departement/organisation/security/publikationen.ContentPar.0011.DownloadFile.tmp/Sicherheitspolitischer%20Bericht%202000.pdf>.

¹¹⁷ Cantons are the states of the Federal State of Switzerland

¹¹⁸ Interview with CH02, held June 03, 2008

¹¹⁹ Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS). <http://www.vbs.admin.ch/internet/vbs/en/home.html>.

¹²⁰ Bundesamt für Kommunikation (BAKOM). <http://www.bakom.ch/en/index.html>.

¹²¹ Bundesamt für Informatik und Telekommunikation (BIT). <http://www.efd.admin.ch/e/dasefd/aemter/bit.htm>.

¹²² Informatikstrategieorgan Bund (ISB). <http://www.isb.admin.ch/internet>.

¹²³ Interview with CH02, held June 03, 2008

Table 33: Relevant Legislations

Laws and Legislation
Swiss Penal Code



To-Note: The guiding principles of Swiss Federal Government initiatives are all hazards approach, integrated risk management, public-private partnerships, conscious avoidance of policy duplications and a one coherent national approach. These principles find parallelism with the initiatives of other modeled countries. The difference is in the style of implementation, which largely depends on the socio-political setup of the country.

4.2.3.2 Public-Private Partnerships

Switzerland has a long tradition of public-private partnerships, which is due to the tradition of part-time service in a strong militia system (Dunn & Abele-Wigert, 2006b). The InfoSurance Association was founded by a number of companies in support of the Swiss government. It is an association that aims to increase awareness of the information assurance issue and to establish networks of cooperation among the various players (Dunn & Abele-Wigert, 2006a). Another important public-private partnership is the NES, which works in close cooperation with the private sector as well as with cantonal and municipal authorities. NES deals with all prolonged disruptions of the information and communication infrastructures affecting the whole Switzerland (Dunn & Abele-Wigert, 2006b).

Table 34: PPP Initiatives

PPP Initiatives
InfoAssurance Association ¹²⁴
NES ICT-I ¹²⁵
CLUSIS
MELANI ¹²⁶
SONIA ¹²⁷

There are a number of initiatives that are government-driven that allow participation of the private sector. These are the last two initiatives in the list above. MELANI works together with partners in the area of critical infrastructure protection, security of computer systems and internet¹²⁸. It is coordinated by Federal Strategy Unit for Information Technology. The Federal Police Office operates the analysis centre of MELANI to collect information from both public and private critical infrastructure operators¹²⁹. The success of MELANI as a reporting and analysis center for information assurance largely depends on its close cooperation with the public and private sector¹³⁰. SONIA, on the other hand, is a special task force for information assurance that intervenes in crisis situations caused by problems in the ICT infrastructure. It comprises decision-makers of critical infrastructures from both public and private sectors. It is headed by the Delegate for the Federal Strategy Unit for IT¹³¹.



To-Note: Public-Private Partnership is an important element in the national strategy of Switzerland. The government leads in the initiatives through providing an avenue for the private sector to participate¹³². There is not much difficulty in getting the private sector on board due to the already established culture of collaboration that rooted from the strong long-standing tradition of militia system.

¹²⁴ <http://www.infosurance.ch>.

¹²⁵ <http://www.bwl.admin.ch/deutsch/themen-infra-ict.asp>.

¹²⁶ <http://www.melani.admin.ch/index.html?lang=en>

¹²⁷ <http://www.isb.admin.ch/themen/sicherheit/00152/00176/index.html?lang=en>

¹²⁸ Interview with CH02, held June 03, 2008

¹²⁹ Interview with CH02, held 03, 2008

¹³⁰ Interview with CH02, held 03, 2008

¹³¹ <http://www.isb.admin.ch/themen/sicherheit/00152/00176/index.html?lang=en>

¹³² Interview with CH02, held June 03, 2008

4.2.3.3 Lessons Identified

Table 35: Lessons Identified from the Activities of Switzerland

Essential Policy Lessons to be Derived from Switzerland
Government-Military Driven
All hazards approach
Integrated risk management
Public-Private Partnership
Coherent national strategy
Avoids duplication

The national arrangement of Switzerland has shown us another manner of implementation of national strategy for infrastructure assurance. The government-military setup finds it suitable for Switzerland because of socio-political and historical reasons. Culture of collaborations has been established, which attributes to the reason that the private sector easily participates. This might not be the same to other countries. Switzerland stresses its guiding principles in creating a national strategy for infrastructure assurance. This finds parallelism with other modeled countries and this study considers these principles “good” practices, which will define the policy baseline developed in this study. To restate Switzerland’s principles on infrastructure assurance, the strategy should be all hazards-approach, integrated risk management, public-private partnerships, avoids overlapping and uses synergies.

4.2.4 Comparative Analysis of the Model Countries

The table below highlights in summarized form the policy lessons identified in each of the model countries.

Table 36: Comparative Analysis Table

Policy Lessons Identified from Model Countries			
Dimension	Netherlands	Germany	Switzerland
Coordination Mechanism	Private Sector Driven	Government Driven	Government-Military Driven
Strategy	Coherent National Strategy	Coherent National Strategy	Coherent National Strategy
Overall CIP	Multi-sector	Multi-sector	Multi-sector
Arrangement	Public-Private Partnership	Public-Private Partnership	Public-Private Partnership
Hazards Approach	All Hazards	All Hazards	All Hazards
Management Approach	Risk-Based	Risk-Based	Risk-Based
Third Party Platform	Yes (NCO-T)	Yes (No Formal Organization)	Yes (MELANI)
International Coordination	Yes	Yes	Yes

There are policy lessons that stand out from the undertakings of the three model countries. By such reason, this study considers those policy lessons “good” practices and become the basis in defining the preliminary baseline as the main output of this study. These policy lessons are shortly stated as follows.

- The analysis raises the need for the creation of a coherent national strategy for mobile telephony infrastructure assurance that is based on:

- Integrated risk analysis and management
- Public-private partnership
- All hazards approach
- Multi-sector (for overall infrastructure assurance strategy)
- Formation of a trusted platform
- International coordination

4.2.5 Philippines

This part discusses the infrastructure assurance of the Philippines in line with the aim of this study of including a developing country to assess the suitability of the proposed policy baseline that will be developed. In the Philippines, the approach for infrastructure assurance is seen to be government-centric and initiatives are terrorism focused¹³³. The country has long been struggling with minority vandals (e.g. terrorists, peace wrecker, etc.) who flaunt their hostages every now and then, ruin infrastructures and leave threats to people in both private and public places (e.g. bomb in the airport, stations, etc.)¹³⁴. They are purported to be internationally-linked terrorists thriving within Philippine boundaries. There are a number of times that cell sites are bombed¹³⁵ and communications to the place is cut because other means to communicate (e.g. fixed line) are simply unavailable. Or bombs explode which are cellphone detonated¹³⁶. Or the illegal interception of frequencies (cellular snooping)¹³⁷ to transgress privacy of public and private persons (even the president¹³⁸ herself was a victim of “wireless”-tapping in the infamous “Hello Garci” scandal). These and other many circumstances undermine the reputation of the infrastructure to be secure and reliable. Much more that mobile telecommunication in the Philippines is the prime means of communications and more facilities for important transactions are being added to the infrastructure¹³⁹. Indeed, in the Philippines, the mobile telephony (both voice and data) is a critical infrastructure that demands immediate actions for assurance¹⁴⁰.

Amidst its threats and vulnerabilities, Philippine mobile telephony, however, continues to be an example of success in the launching of essential features that performs important transactions through the mobile phone¹⁴¹. The country has been known as the “SMS” capital of the world due to the beyond belief use of SMS for communication¹⁴². A former president of the country was even ousted from office through the so-called mass organizing¹⁴³ “SMS”-revolution (Colonel, 2001). This is a prime example of the impact of mobile telephony in political arena. Many business models have been created in this SMS phenomenon such as money transfer¹⁴⁴, mobile banking, m-commerce, m-auctions all-in-one messaging service, at present, etc. aggravated by the present huge of Filipino “diaspora” abroad, where substantial amount of remittances are derived and transferred through the mobile phone¹⁴⁵. The Philippine mobile telephony market is described in Appendix E1 and products and services of leading Philippine network operators are placed in Appendix E2.



To-Note: The Philippines has a promising mobile telephony market in a harsh setting due to the disorganized institutions that should have supported the infrastructure. Amidst the obliviousness of the institutions of their important role, mobile telephony continues to be a vibrant infrastructure serving as the prime means of telecommunications in the country.

¹³³ Interview with PH02, held on July 03, 2008

¹³⁴ <http://edition.cnn.com/2008/WORLD/asiapcf/05/29/philippines.explosion.ap/index.html>

¹³⁵ <http://www.cleveland.com/newsflash/international/index.ssf?/base/international-29/1214894942258420.xml&storylist=international>

¹³⁶ <http://edition.cnn.com/2008/WORLD/asiapcf/05/29/philippines.explosion.ap/index.html>

¹³⁷ <http://www.pcij.org/blog/?p=100>

¹³⁸ <http://www.gmanews.tv/story/57157/Doble-Hello-Garci-wiretap-ops-done-through-Smart-mole>

¹³⁹ Interview with PH02, held on July 03, 2008

¹⁴⁰ Interview with PH02, held on July 03, 2008

¹⁴¹ Interview with PH02, held on July 03, 2008

¹⁴² Pinoy Internet: Case Study of Telecommunications Market, ITU, 2002

¹⁴³ <http://mobileactive.org/mobiles-in-mass-organizing>

¹⁴⁴ <http://smart.com.ph/>, <http://www1.globe.com.ph/index.aspx>

¹⁴⁵ Interview with PH02, held on July 03, 2008

4.2.5.1 Government Initiatives

As said above, the approach to infrastructure protection in the Philippines is government-centric and initiatives are terrorism driven. At the moment, there is no clear delineation yet of where mobile telephony fits in the whole scheme¹⁴⁶. The style has been reactive, such as: if there is an attack, it is only then that the government and military will respond. Due to the nascent stage of mobile economy, assurance issues are not the priority of many stakeholders¹⁴⁷. Government and private sector collaboration has not yet come to a plethora in the Philippines¹⁴⁸. Even among government agencies, linkages of activities are yet hard to find. This means that fragmentation of institutions is indeed occurring in the country¹⁴⁹.

Some of the initiatives done by the government to protect the infrastructure are listed in the table below. Since assurance should be a proactive approach, it is bit a stray to describe the government initiatives as such for most of those being conducted are reactive in nature. One of those is the “Balikatan exercise”¹⁵⁰, a combined planning with the US, that trains people to combat the attacks of terrorist to infrastructure, community, or entire civil society, etc (Radics, 2004). The National Bureau of Investigation (NBI) under the Department of Justice conducts initiatives in deterring crimes related to the critical infrastructures or critical (information) infrastructures. NBI Forensics laboratory played a critical role in the deliberation of the “I Love You” virus case¹⁵¹. The national agencies below are the present important players in the protection of the infrastructure.

Table 37: National Arrangement in the Philippines

National Arrangement
National Bureau of Investigation ¹⁵²
National Police ¹⁵³
National Security Council ¹⁵⁴
National Telecommunications Commission ¹⁵⁵
National Economics and Development Authority

The Philippines legislations related to mobile telephony are listed in the table below.

Table 38: Philippines Laws and Legislations dealing with Telecommunications/CIIP

Laws and Legislations
RA No. 7925, Public Telecommunications Policy Act ¹⁵⁶ (this law specifically institutionalizes competition and liberalization, mandates extension of services to unserved and underserved areas)
Republic Act No. 8792, Philippines E-Commerce Law ¹⁵⁷



To Note: The government approach, at present, is terrorism focused. This is because of the colossal problem the country is facing with alleged “international terrorists” thriving in the country who take advantage of the country’s disorganized setting of institutions. Activities for other hazards, such as in the scope of operation and maintenance, etc., of the infrastructure are yet unclear or not delineated. If there are initiatives, they are not nationally coordinated. The approach is individual protection of their own-managed infrastructure.

¹⁴⁶ Interview with PH02, held July 03, 2008

¹⁴⁷ Interview with PH02, held July 03, 2008

¹⁴⁸ Interview with PH01, held July 03, 2008

¹⁴⁹ Interview with PH02, held July 03, 2008

¹⁵⁰ <http://www.globalsecurity.org/military/ops/balikatan.htm>

¹⁵¹ Interview with PH01, held July 03, 2008

¹⁵² <http://www.nbi.doj.gov.ph/>

¹⁵³ <http://www.pnp.gov.ph/>

¹⁵⁴ http://www.op.gov.ph/profiles_gonzalesn.asp

¹⁵⁵ http://portal.ntc.gov.ph/wps/portal/!ut/p/_s.7_0_A/7_0_9D?cID=6_0_FM&nID=7_0_LU

¹⁵⁶ http://www.lawphil.net/statutes/repacts/ra1995/ra_7925_1995.html


¹⁵⁷ <http://www.news.ops.gov.ph/e-commerce.htm>

4.2.5.2 Public-Private Partnerships

Public-private partnership is yet an elusive undertaking in the Philippines¹⁵⁸. Public-private partnership presently has a binding legislative image, in which voluntary actions to participate is yet an aloof thought. The present setup in infrastructure assurance for mobile telephony is that protections are provided in areas where facilities are under threat or have been destroyed already and repairs are to be undertaken¹⁵⁹. The concerned telecom company normally requests assistance/support/protection from the police and army in coordination with the local government units¹⁶⁰. Thus, as of now, government’s role is limited to providing security support to augment the security guards of the private companies¹⁶¹. There is one private initiated project involving the government, though in the area of cybersecurity as shown in the table below.

Table 39: Public-Private Partnership in the Philippines

Public-Private Initiative
Philippine Honeyjet Project ¹⁶²

 To-Note: Public-private partnership has a binding legal image in the Philippines. Such kind of perception drives stakeholders away from participating because involvement means coercion through regulation and the undertaking is resource-intensive. This image has to be changed so that it can be shaped to the kind of public-private partnership envisioned suitable for infrastructure assurance initiatives.

4.2.5.3 Lessons Identified

As an analysis to the current undertakings in the Philippines, the approach seems to be fragmented, central-governance oriented, single hazard focused, qualitative assessment of risks, and single-sector oriented. Learning lessons from the modeled countries, infrastructure assurance initiatives have to be based on trust realized through public-private partnership, have one national strategy to avoid overlapping of initiatives, focused on many hazards possible (e.g. include disasters, technical and procedural failures, inappropriate policies, mismatched institutional arrangements, etc., quantitative manner of assessment, and include other sectors to determine (inter)-dependencies. The realities of the initiatives of infrastructure assurance in the Philippines are compared to the guiding principles derived from the analysis of the initiatives of the modeled countries in the table below.

Table 40: Observation on Philippines National Arrangement as Compared to the three Modeled Countries

Essential Observations on the Philippines Arrangement	
Policy Lessons Identified from Three Modeled Countries	Present Philippine Arrangement on Infrastructure Assurance
<p>Public-Private Partnership One National Strategy All Hazards Integrated Risk Management (Both qualitative and quantitative)</p> <p>Multi-sector approach to CIP Existence of Information Sharing Platform</p>	<p>Less Private Sector Participation Fragmented Terrorism Focused SWOT (Qualitative)</p> <p>Single Sector approach to CIP No information sharing platform at present</p>

¹⁵⁸ Interview with PH02, held July 03, 2008

¹⁵⁹ Interview with PH02, held July 03, 2008

¹⁶⁰ Interview with PH02, held July 03, 2008

¹⁶¹ Interview with PH02, held July 03, 2008

¹⁶² <http://www.philippinehoneyjet.org/>

4.2.6 Integration of the Policy Lessons Identified from Model Countries and its implications to the Philippines Infrastructure Assurance Setting

The table below places in a nutshell the infrastructure assurance initiatives of the four selected countries.

Table 41: Infrastructure Assurance Arrangements in Four Selected Countries

	Netherlands	Germany	Switzerland	Philippines
General Approach	<ul style="list-style-type: none"> • Private sector driven • Active in international coordination • Bottom-up approach to avoid regulation • Risk-based, all-hazards, multi-sector 	<ul style="list-style-type: none"> • Government leads the initiatives • Legislations make binding coordination • International coordination is considered • Risk-based, all-hazards, multi-sector 	<ul style="list-style-type: none"> • Government has the highest role to protect critical infrastructures such as mobile telephony • Infrastructure assurance is seen as a military operation • Risk-based, all-hazards, multi-sector • Coordinate internationally 	<ul style="list-style-type: none"> • Government driven; initiatives are terrorism-focused • Infrastructure assurance is seen to be the sole function of the government • International coordination needs to be strengthened
Government Initiatives	<ul style="list-style-type: none"> • Perform risk and vulnerability assessment • Encourage private sector cooperation in defining initiatives • Act as an advisory body 	<ul style="list-style-type: none"> • Pivotal role heavily relies on the government • Private sector participates through the activities of the government • Private sector is actively participating so far 	<ul style="list-style-type: none"> • Pivotal role heavily relies on the government • Private sector is actively participating so far 	<ul style="list-style-type: none"> • Government plays the leading role • Approach is through binding agreements • Infrastructure Assurance is less of a priority
Public-Private Partnership	<ul style="list-style-type: none"> • Public-private partnership is an essential element • Public-Private Partnership is voluntary • Creation of a third platform established in the atmosphere of trust 	<ul style="list-style-type: none"> • Public-Private Partnership is essential • Government provides the atmosphere of trust • There are binding agreements for PPP 	<ul style="list-style-type: none"> • Public-Private Partnership is essential • Government leads the initiatives • Private sector voluntarily collaborate attributed to their long PPP tradition in militia system 	<ul style="list-style-type: none"> • Public-private partnership occurs in binding agreements • Atmosphere of trust is yet to be established

The model countries illustrated the essential roles of both the government and the private sector in providing assurance to infrastructure. The government has a pivotal role to play; together with that is the irreplaceable function of the private sector that no one else of the other actors can perform. Indeed, it is strongly shown by the three model countries that infrastructure assurance is a public-private undertaking. Both the government and the private sectors provide means and ways to build a trusted common ground for them to discuss and share the problem and solution.

The manner of implementation varies in each of the countries; the manner on how the country is arranged has lots to do with cultural atmosphere, tradition of trust, stakeholders' active participation, etc. The approach to the issue of the model countries is almost the same and such implies comprehensiveness by involving multi-stakeholders. "Sense of powers and authorities" varied in dynamics in each of the country but the manner of dealing the issue itself is almost the same. The Netherlands, for example, is described more of employing the bottom-up approach. The private sectors themselves are very active in the provision of initiatives of infrastructure assurance. The government, on the other hand, though plays less of a role, provides an environment where stakeholders can voluntarily interact. This "easiness" or almost automatic sense of collaborative undertaking among stakeholders can be attributed to the long-standing culture of the country ("Dutch polder" model approach) of building a "coming to the table to discuss" scenario. This bottom-up approach has become a basic way of doing things in the Netherlands. In the Netherlands, high level of trust is given to each of the ground players of the infrastructure. This sense of "coming to the table" scenario is yet very hard to establish to other countries more especially in developing countries, in which the approach is rather individualistic. This kind of setup is common to a country where the environment is harsh and the institutions are disorganized. There is no way for the ground players but to individually protect themselves. In Germany, on the other hand, the initiatives instituted for infrastructure assurance are laid down emanating from the "creative minds" of the government. The government agencies themselves are the ones who designate the initiatives and the private sectors participate. This manner of implementation is the opposite from that of the Netherlands but they both have almost the same approach of dealing the issue, which stresses much on comprehensiveness and applies multi-perspectives as possible. This "top-down" approach for Germany may have lots to attribute from the history and cultural setting of the country, and its large size that makes coordination from the bottom appeals difficult. The striking fact, though, is that the private players have a high level of trust to the government and for that active participation from the private sector to the initiatives of the government on infrastructure assurance is observed so far. The government believes, which is explicitly expressed in its constitutions, that infrastructure assurance, as part of national security, is its main responsibility and not of the ground players of the infrastructure. Because of the high trust of the people to its government, participation of the constituents is not uncommon. This kind of approach is, as well, seen in Switzerland where the government takes much of the leading role. The government provides the initiatives and the private sector participates. Only that in Switzerland, the culture of trust is well-founded on the long-tradition of collaboration in militia system. Collaboration among stakeholders is not a "new thing", and by such reason that any undertaking that is of public concern finds it relatively easy for all stakeholders to get on board to mitigate the issue. Being comprehensive and multi-perspectives in the approach to the issue is also manifested in the activities of Switzerland the same as with to Netherlands and Germany. The application of this discussion then goes on how less developed countries can approach the issue of infrastructure assurance. Because of the desire of harmonizing initiatives, reality of less developed countries is an important element of the issue. The study brings in the realities of the Philippines where mobile telephony is a critical infrastructure placed in an institutionally fragmented environment. Most of the policy lessons derived from the three model countries are almost non-existent in the Philippines. Model countries explicitly showed that the approach has to be comprehensive and multi-perspectives, which means risk-based, all hazards, public-private partnership, extend the insight to other sector (multi-sector), established on trust and internationally coordinated. Most of these are yet far for the Philippines to achieve because it has yet to perform a lot of overhauling to the arrangement of its institutions. The Philippine stakeholders have to recognize these policy lessons and infuse them as much as possible to their manner of dealing to the issue. The institutional setting is very important for the Philippines, and any other countries, to achieve greater level of infrastructure assurance in the society. The Philippines has yet a long way to go. Its present style of government centric and terrorism-focused approach has to be extended to other facet of infrastructure assurance. The undertaking has to become proactive and not reactive as what is currently observed in the study. Other factors that undermine the assurance of infrastructure have to be also given due attention. The Philippines is yet in a very basal stage and actions have yet to be done in order to achieve that culture of trust and cooperation. Its present undertakings could be a start of the process, but the insights towards the approach has to be extended; in other words, policy lessons from "good"

practices have to be acknowledged and be infused to the initiatives instituted. The policy baseline might help in the acceleration of the learning curve of the Philippines, and other less developed countries, in their response towards infrastructure assurance. Helping the less developed countries to hasten their learning process is the rationale of defining a policy baseline.

4.2.7 Sample Benchmarking Exercise

Chapter 3 (Theory) described the function of benchmarking in coordinating policy initiatives in the area of infrastructure assurance for mobile telephony. This mechanism is appropriate because of the largeness of the scope of the infrastructure and the non-desirability of regulation in this respect. In this section, the study performs a sample international benchmarking exercise using the information derived from the various research methods conducted. Appropriate international organization and national institutions perform and implement the real benchmarking exercise with the due involvement from the stakeholders in defining its contents and process.

The study uses the criteria below in assessing the “appropriateness” of the policy initiatives instituted in selected countries in the area of infrastructure assurance for mobile telephony. The criteria are derived from the aim of improving infrastructure assurance, anchoring the advocated role and responsibilities of relevant stakeholders. Explanations of the choice of criteria are also provided.

Government Initiatives

- 1.) Mobile telephony infrastructure assurance as part of overall national strategy
- 2.) All-hazards approach through implementation of comprehensive risk management (including threats and vulnerabilities)
- 3.) Voluntary implementation of the scheme
- 4.) Active International collaboration

Explanation: Through the analysis of the government initiatives of the model countries, the four criteria above abide to the policy lessons identified. This means that the government has to create a comprehensive and coherent national strategy for infrastructure assurance in which the sector of mobile telephony is clearly delineated. The first criterion specifies that mobile telephony should be part of the overall national strategy for infrastructure assurance. By such a manner, a coherent strategy is created and overlapping of activities is avoided. The creation of a national strategy implies the awareness of the government to the issue and the desire of a clear and concrete action to mitigate the issue. The second criterion specifies the comprehensiveness of the approach. This criterion implies that all-hazards should be taken consideration in the planning of strategy. A narrow focused approach (e.g. technical only or terrorism-oriented only) does not provide a proactive approach to the issue. An eye to include all possible hazards is suitable for a “network of networks” infrastructure because threats and vulnerabilities are amplified by such an arrangement. The third criterion admits the need for a voluntary mechanism because direct regulation has been shown the least desirable for a liberalized and privatized sector. Lastly, the fourth criterion demands the need for international coordination because of the advocated multi-level and multi-lateral approach to mitigating the issue. The next set of criteria roots from the “good” practices of the model countries in the area of public-private partnership.

Public-Private Partnerships

- 1.) Existence of legislations/national policies established for infrastructure assurance
- 2.) Establishment of trusted third party platform for infrastructure assurance
- 3.) Comprehensive approach of the public-private initiative
- 4.) Voluntary participation to the public-private initiative

Explanation: The public-private partnership defines the collaboration of both the government and the private sector in assuring the infrastructure. The study believes that such arrangement is the most efficient means to move forward for such an issue of infrastructure assurance in liberalized and privatized environment. The first criterion is the existence of legislations and/or national policies providing a public-private atmosphere of collaboration and paving way to the eventual establishment of a trusted environment. These binding agreements are not interventions to the operation and maintenance of the infrastructure but express a convergence of will that public-private partnership is necessary for greater provision of infrastructure assurance. The second criterion is the establishment of a trusted third party platform that provides an avenue for both the government and the market players to freely share sensitive information needed for the due deliberation of the issue and discussion of possible solution. The likes of NCO-T¹⁶³ of the Netherlands and the MELANI¹⁶⁴ of Switzerland could be an appropriate model for this third-party platform. In Germany, it is the government itself that provides the trusted platform. The third criterion expresses again the need for comprehensiveness of the public-private initiatives. The approach should be based on risk taking grounds from vulnerability and threats analyses. Lastly, the fourth criterion again is the provision of voluntary atmosphere to participate in the initiatives as it is believed that coercion rather induces repulsion. Allow the stakeholders to realize the need by themselves and their participation implies support to the implementation of initiatives. The last set of criteria that pertains to the network operators will be enumerated and then explained below.

Network Operators Approach

- 1.) Implementation of Information Security Management System
- 2.) Implementation of Business Continuity Planning and Management
- 3.) Participation in information sharing activities
- 4.) International Collaboration

Explanation: The last, but certainly not the least important stakeholder of mobile telephony infrastructure, is the network operator. This stakeholder has very important role to play in assuring the infrastructure. In the first place, its network is its own management. Employing the needed assurance measures in its own jurisdiction would alleviate greatly the condition of infrastructure assurance. The first criterion dictates the implementation of Information Security Management System (ISMS) to its own network to assure information-dependent facilities. Basically, a mobile telephony infrastructure is a critical information infrastructure by itself. A number of standardization bodies (e.g. ITU-T, ISO, ETSI, etc.) provide technical standards and standard operating procedures for the proper implementation of ISMS. The second criterion demands the execution of Business Continuity Planning and Management (BCMP) that assures those assets aside from information-dependent facilities, such as human resource, hardware, organization, external services and environment. There are also standards (technical and procedural) provided by formal standardization organizations such as ISO, BSI, ITU-T, etc. The framework of ISMS and BCMP is described in Appendix H. The third criterion is the active voluntary participation of the network operator to information sharing activities. This is connected to the public-private initiatives in the second set of criteria. Voluntary sharing of information in the trusted environment facilitates a more efficient deliberation of the problem and solution. Lastly, the fourth criterion expresses the need for network operators to collaborate with international bodies in order to coordinate assurance initiatives. The network operator has to participate with the benchmarking exercise in collaboration with the government and international organizations to assess and improve the present status of infrastructure assurance in mobile telephony.

