



9th Global Symposium for Regulators (Beirut, 2009)

Hands-on or Hands-off? Stimulating growth through effective ICT regulation

Background Papers for Information

This PDF is provided by the International Telecommunication Union (ITU) Library & Archives Service from an officially produced electronic file.

Ce PDF a été élaboré par le Service de la bibliothèque et des archives de l'Union internationale des télécommunications (UIT) à partir d'une publication officielle sous forme électronique.

Este documento PDF lo facilita el Servicio de Biblioteca y Archivos de la Unión Internacional de Telecomunicaciones (UIT) a partir de un archivo electrónico producido oficialmente.

یجرى نورکتلا فملنم تذخوماً ی هو ت اظوفحموال ٲمکتبال قسم ، (ITU) للاتصالات الدولي الاتحاد من مقدمة PDF ینسق النسخة هذه امیرسٲ إعداده.

本PDF版本由国际电信联盟（ITU）图书馆和档案服务室提供。来源为正式出版的电子文件。

Настоящий файл в формате PDF предоставлен библиотечно-архивной службой Международного союза электросвязи (МСЭ) на основе официально созданного электронного файла.

Draft October 2009

Draft Background Paper

Cybersecurity: The Role and Responsibilities of an Effective Regulator

9th ITU Global Symposium for Regulators

**Beirut, Lebanon
November 2009**

Acknowledgements

This draft background paper on **Cybersecurity: The Role and Responsibilities of an Effective Regulator**, was commissioned by the ITU Telecommunication Development Sector's ICT Applications and Cybersecurity Division and Regulatory and Market Environment Division. The paper was prepared by Eric Lie, Rory Macmillan and Richard Keck of Macmillan Keck (Attorneys and Solicitors), for the 9th ITU Global Symposium for Regulators held in Beirut, Lebanon (10-12 November 2009).

The background paper on **Cybersecurity: The Role and Responsibilities of an Effective Regulator** is available online at:

www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/papers.html

All rights reserved. No part of this publication may be reproduced in any form or by any means without written permission from ITU.

Denominations and classifications employed in this publication do not imply any opinion concerning the legal or other status of any territory or any endorsement or acceptance of any boundary. Where the designation "country" appears in this publication, it covers countries and territories.

This document has been issued without formal editing.

For further information on the paper, please contact:

ICT Applications and Cybersecurity Division (CYB)
Policies and Strategies Department
Bureau for Telecommunication Development
International Telecommunication Union
Place des Nations
1211 Geneva 20
Switzerland
Telephone: +41 22 730 5825/6052
Fax: +41 22 730 5484
E-mail: cybmail@itu.int
Website: www.itu.int/ITU-D/cyb/

Disclaimer

The opinions expressed in this report are those of the author(s) and do not necessarily represent the views of the International Telecommunication Union (ITU) or its membership. The designations employed and the presentation of material, including maps, do not imply the expression of any opinion whatsoever on the part of ITU concerning the legal status of any country, territory, city or area, or concerning the delimitations of its frontiers or boundaries. Mention and references to specific countries, companies, products, initiatives or guidelines do not in any way imply that they are endorsed or recommended by ITU in preference to others of a similar nature that are not mentioned.

© ITU 2009

Table of Contents

1	Introduction	4
1.1	What is cybersecurity?	4
1.2	What is in this paper?	6

Part I: Cybersecurity Roles and Responsibilities - An Overview

2	Cybersecurity and the public sector.....	7
2.1	Role and responsibility of government.....	7
2.1.1	Policy-making (and establishing a national cybersecurity strategy)	8
2.1.2	Legal Measures.....	8
2.1.3	Organizational Structures	9
2.1.4	Capacity Building.....	11
2.1.5	Public-private sector cooperation and industry regulation	11
2.2	Delegating cybersecurity responsibilities among government institutions	12
3	Cybersecurity and the private sector	15
3.1	The role of the private sector.....	15
3.2	Cybersecurity and the bottom line.....	15
4	Cybersecurity and the individual.....	16
4.1	The role of the individual	16
4.2	The role of civil society.....	16
5	Cybersecurity and international cooperation.....	17

Part II: The Evolving Role of the Regulator in the Area of Information and Network Security