¹⁶³ http://www.ez.nl/english/Subjects/Digital_security/Continuity_and_Crisismanagement/NCO_T?rid=150708

¹⁶⁴ <http://www.melani.admin.ch/index.html?lang=en>

4.2.8 Defining Levels of Assurance

The study defines “levels” to heuristically approximate the condition of assurance for each of the selected countries. Assurance is assessed through the “appropriateness” and “comprehensiveness” of the initiatives. “Appropriateness” indicates the suitability of the initiatives in reference to the contextual setting. “Comprehensiveness” specifies if the effort reflects the consideration of all relevant factors both in scope and participation of stakeholders. Comprehensiveness and appropriateness are “quantified” through a defined set of criteria, cross matching the conformance of the initiatives to what the criteria denote. The table below provides the meaning and description of these levels.

Explanation of Levels:

Table 42: Level of Infrastructure Assurance Measured through Initiatives Instituted

Level	Meaning	Description
Level 0	No initiatives	None of the criteria is accomplished
Level 1	Limited Initiatives	Only one of the criteria is accomplished
Level 2	Few Initiatives	Only two of the criteria are accomplished
Level 3	Medial initiatives	Three of the criteria are accomplished
Level 4	Substantive Initiatives	All of the criteria are accomplished



























Meaning of Levels:

Level 0 (zero) indicates that none of the criteria is accomplished. This would imply that the stakeholders in the country are either not aware of the issue or aware but do not have the capacity to institute initiatives, thereby, needing assistance from relevant partners. Level 1 (one) indicates that only one of the criteria forwarded in this study is accomplished. This implies that only little or limited initiatives have been instituted. The approach implemented is not comprehensive and stakeholders are not in active participation. There is huge institutional fragmentation occurring in the country that collaboration among stakeholders to provide comprehensive initiatives is difficult to achieve. As above, this would mean that the country is oblivious of the issue. If aware, it does not have sufficient capacity to institute comprehensive initiatives, thereby, needing assistance from relevant partners. Level 2 (two) indicates that only two of the criteria are accomplished. This shows that the country well-acknowledges their stakes to infrastructure assurance but institutional fragmentation (and other problems) is hindering stakeholders to collaborate and provide comprehensive actions. Level 3 (three) indicates that more than half of the criteria are accomplished. This indicates that the country sees and acknowledges the need for instituting initiatives and medial effort has been executed to assure the infrastructure. There is yet to be done, though, to achieve a greater level of assurance. Level 4 (four) indicates that substantive effort has been attained. The effort is appropriate and comprehensive. This denotes that the country acknowledges their stakes on the assurance of infrastructure and instituting comprehensive and appropriate initiatives is its priority. In this level all the relevant actors are involved in the process of providing assurance to the infrastructure.

Using the criteria and levels defined above, assurance performance of the country can now be measured. The table below assesses the initiatives of the selected countries. This has to be kept in mind, though, that this exercise is a heuristic approximation of the assurance performance of the country. It is a gross simplification of the very complex process of measuring performance in the area of public concern such as infrastructure assurance. The aim of the exercise is to provide workable (“rule of thumb”) description of the condition that serve to guide decision processes to mitigate the problem.

4.2.9 International Benchmarking Exercise

Table 43: Sample Benchmarking Exercise Table

Dimensions	Netherlands	Germany	Switzerland	Philippines
<u>Government Initiatives</u> 1.) Mobile Telephony Infrastructure Assurance as part of overall national strategy 2.) All hazards approach through implementation of comprehensive risk management 3.) Voluntary implementation of the scheme 4.) Active International collaboration		 Regulated		No Strategy for Mobile Telephony Terrorism-focused only No clear Scheme yet 
<u>Rate</u>				
<u>Public-Private Partnerships</u> 1.) Existence of legislations/Policies established for infrastructure assurance 2.) Establishment of trusted third party for infrastructure assurance 3.) Comprehensive approach of the public-private initiative 4.) Voluntary participation to the public-private initiative	Incomplete legislations/policies 	 Government assumes to be the trusted party  The approach is binding	Incomplete legislations/policies 	Incomplete legislations/policies No third party No PPP initiatives No PPP initiatives
<u>Rate</u>				None
<u>Network Operators Approach</u> 1.) Implementation of Information Security Management System 2.) Implementation of Business Continuity Planning and Management 3.) Participation in information sharing activities 4.) International Collaboration	  Does not see much of the need	 	 	Respondents did not provide information for security reason No information sharing 
<u>Rate</u>				

From the table above, we can heuristically quantify the assurance level of the selected countries. The initiatives instituted serve, in this study, as the basis for measuring performance. This study presupposes that it is the comprehensiveness and appropriateness of the initiatives that assure the infrastructure. The number and impact of failure and disruption are believed to be “side-effect” implications of the insufficient level of measures afforded. Thus, they are not the real cause of “inassurance” but the lack of initiatives to mitigate the problem.

The next table quantifies the level of efforts afforded to assure the infrastructure. The number is based on the conformance of the initiatives to the criteria defined in this study. This is an extension of the benchmarking table provided above. The descriptive matrix follows after the next table.

Table 44: Initiatives Compared

	Government Initiatives	Public-Private Partnership	Network Operator Approach
Netherlands	4	3	3
Germany	3	2	4
Switzerland	4	2	4
Philippines	1	0	1

The table above shows that Netherlands and Switzerland have substantive initiatives from the government side based on the criteria provided. Germany fails in one point due to its strong government-centric approach. It is, thus, recommended that Germany has to involve more the private sector in the creation and implementation of initiatives. The Philippines fails to create a national scheme that demands a comprehensive consideration. In this case, the Philippines needs assistance in building its national capacity to assure the infrastructure. The table also shows that the Netherlands has the highest level in public-private partnership. This can be attributed to the private-sector push of the setup. The bottom-up approach of the Netherlands encourages greater participation from the private stakeholders. Germany and Switzerland scored the same and Philippines shows no effort to establish public-private partnerships. Lastly, the table also compares the effort of the network operators. Both Germany and Switzerland scored the highest level based on the criteria provided. Their network operators employ the necessary technical and procedural measures and collaborate internationally. The network operator in the Netherlands employs the necessary technical and procedural measures, but it was expressed that not much international collaboration has been done so far. The Philippines does collaborate internationally but it was not provided if they employ technical and procedural measures for infrastructure assurance for the reason of privacy and sensitivity. At the moment, there is no information sharing initiatives between the network operators and the government and among network operators. The benchmarking matrix is shown below.

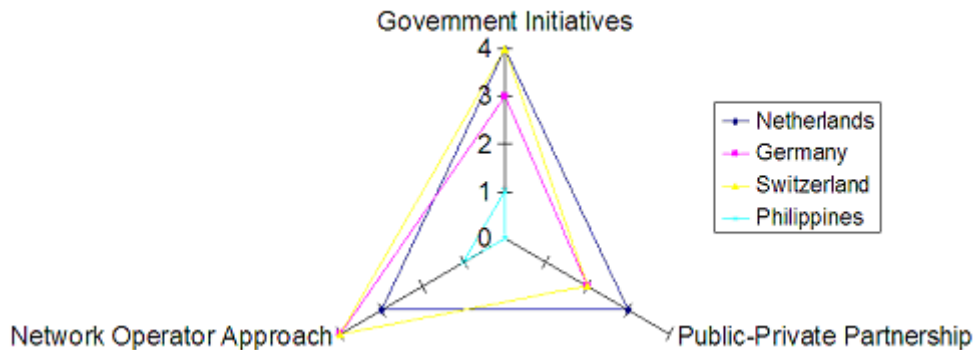


Figure 19: Benchmarking Matrix

The figure above shows the result of the sample international benchmarking exercise. The criteria were identified through the “good” practices of the model countries. In this exercise, countries are able to assess their performance in reference to others. Countries that lag behind know their failing points and, from such undertaking, can appropriately employ measures to areas that need mitigations. The structure/status of the implementing body should provide incentives for countries to participate. In the same manner, provided by the induced “pressure” from above, national governments employ benchmarking exercise to its network operators, using the general framework defined in the international level with specifics framed in the local level. Everything in the mechanism is voluntary. Only the perception of structural power and the incentives to improve and to achieve better global impression play the interworking force in the game. The illustration below shows the mechanism. Both countries and the network operators are benchmarked.

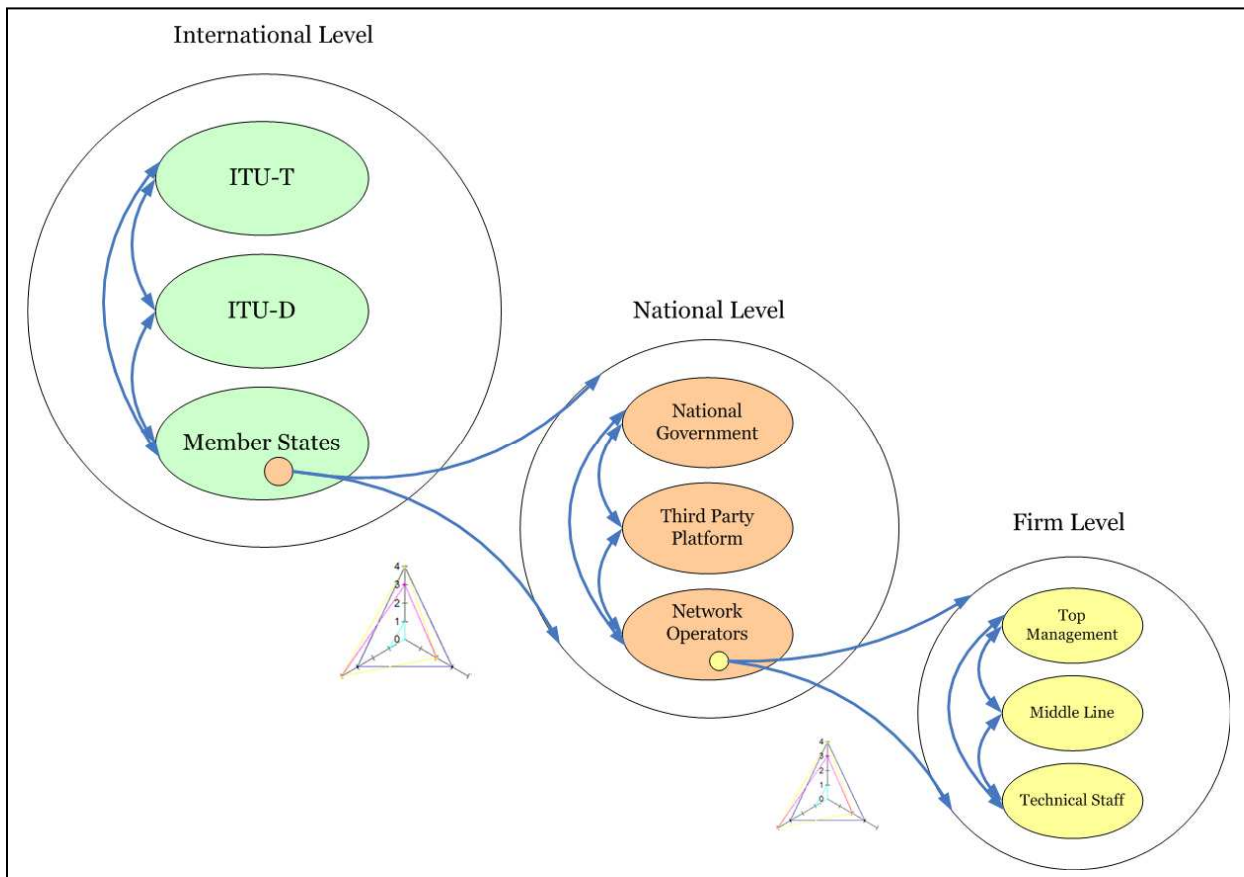


Figure 20: International Coordination Mechanism

In the international level, the standardization and development bureaus coordinate to one another to develop the policy baseline executed through the standardization process to achieve greater representation. The developed policy baseline is benchmarked to its member states. In the national level, governments appropriate their initiatives according to the stipulation of the policy baseline considering contextual setting. All stakeholders in the national level should be involved in contour fitting the general policy baseline unto its frame. In the network operator level, initiatives are conducted in reference to the provided policy baseline that is defined in international level and contour fitted in the national level. The regular benchmarking assessment, being known to all the players of the exercise, will provide an “induced” push for stakeholders to improve.

4.3 What are the present initiatives of the selected international organizations?

4.3.1 International Telecommunication Union

In harmonizing global initiatives for infrastructure assurance, international organizations are in the spotlight with essential role to play¹⁶⁵. International organizations are in the position to gather “good” practices across sectors and across national boundaries. The ITU, as the intergovernmental agency of UN in telecommunications has a membership mandate to build greater confidence to the usage of telecommunications infrastructure. The three bureaus of the organization (ITU-T, ITU-R and ITU-D)¹⁶⁶ have activities to address this mandate¹⁶⁷. At present, present initiatives are mostly in the protection of cyberspace¹⁶⁸. The assurance of mobile communications has not yet provided sufficient attention in this level¹⁶⁹. This study maneuvers from such an angle to push into international discussion the assurance of mobile telephony. More detailed discussion of the initiatives of ITU in the area of infrastructure assurance is provided in Appendix G. The ecosystem of infrastructure assurance with ITU as the facilitating organization is placed in Appendix The ITU has to strengthen its effort on infrastructure assurance for mobile telephony in the following areas:

- sharing information on national approaches;
- good practices and guidelines;
- technical standards and industry solutions;
- harmonizing national legal approaches and international legal coordination;

A number of technical and procedural standards have been developed by ITU-T for mobile telecommunications security. The full standards for mobile security are yet incomplete and some are still in the development process¹⁷⁰. Technical and procedural standards are in the responsibility of ITU-T. Policies and strategies to ensure the global infrastructure are the tasks of ITU-T. The case of infrastructure assurance is a hybrid of both responsibilities, thus, collaboration between them is essential. The figure below shows the standardization initiatives of ITU-T in telecommunications security. Initiatives of ITU-D and ITU-R are described in Appendix G. More detailed description is in the ITU website: <http://www.itu.int/net/home/index.aspx>

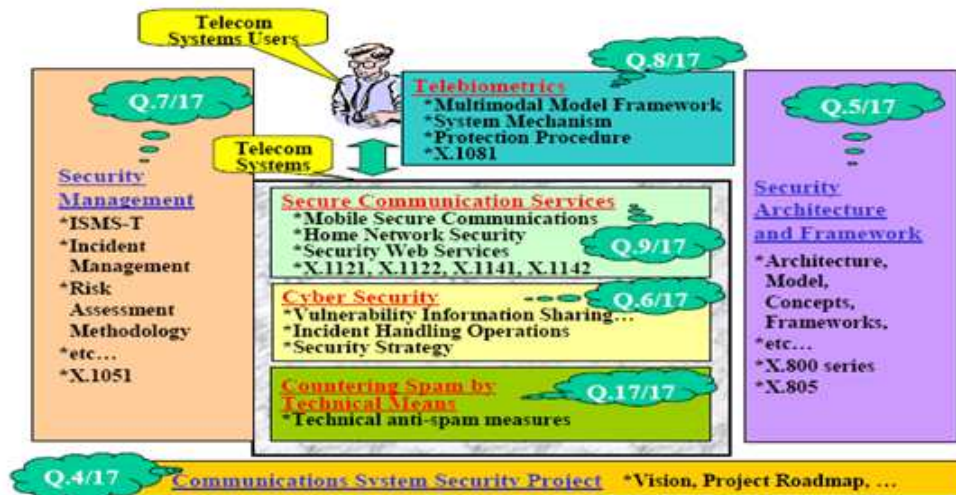


Figure 21: Study Group 17 Inquiries (Source: ITU)

¹⁶⁵ Interview with ITU03, held May 26, 2008

¹⁶⁶ ITU-R : Radiocommunication Bureau, ITU-T: Standardization Bureau, and ITU-D: Development Bureau

¹⁶⁷ Interview with ITU03, held May 26, 2008

¹⁶⁸ Interview with ITU04, held May 26, 2008

¹⁶⁹ Interview with ITU04, held May 26, 2008

¹⁷⁰ Interview with ITU04, held May 26, 2008

Table 45: SG 17 Inquiries

Study Group 17 ¹⁷¹ Inquiries and Description	
Inquiry	Description
Q. 9/17	Secure communications services
Q. 5/17	Security Architecture and Framework
Q. 7/17	Security Management
Q. 4/17	Communications System Security Project
Q. 6/17	Cybersecurity Project
Q. 17/17	Countering spam by technical means
Q. 8/17	Telebiometrics

The table shows the technical and procedural standards that have been developed. The table also strives to trace the assurance value that each of the standards can potentially provide.

Table 46: Standards presently available and the assurance value they provide

ITU Standardization Initiatives on Mobile Telecommunications Security		
Standards	Description	Assurance Value
X.1121	Framework of security technologies for mobile end-to-end communications	Security
X.1122	Guideline for implementing secure mobile systems based on PKI	Security
X.1051	Information security management system – Requirements for telecommunications (ISMS-T)	Security
X.805	Security architecture for systems providing end-to-end communications	Security
E.408	Incident organization and security incident handling: Guidelines for telecommunication organizations	Security, Reliability
E.409	Telecommunications Network Security Requirements	Security

From the discussion above about the initiatives of the ITU in infrastructure assurance, it can be said that both the important bureaus (ITU-T and ITU-D) have been instituting initiatives to improve the assurance condition of the global telecommunication infrastructure. Technical and procedural standards have been specified and development policies and strategies have been laid out. This study provides a mechanism to ensure the diffusion of these initiatives of the ITU into the intended local recipients. This study advocates that this is the niche of the policy baseline. Benchmarking a policy baseline, developed through standardization process, could ensure the diffusion of the needed initiatives.

¹⁷¹ Study Group 17 is tasked to perform standardization initiatives for telecommunications security.

4.3.2 GSM Association

GSM Association¹⁷² is an international organization formed by private network operators of mobile telephony themselves whose technology is based on GSM standards. It is the global trade association representing over 700 GSM mobile phone operators across more than 215 countries (Wikipedia, 2008). There are also more than 180 manufacturers and suppliers support the Association’s initiatives as key partners. Its aim is to ensure mobile phones and wireless services work globally and are easily accessible, enhancing creation of new business opportunities for operators and their suppliers (Wikipedia, 2008). By having said so, GSMA has, therefore, direct links to the concerns of private network operators¹⁷³. Industry wide, the issue of mobile telephony infrastructure assurance can be discussed and industrial solutions can be provided. Infrastructure assurance, though, is not just an industry-wide concern. GSMA serves the industry sector and should engage in a dialogue with other stakeholders such as national governments, and international organizations discussing solutions in providing greater assurance to mobile telephony¹⁷⁴. Involving the government in the issue demands a third party platform¹⁷⁵. Thus, GSMA can provide a greater push of the issue through elevating it to the third party platform. The stature of GSMA as an industry organization of the GSM operators can pave way to providing support for the greater deliberation of the issue. Its Public Policy Department for Fraud and Security is the main arm responsible for mobile telecommunications security. The initiatives, though, are industry-level oriented. In the issue of regulation to achieve infrastructure assurance for mobile telephony, if there is one to be made, the following are the important points the association would like to emphasize^{176 177}.

Table 47: GSMA Perspectives on Regulation

GSMA Insights on Mobile Telephony Regulation
<ul style="list-style-type: none"> ■ should seek a balance between the benefits and costs of intervention ■ should be based on clearly defined goals and policy objectives ■ should be kept to the minimum needed means to meet these objectives ■ should reflect the market situation and balance the micro and macro views ■ should encourage new investments in telecommunication infrastructures ■ facilitate competition within the sector

4.4 Policy Baseline and the International Organizations

The policy baseline can be developed in the ITU with the support of GSMA. Having the ITU as the “trusted” third party platform, both the government and market players on mobile telephony can sit together to discuss the issue in a trusted environment. If there is regulation to be made, GSMA stresses that it should be kept to the minimum resource to achieve it. With the support of GSMA, the issue can be provided a stronger push to the ITU. In such a manner, a bottom up approach is done from the level of the network operators forwarded to the third-party international platform by the global trade association.

Table 48: Policy Baseline and the International Organizations

GSMA (Private-Initiated Organization)	ITU (Intergovernmental Organization)
<ul style="list-style-type: none"> ■ Discuss policy baseline industry-wide ■ Push the issue to third party platform to accommodate other stakeholders such as the government and other non-members of GSMA 	<ul style="list-style-type: none"> ■ Discuss policy baseline with key players both from the government and industry ■ Perform standardization and benchmarking processes

¹⁷² <http://www.gsmworld.com/using/security/index.shtml>

¹⁷³ Interview with GSMA02, held June 03, 2008

¹⁷⁴ Interview with GSMA02, held June 03, 2008

¹⁷⁵ Interview with GSMA02, held June 03, 2008

¹⁷⁶ Interview with GSMA02, held June 03, 2008

¹⁷⁷ Interview with GSMA02, held June 03, 2008

4.5 What can be learned from experts?

An expert discussion was conducted in the months of May to June of 2008 in which selected stakeholders were asked about their perspectives on the various issues concerning infrastructure assurance for mobile telephony. The selected stakeholders were from international organizations, national government agencies, and network operators for the private sectors. Together with the results from open-ended questions, a survey on the perception of experts on the various issues surrounding infrastructure assurance was conducted. The table below presents the result of the perception test conducted. The rationale of choosing these stakeholders is presented in the Introduction and in Appendix A.

Inquiry	Subdivision	Remark
1. Criticality of Mobile Telephony	Present	Relatively High
	Future	Very High
2. Urgency of the Issue	Developing Countries	Very High
	Developed Countries	Average
3. Usability of the Policy Baseline	Strengths	Relatively High
	Weaknesses	Average
	Opportunities	High
	Threats	Average
4. Feasibility of the Policy Baseline	Desirability	Average
	Practicability	Average
5. Difficulty in Developing the Policy Baseline	Intergovernmental	Average
	Public-Private Partnership	Relatively Low
6. Scope of the Issue	National Government	High
	Inter-governmental	Average
7. Relevance of International Organization	---	Relatively High
8. Involvement of the Private Sector	Present	Relatively Low
	Desired	High
9. Extent of Information Sharing	Present	Low
	Desired	High
10. Efficacy of Regulation	---	Low

Table 49: Perception Test Results

The first column is the list of inquiries asked to the experts/stakeholders. These are the issues where experts' perspectives were obtained. The experts interviewed are representatives of organizations perceived to be stakeholders of the assurance of mobile telephony infrastructure. For international organizations, representatives from ITU and GSMA participated. For national governments, representatives from relevant national agencies in NL, DE, CH and PH shared a view. For network operators, representatives from Royal KPN, T-Mobile, NTTDoCoMo, and Globe Communication were interviewed. The second column shows the subdivisions of the main inquiry. This means that the main inquiry was further divided into partitions. The third column is the overall remark, as the perceptions of experts/stakeholders were tabulated. Average and standard deviation were derived. Corresponding remarks and its respective interpretation was provided in the appendix. Please refer to Appendix A4 for the details. The main expert respondents come from international, national and firm level frames. Invited experts from the academe also provided insights.

4.5.1 Discussion of the Perspectives of Selected Experts/Stakeholders

In discussing experts perspectives on the issues raised, the study groups the 10 inquiries into 5 aspects in which the inquiries are deemed relevant. These 5 aspects of the entire inquiry are: criticality of mobile telephony (in which inquiry 1 and 2 are relevant), relevance of the policy baseline (in which inquiry 3, 4 and 5 are relevant), private sector and information sharing (in which inquiry 8 and 9 are relevant) and efficacy of regulation (in which inquiry 10 is relevant). Specific experts/stakeholders will be quoted whenever their statements are seen appropriate to add validity in the discussion.

4.5.1.1 Criticality of Mobile Telephony

After consolidation of experts/stakeholders perspectives, it is construed that the criticality of mobile telephony is relatively high at present time and very high it will become in the future. Experts regard mobile telephony a critical infrastructure at present and will increase its criticality in the future as more and more end-user important transactions and applications are being done through the infrastructure¹⁷⁸. Internet has been gradually being integrated with the system, and more financial transactions (e.g. money transfer, etc) are done through the mobile phone¹⁷⁹. The mobile phone has been connected to another networks such as banking and finance, health organizations, police and emergency organizations, etc¹⁸⁰. The voice and data service that it provides are essential to the social and economic activities of the society¹⁸¹. There is a consensus that voice¹⁸² is more critical in developed countries and data¹⁸³ (e.g. SMS and MMS) are very critical in developing countries¹⁸⁴. There are a number of reasons provided for this: in developed countries, the functionality and mobility of mobile phone are highly regarded even there are other means of telecommunication available (e.g. fixed-line, internet, etc.). In developing countries, the issue revolves around price and alternatives¹⁸⁵. Universal access is yet a problem for fixed-line telephone and has been like that for ages. SMS is a lot cheaper (sometimes free of charge) as compared to other means of communications¹⁸⁶. The expert discussion then continues to show that, at present, the mobile telephony is more critical in developing countries than in the developed world. These again are due to price and alternatives. More than half (65%) of mobile telephony market is from the emerging countries¹⁸⁷. Thus, the issue of criticality is more urgent to respond in the developing world as compared to the developed¹⁸⁸. Due to its acceptable cost and unavailability of other means, more and more people are being connected, surpassing the number of those connected in the fixed line, and more accessorial applications are added. The number of user and the increasing number of transactions that can be done through the mobile phone are real proof¹⁸⁹ of the increasing importance of mobile telephony to the world.

Key Contribution: Mobile telephony will be more critical in the future than it is today. Interconnectivity with mobility will be the prime value of the future. The criticality of mobile telephony is greater felt in the developing countries than in developed countries. This is due to the limited alternative means of telecommunications, thus, its insecurity and unreliability can be of high impact to society. There have been important transactions (e.g. money transfer, internet, etc.) being done through mobile telephony aside from its essential functionality of voice and text.

¹⁷⁸ All experts/stakeholders interviewed verified this statement

¹⁷⁹ Interviewed ITU02, held May 23, 2008

¹⁸⁰ Interviewed ITU03, held May 26, 2008

¹⁸¹ Interviewed KPN 01, held July 02, 2008

¹⁸² Interviewed NL03, held June 02, 2008

¹⁸³ Interviewed PH02, held July 02, 2008

¹⁸⁴ Interviewed ITU 01&02, held May 23, 2008

¹⁸⁵ Interviewed with PH 01&04, held July 02, 2008

¹⁸⁶ Interviewed with PH 01&04, held July 02, 2008

¹⁸⁷ Interviewed with PH 01&04, held July 02, 2008

¹⁸⁸ Interviewed with ITU 01&02, held May 23, 2008

¹⁸⁹ Interviewed ITU03, held July 26, 2008

4.5.1.2 Relevance of the Policy Baseline

Most of the experts are skeptical of the value of the policy baseline if it would mean regulation. It will be difficult to implement the policy baseline because of the differing national mandates and perspectives on the subject matter¹⁹⁰. It is expressed that policy baseline should have the character of a recommendation or guidelines to appeal more to national government and network operators¹⁹¹. The policy baseline should imply that regulation is the least option¹⁹². From the perception test table above, there are high opportunities if a baseline is developed and its strength is relatively high as well. The reason provided were a baseline could provide framework of strategies and better elucidate the issue¹⁹³. It informs stakeholders about the issue and their respective roles to play¹⁹⁴. It encourages discussion and thus enlightens solutions¹⁹⁵. If the baseline is developed in international level, then it becomes an instrument for harmonization since it is based on various national arrangement “good” practices available in the world. This is a great aid for developing countries, who do not have the means and capacity to design their own strategy¹⁹⁶. This is a cheap cost of harmonizing initiatives and a good means in setting achievable goals¹⁹⁷. Policy baseline provides then a clear direction on how to assure infrastructure¹⁹⁸. Some experts are skeptical about the weaknesses and threats, which are both rated as average. Implementing the baseline in global scale for harmonization entails a tedious work to achieve. The coordination mechanism must be very efficient and incentives to conform must be appropriate¹⁹⁹. This is difficult because of the differing mandates in each of the countries. Some have assurance policies and programs but most of the others do not. The international platform must have an influential image that can encourage member countries to voluntarily participate²⁰⁰. In the same manner, the feasibility of the policy baseline is also rated average. The experts again expressed the concern about what comprises the policy baseline. If it consists of regulatory instruments, it becomes undesirable because most of the owners of the mobile telephony infrastructure are from the private sector and are risk averse to any form of regulations²⁰¹. They would rather solve the problems by themselves than being forced to invest money on programs with the government that they do not see a direct benefit. The practicability of a regulatory instrument can get a number of opposition, unless the contents of the baseline proved to be useful in assuring the infrastructure. The difficulty of creating a baseline can be easily done through public-private partnerships of the government and the industry²⁰². If the government solely does it for itself, it cannot get the support from the industry. If the industry players develop the baseline by themselves, they miss the facilitating power of the government and its capacity to legislate laws and create policies that are useful for all. Industry players have high strategic behavior and cooperation among one another²⁰³.

Key Contribution: The relevance of policy baseline received varied reviews. Most of them are skeptical about its practicality if it is about regulation. Most of them agreed too that the policy baseline is practical and useful if appropriately defined. It has the capacity to involve stakeholders into the effort of assuring the infrastructure. Some suggested that it should be voluntary like recommendations or guidelines but must provide a mechanism too that attracts the stakeholders to comply. International organizations should exploit its strength and opportunities.

¹⁹⁰ Interviewed with ITU 02,03&04, held May 23&26, 2008

¹⁹¹ Interviewed with ITU 02&04, held May 23&26, 2008

¹⁹² Interviewed with NL 01&02, held June 02, 2008

¹⁹³ Interviewed with NL 02,ITU 02&03, held June 02, 2008&May 23&26 respectively

¹⁹⁴ Interviewed with DE03, held June 02, 2008

¹⁹⁵ Interviewed with DE03, held June 02, 2008

¹⁹⁶ Interviewed with ITU04, held May 26, 2008

¹⁹⁷ Interviewed with DE02, held June 02, 2008

¹⁹⁸ Interviewed with CH02, held June 03, 2008

¹⁹⁹ Interviewed with NL 03, held June 02, 2008

²⁰⁰ Interviewed with NL 03, held June 02, 2008

²⁰¹ Interviewed with NL 03, held June 02, 2008

²⁰² Interviewed with CH01, held May 28, 2008

²⁰³ Interviewed with DE02, held June 02, 2008

4.5.1.3 Scope of the Issue

The scope of the issue is national, as the perception test table proves. International coordination is recommendable but the approach should be national²⁰⁴. Infrastructure assurance is highly bounded by specific national mandates²⁰⁵. Although there are some international regulations, especially for telecommunications, the national jurisdiction has greater dominance over the infrastructure. This, then, again shows that an international regulation for infrastructure assurance could find its way towards implementation difficult²⁰⁶. It appears that, although, international coordination is highly favorable but doing it through regulation will prove its worth the opposite²⁰⁷. The mechanism should be, thus, voluntary but reflects the real need of the sector and provides a means for the participation of both the industry and the government²⁰⁸. The relevance of an international organization rated relatively high. The experts acknowledged the importance of the international organization of the sector²⁰⁹. For mobile telephony, they could be the ITU, a UN intergovernmental agency, or the GSMA, the private association of GSM network operators²¹⁰. It could be that the GSMA could provide the greatest support for the issue to be raised unto the ITU level²¹¹. But GSMA is firstly directed by its private sector membership. Thus, the need should come from the private industry players and bring up to higher level of bodies that have better to tackle the solution in a more encompassing context²¹². The ITU has a mandate to build confidence in the use of telecommunications and information infrastructure, thus, it is useful if the initiatives take strength from this direction²¹³.

Key Contribution: Infrastructure assurance is a national issue with international weight. Mobile telephony is within national jurisdiction. It has acquired permit to operate through a national body. Initiatives for infrastructure assurance, thus, should be nationally grounded. It is the stakeholders within a national scope have the greatest role to play. International organizations, such as ITU or GSMA, do not have the mandate to intrude national policies. Their role is more on external advising or they can provide non-binding mechanism to encourage or assist national governments as they build their own national capacity for infrastructure assurance.

4.5.1.4 Private Sector and Information Sharing

There is a consensus from the interviewed experts/stakeholders that the way to ensure infrastructure assurance is through private-public participation (PPP). If the government does more the initiatives and the industry is lagging behind (and vice versa), the effort is imbalance²¹⁴. The industry players mostly own the infrastructures and, technically, are the experts in assuring the infrastructure²¹⁵. The government on the other hand has the formal function to legislate policies needed for infrastructure assurance²¹⁶. It has the facilitating role to bring in all stakeholders together²¹⁷. Both have stakes to the security and reliability of the infrastructure and their respective functions are needed to ensure assurance. The table above shows that the extent of information sharing at present is low. It means that PPP in assuring the infrastructure is yet a novel initiative. This is especially more of the picture in developing countries where PPP is deterred by fragmentation²¹⁸. The three model countries have shown significant initiatives in making infrastructure assurance a PPP. These countries strongly believed that the extent of the

²⁰⁴ Interviewed with CH02, held June 03, 2008

²⁰⁵ Interviewed with DE01, held June 02, 2008

²⁰⁶ Interviewed with ITU02, held May 23, 2008

²⁰⁷ Interviewed with ITU02, held May 23, 2008

²⁰⁸ Interviewed with ITU04, held May 26, 2008

²⁰⁹ Interviewed with ITU04, held May 26, 2008

²¹⁰ Interviewed with ITU02, held May 23, 2008

²¹¹ Interviewed with ITU02, held May 23, 2008

²¹² Interviewed with ITU01&02, held May 23, 2008

²¹³ Interviewed with ITU02, held May 23, 2008

²¹⁴ Interviewed with ITU02, held May 23, 2008

²¹⁵ Interviewed with CH01, held May 28, 2008

²¹⁶ Interviewed with CH02, held May 28, 2008

²¹⁷ Interviewed with NL01, held June 02, 2008

²¹⁸ Interviewed with PH01, held July 03, 2008

desired PPP should be high enough to confidently share information and discuss mitigations in a trusted environment. PPP demands a trusted atmosphere that can only occur when stakeholders trust one another or there are encompassing provisions that mandate the creation of a trusted platform where the issue can be tackled.

Key Contribution: Infrastructure assurance is a public-private partnership. Both the government and the private sector have high stakes to the security and reliability of mobile telephony. A trusted environment has to be created so that this kind of partnership will occur. This trusted environment is needed in order for stakeholders to freely and voluntarily share information and solution without the risk of being liable to the vulnerabilities of their infrastructure.

4.5.1.5 Efficacy of Regulation

The table above shows that regulation, as an instrument for implementing infrastructure assurance, is the least desired solution to the problem. Majority of the experts/stakeholders interviewed expressed that regulation is not appealing to network operators due to the added burden it brings as operators seeking for greater efficiency in resource as they compete in the market. There is no reason to “bring back the genie to the bottle”²¹⁹ after liberalization/privatization. With too much regulation, why liberalize in the first place?²²⁰ GSMA has strong appeal that regulation should be the last solution. Strive to seek first for other means to ensure the infrastructure without coercive actions through regulations. Forced implementation can detract industry players to think what is best for them²²¹. Regulation can damage the capacity of network operators to think of solution by themselves on how they can assure their infrastructure. The mechanism advocated is thus voluntary. It should also have the economic-incentives in order for market players to participate

Key Contribution: Regulation should be the last resort for infrastructure assurance. Too much regulation is seen to be inappropriate for a liberalized and privatized environment. The mechanism advocated is voluntary with some economic incentives that drive market stakeholders to participate.

4.6 Insights Identified from Selected Stakeholders’ Perspectives

The table below summarizes the various insights derived from the experts interviewed.

Table 50: Insights from Experts/Stakeholders Interviewed

Aspects of the Inquiry	Insights Identified
Criticality of mobile telephony	Mobile telephony is a critical infrastructure that demands initiatives from its stakeholders for infrastructure assurance.
Relevance of the policy baseline	Exploit the strength and opportunities of developing a policy baseline. Mitigate its weakness and threats. It is an essential tool to coordinate infrastructure assurance initiatives.
Scope of the issue	Infrastructure assurance is a national issue with international weight.
Private sector and information sharing	Public-private partnership is the only way to move forward for infrastructure assurance.
Efficacy of regulation	Regulation should be the last resort. Appropriate mechanism is seen to be voluntary and economic-incentive driven.

²¹⁹ Expression that there is no need to regulate too much after the decision to liberalize/privatize

²²⁰ Interviewed with ITU02, held May 23, 2008

²²¹ Interviewed with ITU02, held May 23, 2008

4.7 The Design of the Policy Baseline

Allow this part to integrate the various lessons identified from all the research methods conducted. This integration will be the focal ground in identifying the essential contents of the preliminary policy baseline and the provisions for its further development and implementation. This integration is shown through the table below.

Table 51: Integration of Insights Derived from Results

Integration of the Insights Derived from the Various Research Methods			
Theoretical Concepts	Comparative Analysis of national arrangements	International Organization Initiatives	Experts Perspectives
<p>Infrastructure assurance in a global setting demands harmonization of initiatives. Harmonization, as the study advocates, can be achieved through standardization and benchmarking processes. Standardization <u>collaborates</u> with stakeholders to gain support, while benchmarking <u>coordinates</u> with stakeholders with an incentive to improve (adjust) performance.</p>	<p>There is a need to create a <u>coherent</u> national strategy that employs a comprehensive approach. The policy lessons identified are: risk-based, all hazards, PPP, multi-sector and international coordination. Coherence of national strategy demands <u>coordination</u> with relevant stakeholders. A <u>PPP</u> approach implies an undertaking of all.</p>	<p>There is a need for international <u>collaboration</u>. The industry players, though its focal organization, has to bring the issue to the international level for better deliberation. The mechanism needed for assuring mobile telephony is international, thus, relevant international organizations should <u>coordinate</u> to one another to initiate undertakings needed for infrastructure assurance.</p>	<p>Mobile telephony, in the global setting, is a critical infrastructure that demands assurance from its stakeholders. It has a national jurisdiction with international weight. Thus, national and international bodies should <u>coordinate</u> to one another for assurance initiatives. Regulation is no way to go. The mechanism to be employed should be <u>voluntary and economic-incentive driven</u>.</p>
<p><u>General Insight:</u></p> <p>Infrastructure Assurance for mobile telephony, in the global setting, demands <u>collaboration</u> of stakeholders and <u>coordination</u> of initiatives. The creation of national strategy should also be based on the value of collaboration and coordination. Risk-based approach, PPP, multi-sector, all hazards and international coordination are all policy lessons demanding coordination and collaboration. Harmonization, through standardization and benchmarking, implies the need of collaborative and coordinated undertaking. The voluntary and economic-incentive driven mechanism also requires coordination and collaboration between institutions. Collaboration and coordination can only be achieved through trusted <u>communication</u> among stakeholders.</p>			
<p><u>Policy Baseline Deduced:</u></p> <p>As construed from the analysis above, trusted communication among stakeholders is the basic requirement to induce collaboration and coordination. It is then the minimum required policy in order to get stakeholders together in the unified effort to assure mobile telephony in the global setting. Communication, as the minimum necessary policy, is indispensable to bring stakeholders to one coordinated and collaborated action to ensure the infrastructure in a fragmented environment. <u>Communication is the policy baseline deduced out from this study.</u></p>			

From the analysis provided above, the rest of this section will be spent in detailing this policy baseline. It strives to place in more vivid illustrations how this policy baseline will be defined in more details. Policy lessons from the various research methods conducted will be carried over in this discussion to provide more concrete definition of the policy baseline. This is reiterated below.

- Harmonization done through standardization and benchmarking
- Coherent national strategy that emphasizes public-private partnership, risk-based analysis and management, multi-sector perspectives, all hazards and international coordination

The figure below shows that full assurance is a comprehensive undertaking. It is achieved through conscious intervention of actions that stem from the contributions of stakeholders. The figure illustrates through blocks the full achievement of assurance. Each block depends and is built on one another to create the comprehensive “wall”²²² that assures the infrastructure. Each of the block contributes to various assurance values needed for continued security and reliability of the infrastructure. Block 1 defines personal value of trust and confidence, which is a basic necessity for infrastructure assurance. Developed countries might already have achieved this block, while developing countries are yet on the process to create one. Block 2 specifies technical and organizational measures that can appropriately afforded by the private sector (in this case, the network operators). The effectiveness of the measures of Block 2 largely depends upon the substantive fulfillment of block 1. Block 3 dictates the need for institutional cooperation. Developed countries might already have this kind of cooperation, while in developing this is yet uncommon. The effectiveness of block 3 to assure the infrastructure has so much reliance on the fulfillment of the previous blocks. Block 4 puts forward the need for a national strategy and international coordination. The national government has the pivotal role to play to create this block. The effectiveness of this block to assure the infrastructure is highly dependent on the fulfillment of the previous blocks. From the illustration, it is deduced that comprehensive assurance is the undertaking of all stakeholders. The full provision of assurance values relies on the conscious intervention of each of the stakeholders to build the “wall” that assures the infrastructure. Definitions of the assurance value are provided by the table that follows.

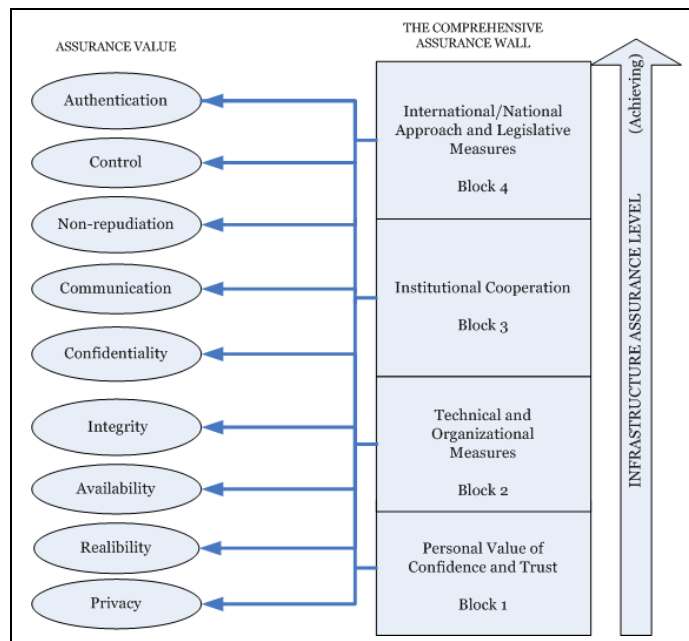


Figure 22: Infrastructure Assurance Level

²²² Used as a symbol for measures that assure the infrastructure

These terms are commonly used in technical context. In this study, the meaning of these terms extends beyond their technical definitions. They are modified to fit in the context of policy discussion.

Table 52: Definition of Assurance Values (Adapted ITU, 2003)

Assurance Value	Definition
Authentication	Confirms identity.
Control	Protects against unauthorized use of resources.
Non-Repudiation	Prevents an individual or entity from denial of having performed a particular action.
Communication	Ensures that information flows only between the authorized end points.
Confidentiality	Protects data from unauthorized disclosure.
Integrity	Ensures the correctness or accuracy of data.
Availability	Ensures that there is no denial of authorized access to network elements, stored information, information flows, services and applications due to events impacting the network.
Reliability	Ensures continuity of service amidst attack or failures.
Privacy	Provides for the protection of information that might be derived from the observation of network activities.

Infrastructure Assurance is the set of planned and systematic actions necessary to provide confidence that the infrastructure is secure and reliable (Moteff & Parfomak, 2004). This is expounded by the below.

Table 53: Infrastructure Assurance Defined

Assurance Value	
1. Security	Defined by authentication, control, communication, non-repudiation, confidentiality, availability and privacy
2. Reliability	

As said, infrastructure assurance is an issue of national jurisdiction. But because the infrastructure involved (mobile telephony) is a network of networks that anchors international scope, the issue, therefore, has international weight in it. The emphasis is national because the actual implementers of assurance initiatives are national bound—the government and the private sector (in this study, the network operators). International organizations do not have the capacity to intrude national mandates. Their role is essential in initiating mechanisms that assist governments to build national capacity but not in the actual implementation of the assurance measures within the national boundary. As has been advocated, the approach is national with the advisory and assistance of international bodies.

The figure below casts responsibilities to the stakeholders of the infrastructure. It shows that the policy baseline, which is communication, is the one that links institutions. Communication is the one that bonds institutions leading to collaborative and coordinated undertaking to assure the infrastructure. The figure shows the responsibility assigned to the government, the private sector and the partnership that is built between them. Communication is the first level step to start the

process of assurance. But such can be a challenge for very fragmented society. As shown by the figure below, network operators can assure the infrastructure through employing Information Security Management System (ISMS)²²³ that ensures assurance value of information assets. Mobile telephony, as an information infrastructure by itself highly dependent on various information processes, is seen to have a need to conduct ISMS requiring a systematic approach to managing sensitive information. Aside from assuring the information, network operators can increase its capacity to recover and restore operation during disruption incidents through Business Continuity Planning and Management (BCPM)²²⁴. Incidents could include local incidents like building fires, regional incidents like earthquakes, or national incidents like pandemic illnesses²²⁵. With BCPM, assurance extends to other assets of the organization aside from information. There are standardized procedures on how to perform ISMS and BCPM provided by a number of formal standardization bodies such as ISE/IEC, ITU-T and BSI. ISO/IEC 27001 incorporates the “Plan-Do-Check-Act” approach for continuous appraisal. The best-known ISMS is described in ISO/IEC 27001 and ISO/IEC 27002. The ITU-T Recommendation X.1051 specifies the requirements for establishing, implementing, operating, monitoring, maintaining and improving a documented ISMS. BS 25599 provides guidelines for BCPM. ITU-T Recommendation E.409 provides guidelines for telecommunications organizations to analyze, structure and suggest a method for establishing an incident management organization. Aside from these technical and procedural measures, network operator is needed to build partnership with the government and other stakeholders. The government is seen to have the need to create a coherent national strategy for infrastructure assurance that emphasizes public-private partnership, risk-based management and international coordination. Passing of appropriate legislations is part of its scope, together with incident capacity handling and awareness raising. Part of the responsibility of the government also is to provide mechanism that assesses assurance performance of network operators. The public-private partnership that is formed by the government and private sector can provide opportunity to perform risk analysis that demands participation of stakeholders from both the government and the private sector. This risk analysis is based on threat information, vulnerability assessment, asset identification, and dependency analysis. As illustrated below, communication is the one that links institutions to one another to perform a collaborative undertaking in assuring the infrastructure.

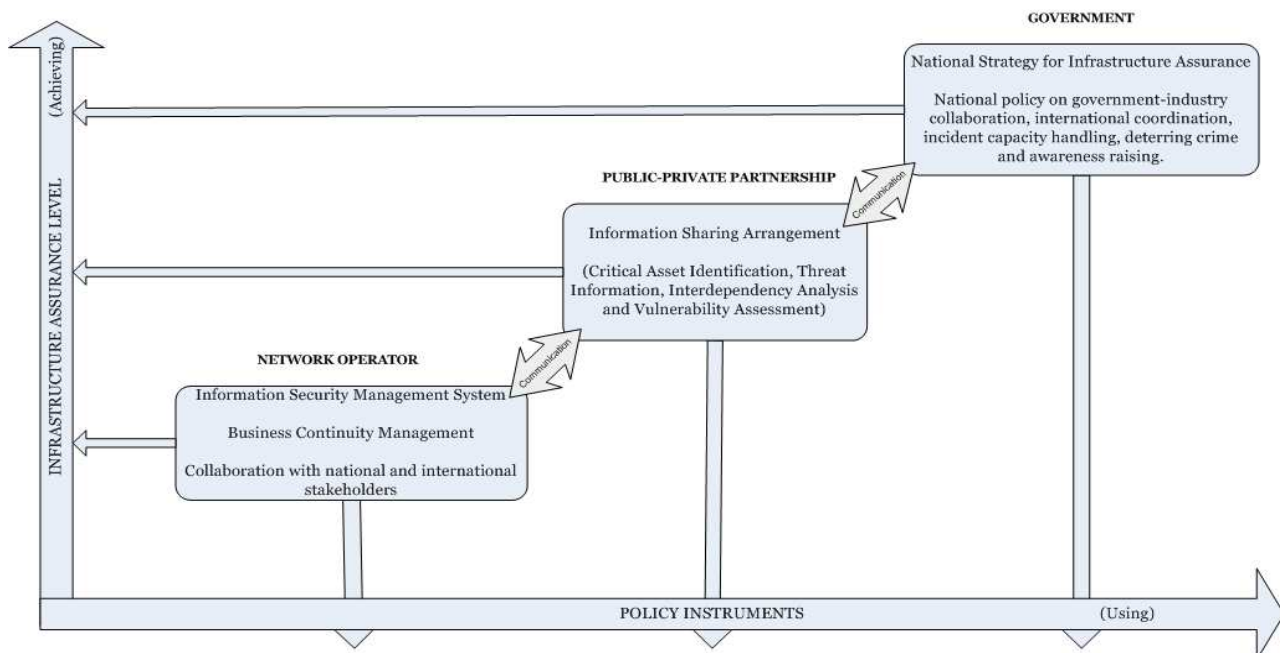


Figure 23: Casting Roles for Stakeholders

²²³ <http://www.bsi-emea.com/InformationSecurity/index.xalter>

²²⁴ <http://www.thebci.org/standards.htm>

The figure below shows in more detail how those measures provided above can be implemented. The arrows designate the importance of communication that links stakeholders to one another. The figure emphasizes the role of international organization in coordinating initiatives and developing recommendations to assure infrastructure. For the network operator, various ITU standards (technical and procedural) for mobile telephony assurance are shown. The cyclic arrows signify that the measures suggested (ISMS, CBMP and PPP) are processes demanding regular assessment and updates. The public-private partnership emphasizes the importance of conducting risk analysis in collaborative manner with the necessary threats, vulnerability and dependency information. All the arrows direct to risk analysis for they are the elements that define the process. Each of the information needed can be acquired from the participation of relevant stakeholders. In the same manner with the government, all arrows direct to the creation of national strategy for they are the elements needed to define the initiative.

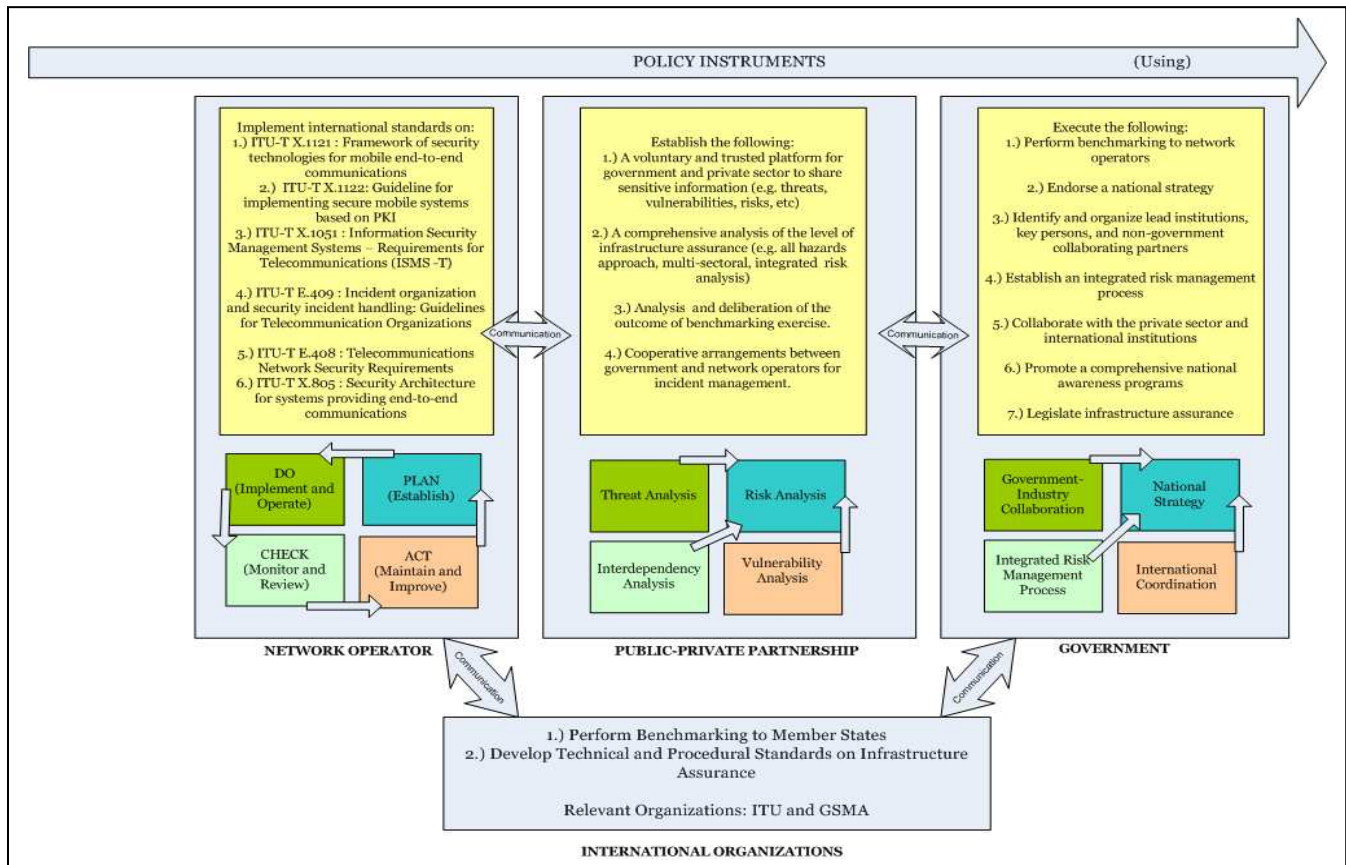


Figure 24: Recommended Policy Instruments for Each of the Stakeholder

Through the lessons derived from the theories, model national arrangements, initiatives of international organizations and expert interviews, the following conditions and constraints are important to be taken a serious consideration. The full preliminary policy baseline is shown as follows.