6	The role of the regulator	19
6.1	The core duties of the regulator.....	19
6.2	The evolving role of the regulator	19
7	The role of the regulator in cybersecurity	20
7.1	Cross-cutting competencies and prerequisites.....	20
7.1.1	Institutional maturity	20
7.1.2	Engagement of the private sector	21
7.1.3	Technical and industry expertise	21
7.1.4	Mandate and jurisdiction	21
7.1.5	Appropriate resourcing.....	22
7.2	Engagement in international cooperation	23
7.3	Policy-making.....	24
7.4	Legal measures	27
7.5	Organizational structures.....	29
7.5.1	Institutional organization and coordination	29
7.5.2	Incident management and cybersecurity readiness assessment.....	31
7.6	Capacity building.....	33
7.7	Private sector cooperation and industry regulation	35

Part III: Conclusions and Recommendations

8	The ICT/telecom regulator - a key player in a national team	39
---	---	----

1 Introduction

Information Communication Technologies (ICTs) are rapidly evolving while at the same time their usage is expanding. Today, Internet and mobile services have become an indispensable part of daily life for many around the world. While the benefits of ICT adoption have multiplied, the risks and dangers associated with their use have also similarly increased. Cybercrimes such as phishing, spam, computer-related fraud and other similar offences are rapidly increasing and evolving in step with the development and adoption of new ICT services.

In response to this situation, an increased emphasis on enhancing cybersecurity is being placed in all countries. While cybersecurity is a shared responsibility of government, the private sector and individuals alike, only national governments are in a position to lead a collective national cybersecurity effort. Only when governments establish common objectives, define ways to achieve them and clarify the roles and responsibilities of stakeholders can cybersecurity be comprehensively addressed.

As an integral part of government, ICT/telecom regulators play a key role in the national cybersecurity effort of many countries. Their broad competencies in the ICT sector, their familiarity with the ICT industry and their expertise in ICT networks and infrastructure have naturally positioned them as key players in the field of cybersecurity. However, given the constantly changing ICT environment and the dynamics of cybersecurity, the role of the regulator in this area has to evolve and adapt. Institutional improvements and other changes may be necessary to ensure that regulators remain relevant in this dynamic environment. It is in this context that this paper examines and discusses the roles and responsibilities of regulators in the field of cybersecurity.

1.1 What is cybersecurity?

In a discussion of security in the context of ICT, a number of terms are often used to describe different aspects of a common concept. In many instances, terms like cybersecurity and Critical Information Infrastructure Protection (CIIP) are used interchangeably, while in other cases they are used to describe different concepts.

In any discussion of cybersecurity, it is useful to first understand the following terms: cybersecurity, critical infrastructure (CI), critical information infrastructure (CII), critical infrastructure protection (CIP), critical information infrastructure protection (CIIP) and non-critical infrastructure.¹

While the exact definitions may vary slightly from country to country, CI typically encompass the vital systems, services and functions whose disruption or destruction would have a debilitating impact on public health and safety, economic activity, and/or national security. CI includes physical elements (such as physical infrastructure and buildings) and virtual elements (such as networks and data). What constitutes “critical” varies from country to country, but typically includes elements of communications, energy, public utilities, finance, transportation, public health, and essential government services.

¹ Also see ITU, List of Security-Related Terms and Definitions, available at: http://www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D00000A0002MSWE.doc.

CII comprises the communications network that enables these elements to operate and deliver their services. Disruption to the CII can have an equally debilitating impact on CI that reaches beyond just the ICT sector.

CIP involves identifying, assessing, and managing risks to deter or mitigate attacks on CI and the promotion of its resiliency. CIIP describes the range of activities that are undertaken to protect the CII. It focuses on the prevention and deterrence of specific ICT related risks and threats.

Cybersecurity is a broad term that encompasses CIIP as well as elements that may not be considered to be critical information infrastructure, such as the computer networks of small and medium enterprises, or home personal computers. Cybersecurity aims to prevent all malicious cyber incidents that affect the critical and non-critical information infrastructures alike. Such incidents can include denial of service attacks, the distribution of spam and malware, phishing and pharming and other cybercrimes.

ITU-T Recommendation X.1205 defines cybersecurity as:

“the collection of tools, policies, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets. Organization and user’s assets include connected computing devices, users, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity ensures the attainment and maintenance of the security properties of the organization and user’s assets against relevant security risks in the cyber environment. The security properties include one or more of the following: availability; integrity (which may include authenticity and non-repudiation); confidentiality”.