- Not a regulatory instrument. Or at least never start with regulation.
- A coherent national approach, but with an international perspective
- Public-Private Partnership is the only means to move forward, thus, information sharing is essential. In this case, the establishment of a trusted environment is an immediate need. A trusted third party might be needed.
- Involve the private sector in the development of the policy baseline. Get the market players involved in the process as early as possible.
- The mechanism for coordination should be economic-driven to correspond to the incentives entrenched in the present setup of the infrastructure.
- The approach to assurance is comprehensive: all hazards, risks-based, multi-sector, multi-levels and multi-stakeholders. International coordination, issue awareness and institutional collaboration should be part of the strategy.

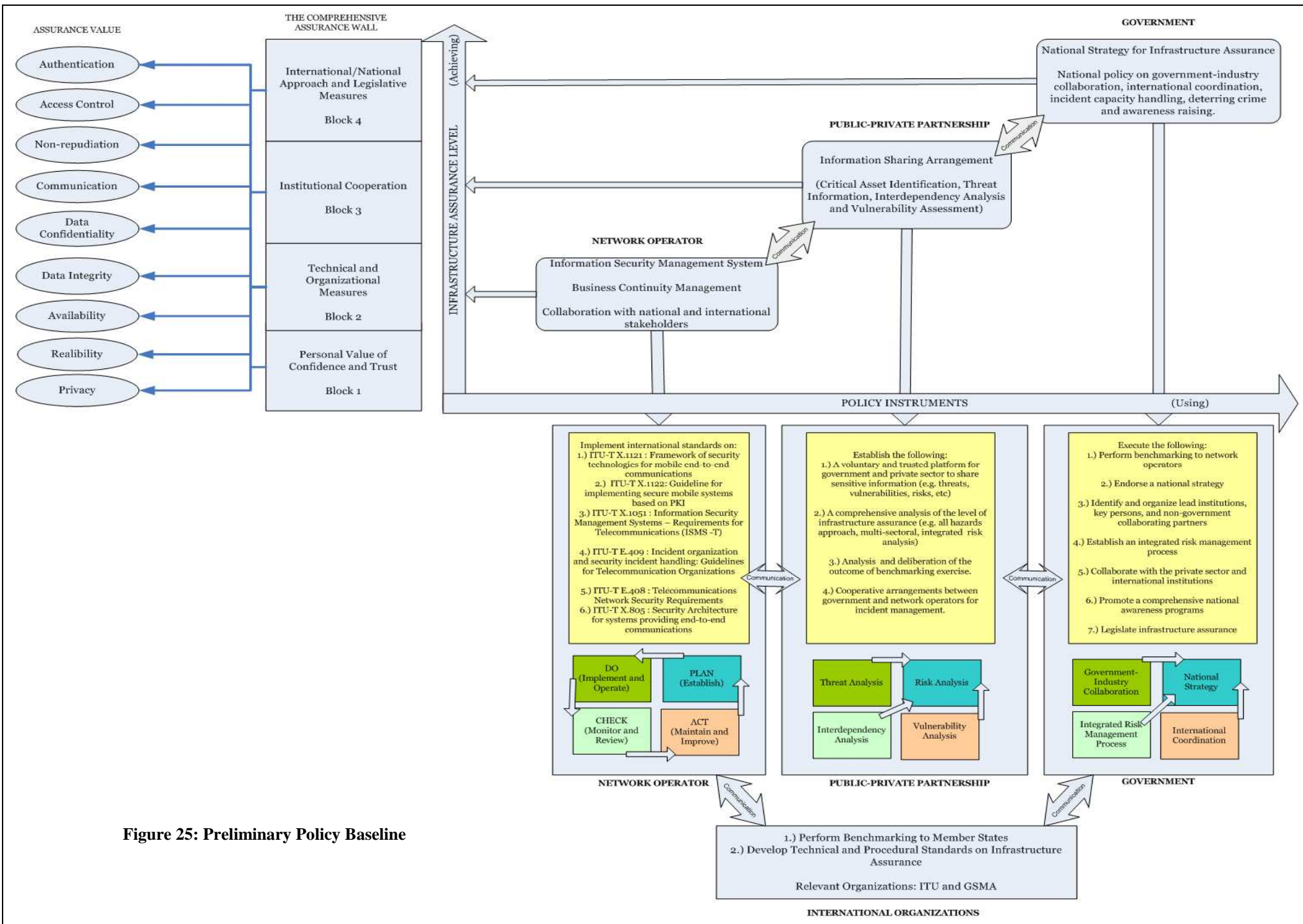


Figure 25: Preliminary Policy Baseline

4.8 Key Messages of Chapter 4

- Infrastructure assurance in a global setting demands harmonization of initiatives. Harmonization can be achieved through standardization and benchmarking processes.
- Standardization collaborates with stakeholders to gain support, while benchmarking coordinates with stakeholders with an incentive to improve (adjust) performance.
- There is a need to create a coherent national strategy that employs a comprehensive approach. The policy lessons identified are: risk-based, all hazards, PPP, multi-sector, and international coordination. Coherence of national strategy demands coordination with relevant stakeholders. A PPP approach implies an undertaking of all.
- There is a need for international collaboration. The industry players, though its focal organization, has to bring the issue to the international level for better deliberation. The mechanism needed for assuring mobile telephony is international, thus, relevant international organizations should coordinate to one another to initiate undertakings needed for infrastructure assurance.
- Mobile telephony, in the global setting, is a critical infrastructure that demands assurance from its stakeholders. It has a national jurisdiction with international weight. Thus, national and international bodies should coordinate to one another for assurance initiatives. Regulation is no way to go. The mechanism to be employed needs to be voluntary and economic-incentive driven.
- Infrastructure Assurance for mobile telephony, in the global setting, demands collaboration of stakeholders and coordination of initiatives. Collaboration and coordination can only be achieved through trusted communication among stakeholders.
- Trusted communication among stakeholders is the basic requirement to induce collaboration and coordination. It is then the minimum required general policy in order to get stakeholders together in the unified effort to assure mobile telephony in the global setting.
- Communication, as the minimum necessary policy, is indispensable to bring stakeholders to one coordinated and collaborated action to ensure the infrastructure in a fragmented environment. Communication is the general policy baseline deduced out from this study.
- The conditions and constraints dictate that regulation has to be last resort instrument to ensure assurance. Too much regulation can harm the innovative capacity of the infrastructure. At least never start with regulation.
- The issue of infrastructure assurance for mobile telephony is national in jurisdiction but has inbuilt international weight. The mechanism for coordination should be economic-driven to correspond to the incentives entrenched in the present setup of the infrastructure.
- Public-Private Partnership is the only means to move forward, thus, information sharing is essential. In this case, the establishment of a trusted environment is an immediate need. A trusted third party might be needed. Involve the private sector in the development of the policy baseline. Get the market players involved in the process as early as possible.

5

Evaluation of the Proposed Policy Baseline

The extent of efficacy of the preliminary policy baseline that was developed in the previous chapter will now be evaluated. For this study, this is done through two analyses (done ex-ante), namely: SWOT analysis and Policy Transplantation Assessment. SWOT Analysis is a strategic planning method that identifies the internal and external factors that are favorable and unfavorable to achieving the policy goals. The Policy Transplantation Assessment, on the other hand, evaluates the suitability (and practicability) of the policy baseline as it is framed to local utilities. In this case, the policy transplantation part is done with the Philippines arrangements as the example setting. It is one of the developing countries where mobile telephony is found vital and critical in the society.

5.1 Aim of the Chapter

The chapter, as a whole, strives to answer the following sub-research question:

“Based on the two evaluative (ex-ante) analyses conducted, what hints can be provided on the effectiveness and suitability of the policy scheme proposed to ensure the assurance of mobile telephony?”

SWOT Analysis is discussed first, then followed by the Policy Transplantation Assessment.

5.2 SWOT Analysis

SWOT Analysis is a useful technique in analyzing the Strengths, Weaknesses, Opportunities and Threats. Although it is used primarily for business and marketing, its application in policy issues also gives a broad overview of the “effectiveness” of a policy. This is shown by the table below.

Strengths <ul style="list-style-type: none">■ A coordinated mechanism to ensure infrastructure assurance■ Indispensable for national capacity building■ Clear delineation of actors and responsibilities■ Means of assessing assurance performance■ Groundwork for discussion	Weaknesses <ul style="list-style-type: none">■ Long-term impact is not immediately visible■ Political and commercial sensitivity of the issue■ Reluctance to share security information■ Technology is innately vulnerable■ Long standardization process time
Opportunities <ul style="list-style-type: none">■ Shared policy learning■ More potential user applications■ Institutional coordination and cohesion■ Sector-wide discussion of what to be safeguarded■ National Awareness	Threats <ul style="list-style-type: none">■ Incompliance■ Distrust to the proposed policy baseline■ Be used as the ceiling requirement instead of being the baseline■ Unsuitability to the country■ Weak synergy from international organizations

5.2.1 Strengths of the Proposed Policy Baseline

5.2.1.1 A coordinated mechanism to ensure infrastructure assurance

The proposed scheme provides a means to keep track of the infrastructure assurance initiatives of government and network operators around the world. Such leads to policy learning and ensures that “good” practices are the ones being deployed. A coordinated effort to assure the infrastructure utilizing the available “good” practices improves the security and reliability of infrastructure.

5.2.1.2 Indispensable for national capacity building

A defined set of “good” practices available for countries can be found useful in building national capacity to assure the infrastructure. There are many countries, especially the developing countries, do not have the full access of “good” practices information, thus, the policy baseline created can guide them in drafting their national strategy for infrastructure assurance.

5.2.1.3 Clear delineation of actors and responsibilities

Identification of actors and responsibilities is a crucial step in the assurance of the infrastructure. There are many countries cannot create a national strategy because who will be involved and what are to be done are unknown. The policy baseline raises awareness of actors’ responsibilities. It elucidates the ambiguous process of casting roles on how to assure the infrastructure. The policy baseline imposes a sense of validity since it is based on “good” practices available.

5.2.1.4 Means of assessing assurance performance

The proposed policy scheme allows stakeholders (both government and network operators) to measure their assurance performance in reference to the policy baseline created from the “good” practices of others. Through such scheme, the “sense of assurance” is quantified and the issue can, thus, be better delineated. Stakeholders are able to possess a concrete grip of their assurance position because they are able to assess their situation in reference to the model policy baseline.

5.2.1.5 Groundwork for discussion

The proposed policy scheme paves way towards deliberation of the politically and economically sensitive issue of infrastructure assurance. It can serve as a basal document geared to spark policy discussion on the issue. Discussions on this issue can further delineate the problem and elucidate the needed solution.

5.2.2 Weaknesses of the Proposed Policy Baseline

5.2.2.1 Long-term impact is not immediately visible

As said, infrastructure assurance is a gradual process of learning and re-learning. The perception of end-users of a secured and reliable infrastructure cannot be immediately attained by one assurance undertaking. It is a series of comprehensive endeavor requiring participation of all stakeholders concerned. Not being able to see immediate results could detract stakeholders from involving in the process of assuring since the undertaking does not immediately provide them immediate benefit. This can be a weakness because it can slow down the deployment of the policy baseline due to possible opposition.

5.2.2.2 Political and commercial sensitivity of the issue

Due to the contentiousness of this case, there is much difficulty to retrieve data and information about threats and vulnerabilities. This is the reason why a trusted environment is needed to be established to facilitate free and voluntary flow of needed information; thus, a more trusted analysis is performed. This weakness of the issue itself can lead to aversion from tackling the issue since the needed data for analysis are not directly available. Stakeholders also are more inclined to not discussing the issue since this can cause possible exposition of their sensitive vulnerability information, which can be the source of possible liability risk that can undermine the reputation of their network. This is a weakness because its sensitivity can hinder the further deliberation of the issue.

5.2.2.3 Reluctance to share security information

This related to the premise provided above. But this weakness derives its angle from stakeholders' perspectives. The above-mentioned weakness is inherent to the issue itself. Stakeholders are reluctant to share their information because of the various risk factors that they fear can jeopardize their position. This area can also be a source of strategic behavior to not unveil or to not fully unveil their assurance situation. Having known the assurance situation of others allows them to create strategy in expense of the others. Thus, most stakeholders at present prefer not to share their assurance situation. This can also be attributed to the lack of anti-liability law for infrastructure assurance. Reluctance is a weakness because it hinders the further deliberation of the issue.

5.2.2.4 Technology is innately vulnerable

Technologies are innately vulnerable. There are always means and ways to jeopardize technology if pursued. There are always vulnerabilities and threats that can imperil the assurance situation of the infrastructure. A 100% security and reliability is a utopia. The advocacy of the study is to reduce vulnerabilities and be aware of the surrounding threats. This innate vulnerability of technology is a weakness because it can be used as argument to rather not employing initiatives because of the reason that vulnerabilities will always exist.

5.2.2.5 Long standardization process time

Due to its principle of consensus and democracy, the standardization process has been having the reputation of being slow and frigid. It is possible that what is deliberated in the standardization process is not already occurring in the actual situation. Technology is dynamic and evolves over time. This long process time can be a weakness because stakeholders might prefer to institute initiatives by themselves (and stayed uncoordinated) without engaging to the process of standardization that takes in points of others through deliberation and consensus but requires a long time to arrive to the outcome.

5.2.3 Opportunities of the Proposed Policy Baseline

5.2.3.1 Shared policy learning

The proposed policy scheme encourages sharing of “good” practices information. In the process of collaborating and coordinating, stakeholders are able to reflect on their own assurance situation and learn from the initiatives of others. This is an opportunity because sharing of policy learning based on “good” practices improve situation. Stakeholders who are ambiguous of what policy initiative to institute can learn and adjust actions in response to the “good” practices available.

5.2.3.2 More potential user applications

As the infrastructure becomes more assured, more and more applications will be added to its utility, thus, becomes more useful to the people. As the mobile phones are better protected, more people will use the infrastructure, which paves way to greater welfare of the whole society.

5.2.3.3 Institutional coordination and cohesion

A policy baseline that emphasizes on public-private partnership, greater cohesion among institutions involved is inclined to occur. When institutions collaborate to one another, the benefits of the impact are wide-ranging. This is especially useful for developing countries where institutions are hugely fragmented from one another. Collaboration among institutions in developing countries is yet an uncommon thought. By having the policy baseline as the point of connection for interaction, trust and confidence will thrive and cooperation is not far to occur.

5.2.3.5 Sector wide discussion of what to be safeguarded

The policy baseline encourages sector wide discussion of the issue. It serves as a working document to start the deliberation. It should be noted that the discussion has to extend beyond the boundary of the sectors looking at how mobile telephony is connected (dependent) with other infrastructures. Through this exercise, the sector will be able to know the points and junctions to be safeguarded. In such a manner, it elicits information sharing leading to learning and adjustment.

5.2.3.6 National Awareness

Since the policy baseline is a multi-stakeholder undertaking, information sharing occurs among players. In such a manner, awareness to the issue is afforded to stakeholders concerned. If the policy baseline involves all relevant stakeholders, a national awareness can be achieved.

5.2.4 Threats of the Proposed Policy Baseline

5.2.4.1 Incompliance

Advocating voluntariness in the process also poses the risk of incompliance. Stakeholders might not find the whole process appealing, or would not find the benefit of participating. Voluntariness should include in it the appropriate incentives so that stakeholders would have the drive to get on board. Nevertheless, due to differing interests, one cannot always assume full conformity to the policy scheme proposed.

5.2.4.2 Distrust to the proposed policy baseline

Skepticism to the validity and representativeness of the policy baseline is not far to occur. It possesses threat due to the long delay it can give to the process caused by skeptical oppositions. These stakeholders do not have confidence on the manner the policy baseline was deliberated and implemented. The need and the manner of development and implementation are questioned.

5.2.4.3 Used as the ceiling requirement instead of being the baseline

Having the policy baseline be viewed as the maximum requirement can become a threat to the establishment of the desired infrastructure assurance. This is because the policy baseline only stipulates the baseline requirement needed to be instituted. Conformance to just the baseline detracts innovativeness in ensuring assurance. As mentioned, threats and vulnerabilities are

dynamic in mobile telephony, thus, a constant review and analysis to the process have to be done. There are more creative initiatives that can be done than just conforming to the baseline. The policy baseline just provides the general framework, or the nature of what has to be done, but the creativity in the implementation relies heavily on the specific response of the stakeholders.

5.2.4.4 Unsuitability to the country

Differences in the setting where the policy lessons are derived to the setting where they will be applied would make the implementation process difficult. Resources and even cultural differences can forward a hindrance to the advancement of the process. A conscious noting of the differences have to be provided with the eye on appropriating mitigations suitable for the context.

5.2.4.5 Weak synergy from international organizations

Weak co-action among international organizations themselves could also slow down the process. It can also be possible that the international organizations given the responsibility to execute standardization and benchmarking would show less action because fragmentation also occurs in them. This can be a threat because the whole scheme cannot be substantively afforded if international players are disorganized.

5.3 Policy Transplantation Assessment

Policy transplantation assessment analyzes (ex-ante²²⁶) the suitability and practicability of a policy that is modeled externally. Its application is commonly used in the area of institutional model borrowing, but it can also give insight on policy lessons identification being applied to local context.

The policy baseline will be assessed through its six propositions. The context of the sample setting is the mobile telephony environment of the Philippines. Mobile telecommunication market²²⁷ in the Philippines is one of the most vibrant in the world. This country has been tagged as the “SMS” capital of the world. Due to the undeniable importance of this infrastructure in the country and the lack of alternative means for telecommunications make the infrastructure critical. The table below shows the six propositions of policy transplantation. The policy baseline will be assessed through the provisions of these propositions.

Table 54: Policy Transplantation Propositions

The Six Propositions of Policy Transplantation	
1.	External imposition makes implementation of policy lessons less easy than voluntary adoption
2.	Adaptation of implementation approach to local circumstance is easier than exact copying of policy models
3.	More loosely defined models or even multiple models are easier to follow.
4.	Similarities between the model and intended recipient facilitate the diffusion process. Differences make the process more difficult.
5.	More general and abstract policy lessons are less problematic than specific legal or technological frameworks or procedures
6.	Sense of emergency or urgency creates policy windows that provide easier facilitation of diffusion process, as compared to period of stability.

²²⁶ Ex-ante evaluation refers to forward looking assessments of the likely future effects of the new policies and proposals

²²⁷ Its description is provided I Appendix E.

The table below shows the result of the assessment of the suitability and practicability of the proposed policy baseline in the realities of the Philippines. The details of the reasoning afterwards.

Table 55: Result of the Policy Transplantation Assessment

The suitability and practicability of the Policy Baseline to the Philippine Setting	
1. Imposed?	The policy baseline advocates voluntary implementation; Thus, the process is not imposed. (Rated Suitable)
2. Xeroxed?	The policy baseline does not strive to create the exact copy of the model. It is adapted to local circumstances. (Rated suitable)
3. One Clear Model?	The policy baseline is derived from multiple models with differing context and implementation process. The policy baseline is enhanced by literature findings and expert interview. (Rated suitable)
4. Like-to-Like?	The models are derived from western highly developed societies. There are mitigations needed to be provided in response to the possible impact of the differences as developing countries employ the policy scheme. The implementation process has to recognize salient differences. (Rated unsuitable)
5. Concrete Procedures	The policy baseline does not follow concrete procedures but only policy lessons. (Rated suitable)
6. System Upheaval/ performance crisis or protracted sense of policy dissatisfaction?	Being viewed as critical infrastructure, mobile telephony in developing countries demands immediate actions for assurance. Urgency of this issue is higher in developing countries, which creates policy windows for easier facilitation of the process. (Rated suitable)

5.3.1 Proposition 1: Imposition versus Adoption

■ Imposition implies that the policy baseline is imposed by international organization, while adoption means that the country/network operator decides to adopt policy lessons derived from foreign models at one's own volition (De Jong et al., 2003).

- The policy baseline developed in an international platform is meant to be voluntarily implemented. The mechanism of implementation is through international benchmarking, a non-regulatory market-driven approach that encourages stakeholders to participate. In this kind of setting, the policy baseline is rated high suitability. As propositions 1 dictates: a voluntary adoption makes the implementation less difficult.

5.3.2 Proposition 2: “Xeroxing” versus Adaptation

■ Xeroxing refers to the trial to create an exact copy of the original as best as one can, sometimes with the help of the involvement of people from the modeled countries. Adaptation refers to the inclination of involved actors in the host country to deal flexibly with the model and reframe it to fit local circumstances and desires (De Jong et al., 2003).

- The policy baseline developed aims to institute reference policies needed to achieve greater infrastructure assurance. It identifies what policies are needed to be instituted. It provides a general framework but the specifics of implementation depend on how the stakeholders will fit the policy baseline according to their circumstance. Given such

criteria, the policy baseline is rated high suitability because proposition 2 states that adaptation to local circumstance is easier than exact copying of policy models.

5.3.3 Proposition 3: Single Model versus Multiple Models

■ Single model implies drawing from one clearly identifiable model existing in another country, as opposed to drawing eclectically from a more loosely defined model or even multiple models (De Jong et al., 2003).

- The policy baseline is derived from the “good” practices of multiple countries. In this manner, the policy baseline is not modeled from one single perspective. Multiple models have greater tendency to include as many realities possible of other context. By this, the policy baseline is rated high suitability because proposition 3 states that more loosely defined models or even multiple models are easier to follow.

5.3.4 Proposition 4: Endogamy versus Exogamy

■ Endogamy refers to drawing from a country supposedly belonging to the same family group or having at least very similar legal and cultural characteristics. Exogamy refers to drawing lessons from a country with very different characteristics (De Jong et al., 2003).

- As said, the policy baseline is developed through learning from the approaches of three modeled countries, which is as well enhanced through literatures and expert interview. The Philippines and the three model countries belong to different family group of countries and there are substantial dissimilarities in their legal and cultural characteristics. The Philippines belongs to a combination of Asian and Latin family groups. Netherlands, Germany and Switzerland are western European countries. This is to imply that cultural differences occur. Level of development largely differs. Conscious awareness of dissimilarities has to be afforded in the implementation of the policy baseline in the context of the Philippines. The policy baseline, in this respect, is rated less suitable because proposition 4 asserts that similarities between host and donor of policy facilitate more easily the diffusion process, as compared to differences. Mitigation has to be provided on how to lessen the impact of this criterion.

5.3.5 Proposition 5: Concrete Procedures versus Guiding Principles

■ Concrete procedures implies copying the specific legal framework and procedures from the model while guideline principles refers to adopting just its more abstract policy ideas, ideologies or lessons within rather judicial constraints (De Jong et al., 2003).

- The policy baseline identifies policy lessons of the model countries. Policy lessons are not specific technological, legal or procedural framework to be followed. These policy lessons are contextualized in the setting of the host country. In such a description, the policy baseline is rated high suitability because proposition 5 asserts that more general and abstract policy lessons are less problematic than specific legal or technological frameworks or procedures.

5.3.6 Proposition 6: Performance crisis versus protracted sense of dissatisfaction

■ The first refers to period of urgency, national emergency, system upheaval, etc., and the second is when the policy baseline is introduced outside such dramatic periods (De Jong et al., 2003).

- The need for infrastructure assurance for mobile telephony is urgent in the Philippines. This might be the same also with other developing countries. Mobile telephony (voice and

SMS) is the prime means of telecommunications in the country. Alternatives for other means to communicate are limited, majority of the people are connected to the network, and there are important transactions have been being done through the mobile phone. Knowing the present status of Philippines economy, the vulnerabilities of the infrastructures and the surrounding threats provided by thriving terroristic activities and more, the mobile telephony becomes critical that its malfunctioning would cause a debilitating effect to the normal functioning of whole society. Thus, this issue finds urgency in the context of many countries in the world. Having said so, the policy baseline is rated high suitability because proposition 6 states that sense of urgency creates policy windows that provide easier facilitation of diffusion process, as compared to period of stability.

5.4 Performance of the Proposed Policy Baseline

Table 56: SWOT Analysis Result

Based on SWOT Analysis	
Criteria	Performance
1. Strength	Relatively High
2. Weaknesses	Average
3. Opportunities	High
4. Threats	Average

Table 57: Policy Transplantation Assessment Result

Based on Policy Transplantation Assessment	
Criteria	Performance
Proposition 1	High Suitability
Proposition 2	High Suitability
Proposition 3	High Suitability
Proposition 4	The policy baseline fails in this respect.
Proposition 5	High Suitability
Proposition 6	High Suitability

5.4.1 Based on SWOT Analysis

The strengths of the adaptive policy baseline implemented through international benchmarking are greatly inclined to provide harmonization in mobile telephony infrastructure assurance initiatives. Its capacity to cast responsibilities, to serve as a roadmap for developing countries, to assess level assurance through comparing initiatives makes the policy baseline a potential instrument for harmonization. The non-regulatory nature and the incentives that benchmarking provides will make the facilitation of harmonization less difficult. Based on expert interviews, the impact of the strengths of the policy baseline on the greater harmonization of policy initiatives is rated relatively high

The inherent weaknesses identified are mostly due to the uncertainty of long-term impact, the innate vulnerability of technology, and the political and commercial sensitivity of infrastructure assurance. These weaknesses have to be hurdled by the implementers through providing mitigation mechanisms that lessen their opposing impact to harmonization. Based on the interviews with the experts, the impact of the weaknesses of the policy baseline on the greater harmonization of policy initiatives is rated average.

The opportunities of the policy baseline being implemented through international benchmarking lie on what a secure and reliable infrastructure can potentially offer, which is greater utility of mobile telephony to society. The more assured the infrastructure is, the more confident the people to use the infrastructure, the more indispensable the infrastructure becomes to society. The policy baseline also induces sharing of policy learning, societal cohesion, national awareness and sector wide deliberation of what to be assured. Information sharing leads to greater societal welfare. Based on the interviews with the experts, the impact of the opportunities of the policy baseline on the greater harmonization of policy initiatives is rated high.

The threats identified are indeed realistic. Mitigations are provided in the recommendation to lessen their impact on the smooth and effective implementation of the policy baseline. Based on the interviews with the experts, the impact of the threats of the policy baseline on the greater harmonization of policy initiatives is rated average.

5.4.2 Based on Policy Transplantation Assessment

Five out of the six propositions of policy transplantation being met proves that the policy baseline developed, and implemented through international benchmarking, is suitable and practicable in the context of - as example - the Philippine setting, a developing country which views mobile telephony a critical infrastructure that demands assurance. The voluntary adoption of the policy baseline and its adaptive nature to local circumstances provide an easy facilitation of its implementation. Having multiple models and the approach of using policy lessons, discounting specific and concrete country-specific procedures, make the policy baseline easier to be contour fitted to local utilities. The sense of urgency of infrastructure assurance in mobile telephony attributed to its criticality, more especially in developing countries, provides policy windows for instituting the proposed policy baseline. Where feasible, mitigations to lessen the impact of the differences of culture and resources between the highly developed model countries and the realities of the developing country could provide greater diffusion of the policy baseline.

5.5 Key Messages of Chapter 5

- The policy baseline is shown to be an instrument in ensuring infrastructure assurance. It is indispensable for further deliberation of the issue, national capacity building, casting national actors and responsibilities and performance measurement.
- It can induce policy learning, create more beneficial consumer applications, institutional coordination and cohesion and national awareness.
- Its long-term impact though is not immediately visible. The political and commercial sensitivity of the issue makes stakeholders reluctant to share information. The innate vulnerability of technology and the process time of standardization are also found as the scheme's weakness.
- The threats of incompletion, distrust to both contents and process and differences in contextual settings are undermining the feasibility of implementation of the process. Be used as a ceiling requirement and weak synergy from international organizations hinder the greater diffusion of the policy baseline.
- Based on SWOT Analysis, the proposed policy baseline and the mechanism of its implementation are found favorable in the greater harmonization of initiatives in the assurance of mobile telephony.

- The policy baseline advocates voluntary implementation; Thus, the process is not imposed. It does not strive to create the exact copy of the model. It is adapted to local circumstances.
- It is derived from multiple models with differing context and implementation processes. The policy baseline is enhanced by literature findings and expert interview. The “goodness-of-fit” of the policy baseline is high.
- The models are derived from highly developed societies. There are mitigations needed to be provided in response to the possible impact of the differences as developing countries employ the policy scheme. The implementation process has to recognize salient differences.
- The policy baseline does not follow concrete procedures but only policy lessons. The urgency of the issue creates policy windows that cater easier facilitation of the process.
- Based on Policy Transplantation Assessment, the proposed policy baseline and the mechanism of its implementation are found suitable and practicable in the example context of the Philippines, a developing country which views mobile telephony a critical infrastructure that demands immediate actions for assurance.

6 Conclusion and Recommendations

The preliminary policy baseline is defined and evaluated in the preceding chapters. In this chapter, salient findings will be wrapped up and further recommendations will be provided both to the preliminary policy baseline proposed and to relevant stakeholders.

6.1 Conclusions

This part strives to answer the main research question through responding to the various sub-research questions raised in the previous chapters. The main research question will be restated as follows.

“How to ensure infrastructure assurance for mobile telephony in the global setting?”

■ Introduction (Chapter 1): Why the interest on global infrastructure assurance for mobile telephony?

- Infrastructure assurance is a stake of whole society. Infrastructure facilitates efficient socio-economic functioning and a disruption of its operation is never desirable.
- Stakeholders are fragmented more than ever. This is due to the shift in economic model towards liberalization and privatization believed to provide greater socio-economic efficiency. The concern of infrastructure assurance, on the contrary, demands stakeholders to get together again for such is the only way to arrive to an integrative response. A mechanism on how to bring stakeholders together, set on liberalized and privatized environment, is the perceived necessity to arrive to the desired integrative mitigation.
- Mobile telephony is one of those global infrastructures demanding, from its stakeholders, actions for greater assurance.

Key Contribution: Infrastructure assurance is an emerging policy field with irrefutable social relevance. Society is highly dependent on the secure and reliable operation of its infrastructures. Amidst colossal challenges on bringing stakeholders together on board, infrastructure assurance persists to demand deliberation in order to arrive to workable mitigations.

■ Problem Analysis (Chapter 2): Why does the existing situation demand harmonization of initiatives to improve infrastructure assurance for mobile telephony?

- Mobile telephony is a global infrastructure. It is a network of networks with scope extending national boundaries. The threats and vulnerabilities of mobile telephony are global in character.
- Due to the increasing importance of mobile telephony to the functioning of society and the lack of other alternatives for telecommunications, mobile telephony becomes a critical infrastructure in developing countries. The increasing number of important transactions being done through the mobile phone implies a demand for greater assurance initiatives from its stakeholders. The urgency to assure mobile telephony is higher in developing countries as compared to the developed countries.

- Due to the incapacitation of policy makers from developing countries to execute relevant, focused and effective national assurance strategies, assistance from an international institution, which is in the best position to gather, analyze and disseminate “good” practices, is invaluable.
- Harmonization allows countries and network operators to measure their level of assurance as compared to other systems. Through assessing initiatives by a reference framework, derived from “good” practices, allows information sharing that leads to learning and improvement. To achieve greater assurance for mobile telephony, international coordination is, thus, demanded.

Key Contribution: Mobile Telephony, being a global infrastructure, inherits with it threats and vulnerabilities global in character. It is a network of networks that extend national boundaries, anchoring not only stakeholders from outside national jurisdiction but also from different power levels. By such a setup, multi-level and multi-lateral approach of coordination mechanism is, hereby, appropriate. Harmonization that leads to learning and correction can only be fittingly implemented through international coordination.

■ Theory (Chapter 3): Based on theoretical concepts, how can the harmonization of initiatives be achieved in an efficient and effective way?

- The standardization process expresses that the definition of the policy baseline be done through an open, voluntary, due process, democratic manner of deliberations. These are the traditional principles of standardization invaluable for the efficient and effective deliberation of the policy baseline. The development of the policy baseline should involve the concerned stakeholders (etc. government and network operators) to gain greater support in its implementation. Support is the essential value that can be derived from the standardization process leading to greater harmonization of initiatives. Those who are involved in the process of defining the policy baseline will hold greater stakes in its successful implementation. In such a manner, the policy baseline is better diffused.
- The benchmarking process places it forward that the content and process of the policy baseline should reflect trust and interaction, content and variety, and liveliness and dynamics that adjust behavior of stakeholders in response to the incentive of improving performance. Adjustment is the essential value derived from the benchmarking process leading to greater harmonization of initiatives. Since the benchmarking is done after the policy baseline is defined, benchmarking reinforces the harmonization effect provided by standardization. In such a manner, an increased level of diffusion of the policy baseline is achieved.

Key Contribution: The standardization process provides the essential value of “support” leading to greater harmonization of initiatives. Its traditional principles draw out greater stakes increasing support to the implementation process. Standardization process is employed in the defining stage of the policy baseline. The benchmarking process, on the other hand, affords the essential value of “adjustment” of stakeholders to the defined policy baseline leading to learning and correction. In such a manner, harmonization is achieved. Since benchmarking is employed in the implementation stage, the harmonization effect of benchmarking reinforces that of standardization process. As a result, an increased level of harmonization is derived.

■ Formulation of the Preliminary Policy Baseline (Chapter 4): In considerations to the results of various research methods conducted, what are the elements and provisions of the preliminary policy baseline that ensure the global assurance of mobile telephony infrastructure?

- Regulation for infrastructure assurance is found to be less desirable. Thus, the mechanism to implement the policy baseline should be non-regulatory in nature. It is also economic-driven, which provides greater incentives for market players to participate. International benchmarking, as a policy tool to implement the baseline, is advocated by this study as its prime mechanism. This tool has its flaws that also demand appropriate mitigations.

- Infrastructure assurance is a public-private partnership. It means that both the government and the private sector (in this study the network operators) should be held responsible for the greater assurance of the infrastructure. Information sharing must exist among stakeholders and a trusted environment is demanded to achieve an open and voluntary facilitation of sensitive important information. Establishment of a trusted environment might take quite a time to attain depending on socio-cultural factors.
- Infrastructure assurance demands a proactive national approach in line with an international perspective. International standards and “good” practices are excellent starting point. The baseline developed stresses that the government should create a national strategy for infrastructure assurance that anchors a public-private partnership approach, embraces international coordination and conducts an integrated risk management.
- Integrated risk analysis is based on the understanding of threats, vulnerability and interdependencies of the infrastructure.
- Information sharing arrangement is a necessity for greater infrastructure assurance. Conducting a risk analysis is a starting point for a collaborative undertaking. The private sector has better knowledge of the vulnerabilities of the infrastructure as compared to the government. The government might have greater knowledge of the threats and interdependencies as compared to individual network operator. The collaboration of these stakeholders will lead to a more comprehensive analysis of the risks that confronts the infrastructure.
- The risk of liability to share sensitive information about vulnerabilities should be afforded attention. Appropriate mitigations should be provided. The fear of liabilities hinders the establishment of a trusted information sharing arrangement essential for greater assurance of infrastructure.
- The following shows the elements of the policy baseline and the provisions for its further development and implementation.

Elements of the Policy Baseline		Provisions for its further development and implementation
General Lesson	Specific Policy Lessons (General Lesson achieved through the following specific policy lessons)	
<p>Communication leading to interaction and collaboration</p> <p><u>Requisite:</u> Atmosphere of trust</p>	<ul style="list-style-type: none"> ➤ Coherent national strategy ➤ Public-Private Partnership ➤ Risk-Based Analysis and Management ➤ All hazards ➤ Multi-sector perspective ➤ Creation of a trusted third party platform 	<ul style="list-style-type: none"> ➤ Perform the standardization process in developing the content of the policy baseline (voluntary and consensus-driven, support-inducing) ➤ Execute a benchmarking exercise to better diffuse the policy baseline (voluntary and incentive-driven, adjustment-inducing)

Key Contribution: Through the analysis of the results derived from the various research methods, the policy baseline proposed in this study lays down into open the fundamental necessity of communications among stakeholders in the middle of fragmented institutions. The provision of mechanisms that allow stakeholders to communicate more with other stakeholders in a cooperative atmosphere is the minimum policy demanded to ensure the assurance of an infrastructure. More than ever, communication is needed to create a sense of unified responsibility for assurance is basically the stake of everybody amidst the fragmented environment. Communication, however, is not an instant remedy. Before stakeholders can freely communicate among one another, an environment of trust has to be established. This atmosphere of trust does not happen overnight for it demands a gradual process--- a series of learning and relearning processes. This case is more aggravated in developing countries where trust among institutions is yet a far-fetched thought. A conscious effort to establish such kind of atmosphere is

demanded in order to arrive to the desired trust-based culture. The government has the role to initiate activities to achieve greater interaction with the private sector stakeholders. The private sector, on the other hand, makes it part of their system to coordinate with the government and find their niche in the whole undertaking Stakeholders from international organizations could provide leverage for stakeholders to communicate through instituting mechanisms that let the government and the private players to collaborate even more.

■ Evaluation of the Proposed Policy Baseline (Chapter 5): Based on the two evaluative (ex-ante) analyses conducted, what hints can be provided on the effectiveness and suitability of the policy baseline to improve infrastructure assurance for mobile telephony?

- SWOT Analysis reveals that the strengths and opportunities of the proposed policy baseline are promising. There are weaknesses and threats seen, both in its content and process, and that should be made known to the stakeholders. Stakeholders should provide mitigation in order to exploit more the strengths and the opportunities of the proposed mechanism and reduce the impact of its weaknesses and threats. This study also recommends mitigation policies to lessen the undesirable impact that undermine the validity of the proposed mechanism.
- Through the (ex-ante) Policy Transplantation Analysis it shows that a policy baseline coordinated through benchmarking can be found indispensable in order for developing countries to get into the track of assurance. Such mechanism elucidates policy lessons and delivers concrete actions. Developing countries are able to assess their system, provide adjustment and seek out for assistance if necessary. To harness greater gain out from the implementation of the mechanism, the analysis emphasizes that countries involved have to understand their peculiar realities as they conform to the general framework of policy lessons provided by the policy baseline to create a sense of ownership paving to greater support.

Key Contribution: The two (ex-ante) evaluative analyses have shown that the proposed mechanism can be an effective and suitable means to ensure the assurance of infrastructure if appropriately implemented. Strengths and opportunities have to be exploited; weaknesses and threats have to be mitigated. Differing local realities have to be recognized and the implementation of the policy lessons has to be aligned in the framings of local situations.

■ Main Research Question:

How to ensure infrastructure assurance for mobile telephony in the global setting?

- Ensuring assurance of infrastructure in a global setting can be an overwhelming task. An appropriate mechanism should be instituted to gather stakeholders together to discuss the problem and solution in a trusted environment. The study puts forward the necessity of communication among stakeholders amidst the fragmented institutions caused by shifts in economic arrangements. To bring stakeholders to collaboration and coordination, communication is the minimum general policy requirement in order to create partnership. The challenge is that this needed communication only takes place when a trusted environment is established, and such is a gradual process of learning and re-learning. This study, thus, puts forward the need of employing conscious intervention, a social construction of stakeholders themselves, that allows fragmented stakeholders to communicate leading to interaction and collaboration. In a global setting, one is dependent on the contribution of the other. Therefore, a partnership of all stakeholders involved is needed to achieve the common goal of global infrastructure assurance. In concrete terms, the study concludes that a non-regulatory (voluntary) and incentive-driven mechanism has to be afforded in assuring the infrastructure. The study advocates the use of adaptive policy baseline (international) benchmarking as a concrete mechanism that allows stakeholders to communicate, interact and collaborate to the effort of ensuring the assurance of infrastructure in the global setting.

6.2 Recommendations

This part strives to provide concrete policy advice for the better implementation of the proposed policy baseline.

6.2.1 in Response to the Evaluation of the Policy Baseline

6.2.1.1 In reference to SWOT Analysis

In order to utilize the strength of the proposed mechanism, exploit its opportunities, reduce its weaknesses and safeguard from surrounding threats, this section recommends various strategies for the main problem owner, which is the relevant international organization. These are shown by the table that follows.

Table 58: Strategies Derived from SWOT Analysis

	Opportunities (O) <u>How to exploit the opportunities?</u>	Threats (T) <u>How to be safeguarded from threats?</u>
	<ul style="list-style-type: none"> ■ Shared policy learning ■ More potential user applications ■ Institutional coordination and cohesion ■ Sector-wide discussion of what to be safeguarded ■ National Awareness 	<ul style="list-style-type: none"> ■ Incompliance ■ Distrust to the proposed policy baseline ■ Be used as the ceiling requirement instead of being the baseline ■ Unsuitability to the country ■ Weak synergy from international organizations
Strengths (S) <u>How to utilize strengths?</u> <ul style="list-style-type: none"> ■ A coordinated mechanism to ensure infrastructure assurance ■ Indispensable for national capacity building ■ Clear delineation of actors and responsibilities ■ Means of assessing assurance performance ■ Groundwork for discussion 	S-O Strategies <ol style="list-style-type: none"> 1. Conduct standardization process in defining the policy baseline 2. Perform benchmarking exercise as a voluntary, economic-driven mechanism to ensure assurance in the global setting 	S-T Strategies <ol style="list-style-type: none"> 1. Employ a voluntary certification scheme to confirm compliance 2. More aggressive information dissemination of the proven empirical benefits of the good practices outlined in the policy baseline
Weaknesses (W) <u>How to reduce weaknesses?</u> <ul style="list-style-type: none"> ■ Long-term impact is not immediately visible ■ Political and commercial sensitivity of the issue ■ Reluctance to share security information ■ Technology is innately vulnerable ■ Long standardization process time 	W-O Strategies <ol style="list-style-type: none"> 1. Provide a regular report of incidents of insecurity and unreliability 2. Create more policy opportunities to collaborate with stakeholders 	W-T Strategies <ol style="list-style-type: none"> 1. More aggressive promotion of the passing of legislations needed for the establishment of trusted platform to share information (e.g. privacy/liability laws) 2. Invest on R&D to search for means to better assure the infrastructure

■ S-O Strategies

To utilize the strengths and exploit the opportunities derived from the creation of a policy baseline, the study advocates the use of a consultative mechanism in the development of its contents and economic incentive-driven mechanism in its implementation. The mechanisms should be voluntary. The consultative mechanism assures the relevance and validity of the policy baseline and the economic incentive-driven mechanisms provides greater drives for stakeholders to conform to the developed policy baseline. Relevance, validity and drives allow stakeholders to be better aware of the issue and encourage them to institute initiatives aimed for ensuring assurance. Thus, the international organization is recommended to create a specific study group (or any kind of arrangement in the organization), devoted for the conduct of the standardization and benchmarking processes.

■ S-T Strategies

To utilize the strengths and to be safeguarded from threats, employing a voluntary certification scheme could mitigate the threat of incompliance. This mechanism plays with the “impression” that “voluntariness” can bring forth to countries and network operators. Countries and operators who volunteer to comply provide the impression that they are responsible and trustable. It also informs the general consumers that such a government or network operator is abiding assurance compliance. The certificate from a “well-respected” institution could provide them a drive to volunteer to implement measures. The certificate will be a proof of compliance and useful for advertisement and market purposes. More importantly, the information derived from the voluntary certification scheme will be indispensable for the detailed analyses of threats, vulnerabilities, critical assets and dependencies of the infrastructure for R&D purposes. The aggressive information dissemination of “good” practices and their proven benefits would mitigate the threats on distrust, being used as ceiling requirement, skepticism to its suitability to the country due to the provision of empirical proofs. These strategies recommended elicit cooperation among relevant international organization mitigating the threat on weak synergy.

■ W-O Strategies

To reduce weaknesses and exploit the opportunities, provision of regular reports of incidents when the infrastructure becomes insecure and unreliable will help to mitigate skepticism on its long-term impact. This undertaking would be indispensable for risk analysis and management. Through this regular report, stakeholders are able to trace trends of attacks and vulnerabilities. This report shows progress in the implementation of initiatives in assuring the infrastructure. This mechanism, as well, paves way to more research and investigative studies done in this novel field of public policy. Creation of policy opportunities where stakeholders can collaborate can pave way to a more trustable environment. Policy opportunities such as instituting standardization and benchmarking exercises would lead stakeholders to come to the table for discussion of the issue. In such a manner, “sense of cooperation” is attained in this area of public concern. In this undertaking, sensitivity, reluctance, innate vulnerability and long process time can be deliberated further for elucidation of the issue and mitigations.

■ W-T Strategies

To reduce the weaknesses and be safeguarded from the threats, strategies forwarded are the promotion of passing of legislations that ensures stakeholders from being liable in exposing vulnerabilities of their networks. These legislations create a trusted environment where a free flow of information and insights to mitigate the problem is served. A trusted environment should be built on strong grounds such as legislations to institutionalize the issue. The second strategy is to invest more on R&D to enrich information and knowledge in this novel field of public policy. Weaknesses and threats are responded better if the needed information is available. The following legislative issues are in need to be addressed.

Infrastructure Assurance Legislative Issues		
Issues	Main Inquiry	Possible Mitigation
1. Liability Issues	How can stakeholders share information without being subject to additional liability risk?	Passing of anti-liability laws
2. Antitrust Issues	How can anti-trust laws accommodate infrastructure assurance?	Lifting specific aspects of anti-trust laws
3. Protection of trade secrets and proprietary business information	How can laws protect trade secrets and proprietary information from general disclosure?	Lifting specific aspects of freedom-of-information acts

6.2.1.2 In reference to Policy Transplantation Assessment

■ The unsuitability of the policy baseline

- Unsuitability can be a risk that the baseline will not work. Using the policy transplantation assessment, the policy baseline fails in Proposition 4 (Like-to-Like?) as it is assessed in the context of the Philippines. Mitigation is provided.

Assessment: The policy lessons are derived from three highly developed countries where the resources are relatively high and a collaborative culture is already established. Developing countries are yet far behind both in the reason of lack of resource and absence of trusted culture.

Mitigation: Developing countries have to be aware of the realities of their circumstance and derive mitigations out from there. The specifics of the policy baseline proposed advocates comprehensiveness in the strategies instituted. Developing countries might fail in providing comprehensive mitigations by mere reason of lack of resource. It is thus recommended that developing countries will start with the foundational need of the whole scheme, which is communication among stakeholders. Build communication links according to the manner your culture defines it and according to the means you have to implement it. Everything starts with communication and such leads to interaction and collaboration. Hurdle the walls of fragmentation through initiating communication links that connect the institutions. In the process, partners from outside and inside the country would come to assist in the creation of a comprehensive national strategy. Start with the least requirement (policy on communication among institutions), and then look at the specifics of the proposed policy baseline as roadmap of what else yet to be achieved.

6.4 Recommendations to the Standardization Process

- Include as many representative stakeholders as possible. Strive to fill in the representation gap in the standardization process. Include stakeholders from developing countries. Encourage participation from minority voices to avoid catastrophic consensus challenges later in development process.
- Stakeholders should come from different jurisdictional level. Include experts from international parties, government, and industry. Consult perspectives of end-users.
- Strive for genuine adherence to the ideologies of standardization: consensus, voluntary, democratic, coherence, and rationality. The process must be conducted in an environment that promotes trust, respect and expertise sharing.
- Provide means to reduce timescale of standardization processes as it is said that it is one of the weaknesses of the whole scheme provided in this study. Parallel sub-groupings (e.g. study groups) on the various elements of the issue might help. Increasing funding to the body that defines the policy baseline might be of help to provide economic-incentives that propel support and participation.

- Improve memory and knowledge dissemination to encourage the reuse of the experience of the participants in defining the policy baseline, as the policy baseline will be updated as needed. This documents previous experiences in the standardization process and improves future standardization undertaking.
- Focus more on consensus formation. Identify the area where consensus will be difficult and develop approach to resolve it. Representativeness is important for the “effectiveness” of the policy baseline; thus, attaining genuine consensus is a focal value in the standardization process. Stakeholders respond if the policy baseline is more of a representative of the perspectives of greater majority.
- Maintain formal and informal contacts to encourage dissemination of experience and expertise.
- Encourage good leadership style to enable appropriate coordination of work.

6.5 Recommendations to the Benchmarking Exercise

- Collaborate with the standardization group so that the dimensions and criteria of the policy baseline will be reflected on what is to be benchmarked.
- Stimulate sense of competition in the network operators through the result derived from the benchmarking exercise. Learning is generally induced if stakeholders come under pressure. Competition is a great pressure for them to improve. Results can be used for marketing purposes, for example. Consumers generally would like to use an infrastructure perceived to be secured and reliable.
- Competition could also provide pressure for the government to improve. With globalization, competition between nations and regions has increased. A country perceived to be assured generally has good credits in the international sphere.
- Show as vivid as possible the social and economic benefits of an assured infrastructure. Stakeholders are always on the look out on what they can derive from the undertaking.
- Lessons learned in the benchmarking activity should become the source for continuous improvement of the benchmarking process. These lessons have to be documented and used as basis for the new planning cycle.
- Benchmarks have to be reconsidered periodically in the light of changes in those policies that have impact on assurance performance and “good” practice.

6.6 Recommendations to Specific Stakeholders

6.6.1 Recommendation to ITU

- Institute more discussion on the assurance of mobile telephony. Clarify its niche in the Global Cybersecurity Agenda.
- Create a study group for infrastructure assurance for mobile telephony anchoring technical and procedural measures and policies and strategies. This document can be used as groundwork for discussion.
- Perform standardization processes and international benchmarking exercise as what this study advocates.
- Encourage greater participation from stakeholders in the development of technical standards in infrastructure assurance. Institute voluntary tracing mechanism on how these technical standards are diffused to the market. Encourage experts from developing countries to participate.
- Together with the Cybersecurity/CIIP issue, create a unique body that responds to the issue of infrastructure assurance. This issue is a combination of the works of ITU-T and ITU-D and to some extent ITU-R. Strive to attain greater integration of initiatives of bureaus in the issue of infrastructure assurance, CIIP, or cybersecurity.
- Provide monitoring scheme on how each of the member state benchmarks their network operators. This is to have knowledge of the level of diffusion of the policy baseline.

6.6.2 Recommendation to ITU's Member States

- Coordinate with international organizations (such as ITU or GSMA) on assurance initiatives.
- Coordinate with regional organizations (such as EU, APEC, etc.) to establish partnership in the establishment of national capacity
- Create a national strategy for infrastructure assurance. Delineate the niche of mobile telephony in the national strategy. Define the criticality of mobile telephony with considerations on contextual setting.
- Involve the private sector in the process.
- Strive to be comprehensive in approach: all hazards, multi-sector, and integrated risk-based analysis and management.
- Surpass institutional fragmentation. Communicate with stakeholders. Establish trust with stakeholders.

6.6.3 Recommendation to GSMA

- Gather GSM network operators for an industry-wide discussion of infrastructure assurance. Deliberate the issue industry-wide.
- Clarify and intensify mechanism on the voluntary security accreditation scheme
- Include as part of the public policy section the issue of assurance of mobile telephony
- Coordinate initiatives with ITU and other relevant international organizations

6.6.4 Recommendation to Network Operators

- Employ Information Security Management System
- Execute Business Continuity Planning and Management
- Collaborate with the government and international organizations
- Employ international standards on telecommunications security

6.6.5 Recommendation for End-Users Awareness

- Strongly promote information awareness to end-users about infrastructure assurance for mobile telephony. Establish public-private partnerships for awareness raising and educational training.

6.6.6 Recommendation to the Philippine Government

- Create a unified and comprehensive approach to infrastructure assurance. Start the process of enforcing conscious efforts to mitigate fragmentation and obliviousness of institutions.
- Organize a clear national strategy on infrastructure assurance. Government agencies and private entities should discuss the issue. Pursue a national key program based on public-private partnership and international cooperation.
- Do not delay the passing of legislations (e.g. liability laws, aspects of anti-trust laws and freedom-of-information acts) that address the establishment of trusted environment for the stakeholders.
- Collaborate with overseas parties. Coordinate with international and regional organizations.
- Enhance nation's intelligence capacity. Security plans has to be updated, funded and implemented. A focal point of the strategy has to be known.
- Start to build a strong mutual trust, establish a systematic contact system, and design real time information to exchange.
- Conduct risk vulnerability assessment, standards and participate in voluntary certification schemes

6.7 Further Research Recommendations

- Conduct comparative analysis to greater number of countries employing “good” practices.
- Validate policy baseline to greater number of assurance aspiring countries.
- Provide a focus on information sharing model.
- Establish a stronger stance on how a standard can become a benchmark.
- Study legislative issues in infrastructure assurance.
- Explore more on the cost issues of standardization and benchmarking processes for infrastructure assurance.
- Create incentive structures on how stakeholders will better respond to infrastructure assurance, especially those from the private sector.
- Execute a more detailed stakeholders’ analysis.
- Extend to other stakeholders. Not only the network operator (e.g. end-users, manufacturers, non-governmental organizations, regional organizations, etc.)

7

Reflection

Privatization and liberalization of large-scale technical infrastructures have been the economic models pursued by many countries in the world for many years now. The greater welfare it provides, as compared to monopolistic arrangement, has been shown, in many empirical proofs, convincing in the provision of efficient products and services. Together with myriad threats and vulnerabilities confronting large-scale technical infrastructures, these economic models, however, have also caused fragmentation among stakeholders that deter collaboration for a common concern. This fragmentation is seen as the main hindrance in the establishment of unified actions for mitigation. Infrastructure assurance is one of those public issues presently exhibiting isolated and fragmented initiatives.

Nevertheless, there is no point in raising the notion of the need of “bringing back the genie to the bottle” as a solution to this perceived fragmentation. With regulation, why liberalize in the first place? The welfare of liberalization is sufficient enough to convince that too much regulation does harm the innovative and investment capacity of the infrastructure, which is indeed undesirable. This study strived to enlighten how can this fragmentation be mitigated to execute a collaborative undertaking to achieve a common goal avoiding the harm of too much regulation.