In addition to the terms defined above, the term “cybercrime” is also used extensively in the discussion of security in the context of ICT. The prevention of cybercrime is a key objective of cybersecurity.

A broad definition of cybercrime describes it as encompassing any activity in which computers or networks are a tool, a target or a place of criminal activity. To better understand some of the implications of cybercrime and the need to criminalize the misuse of information and communication technologies, ITU has developed a set of dedicated cybercrime legislation resources. An ITU publication on Understanding Cybercrime: A Guide for Developing Countries and a Toolkit for Cybercrime Legislation are currently available to assist countries in understanding the legal aspects of cybersecurity and to help harmonize legal frameworks².

However, the definition of the term cybercrime is not a uniform one internationally, with different legal instruments in different countries using the term to describe a range of offences. The following categories used by several regional and international instruments illustrate a possible approach:

- Offences against the confidentiality, integrity and availability of computer data and systems (i.e., illegal access, illegal interception, data interference, system interference, and misuse of devices);
- Computer-related offences (i.e., computer related forgery, and computer related fraud);

² For more on the definition of “cybercrime” and an in-depth discussion on cybercrime in general, see Understanding Cybercrime: A Guide for Developing Countries, ITU, 2009 available at: <http://www.itu.int/ITU-D/cyb/cybersecurity/projects/crimeguide.html>

- Content-related offences (i.e., offences related to child pornography); and
- Copyright-related offences (i.e., offences related to infringements of copyright and related rights);

While some overlap exists between categories, the categories nevertheless serve as a useful illustration of what is involved in the phenomena of cybercrime.

1.2 What is in this paper?

This paper provides a framework for discussion on the role of the regulator in cybersecurity.

Part I focuses on the roles and responsibilities of cybersecurity stakeholders: government, the private sector and individuals. As the role of government frames the eventual role of the regulator in cybersecurity, particular emphasis is paid here to the different aspects of cybersecurity in which government plays a significant part. Part I also looks at the range of international cybersecurity efforts where governments play a large role.

Part II looks in depth into the role of the regulator in cybersecurity. It first traces the evolution of the role of the regulator. It then goes on to discuss the range of roles available to regulators in the context of government involvement in cybersecurity. In that discussion the issues associated with the assumption of those roles and the core competencies necessary on the part of the regulator to fill those roles are highlighted.

Part III highlights some of the main findings of Part I and Part II, and makes some recommendations on the core competencies of regulators in cybersecurity issues.

PART I:

CYBERSECURITY ROLES AND RESPONSIBILITIES - AN OVERVIEW

In today's modern society, ICTs have become an essential component in all aspects of daily life, from the political, the economic and the social. They ensure economic stability, support national security and facilitate social interaction within nations as well as between nations. However, as a largely open, interdependent and interconnected global system, ICTs are by their very nature prone to vulnerabilities and the risk of exploitation.

In order to ensure that society continues to enjoy the benefits that ICTs bring, these vulnerabilities and risks are managed, to some extent or other, through the cybersecurity efforts of the stakeholders that own, develop, operate and use these networks. These stakeholders include government, business, other private sector organizations and individual users.

In the context of this paper, it is important to understand the relative roles and responsibilities of all stakeholders in order to properly situate that of the regulator's.

2 Cybersecurity and the public sector

To a large extent, only national governments are in a position to lead national cybersecurity efforts that involve all national stakeholders. In addition to putting in place substantive measures to counter cybersecurity threats, governments have the central task of establishing, among all stakeholders, a common awareness and understanding of cybersecurity as well as a common recognition of each stakeholder's roles and responsibilities.

2.1 Role and responsibility of government

The role and responsibility of government in cybersecurity is extensive. Given the vital role of ICTs in the nation, the wide range of threats and vulnerabilities and the cross-sector nature of cybersecurity, a large number of national governments assume a variety of roles and shoulder an extensive array of responsibilities ranging from national level policy-making to citizen level capacity-building.

From a brief survey of international practice and by building on the areas emphasized in the pillars of the ITU Global Cybersecurity Agenda (GCA)³ and the related elements highlighted in the ITU National Cybersecurity/CIIP Self-Assessment Tool⁴, the cybersecurity roles and responsibilities of government can be organized loosely into the following categories:

- Policy-making;
- Legal Measures;
- Organizational Structures;
 - Institutional organization and coordination; and
 - Incident management and cybersecurity readiness assessment;
- Capacity building;
- Public-private sector cooperation and industry regulation.