The general policy baseline that is deduced out from the study is the value of communication among stakeholders. Communication is seen as a need, more than ever because of the present setup of liberalization and privatization, to reach out for fragmented stakeholders of the infrastructure and bring them to a common ground to discuss and deliberate the problem and solution to the issue. It is the starting point of a trusted environment. Communication, as simple as it may seem, can be very hard to achieve for a society not accustomed to the setting of collaboration and coordination. Many countries in the world, most especially developing countries, experiences fragmentation due to the lack of communication links between institutions.

Communication is believed to lead to interaction, which pave way to partnership. By such rationale, communication is the minimum policy requirement essential for the establishment of collaborated and coordinated actions. Communication is a foundational tool needed for collaborative undertaking. It is the one that makes for stakeholders see their part in the whole process. As the study has advocated, when stakeholders see an undertaking as their own social construction, it is more likely that they will support it. They have provided much resource and effort on it, thus, their stake for its success is increasing. Communication leads to trust and partnership.

Trust is an important value in performance measurement such as in the area of infrastructure assurance. As soon as mistrust among players exists, there is a strong incentive to pervert the system. Trust exists only if performance measurement is based on and a result of interaction. An undertaking as a result of interaction leads to support of tradeoffs of conflicts, ownership of the system by stakeholders, and mutual trust. Moreover, a public concern is a nature of multiple value--- there are multiple criteria involved that demand ever-changing tradeoffs. If the criteria are derived from a single perspective, the undertaking becomes illegitimate that leads to perversion; and, the whole process becomes unusable and stays unsupported. The process and

content of the undertaking have to reflect the perspectives and interests of the stakeholders for it to gain support towards its implementation.

Infrastructure assurance is seen to be a public policy issue of national scope. Infrastructure assurance for mobile telephony, on the other hand, is a national issue with inbuilt international weight. Mobile telephony is a global infrastructure and, therefore, the relevant international organizations can have important role to perform. International organizations, though not having a national mandate, can induce drives for national stakeholders to assure the infrastructure. International organizations can initiate mechanisms that trigger national stakeholders to participate. The mechanisms should leverage the process of communication leading to partnership in the effort of assuring the infrastructure. The mechanism provided in this study is public-private partnership driven. Such arrangement is the most cost effective because risk and resources are dispersed to stakeholders. Collaboration is less resource-intensive and carries lesser burden to individual stakeholder as compared to sole implementation. Public-private partnership is the only way to move forward for a public concern such as infrastructure assurance.

The challenge, though, that one has to hurdle is the establishment of the trusted environment where this collaboration is set. As said by the study, a trusted environment is created through a gradual process of learning (and re-learning) from one another over a period of time. It does not occur in a snap of time. The level of trust is largely varying from one society to another and developing countries are yet in the start of the process. But how can this infrastructure assurance be placed in position amidst the surrounding impediments? The answer would lead us back again to the value of communication as an essential requirement to get things started and an important element for the sustenance of partnership. Communication that leads to interaction and collaboration has been a consistent advocacy of this paper. Involve the stakeholders in the process. Make infrastructure assurance a social construction.

Appendices

A. Respondents and Inquiries

A1. List of Interviewees

<p>International Organizations</p> <p>Martin Adolph Tim Kelly Christine Sund Xiaoya Yang</p> <p>Tom Phillips Jeanine Vos</p>	<p>ITU-Strategy and Policy Unit ITU-Strategy and Policy Unit ITU-D Policy and Strategy Department ITU-T Study Group 17</p> <p>GSM Association GSM Association</p>
<p>Selected National Governments</p> <p><u>Netherlands (NL)</u> Hans Oude Alink Jacqueline de Braal-Schouten Simon van Merkom</p> <p><u>Germany (DE)</u> Herbert Buchta Timo Hauschild Dirk Reinermann</p> <p><u>Switzerland (CH)</u> Stephan Brem March Henauer</p> <p><u>Philippines (PH)</u> Edgardo Cabarios Kenneth Tanate</p>	<p>Ministry of Economic Affairs Ministry of Economic Affairs Ministry of Economic Affairs</p> <p>Federal Network Agency Federal Office for Information Security Federal Office for Information Security</p> <p>Federal Department of Defense, Civil Protection and Sport Federal Office of Police</p> <p>National Telecommunications Commission National Economic and Development Agency</p>
<p>Network Operators (NO)</p> <p>Benjie Aquino Ryo Kitahara Michael Vocke Jenny Yap-Minoza Mark Younge</p>	<p>Globe Telecom NTT DoCoMo Royal KPN Globe Telecom T-Mobile</p>
<p><u>Supervisors/Invited Experts (EX)</u></p> <p>Jan van den Berg Mark de Bruijne Michel van Eeten Tineke Egyedi Eric Luijff Jos Vracken</p>	<p>TU Delft TU Delft TU Delft TU Delft TNO-Defence, Safety and Security TU Delft</p>

■ A2. How were the respondents chosen?

The respondents were selected in a manner that the aim of arriving to a more representative preliminary policy baseline will be achieved. The study sought for perspectives that stem from international, national, and firm level frames. Due to the nature and wide scope of the study, a multi-level and multi-lateral approach in the research framework is viewed as appropriate. A careful thought was provided in choosing representatives of organizations whose views will be considered important in shaping the conclusion of the study.

The highest inter-governmental organization for mobile telephony is the International Telecommunication Union (ITU) and it is just proper to obtain its various perspectives on the issue. It is the international third party platform that could provide an avenue for a balanced and neutral facilitation of the issue. There were three ITU Bureaus included, namely: ITU-SPU which deals with general ITU policies and strategies, ITU-T which is main responsible for standardization activities in the area of telecommunication security, and ITU-D which has various development-oriented activities on Critical (Information) Infrastructure Protection, Cybersecurity, etc. initiated and implemented for its member states. The representatives interviewed are key persons in this issue of infrastructure assurance in their respective bureaus in ITU. Allow me not to explicitly state their position in the organization for reasons of privacy and protection. Another organization was chosen in the category of international organization, namely GSM Association. It is the largest international organization of mobile telephony network operators. This organization is privately initiated. As a principle, its membership is only for mobile telephony network operators. This organization was chosen to be included in the study because of its important position in the matters that concern GSM-based networks. Since GSM is the most popular mobile telephony global standard, GSMA can provide an industry-wide discussion of the infrastructure assurance issue. In such a manner, the organization can also provide a greater push of the issue, as it will be deliberated together with other stakeholders outside the industry.

Various agencies of national governments participated in this study. The rationale of such inclusion is that infrastructure assurance in mobile telephony is believed to be an issue of national credence framed in a greater international context. The approach is national with an international perspective. National arrangements are important factors of infrastructure assurance performance. Greater infrastructure assurance is believed to be achieved if initiatives in the national level are coordinated internationally. The three-modeled countries, namely the Netherlands, Germany and Switzerland, are the countries which already have established clear and concrete initiatives on infrastructure assurance for critical infrastructures. They have advanced national arrangements consciously created to improve their infrastructure assurance condition. In addition, these countries are using GSM standards and, thus, more suited in the context of this study. The Philippines is also included as a sample developing country. Since the aim of the study is harmonization, a country that needs to adjust to a reference baseline has to be illustrated. The context of the Philippines was intensively used in the policy transplantation part. Philippines is a GSM country and mobile telephony is viewed as a critical infrastructure makes this country suited for this study. Due to important role that mobile telephony plays in the Philippines (e.g. due to diaspora, limited telecom infrastructure, etc.) makes infrastructure assurance a relevant issue worth an attention. The representatives participated come from main national agencies responsible in the area of critical infrastructure assurance. Allow me again in this part to not explicitly specify their position in the organization for reasons of privacy and protection.

Lastly, a number of representatives of network operators participated. They can provide a view on infrastructure assurance in the firm level frames. Most of those participated are operating a network in the countries included in this study except for NTTDoCoMo and none from Switzerland. The respondents have positions that directly deal with the protection of their respective mobile telephony network. Thesis supervisors and invited experts from the academe also provided some light in making a more substantive report.

Analysis of the data is done through determining the trend of the perception of the experts on the various inquiries raised. Expert perspectives, lessons from modeled countries, theories, various organization initiatives and own analysis are the foundation of the result and conclusion of this study. Results and analysis are immediately infused to sentences wherever they become relevant. A summary of inquiries asked to various stakeholders is provided through the table below.

A3. List of Inquiries

International Organizations (For ITU and GSMA)

1. Do you find mobile communications a critical infrastructure?
2. What are the various vulnerabilities of GSM technology?
3. Do you have technologies that reduce these vulnerabilities?
4. What you think about government intervention in the protection of mobile communications?
5. How to improve reliability and security of mobile infrastructure utilizing GSM technology?
6. Do you see the potential of a public-private partnership in the protection of your mobile communications infrastructure? If yes, how should the role assignments for public (government) and private players be done?
7. Do you see the potential of a policy baseline to benchmark by countries as an instrument in harmonizing initiatives in critical infrastructure protection? Could you elaborate your answer?
8. Do you agree that Critical Infrastructure Protection (CIP) should be part of the requirements in acquiring permit to operate?
9. Do you see a role of an international organization (e.g. ITU) in regulating the network in the area of infrastructure protection?
10. Do you have jurisdiction to intervene national critical infrastructure protection?
11. What you think is your role as an international organization in the protection of mobile communications as a critical infrastructure?
12. What are the current approved standards you have for the protection of critical telecommunications infrastructure?
13. What you think are the areas in telecommunications protection that demands standardization?
14. Information disclosure questions
15. SWOT and Policy Transplantation analyses questions

Selected Government Agencies (For relevant agencies in NL, DE, CH and PH)

1. What have been the Infrastructure Assurance initiatives of your government in mobile communications infrastructure? Thank you for listing them down.
2. Since most of the mobile telephony networks in your country are privately owned, how does the government collaborate with the private owners to build assurance in the infrastructure?
3. Are there already public-private participation initiatives for infrastructure assurance in your country? If yes, could you describe how they are/were done?
4. Do you consider mobile communications a critical infrastructure? Thank you for explaining more.
5. What you think are the appropriate regulatory mechanisms for Critical infrastructures (CIs) such as mobile telephony in the area of infrastructure assurance?
6. How difficult is it to involve the private sector in the issue of public concern such as infrastructure assurance?
7. What have been the information sharing arrangements for infrastructure assurance in your country?
8. What you think are the appropriate incentives for private sectors to participate and share information about how they secure and make their network reliable?
9. Do you have experiences implementing policies derived from abroad? If yes, thank you for describing them more.
10. What is the level of practicability and feasibility of conformance to policies modeled from foreign countries?
11. Information disclosure questions
12. SWOT and Policy Transplantation analyses questions

Network Operators (For Royal KPN N.V., Globe Telecom, T-Mobile, and NTTDoCoMo)

1. Do you consider mobile communications infrastructure a critical infrastructure? What you think are the vulnerabilities of GSM-Based networks?
2. Do you see the potential of a public-private partnership in the protection of mobile communications infrastructure? If yes, how should the role assignments for public (government)

- and private players be done?
3. How does your company coordinate with the government in assuring mobile communications infrastructure?
 4. Since mobile communications has a global scope, do you think an international effort to harmonize initiatives in the protection of mobile infrastructure is needed? Could you elaborate your answer?
 5. Do you agree that Critical Infrastructure Protection (CIP) should be part of the requirements in acquiring permit to operate?
 6. Do you see a role of an international organization (e.g. ITU, EU, etc.) in regulating your network in this area of critical infrastructure protection?
 7. Are you comfortable to disclose the following information if requested by the government?
 - a. Are you employing Security System Management?
 - b. Does your company have Business Continuity Planning & Management?
 - c. What information sharing arrangements you network has with the government?
 - i. Do you reveal critical assets?
 - ii. Do you reveal threat information?
 - iii. Do interdependency analysis?
 - iv. Do vulnerability assessment?
 8. Do you give information if specifics of your network are asked such as:
 - d. Location of the premises, structural design, inner perimeter, protection of buildings?
 - e. Security policy for employees?
 - f. Security policy for outsiders?
 - g. Security policy within the company?
 - h. Security policy outside the company?
 - i. Risks from natural events, human error/technical failure, terrorism and/or criminal abuse?
 - j. Crisis and emergency plans?
 - k. Areas of responsibility in the event of emergency?
 9. SWOT and Policy Transplantation analyses questions

Expert Perception Test (For the main respondents)

Open-Ended Questions:

1. What are the current C(I)IP national arrangements in your country? Does your country have policy framework for infrastructure assurance? How does mobile communications as an information infrastructure fit in this framework?
 - a. Public Authority Identification/involvement
 - b. Legislations & Enforcement
 - c. Information Sharing
 - d. Regulation
 - e. Industry Participation

Infrastructure Assurance Initiatives:

Industry Sector	Public-Private Partnership	Government

2. What you think should be the contents (elements) of a policy baseline for infrastructure assurance?
3. How should this policy baseline for infrastructure assurance be implemented? Should it be coordinated internationally?

Perception Test: 10= highest, 6=passing, 1=lowest

1. Criticality of mobile communications
 - a. Present (2008): Rate -
 - b. Future (2015): Rate -

Motivation:

2. Urgency of the issue:

- a. Developing countries: Rate –
- b. Developed countries: Rate -

Motivation:

3. Usability (practicality) of a policy baseline: Rate:

- a. Strengths
- b. Weaknesses
- c. Opportunities
- d. Threats

Motivation:

4. Feasibility (desirability) of conformance – Rate:

Motivation:

5. Difficulty of developing a policy baseline – Rate:

Motivation:

6. Scope (Level) of national government jurisdiction on the issue – Rate:

Motivation:

7. Relevance of an international organization in the issue of critical mobile communications infrastructure protection – Rate:

Motivation:

8. Degree of involvement of the private sector –

- a. Present: Rate -
- b. Desired: Rate -

Motivation:

9. Extent of information sharing among stakeholders

- a. Present: Rate -
- b. Desired: Rate -

Motivation:

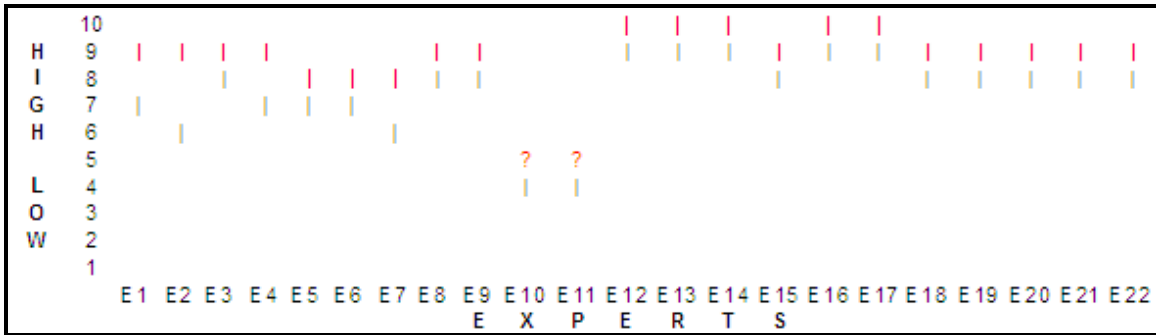
10. Efficacy of regulation in infrastructure assurance - - Rate:

Motivation:

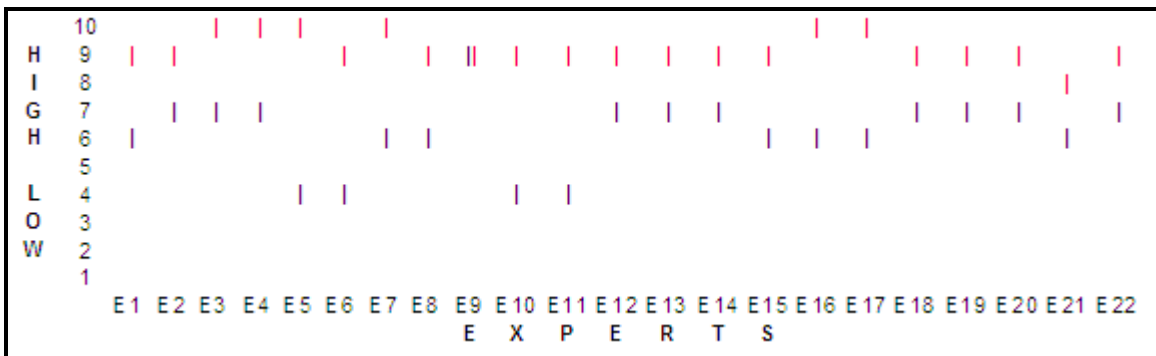
Others (For supervisor, invited experts, etc.)

1. How do conflicting views and interests being resolved in standardization process?
2. What are your experiences in developing standards on issues of public concern?
3. What is your view about benchmarking as a tool to implement policy baseline (reference standards)?
4. What you think are the social benefits and drawbacks of a policy baseline (reference standards)?
5. Do you have experiences in developing standards on issues of public concern?
6. What are the appropriate regulatory mechanisms for CIP?
7. What is your view about benchmarking as a tool to implement policy baseline (reference standards)?
8. What you think are the social benefits and drawbacks of a policy baseline (reference standards)?
9. What you think is the political feasibility of implementing a policy baseline?
10. What you think are the appropriate incentives for private sectors to share information about the threats and vulnerabilities of their networks?
11. SWOT and Policy Transplantation analyses questions

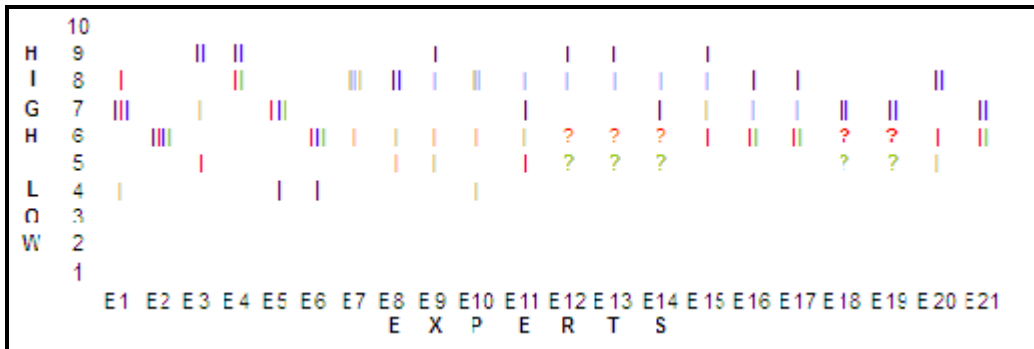
A4. Perception Test Tabulation



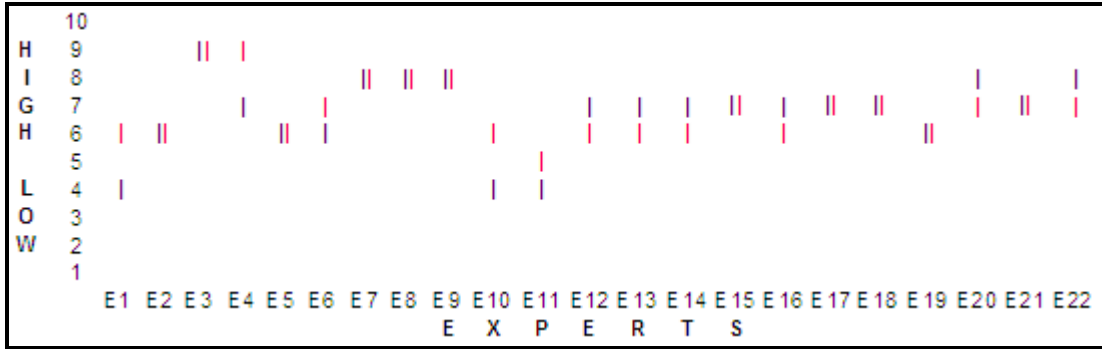
1. Criticality of Mobile Telephony at Present and in the Future



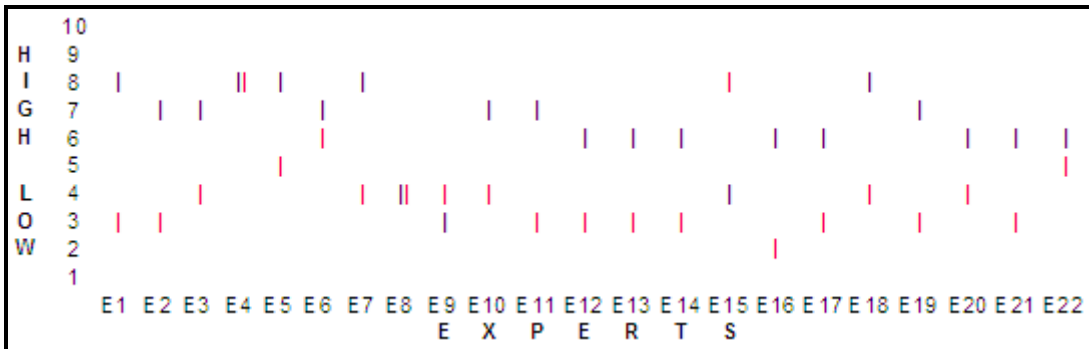
2. Urgency of Infrastructure Assurance in Mobile Telephony in Developed Countries and Developing Countries



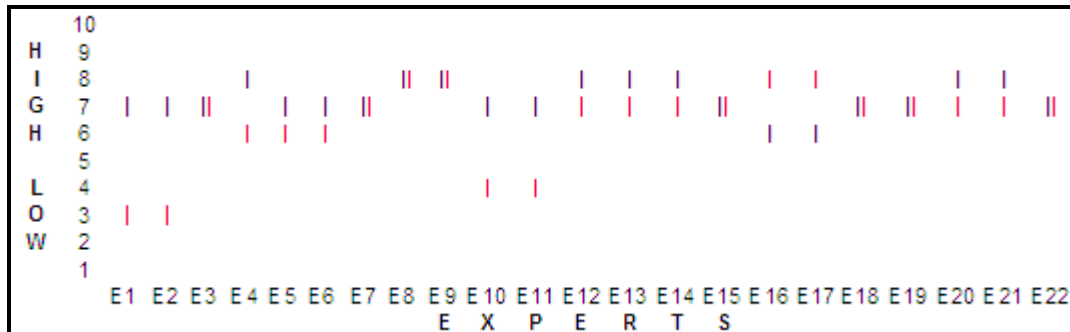
3. Usability of Policy Baseline



4. Feasibility of Conformance



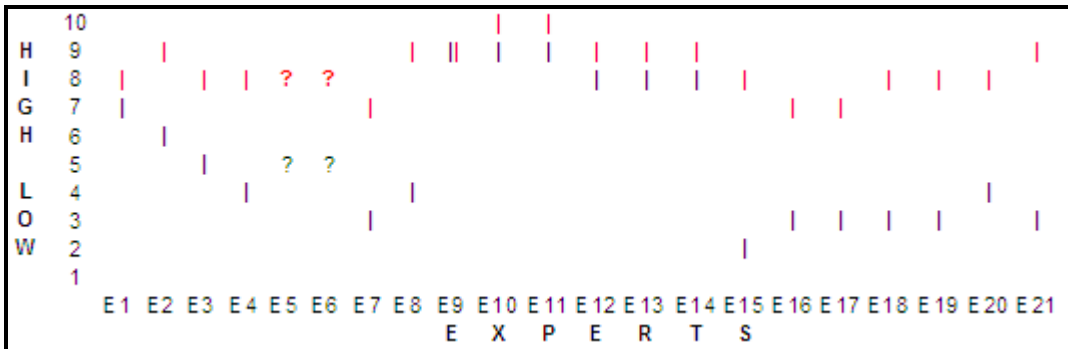
5. Difficulty of Developing a Policy Baseline



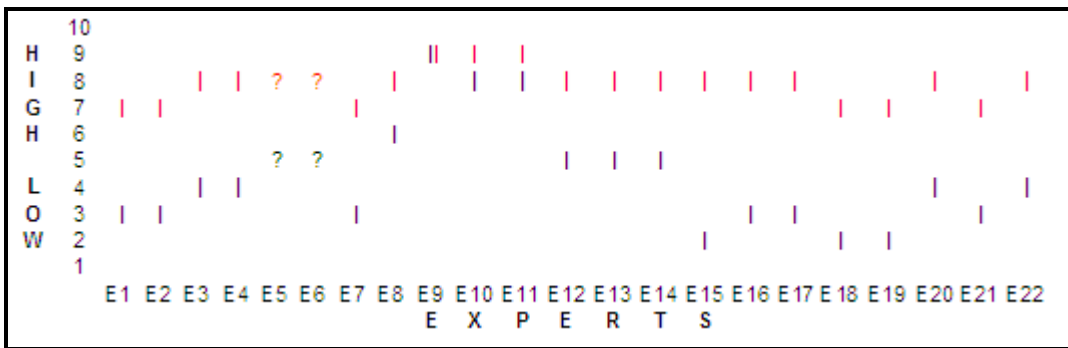
6. Scope of the Issue



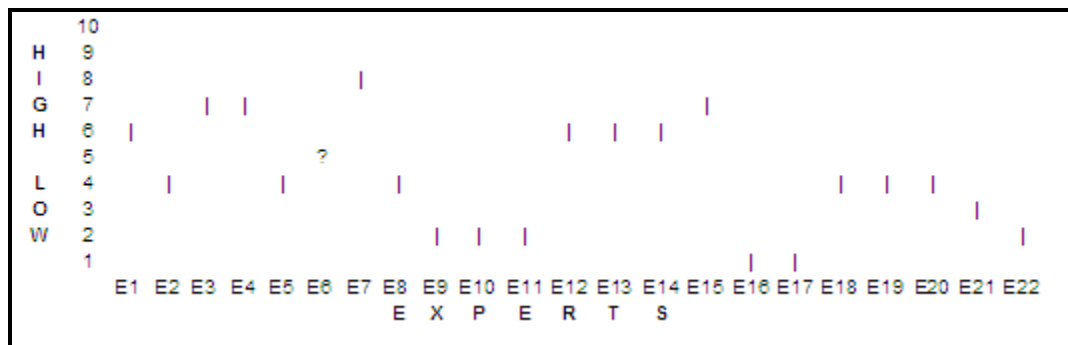
7. Relevance of International Organization



8. Involvement of Private Sector



9. Extent of Information (at Present and Desired)



10. Efficacy of Regulation

Inquiry	Division	Rate		Remark
		Average	Std. Deviation	
Criticality of Mobile Telephony	Present	7.6	1.5	Relatively High
	Future	9.1	0.6	Very High
Urgency of the Issue	Developing Countries	9.2	0.5	Very High
	Developed Countries	6.1	1.1	Average
Usability of the Policy Baseline	Strengths	7.5	1.4	Relatively High
	Weaknesses	6.0	0.7	Average
	Opportunities	7.5	0.8	High
	Threats	6.0	0.9	Average
Feasibility of the Policy Baseline	Desirability	6.8	1.6	Average
	Practicability	6.9	1.2	Average
Difficulty in Developing the Policy Baseline	Intergovernmental	6.5	1.4	Average
	Public-Private Partnership	4.0	1.6	Relatively Low
Scope of the Issue	National Government	7.2	0.6	High
	Inter-governmental	6.4	1.5	Average
Relevance of International Organization	---	7.7	1.3	Relatively High
Involvement of the Private Sector	Present	5.4	2.5	Relatively Low
	Desired	8.4	0.9	High
Extent of Information Sharing	Present	4.4	2.1	Low
	Desired	7.9	0.7	High
Efficacy of Regulation	---	4.1	1.9	Low

Explanation of Remark

Remark	Rate (Combination of Average & Std. Deviation)	Meaning
Very High	Ave.: 8.5 to 10 Std. Dev.: does not matter	The issue raised is of high importance and demands strong consideration
High	Ave.: 7 to 8.5 Std. Dev.: 0 to 1	The issue raised is of high importance and demands due deliberation
Relatively High	Ave.: 7 to 8.5 Std. Dev.: 1 and above	The issue raised is important and demands a discussion
Average	Ave.: 5.5 to 7 Std. Dev.: does not matter	The issue raised is in ambiguous status. It is not known if it has to be given consideration or just ignore.
Relatively Low	Ave.: 3.5 to 5.5 Std. Dev.: 1 and above	The issue raised is of low importance but should be taken a look
Low	Ave.: 3.5 to 5.5 Std. Dev.: 0 to 1	The issue raised is of low importance and can be ignored
Very Low	Ave.: 0 to 3.5 Std. Dev.: does not matter	The issue raised has very low importance and recommended to ignore

B. Electronic Communications Vulnerabilities

The tables that follow are output of the study of ARECI (2007) on the inquiry of vulnerabilities of electronic communications infrastructure. These vulnerabilities are applicable also to mobile telephony infrastructure. The first table shows the eight dimensions of the operation and their definition, the second one lists down the vulnerabilities according to the defined dimensions.

B1. Dimensions of Electronic Communications Infrastructure (ARECI study, 2007)

The Eight Dimensions in the Operation of Electronic Communications Infrastructure

Human

- the personnel involved in the operation of infrastructure

Policy

- the behaviors between entities, namely agreements, standards, policies and regulations (ASPR), national and international scopes, as well as Federal, State and local levels, other legal issues, and any other arrangement between entities, including industry cooperation and other interfaces

Hardware

- the hardware frames, electronic circuit packs and cards, and metallic and fibre optic transmission cables and semiconductor chips

Software

- the physical storage of software releases, development and test loads, version control and management, and software delivery controls.

Networks

- the configuration of nodes and their interconnection, network topologies and architectures, various types of networks, technology, synchronisation, redundancy, and physical and logical diversity, and network design, operation and maintenance

Payload

- the information transported across the infrastructure, traffic patterns and statistics, information interception, and information corruption. It includes both normal and signalling and control traffic

Environment

- buildings, trenches where cables are buried, space where satellites orbit, locations of microwave towers and cell sites, and the ocean where submarine cables reside.

Power

- the internal power infrastructure, batteries, grounding, high voltage and other cabling, fuses, back-up emergency generators and fuel

B2. Vulnerabilities of Each of the Eight Dimensions (ARECI study, 2007)

<p style="text-align: center;">Human Vulnerability</p> <p>physical (limitations, fatigue) cognitive (distractibility, forgetfulness, ability to deceive, confusion) ethical (divided loyalties, greed, malicious intent), user environment (user interface, job function, corporate culture) human-user environment interaction</p>	<p style="text-align: center;">Policy Vulnerability</p> <p>lack of ASPR (agreements, standards, policies, regulations) conflicting ASPR, outdated ASPR unimplemented ASPR (complete or partial) interpretation of ASPR (mis- or multi-) inability to implement ASPR enforcement limitations boundary limitations pace of development information leakage from ASPR processes inflexible regulation excessive regulation predictable behaviour due to ASPR</p>
<p style="text-align: center;">Hardware Vulnerability</p> <p>chemical (corrosive gas, humidity, temperature, contamination) electric (conductive microfibre particles – carbon bombs) radiological contamination physical (shock, vibration, strains, torque) electromagnetic energy (EMI, EMC, ESD, RF, EMP, HEMP, IR) Environment (temperature, humidity, dust, sunlight, flooding) life cycle (sparing, equipment replacement, ability to repair, aging) logical (design error, access to, self test, self shut off)</p>	<p style="text-align: center;">Software Vulnerability</p> <p>ability to control (render a system in an undesirable state, e.g., confused, busy) accessibility during development (including unsegregated networks) accessible distribution channels (interception) accessibility of rootkit to control kernel/core developer loyalties errors in coding logic complexity of programs discoverability of intelligence (reverse engineer, exploitable code disclosure) mutability of deployed code (patches) incompatibility (with hardware, with other software)</p>
<p style="text-align: center;">Network Vulnerability</p> <p>capacity limits points or modes of failure points of concentration (congestion) complexity dependence on synchronisation interconnection (interoperability, interdependence, conflict) uniqueness of mated pairs need for upgrades and new technology automated control (via software) accessibility (air, space or metallic or fibre) border crossing exposures</p>	<p style="text-align: center;">Payload Vulnerability</p> <p>unpredictable variation extremes in load corruption interception emulation encapsulation of malicious content authentication (mis-authentication) insufficient inventory of critical components encryption (prevents observability)</p>
<p style="text-align: center;">Environment Vulnerability</p> <p>accessible exposed to elements dependence on other infrastructures contaminate-able Subject to surveillance continuously being altered identifiable remotely managed non-compliance with established protocols and procedures</p>	<p style="text-align: center;">Power Vulnerability</p> <p>uncontrolled fuel combustion fuel contamination fuel dependency battery combustion battery limitations battery duration Maintenance dependency require manual operation power limitations frequency limitations Susceptibility to spikes physical destruction</p>

C. Description of GSM Family

C1. GSM-Based Technologies

The GSM Family presently consists of the following technologies: GSM, GPRS, EDGE, 3GSM (UMTS) and HSPA. GSM platform is living, growing and evolving offering an expanded and feature-rich “family” of voice and multimedia services (GSMA, 2008).

GSM General Description

Originally Groupe Spécial Mobile, the Global System for Mobile Communications (GSM) has evolved to become the most popular global mobile phone standards (Wikipedia, 2008). The GSM Association estimates that 86%, as of June 2008, of global market uses GSM standard (GSMA, 2007). Its ubiquity makes international roaming possible among mobile operators enabling GSM subscribers to use their mobile phones in almost anywhere in the world. This gives seamless and same standardized number of contactability in more than 170 countries. GSM satellite roaming has extended service access to areas where terrestrial coverage is unavailable (GSMA, 2008). Not only to the subscribers, network operators derive advantage also to the ubiquity of the infrastructure through economics of scale and scope that allow them to purchase and install GSM equipment from many vendors employing GSM standards at a reasonable cost. Another advantage is that the standard includes a worldwide emergency telephone number (112) that makes it easier for international travelers to connect to emergency services without knowing the local emergency numbers (Wikipedia, 2008). Release '97 of the revised GSM standard added packet data capabilities, by means of General Packet Radio Service (GPRS). Release '99 of the revised GSM standard introduced higher speed data transmission using Enhanced Data Rates for GSM Evolution (EDGE).

Brief Technical Description

GSM is a cellular network, which means that mobile connection is established through the immediate cells available in the vicinity. It differs from first generation wireless systems in the sense that it uses digital technology and time division multiple access transmission methods. Voice is digitally encoded via a unique encoder, which emulates the characteristics of human speech. This method of transmission permits a very efficient data rate/information content ratio (GSMA, 2008). Most GSM networks operate in the 900 MHz and 1800 MHz or 1900 MHz bands. GSM uses a variation of Time Division Multiple Access (TDMA). It digitizes and compresses data and sends it down a channel with two other streams of user data, each in its own time slot (GSM Security, 2008). In the 900 MHz band, the uplink frequency band is 890 to 915 MHz, and the downlink frequency band is 935 to 960 MHz. This 25 MHz bandwidth is subdivided into 124 carrier frequency channels, each spaced 200 KHz apart (Wikipedia, 2008). Time division multiplexing allows eight full-rate speech channels per radio frequency channel. There are eight-radio timeslots group into what is called TDMA frame. The GSM system is divided into a number of sections: the Base Station Subsystem, which includes the base stations and their controllers, the Network and Switching Subsystem, which is the part of the network most similar to a fixed network and is sometimes called the core network, the GPRS Core Network, which is the optional part that allows packet based internet connections. All of the elements in the system combine to produce many GSM services such as voice calls and SMS (Wikipedia, 2008).

GPRS General Description

General Packet Radio Service (GPRS) is a connectivity solution based on Internet Protocols (IP) that supports a wide range of enterprise and consumer applications (GSMA, 2008). GPRS customers enjoy advanced, feature-rich data services as internet browsing, mobile email, video streaming, multimedia messages and location-based services. For operators, the adoption of GPRS is a fast and cost-effective strategy that not only supports the first wave of mobile internet services but also represents a big step towards 3GSM (or wideband-CDMA) networks and services (GSMA, 2008). GPRS is a packet-switched service, as opposed to circuit switching, where Quality of Service (QoS) is guaranteed during the connection for non-mobile users. 2G cellular systems combined with GPRS are often described as 2.5G, that is the technology in between 2G and 3G. It provides moderate speed data transfer by using unused TDMA channels of GSM system. GSM is the only kind of networks where GPRS is in use (Wikipedia, 2008).

GPRS Technical Description

Wireless Application Protocol (WAP) is a gateway to access the Internet via mobile phone and vice versa. GPRS data are billed per kilobyte of information transceived, while circuit-switched data connections are billed per minute. In circuit-switched, the bandwidth is used and unavailable to other users even no data are being transferred (Wikipedia, 2008). The multiple access methods used in GSM with GPRS are based on frequency division duplex and TDMA. A user during a session is assigned to one pair of up-link and down-link frequency channels, which is combined with time domain statistical multiplexing that makes it possible for several users to share the same frequency channel. The packets have constant length, corresponding to a GSM time slot (Wikipedia, 2008). The class of the device determines the speed at which GPRS can be used. Class A mobile phones can be connected to both GPRS and GSM services simultaneously. Class B mobile phones can be attached to both GPRS and GSM services, using one service at a time. During voice calls or SMS, GPRS services are suspended and then resumed automatically after the call or SMS session has ended. Class C mobile phones are attached to either GPRS or GSM voice service and one needs to switch manually between services (GSMA, 2008).

EDGE General Description

Enhanced Data rates for GSM Evolution (EDGE) provides further enhancement to GSM networks through increasing data transmission rates and improving data transmission reliability. EDGE provides up to three times the data capacity of GPRS (GSMA, 2008). Operators can handle three times more subscribers than GPRS. It triples their data rate per subscriber and adds extra capacity to their voice communications. EDGE allows the delivery of advanced mobile service such as downloading of video and music clips, full multimedia messaging, high-speed colored internet access and email on the move. Due to the very small incremental cost of including EDGE capability in GSM network deployment, virtually all new GSM infrastructure deployments are also EDGE capable and nearly all new mid- to high-level GSM devices also include EDGE radio technology (GSMA, 2008)

Brief Technical Description

EDGE uses the same TDMA (Time Division Multiple Access) frame structure, logic channel and 200kHz carrier bandwidth as today's GSM networks, which allows it to be overlaid directly onto an existing GSM network. For many existing GSM/GPRS networks, EDGE is a simple software-upgrade (GSMA, 2008). EDGE is implemented as a bolt-on enhancement for 2G and 2.5G GSM and GPRS networks, making it easy for existing GSM carriers to upgrade into it. Although EDGE requires no hardware or software changes to be made in GSM core networks, base stations must be modified. EDGE compatible transceiver units must be installed and the base station subsystem needs to be upgraded to support EDGE. New mobile terminal hardware and software is also required to decode/encode the new modulation and coding schemes and carry the higher user data rates to implement new services.

3GSM General Description

3GSM is the marketed form of Universal Mobile Telecommunications System (UMTS). 3GSM emphasizes the combination of the 3G nature of the technology and the GSM standard in which it was designed to succeed. 3GSM is the latest addition to the GSM family. It enables the provision of mobile multimedia services such as music, TV and video, rich entertainment content and Internet access. The technology on which 3GSM services are delivered is based on a GSM network enhanced with a Wideband-CDMA (W-CDMA) air interface - the over-the-air transmission element. Global operators, in conjunction with the 3G Partnership Project (3GPP) standards organization, have developed 3GSM as an open standard (GSMA, 2008).

Brief Technical Description

3GSM or UMTS combines W-CDMA interfaces, TD-CDMA or TD-SCDMA air interfaces, GSM Mobile Application Part core and the GSM family of speech codecs. For existing GSM operators, it is a simple but costly migration to 3GSM. Much of the infrastructure is shared with GSM but the cost of obtaining new spectrum licenses and overlaying 3GSM (or UMTS) at existing towers can be prohibitively expensive (Wikipedia, 2008). The specific frequency bands defined by 3GSM (UMTS) standards are 1885–2025 MHz for the mobile-to-base (uplink) and 2110–2200 MHz for the base-to-mobile (downlink). The use of the W-CDMA air interface significantly increases the data transfer rate of GSM networks, offering average downlink rates of around 300 kbit/s (GSMA, 2008).

HSPA General Description

High Speed Data Packet Access (HSPA) is a collection of mobile telephony protocols that extend and improve the performance of existing UMTS protocols. Two standards, HSDPA and HSUPA, have been established and a further standard, HSPA+, is soon to be released (Wikipedia, 2008). HSPA offers higher data transfer speeds and greater system capacity that will enhance their ability to provide mobile broadband multimedia services. It will tap the generic benefits of GSM such as global roaming, seamless billing, network compatibility and huge economies of scale (GSMA, 2008).

Brief Technical Description

The two existing standards (HSDPA and HSUPA) in the family provide increased performance by using improved modulation schemes and by refining the protocols by which handsets and base stations communicate. These improvements lead to a better utilization of the existing radio bandwidth provided by 3GSM (or UMTS). Many HSPA rollouts can be achieved by a software upgrade to existing 3G networks, which requires dedicated network infrastructure (Wikipedia, 2008).

C2. Timeline of GSM and 3G Technologies

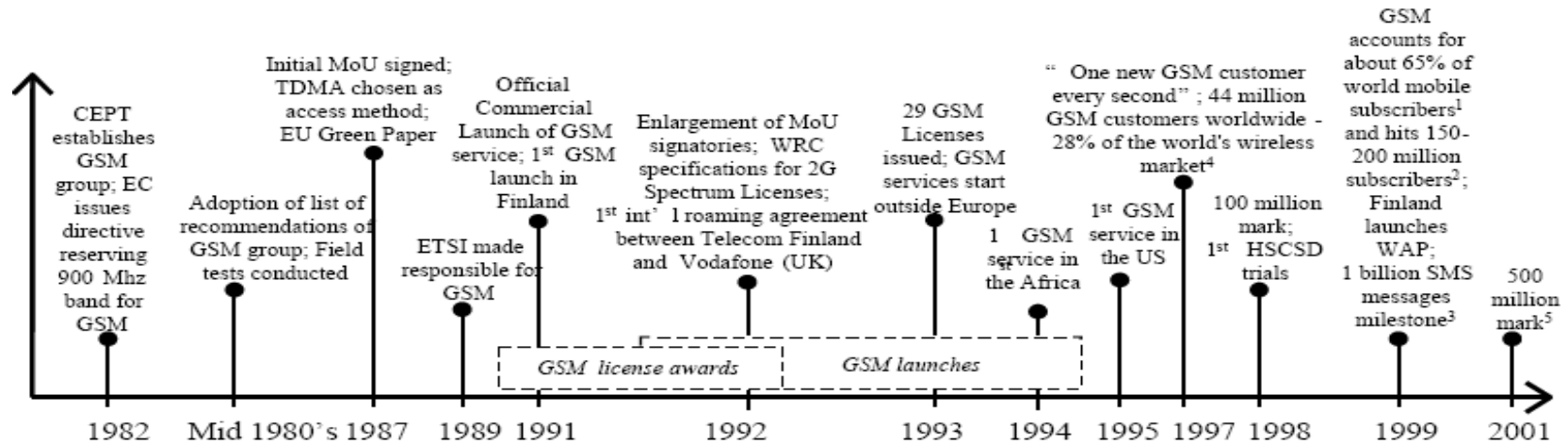


Figure 26: GSM Timeline (Source: ITU)

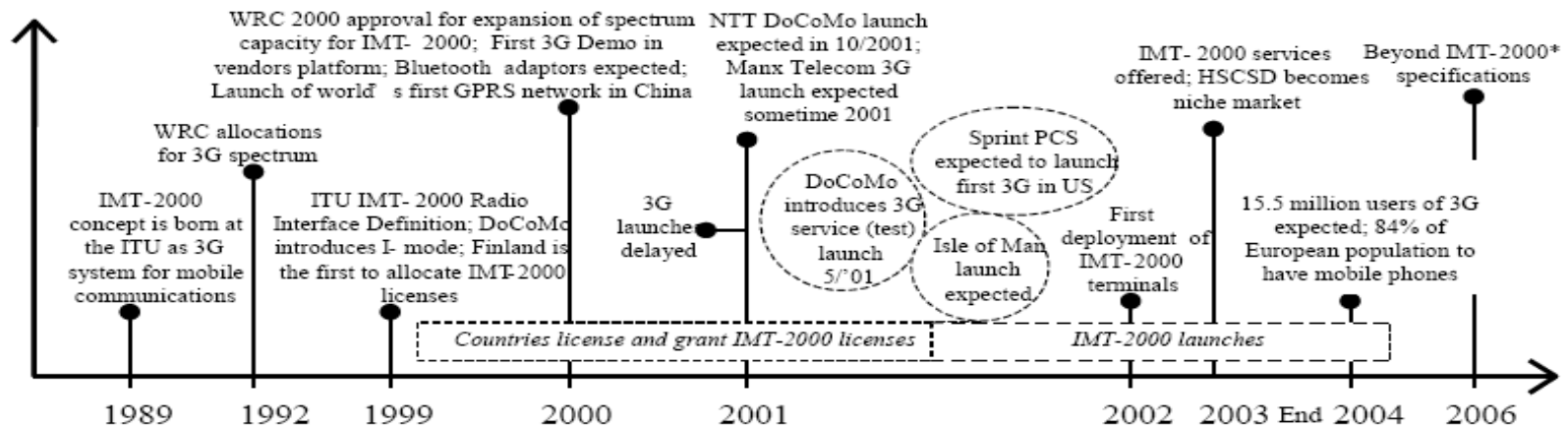
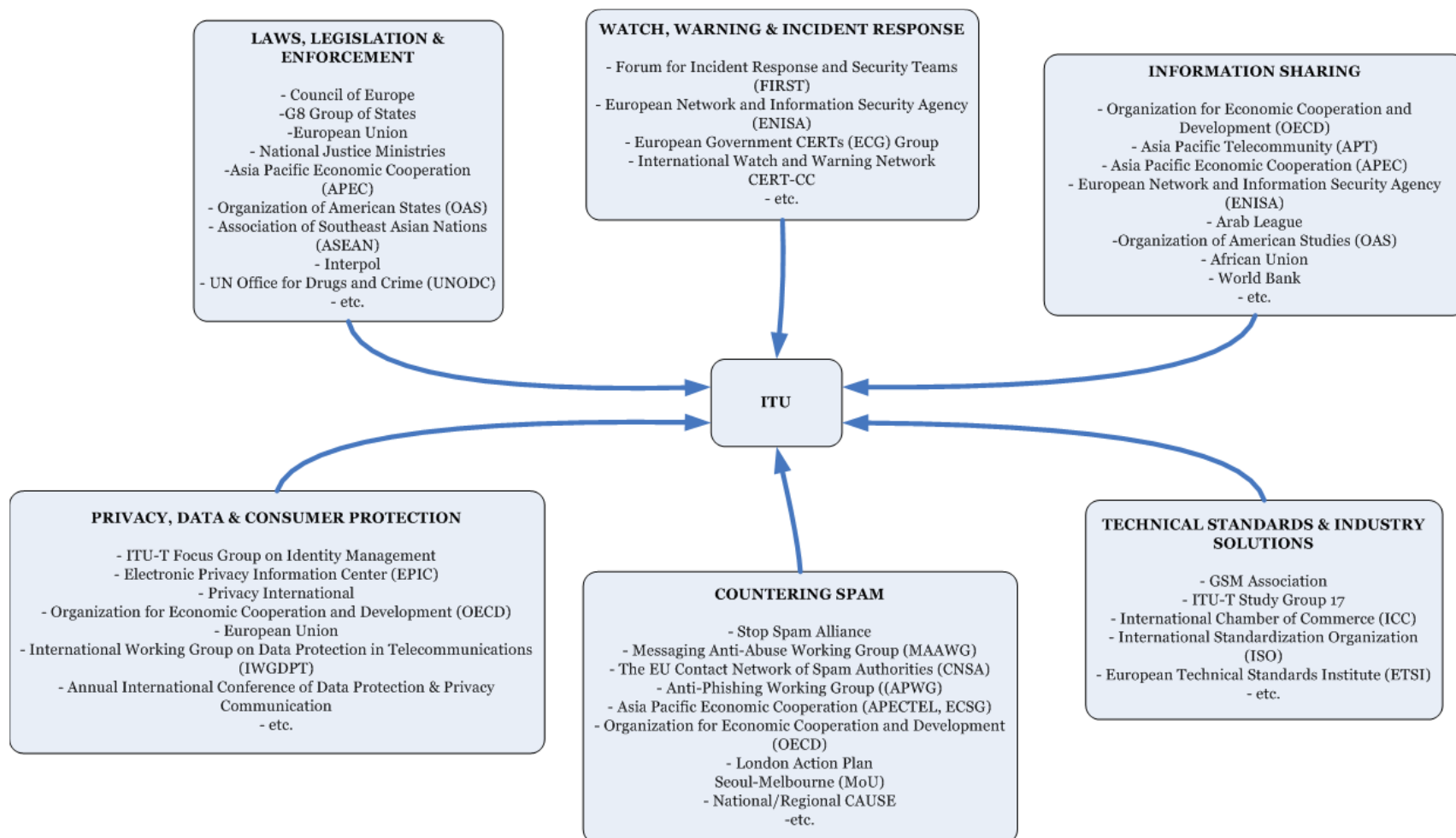


Figure 27: 3G Timeline (Source: ITU)

D. Ecosystem for Infrastructure Assurance with ITU as the facilitating organization (Source: ITU, 2008)



E. Mobile Telecommunications Market in the Philippines

E1. Brief Description of the Philippine Market (Source: (Kelly et al., 2002)

The Philippines mobile cellular market is diverse, with five companies operating seven networks (2 AMPS, 1 CDMA, 1 TACS, and 3 GSM). The market is dominated by two players, PLDT and Globe Telecom, which are both using the GSM technology. PLDT wholly-owns SMART communications and majority-owns Piltel, while Globe Communications purchased Isiacom. These two companies – PLDT and Globe – control 98% percent of all subscribers. The dominance of GSM is almost complete. The Filipino market is one of the fast expanding in the world. Mobile telephony is a way of life in the country and since early 2000, the predominant method of telephone communications. The Philippines became the 13th country in the world where mobile phones passed fixed-lines. Unlike fixed-telephone lines where the Philippines is still playing catch-up, the nation's mobile density is way above the Southeast Asia average.

The factors that drive this rapid mobile growth are the following:

1. One reason is the large number of full service operators. The decision to allow five mobile operators from the mid-1990s made the Philippines one of the most competitive markets in the region. Most of the operators also had international licenses, which made it easier to keep mobile tariffs down. The Philippines has among the lowest tariffs in the region.
2. The second factor was the huge pent-up demand. Though cellular operators had obligations to install several million fixed-lines, there appears to have been a mismatch between supply and demand. Fixed-lines were installed in places where people did not need them, or for prices that they could not afford. Mobile, on the other hand, went where the demand was and thus substituted for fixed line. Mobile was a more attractive proposition not because it was cheaper but it was easier to acquire and prepaid meant that everybody could subscribe.
3. Finally, the craze over Short Messaging System (SMS) drove people to mobile, particularly the fact that mobile text messages are either free or cheaper than a regular mobile call. Mobile has spread like wild fire. Arguably, more Filipinos are within the range of a mobile signal than a fixed-telephone line.

These factors make the Filipino mobile market one of the most dynamic and closely observed mobile markets in the world. The Philippines leads the world in per capita SMS use and is quite advanced in other mobile data applications, considering it is a developing country.

The European engineers who defined the GSM standard did not imagine that their throwaway service would find its apotheosis in the Philippines. SMS creates a considerable revenues for the Philippines' two main mobile operators, Smart and Globe. SMS played an important part in the recent Filipino history. When President "Erap" Estrada refused to stand down, amidst being implicated in a corruption scandal, Filipinos used SMS to coordinate demonstrations that eventually led to his downfall –so called "People Power II". The present administration finds many applications of SMS in providing better governance.

E2. Mobile Telephony Products and Services of the Two Leading Philippine Network Operators

The two tables below show the various products and services of the two leading mobile telephony operators in the Philippines.

E.2.1 Smart Communications

(Source: <http://smart.com.ph/>, Accessed: July 23, 2008)

Smart Communications	
Product/Service	Description
1. Smart Money	Cashless base transaction in a reloadable cash card linked to the Mastercard network
2. Smart Padala	Cash remittance service via text, from a sender outside the Philippines to the cellphone of a beneficiary in Philippines

3. Smart Bro	Direct-To-Home Wireless Internet from Smart base stations
4. Smart 3G	Smart 3G UMTS network that includes video calls, video streaming, high-speed internet browsing
5. Smart Zed	Multi-platform information and entertainment products and services; offers people on the move an access to entertainment, communication and information services, which include games, messaging services and stock prices.
6. Smart Gold	Postpaid plan
7. Smart Infinity	Premium High-End postpaid service
8. Smart Buddy	Prepaid service
9. Smart Kid	Kids' mobile service in prepaid and postpaid
10. Talk N' Text	Low rate Prepaid Sim Card
11. Smart Link	Calling through Satellite receivers
12. Smart ACeS	The Same with smart Link
13. Smart Talk	Payphone with Texts features from smart
14. Addict Mobile	Special Mobile for older teens

E.2.2 Globe Telecom

(Source: <http://www1.globe.com.ph/index.aspx>, Accessed: August 1, 2008)

Globe Telecom	
Product/Service	Description
1. GCash	Access to a cashless and cardless method of facilitating money remittance, donations, loan settlement, disbursement of salaries or commissions, and payment of bills, products and services through a text message
2. Mobile Infotext	Retrieve information through your mobile phone by simply texting an Infotext keyword and sending it to an access number. Available infotext guides: BDO Cash Card, Bank of the Philippine Islands (BPI), HSBC Mobile Banking, myGlobe Tracker
3. Globe Kababayan	Offers services catering to the Overseas Filipino Workers (OFW) – from international remittance to prepaid cards and e-pins
4. Globe Ties	Messaging services to help Filipinos keep constantly in touch with their loved ones across the miles
5. Share-A-Load	Transfer prepaid call and text credits on Globe Prepaid and Touch Mobile via of text message
6. Globe Autoload	Online electronic loading service that allows automatically reloading of credits
7. G-Flex	Consumable plan
8. G-Plan	Call and data
9. GlobeQUEST DSL	Broadband access offering speedy Internet browsing, fast file transfers, an "Always-On" connection, and other extras
10. Visibility	Provides data access via different forms of internet access like GPRS, EDGE, WiFi, and dial-up
11. Globe Touchpoint	Provides 24-hour access to bank accounts and hosts internet banking, mobile banking, and phone banking

F. Relevant Statistics (Source: GSMA, 2008)

1. 85% of world's mobile communications are GSM.
2. 64% of world mobile users are in emerging markets.
3. 85% of the one million new mobile phone subscribers every day are from emerging economies
4. More than 80% of the world's population are covered by GSM networks.
5. People spend 40% more time on mobile calls than they did in 2000.
6. There are 2.6 billion GSM connections worldwide.
7. There are 1.2 million new GSM connections everyday.
8. In 2006, cellular service accounted for 1.6% of the global economy.
9. The world will reach 4 billion mobile communications in the first quarter of 2010.
10. The world's biggest markets are China (483m), India (176m), and Russia (168m).
11. All 220 countries in the world have GSM or 3GSM networks operating today.
12. 350 million people will have access to wireless email by 2010.
13. There are more than 190 million 3GSM connections.
14. It took 12 years to get to 1 billion GSM connections and just 30 months to get 2 billion.
15. Nearly 7 billion text messages are sent everyday.
16. Mobile Broadband (HSPA) networks have been launched in over 70 countries.