³ Information on the Global Cybersecurity Agenda (GCA) is available at <http://www.itu.int/cybersecurity/gca/>.

⁴ ITU National Cybersecurity/CIIP Self-Assessment Tool, ITU, 2009 available at <http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html>

To this, the dimension of engagement in international cooperation must also be added as an indispensable element of a government's role in cybersecurity.

A holistic governmental effort that encompasses all these categories is a prerequisite for an effective national cybersecurity response.

2.1.1 Policy-making (and establishing a national cybersecurity strategy)

Leadership in the area of cybersecurity by national governments is manifested largely through the government's national policy-making role. Governmental policy-making in the area of cybersecurity provides, at the highest level, a common understanding and vision of the problem, allowing for coordinated national action that would realize national cybersecurity objectives.

The preparation of a national cybersecurity strategy is an essential first step in addressing cybersecurity challenges. Such a statement typically:

- highlights the importance of ICTs to the nation (e.g. by providing information on the role of ICTs in the economy, society and national security, and the industrial and governmental processes dependant on ICTs);
- identifies and evaluates potential risks and threats (e.g. cyber-attacks, cybercrime, etc.);
- establishes cybersecurity related objectives (e.g. containment of cyber-attacks, detection and prosecution of cybercrime, protection of data resources, etc.);
- identifies the actions to be taken in order to achieve those objectives (e.g. establishment of incident response centers, adoption of cybersecurity standards, building consumer awareness, etc.); and
- sets out the roles and responsibilities of all stakeholders in the process (including a mechanism for information sharing, cooperation and collaboration).⁵

The national cybersecurity strategy can also place cybersecurity efforts into the context of other national efforts, such as homeland security and the development of an information society.

In many countries, national cybersecurity strategy is typically promulgated at a high level of government, often by the head of government, in order to get the buy-in of all stakeholders. For example, in the case of Brazil, the national cybersecurity strategy is led from the Office of the President (see Box 1 below). At the same time, however, national cybersecurity policy is typically developed cooperatively through consultation with all relevant stakeholders, including other government institutions, industry, academia, and civil society. In some countries, such policies also integrate state, local, and community-based approaches that feed into the larger national context.

2.1.2 Legal Measures

An effective cybersecurity effort requires the establishment, review and, if necessary, amendment of relevant legal infrastructures that support modern ICTs.⁶ This requires

⁵ Ibid. See also ITU Study Group Q.22/1 Report on Best Practices for a National Approach to Cybersecurity, ITU, 2009, available at <http://www.itu.int/md/meetingdoc.asp?lang=en&parent=D06-SG01-C&question=Q22/1>

⁶ For more information on the range of legal measures that can be undertaken in the area of cybersecurity see the section on Legal Matters in the ITU Global Cybersecurity Agenda (GCA) High

updating of criminal laws, procedures and policies to address cybersecurity incidents and respond to cybercrime. As a result, many countries have made amendments in their penal codes, or are in the process of adopting amendments, taking in consideration existing international frameworks and recommendations.⁷ As a priority, criminal law, procedures and policy should be reviewed to ensure the prevention, investigation, and prosecution of all forms of cybercrime.⁸ In addition, legislation that ensures the security of information and information infrastructures should be introduced⁹. Such legislation typically deals with issues that include the following:

- Security in electronic communications
- Fraudulent use of computer and computer systems;
- Protection of personal data and privacy;
- Certification, digital signatures and Public Key Infrastructure (PKI), among others.

Beyond their enactment, cybersecurity laws must also be effectively enforced. An effective anti-cybercrime effort will require the modernization of law-enforcement agencies, the establishment of dedicated cybercrime units, and the training of prosecutors and judges.

As many instances of cybercrime cuts across borders, participation in international efforts to respond to cybercrime forms an integral part of the national cybercrime prevention effort.

2.1.3 Organizational Structures

Institutional organization and coordination

The institutional organization and coordination of government institutions for cybersecurity is a vital element of a successful cybersecurity effort. In the context of the role and responsibility of government, it typically involves the organization and coordination of cybersecurity roles and responsibilities among appropriate government institutions in order to carry out the actions that are required to meet cybersecurity objectives. A detailed organization and cooperation framework is essential in order to avoid institutional gaps in the national cybersecurity effort as well as to avoid overlaps in responsibilities which can prove just as damaging. Where overlaps in responsibilities exist, there is often either a tendency towards passiveness by the institutions concerned, or at the other extreme, a potential for the introduction of conflicting regulations and approaches.

Universally, a concerted cybersecurity effort at the government level requires organizing and coordinating the work of multiple authorities and government departments, who often have

Level Experts Group (HLEG) Global Strategic Report, ITU, 2008 available at http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html

⁷ To better understand some of the implications of cybercrime and the need to criminalize the misuse of information and communication technologies, ITU has developed a set of dedicated cybercrime legislation resources. An ITU publication on Understanding Cybercrime: A Guide for Developing Countries and a Toolkit for Cybercrime Legislation are currently available to assist countries in understanding the legal aspects of cybersecurity and to help harmonize legal frameworks. These resources are available at <http://www.itu.int/ITU-D/cyb/cybersecurity/projects/crimeguide.html> and <http://www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html>

⁸ As an example, the Budapest Convention on Cybercrime (2001) includes minimum requirements: substantive laws (i.e. minimum standards for what is criminalized); procedural mechanisms (i.e. investigative methods); and international legal assistance (i.e. procuring of evidence or extradition). The convention is available from the Council of Europe in various languages at <http://www.coe.int/cybercrime/>

⁹ See the UNCITRAL Model Laws on Electronic Commerce and on Electronic Signatures (2001) and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) for example.

different mandates and perspectives on the problem. As such, the delegation of roles and responsibilities among government institutions is a delicate one and in many cases it is undertaken by a government institution with a high-level mandate, such as the cabinet or the presidential office, as is the case with the National Infrastructure Security Co-ordination Centre (NISCC) in the United Kingdom or the Department of Homeland Security in the United States. Such high level oversight is often necessary to efficiently settle potential conflicts where overlaps in institutional jurisdiction and responsibilities exist.

In practice, the actual delegation of cybersecurity roles and responsibilities among the different government institutions varies widely from country to country as such decisions are based on a wide range of considerations. This topic is discussed further in Section 2.2 below.

Incident management and cybersecurity readiness assessment

The capability to detect, to investigate and analyze, and to respond to cyber-threats and attacks is an indispensable component of cybersecurity. In this respect, computer incident response teams (CIRTs) in various forms have been established by a wide range of groups (e.g. operators, businesses, universities, etc.) at the national and international level.¹⁰ CIRTs vary dramatically in the services they provide and the constituents they serve. Some have national responsibility while most belong to private organizations and are established to fulfill specific functions, depending on their situation. A key function that all CIRTs share is the ability to provide (1) timely information about the latest threats and (2) assistance in response to incidents when needed.

While many CIRTs have been created from the bottom-up, it is generally acknowledged that it is important for governments to establish an incident management capability on a national level to prevent, prepare for, respond to, and recover from cybersecurity incidents. National CIRTs also typically assume responsibilities for readiness and response to large-scale attacks.

Such an incident management capability would necessarily extend beyond the traditional CIRT role to include coordination and management capabilities in terms of cybersecurity crisis. It would also make tactical or strategic information available to key stakeholders within the public and private sectors. Examples of such CIRTs can be found in Canada (Integrated Treat Assessment Center) and in Switzerland (Reporting and Analysis Center for Information Assurance, MELANI).

Given the cross-border nature of cyber threats and attacks, active participation in international and regional cybersecurity incident monitoring activities forms a necessary part of the CIRT national effort. Such activities can include active participation in an international CIRT organization (e.g., Asia Pacific Computer Emergency Response Team (APCERT), Forum of Incident Response Security Team (FIRST), etc.) or international incident management exercises. For example, US-CERT has organized major international exercises (e.g. “Cyberstorm”, involving Australia, New Zealand, and Canada), simulating large-scale attacks on critical sectors.

The conduct of cybersecurity exercises to test readiness and responsiveness form part of the larger role of government to evaluate and review the level of cybersecurity preparedness of

¹⁰ The term CIRTs is often used interchangeably with the terms computer emergency response teams (CERTs) and computer security incident response teams (CSIRTs). A CIRT is essentially a team of IT security experts whose main business is to detect, analyze, monitor and respond to computer security incidents. In some cases, these CIRTs also manage outreach, cyber-security awareness, and partnership efforts to disseminate information to key constituencies and build collaborative actions with key stakeholders.

the nation. Such a role typically involves the organization and execution of periodic cybersecurity risk assessments and strategy reviews on both the national and sector-specific (e.g., financial, manufacturing, retail, etc.) levels. The result of such cybersecurity assessments can, in turn, lead to a thorough review of existing cybersecurity-related legislation and regulation as well as sector specific legislation and regulation, such as financial laws and regulation.

2.1.4 Capacity Building

Generally, many end-users (including private enterprises, public entities, and home users) lack the awareness and resources to manage cyber-security risks adequately. Many information system vulnerabilities exist because of a lack of cybersecurity awareness on the part of users.

End user outreach efforts therefore, at the most basic level, entail the development of a concerted strategy to communicate the importance of cyber-security and their role across the country. Such a strategy would identify practical information for dissemination to their target audiences and initiatives to ensure the adoption of those practices.

Capacity-building in the area of cybersecurity is a necessary complement to the building of cybersecurity awareness. For a culture of cybersecurity to be firmly established, the level of cybersecurity competence in general has to be increased. In part, this can be achieved by making basic cybersecurity-related training more readily available to the public (e.g. through interactive websites) and by promoting industry efforts to train personnel and to adopt widely-accepted security certifications.

In addition, governments must encourage academia to provide for the education of a ready pool of trained cybersecurity professionals to meet the increasing demands of both the public and the private sector in the field.

2.1.5 Public-private sector cooperation and industry regulation

A comprehensive national cybersecurity effort requires the establishment of a coordination and cooperation framework through which all stakeholders, from both the public and private sector, can collaborate in the development and refinement of cybersecurity policy and cooperate in the implementation of cybersecurity operational efforts. In particular, such a framework would allow governments, businesses, civil society and individual users to work together to develop and implement measures that incorporate technical (e.g., standards), procedural (e.g., guidelines, standards, or mandatory regulations) and personnel (e.g., best practices) safeguards. Such measures include, for example, promoting government and industry adoption of international standards related to cybersecurity (e.g., ISO 27001 on Information Security Management System) and the implementation of certification schemes (e.g., Public Key Infrastructure).

Governments in almost all countries have recognized the importance of public-private sector cooperation in cybersecurity. The development of a close mutually beneficial relationship facilitates the overall management of cyber threats and cybersecurity. Realistically, many governments actively promote cooperation and information-sharing with the private sector, as large parts of critical infrastructures are owned and operated by private business. Only by understanding the cybersecurity challenges facing the private sector can an effective national cybersecurity strategy and policy be adopted. Cooperation between government and industry is also essential in the response and recovery phase of cybersecurity incidents.

The exact approach countries take to achieve public-private sector cooperation varies based on local conditions and needs. Examples include government-led task forces, industry-led forums, and joint public-private initiatives. In countries such as Switzerland, Republic of Korea, the United Kingdom, and the United States, strong links have already been established between the private business community and various government organizations in the area of cybersecurity.

A key challenge presented to governments and industry alike in this context is the search for a balance between national cybersecurity requirements and business efficiency imperatives. Satisfying shareholder interests by maximizing company profits has often led to minimal security measures on the part of the private sector partly because businesses tend to view cyber-threats as a tolerable risk. In these situations, governments have sometimes found it necessary to introduce measures that compel or encourage the private sector to prioritize cybersecurity and to adopt sufficient safeguards.

To the extent that government supports science and technology and research and development (R&D) activities, some of its efforts should be directed towards cybersecurity and the protection of information infrastructures. Through partnerships with the private sector and academia, governments can help shape the development of cybersecurity related technologies, techniques, standards and processes that further the national cybersecurity agenda.

2.2 Delegating cybersecurity responsibilities among government institutions

Because of the cross-sector nature of cybersecurity, it necessarily means that various key elements of an overall cybersecurity policy will be implemented in practice through a very diverse set of institutional arrangements that differ from country-to-country. Furthermore, countries at different stages of development will have differing perspectives on the overall vulnerability of their own critical information infrastructures. They are likely to be at different stages of institutional development.

As a practical matter, in most countries responsibility for cybersecurity or CIIP is based on an evaluation of national cybersecurity vulnerabilities and a matching of this to the roles and responsibilities of existing government institutions. Relevant cybersecurity responsibilities are then given to the most well-established institution or institutions that appear suitable for the task (e.g. Ministry of Defense, Department of