G. ITU-T Telecommunications Security Standards

Security Architecture and Frameworks

- X.800 – Security architecture
- X.802 – Lower layers security model
- X.803 – Upper layers security model
- X.810 – Security frameworks for open systems: Overview
- X.811 – Security frameworks for open systems: Authentication framework
- X.812 – Security frameworks for open systems: Access control framework
- X.813 – Security frameworks for open systems: Non-repudiation framework
- X.814 – Security frameworks for open systems: Confidentiality framework
- X.815 – Security frameworks for open systems: Integrity framework
- X.816 – Security frameworks for open systems: Security audit and alarms framework

Telecommunication Security

- E.408 – Telecommunication network security requirements
- E.409 – Incident organization and security incident handling: Guidelines for telecommunication organizations
- X.805 – Security architecture for systems providing end-to-end communications
- X.1051 – Information security management system – Requirements for telecommunications (ISMS-T)
- X.1081 – A framework for the specification of security and safety aspects of telebiometrics
- X.1121 – Framework of security technologies for mobile end-to-end communications
- X.1122 – Guideline for implementing secure mobile systems based on PKI

Protocols

- X.273 – Network layer security protocol
- X.274 – Transport layer security protocol

Security in Frame Relay

- X.272 – Data compression and privacy over frame relay networks

Security Techniques

- X.841 – Security information objects for access control
- X.842 – Guidelines for the use and management of Trusted Third Party (TTP) services
- X.843 – Specification of TTP services to support the application of digital signatures

Directory Services and Authentication

- H.350 – Series – Directory services architecture for multimedia conferencing
- X.500 – Overview of concepts models and services
- X.501 – Models
- X.509 – Public-key and attribute certificate frameworks
- X.519 – Protocol specifications

Network Management Security

- M.3010 – Principles for a telecommunication management network
- M.3016 – TMN security overview
- M.3210.1 – TMN management services for IMT-2000 security management
- M.3320 – Management requirements framework for the TMN X-Interface
- M.3400 – TMN management functions

Systems Management

- X.733 – Alarm reporting function
- X.735 – Log control function
- X.736 – Security alarm reporting function
- X.740 – Security audit trail function
- X.741 – Objects and attributes for access control

Televisions and Cable Systems

- J.91 – Technical methods for ensuring privacy in long-distance international television transmission
- J.93 – Requirements for conditional access in the secondary distribution of digital television on cable television systems
- J.170 – IP-Cablecom security specification

Multimedia Communications

- H.233 – Confidentiality system for audiovisual services
- H.234 – Encryption key management and authentication system for audiovisual services
- H.235 – Security and encryption for H-series multimedia systems
- H.323 Annex J – Packet based multimedia communications systems – Security for simple endpoint types
- H.530 – Symmetric security procedures for H.323 mobility in H.510
- T.123 Annex B – Network-specific data protocol stacks for multimedia conferencing: extended transport connections

Facsimile

- T.36 – Security capabilities for use with Group 3 facsimile terminals
- T.503 – A document application profile for the interchange of Group 4 facsimile documents
- T.563 – Terminal characteristics for Group 4 facsimile apparatus

Message Handling Systems (MHS)

- X.400 / F.400 – Message handling system and service overview
- X.402 – Overall architecture
- X.411 – Message transfer system: Abstract service definition and procedures
- X.413 – Message store: Abstract service definition
- X.419 – Protocol specifications
- X.420 – Interpersonal messaging system
- X.435 – Electronic data interchange messaging system
- X.440 – Voice messaging system

H. ITU and its Infrastructure Assurance Initiatives in Telecommunications

The International Telecommunications Union (ITU) is a specialized United Nations agency for telecommunications and Information and Communications Technologies (ICT). As the global platform for governments and the private sector, ITU's role spans 3 core sectors: radiocommunication (ITU-R), standardization (ITU-T), and development (ITU-D). It also organizes Telecom events and the leading organizing agency of the World Summit on Information Society (WSIS). Membership of ITU is open to governments, private organizations such as carriers, equipment manufacturers, funding bodies, research and development organizations, and international and regional telecommunication organizations. ITU presently has a membership of 198 member states, 568 sector members, and 150 associates. (Source: <http://www.itu.int/members/index.html>, Accessed: June 28, 2008)

ITU-T Telecommunications Security Initiatives

ITU-T holds a unique position in the field of standardization. Its work brings together the private sector and governments to coordinate work and promote the harmonization of security policy and security standards on an international level. Standards help create confidence among providers and end-users that technologies and products have been tested and ensure a known level of performance. ITU's work on security covers a broad range of activities in security from network attacks, theft or denial of service, theft of identity, eavesdropping, tele-biometrics for authentication, security for emergency telecommunications and telecommunication network security requirements. The standard for framework of security technologies for mobile end-to-end communications (X.1121) and the standard guideline for implementing secure mobile systems based on PKI (X.1122) were released in 2004 (in which deliberation was started in 2001). There are standards for mobile security presently developed until 2008, namely X.1123 (for differentiated security services for secure mobile end-to-end data communication), X.1124 (for authentication architecture) and X.1125 (for correlative reacting system in mobile data communication). Within ITU-T, there are 13 technical Study Groups (SGs) who are carrying out the standardization work, and SG 17 has been the designated lead Study Group for Telecommunication Security. (Source: www.itu.int/ITU-T, Accessed June 28, 2008).

ITU-D Critical (Information) Infrastructure Initiatives

ITU-D was established to help spread equitable, sustainable and affordable access to information and communication technologies (ICT) as a means of stimulating broader social and economic development. Through a series of regional initiatives together with comprehensive national programmes, activities on the global level and multiple targeted projects, the Sector works with partners in government and industry to mobilize the technical, human and financial resources needed to develop ICT networks and services to connect the unconnected. ITU-D has been designated by World Telecommunication Development Conference 2006 to make cybersecurity/CIIP as top priority in its initiatives. While some countries are advanced in the formulation of national cybersecurity/CIIP strategies, many developing countries are oblivious or are only just starting to consider the necessary measures to undertake. Developing countries have limited human, institutional, and financial resources to elaborate and implement national policies and frameworks for cybersecurity and CIIP. At present, there is no separate initiative for mobile security in ITU-D. Mobile security is part of the cybersecurity/CIIP initiatives. ITU-D has outlined the framework into five elements, including: 1.) developing a national cybersecurity strategy; 2.) establishing national government-industry collaboration; 3.) creating a national incident management capability; 4.) deterring cybercrime; and 5.) promoting a national culture of cybersecurity. (Source: <http://www.itu.int/ITU-D/cyb/cybersecurity/>, Accessed: June 29, 2008)

ITU-R Initiatives in Security

ITU-R is responsible for managing the international radio-frequency spectrum and satellite orbit resources. It allocates spectrum and register frequency assignments, orbital positions and other parameters of satellites, in order to avoid harmful interference between radio stations of different countries. ITU-R further carries out studies for the development of radiocommunication systems used in disaster mitigation and relief operations. When the "wired" telecommunication infrastructure is significantly or completely destroyed following a disaster, radiocommunication services are the most effective in disaster relief operations. Safeguarding quality of service against degradation or denial of service is vital for the secure functioning of networks in data transmission and service provision. Many of ITU-R recommendations on generic requirements and the protection of radiocommunications against interference are relevant for security. ITU-R established clear security principles for IMT-2000 (3G) networks in which it puts forward that the security provided by mobile broadband should be comparable to contemporary fixed networks. (Source: <http://www.itu.int/ITU-T/studygroups/com17/ict/index.html>, Accessed: June 29, 2008)

I. References

- Abele-Wigert, I. (2006) Challenges Governments Face in the Field of Critical Information Infrastructure Protection: Stakeholders and Perspectives. International CIIP Handbook 2.
- ACIP Consortium. (2003) Analysis and Assessment for Critical Infrastructure Protection (ACIP) final report, EU/DG Information Society and Media, Brussels, Belgium.
- Andersson, J., & Malm, A. (2006) Public-Private Partnerships and the Challenge of Critical Infrastructure Protection. International CIIP Handbook.
- Assaf, D. (2008) Government Intervention in Information Infrastructure Protection. IFIP International Federation for Information Processing, Critical Infrastructure Protection, eds. E. Goetz and S. Sheno; (Boston: Springer) 253, pp. 29-39.
- Aviram, A., & Tor, A. (2004) Overcoming impediments to information sharing, *Alabama Law Review*, vol. 55(2), p. 231.
- Birke, D., & Swann, P. (2005) Network effects and the choice of mobile phone operator, Springer-Verlag
- Block, W. (1983) Public Goods and Externalities. *HJournal of Libetarian Studies*.
- BMI. (2008a) Protecting Critical Infrastructures –Risk and Crisis Management : A guide for companies and government authorities.
- BMI. (2008b) Protecting Critical Infrastructures –Risk and Crisis Management, Federla Ministry of the Interior, Germany.
- Boin, A., & McConnell, A. (2007) Unravelling the Puzzles of Critical Infrastructures, pages 1-3.
- Borodzicz, E. (2005) Risk, Crisis and Security Management. New York: Wiley.
- Chambers, J. (2004) Vulnerability Disclosure Framework, Final Report and Recommendations by the Council.
- Cohen, A. P. (1985) *The Symbolic Construction of Community*. Routledge: New York.
- Colonel, S. (2001) *The Media, the Market and Democracy: The Case of the Philippines*. Philippine Centre for Investigative Journalism.
- Commission, E. (2006) Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment to improve their protection. COM(2006) 787 final, Communication from the Commission to the Council and the European Parliament, Brussels,.
- Cukier, K. (2005) Ensuring (and Insuring?) Critical Information Infrastructure Protection. Rueschlikon Conference, pp. 12-17.
- De Bruijn, H. (2007) *Managing Performance in the Public Sector* (2nd Edition ed. Vol. 122 pages): Routledge.
- De Bruijne, M. (2006) *Networked Reliability: Institutional fragmentation and the reliability of service provision in critical infrastructures*: Febodruk BV, Enschede, The Netherlands.

- De Jong, M., Virginie, M., & Lalenis, K. (2003) *The Theory and Practice of Institutional Transplantation, Experiences with the Transfer of Policy Institutions*: Kluwer Academic Pub.
- De Vries, L. (2004) *Dissertation: Securing the public interest in electricity generation markets*, Delft University of Technology.
- Dunn, M. (2004) *Information Age Conflict: A study of the information revolution and a changing operating environment*, ETH Zurich.
- Dunn, M. (2006) *Understanding Critical Information Infrastructures: An Elusive Quest*. International CIIP Handbook 2.
- Dunn, M., & Abele-Wigert, I. (2006a) *International CIIP Handbook: An inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies (Vol. 1)*: Center for Security Studies, ETH Zurich.
- Dunn, M., & Abele-Wigert, I. (2006b) *International CIIP Handbook: An inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies*. Center for Security Studies, ETH Zurich 1493.
- Dunn, M., & Mauer, V. (2006) *Analyzing Issues, Challenges and Prospects*. International CIIP Handbook 2.
- Dynes, S., Goetz, E., & Freeman, M. (2008) *Cybersecurity: Are economic incentives adequate? Critical Infrastructure*.
- Education Commission. (2004) *From Competing to Leading: An International Benchmarking Blueprint*.
- Efendioglu, A., Yip, V., & Murray, W. (2001) *E-Commerce in developing countries: Issues and Influences*. University of San Francisco.
- Egyedi, T. (1996) *Shaping Standardization: A study of standards processes and standards policies in the field of telematic services*. Delft, The Netherlands: Delft University Press.
- Ellingsen, T., & Johannesson, M. (2007) *Pride and Prejudice: The Human Side of Incentive Theory*
- Farrell, H., & Knight, J. (2003) *Trust, Institutions, and Institutional Change: Industrial Districts and the Social Capital Hypothesis*, *POLITICS & SOCIETY*, Vol. 31 No. 4.
- Firth, L., Boersma, K., & Melody, B. (2006) *Infrastructure Concepts and Classifications: A Framework for Scenario Analysis of Infrastructures in an Economic Perspective*. DIOC Design and Management of Infrastructures.
- Forlin, M., Larcher, R., & Schivo, S. (2008) *Review of current use of mobile telephony in developing regions*.
- Ghosh, A., & Del Rosso, M. (1998) *The Role of Private Industry and Government in Critical Infrastructure Assurance*.
- Goertz, E., & Sheno, S. (2008) *Critical Infrastructure Protection*. IFIP International Federation for Information Processing.
- Gorman, S. P. (2005) *Networks, Security and Complexity* Edward Elgar Publishing Limited.

- Gow, G. A. (2005) Policymaking for critical infrastructure: a case study on strategic interventions in public safety telecommunications. England: Ashgate Publishing Limited.
- GSMA. (2007) <http://www.gsmworld.com/index.shtml>.
- Haimes, Y., Santos, J., Crowther, K., & Henry, M. (2006) Risk Analysis in Interdependent Infrastructures
- Hughes, T. P. (1987) The Evolution of Large Technological Systems: The Social Construction of Technological Systems. Cambridge, MIT Press.
- Hummel, J. R. (1990) National Goods Versus Public Goods: Defense, Disarmament, and Free Riders. *The Review of Austrian Economics*, Vol. 4, pp. 88-122.
- Kelly, T., Minges, M., Magpantay, E., & Firth, L. (2002) Pinoy Internet: Philippines Case Study, International Telecommunications Union, Geneva, Switzerland.
- Killen, P. (1982) Incentive Theory: Models of Choice. Arizona State University.
- Kinkade, S., & Verclas, K. (2008) Wireless Technology for Social Change: Trends in Mobile Use by NGOs, UN and Vodafone Group Foundation.
- Luijff, E., Burger, H., & Klaver, M. (Sept. 2003) Critical (information) Infrastructure Protection in The Netherlands, *Informatik 2003*,
- Luijff, E., Jadoul, M., & De Spiegeleiere, S. (2007) International Benchmarks for at least two LCCI: A preliminary WP3.6 deliverable to be actualised and integrated with the next D3.6.x deliverables, TNO Defence, Security and Safety.
- Luijff, E., Jadoul, M., & Spiegeleiere, S. (2006) Integrated Risk Reduction of Information-based Infrastructure Systems (IRRIIS). *Information Society Technologies*
- Luijff, E., Nieuwenhuijs, A., Klaver, M., Eeten, M. V., & Cruz, E. (2008) Empirical findings on Critical Infrastructure Dependencies in Europe. TNO and TBM TUDelft.
- Luijff, H. A. M., Burger, H. H., & Klaver, M. H. A. (2003) Bescherming Vitale Infrastructuur: Quick-scan naar vitale producten en diensten (managementdeel). [Critical Infrastructure Protection: Quick-scan of critical products and services – management report]. TNO, The Hague, The Netherlands, report FEL-03-C001.
- Maskin, E. (2001) Roy Radner and Incentive Theory. Institute for Advanced Study and Princeton University.
- Meggison, W., & Netter, J. (2001) From State To Market: A Survey Of Empirical Studies On Privatization, *Journal of Economic Literature*.
- Menski, W. (2005) *Comparative Law in a Global Context*, London: Cambridge University Press. page 39.
- Merkom, S. v. (2008) On Specific Elements of National Policies for Critical Infrastructure Protection in the ICT Sector.
- Moteff, J., & Parfomak, P. (2004) Critical Infrastructure and Key Assets: Definition and Identification. CRS Report for Congress.
- Nannestad, P., & Svendsen, S. (2005) Institutions, Culture, and Trust. *Quality of Government: What It Is, How to Get It, Why It Matters*, Gothenburg, Sweden.

- Nellis, J., & Kikeri, S. (2002) Privatization in Competitive Sectors: The Record to Date, World Bank Policy Research Working Paper No. 2860, World Bank.
- OECD. (1997) International Benchmarking: Experiences from OECD Countries.
- Papaioannou, T., Rush, H., & Bessant, J. (2006) Benchmarking as a policy-making tool: from the private to the public sector. Performance Management.
- Radics, G. (2004) Terrorism in Southeast Asia: Balikatan Exercises in the Philippines and the US 'War against Terrorism'. National University of Singapore.
- Riguidel, M. (2006) Security of Networks and Systems. École Nationale Supérieure des Télécommunications, 54 pages.
- Sherif, M. (1999) Contribution towards a theory of standardization in telecommunications. SIIT'99 Proceedings, IEEE.
- Spackman, M. (2002) Public-private partnerships: lessons from the British approach, Economic Systems, 26(3), 283–301.
- Stoneburner, G., Gogue, A., & Feringa, A. (2002) Risk Management Guide for Information Technology Systems. NIST.
- Treheux, M. (1992) Privatization and competition versus public service, Telecommunications Policy, Volume 16, Issue 9, Pages 756-758
- Walker, W., Rahman, S., & Cave, J. (2001) Adaptive policies, policy analysis, and policy-making. European Journal of Operational Research 128, pp. 282-289.
- Wash, R., & MacKie-Mason, J. (2006) Incentive-Centered Design for Information Security.
- Wikipedia. (2008) <http://en.wikipedia.org/wiki/GSM>.
- Yasin, M. (2002) The theory and practice of benchmarking: then and now, Benchmarking: An International Journal, 19(3), 217–243.
- Zairi, M. (1996) Benchmarking for best practice: Continuous learning through sustainable innovation,. Oxford: Butterworth-Heinemann.

PERSONAL NOTES

The thought of studying critical infrastructures started from my short internship in International Telecommunication Union in Geneva, Switzerland in the summer of year 2007. I give a gratitude to Mr. Robert Shaw and Ms. Christine Sund for their warm accommodation and for affording me the opportunity to be involved in the activities of the institution I have always aspired and wondered about since my electronics and communications engineering years. The “nerve” really brought me from the Philippines to Geneva for me to witness how the institution works and to get the vive of what it is to be like working in ITU. Since then, I have participated to a number of workshops and conferences in the area of critical infrastructures with the eye that the learning I would have would help me in my thesis work.

It was in ITU that I was able to know the name of Eric Luijff, my thesis external supervisor from TNO Defence, Security and Safety. He, together with his colleagues, had worked on a discussion paper about international policy framework for protecting critical information infrastructure. As I was tasked in my internship to look for CIIP materials, I was able to come across Eric’s work that inspired me and thought that maybe I could ask him to help me out in my thesis. Little did I know that he is, indeed, a “man of critical infrastructures” in the Netherlands and very active in this area. Almost all my European respondents know him and truly he is a “figure of CI” in the Netherlands. So I am humbled that I have an expert in the area of critical infrastructures in my thesis committee. Even more I was amazed by Eric’s very active participation in my research. He was very committed and very industrious to edit my work, even how voluminous my drafts were, he still provided time and effort to read and edit the full paper. His support was unfailing. He was present in all the thesis committee meetings amidst his very tight schedule. In the first stage of my study, he provided me hints about what specific area in critical infrastructure I would focus my research on. He was the person I asked what good to study in critical infrastructure--the idea of a policy baseline just arose from there. Most of the materials I have about CIP and most of the connections I had with my respondents are done through Eric’s assistance. “I thank you Eric for such a commitment amidst the fact that you are not from the academe and do not have much incentives to provide me assistance. I do not know how to pay you back but I hope that this collaboration you had with my research would provide a kind of fulfillment to you and would lead you to more fruitful undertakings in the area of critical infrastructures.”

I, then, looked for people in TBM faculty who do some works in critical infrastructures. After research and consultations, a number of names popped out but my feet led me to the office of Mark de Bruijne. After a little reflection, he gave me his “yes” to help me out in my study. As I see from his aura, he is a very helpful person and always gives me the boost that I can do it... that I am the captain of my study...that there is a hope that I can finish my study. His accommodating nature provided a kind of feeling that my study will go well as long as I do my part. “Thank you Mark for your warm accommodation and indeed your critical inputs, the books you suggested for me to read, your insights in my conclusion and recommendation and just your mentoring nature lifted me through all throughout the course of my research. I hope you find fulfillment as well in helping me out to successfully finish my work.”

It was through Mark that I found my first supervisor, Tineke Egyedi. I was in the struggle then about the nature of the study since it is about policy baseline and kind of related to standardization. I just did not know at that stage to what extent will standardization be part of the study. I know and I have struggled so much in trying to place the topic in one box in a way that my mind can accommodate. I am aware of the ambitiousness of the project... but the only way out is to move forward.☺ Mark suggested me the name of Tineke as a “real” expert of standardization in the faculty. My graduation coordinator, Jolien Ubacht, also suggested her name. When I say real expert, she indeed is. She is very active in standardization activities in formal standardization organizations and has done already so much in the field. The way she stirred my thinking was awesome. She provided me very straight review of my work that really made me feel that I have to provide an intensive overhaul of my work. She is a woman of details and has always the eye on what she can learn out from such an undertaking. The chapter that I made the most number of

revisions is the theory part—the apple of the eye of my first supervisor.☺ “I thank you Tineke for your push for quality. Indeed, the attitude you have on critical thinking and professionalism is what I admire the most. The “are you sure?” question that you asked me during the time I had confusion really made me ponder about the level of thinking I have provided to the work and gave me the feeling that I have to upgrade my work and live up to the expectation. Amidst your very busy schedules, thank you for providing a time to read my work and provide me feedback. For me, you’ve done an excellent job as my first supervisor!”

It was through Tineke that I was able to know Jan van den Berg, the chairman of my thesis committee. I and Tineke were in Amsterdam then and was, in fact, our first meeting. Tineke suggested his name for he has been doing a number of works in the area of ICT security and she said he is also a wonderful person. And he really is! He also has the “mentoring” aura that confides me that I am tracking the right path. His honest but smooth manner of providing feedback is admirable. “Thank you Jan for your willingness to accommodate my study amidst your voluminous commitments. Thank you for sharing me a portion of your time to take a look at my work and provide me critical suggestions. I most especially thank you, together with other supervisors, for your affirmative assessment of my work during my knee-trembling “greenlight” meeting moment. Your smooth words and heart-warming assessment provided me hope that I will be able to “get the bacon” right on time!”

As one can see that my search for my thesis committee went through a real bottom up style. From just an internship activity to making it a real thesis study. A number of wonderful and very cooperative people are involved to whom I have so much to thank about! “Thank you and it was a wonderful time to be mentored by you!”

Aside from my supervisors, I have people in the background worth mentioning in this section. My family back home in the Philippines always provides me a comfort and backs me up with prayers that I will be fine in my journey here in Europe. They are my very source of inspiration and the very reason why I have come to decide that I will traverse continents and oceans, both in literal and metaphor figures, to come to the Netherlands to follow my dreams. Indeed, a short call in them through the phone and chat on the internet always gives me the strength to carry on.

I also give my thanks to my classmates and friends for the wonderful company we had together for the past two years. Worth mentioning are Umer for the laughs and for just being a wonderful buddy, to my EMIN classmates who provided me some sense of community, to Reza for the various treats and for sharing to me some wonderful life’s visions, to Christine for just being wonderful and inspiring American classmate, to Nicolo for just being a brilliant Italian, to Daphne for just being a warm Dutch, to Hu Hao, and the rest of my Chinese classmates, who provided me company once in awhile. A great thanks I also give to Claudia, my ever loyal Bolivian mentor since my first year, who generously provided me assistance about any questions I have had about scholarships, study, books, projects, even jobs and anything about life. I always say to her that she is an “angel in disguise” to me. “Thank you for being such a wonderful person and for all the help.”

My gratitude as well goes to the wonderful people I met outside the Netherlands who made me realized that people are just the same, worthy of respect and understanding, no matter from what background we all come from.

This part would not be complete if I would not express my gratitude to the two TBM people who provided me opportunity to reach my dream. First is Ms. Toke Hoke for the seemingly endless assistance she provided me. Through her that I was able to get my scholarship that made my dream of studying in TUDelft a reality. “Thank you for all the assistance since day one of my stay here in the Netherlands till the day of my graduation from my EPA program. Your help cannot just be all listed in this paper and I am just overwhelmed by your kindness and generosity.”

Secondly, I thank Jean-François Auger for affording me a number of research opportunities. “You are a wonderful and very generous person worthy of thanks. Your mentoring in the research area

has provided me so much lift in improving my skill. The opportunities you provided me also lead me to greater undertakings. Thank you for such a great concern about my future career.”

This I end through thanking the beautiful person who is the apple of my heart, Michelle Louise Mendoza. Her life inspires me to live life to the fullest and to always lift up the Filipino race in all the ways I can. She has so much contribution to who I become today, we dreamt together and we journey together. This piece of work I dedicate to her for the unfailing love and inspiration she brings me. “Thank you so much for just being around!”

CURRICULUM VITAE

Nelson H. Enano, Jr. is an international graduate student of Delft University of Technology (TUDelft) taking MSc Engineering and Policy Analysis. He is a national of the Philippines. He has a bachelor’s degree (BSc) in Electronics and Communications Engineering from Ateneo de Davao University in Davao City, Philippines, in which he graduated as Cum Laude. During his bachelor’s graduation, he was adjudged as one of the 2003 Ten Outstanding Students of the Philippines (Region XI). After passing the national board examination, he became a registered and licensed electronics and communications engineer in the Philippines.

Due to his desire for greater understanding of his engineering field in a more encompassing context, he wanted to see how his specialized electronics and communications engineering training is placed in greater policy analysis-management/organizational context. He believes that through getting a bigger grasp of his field (with interdisciplinary outlook) he can afford to provide more effective and more sustainable solutions (policy options) to various issues concerning the field. It is by such rationale that he took the graduate study of Engineering and Policy Analysis in the Faculty of Technology, Policy and Management of Delft of University of Technology.

This graduate thesis provided him an integrative feel of his undergraduate field to his present policy analysis area of graduate study. He is hoping that this research project can lead him to an elevated career in the area of telecommunications policy analysis-- the kind of career niche he has always been aspiring for.

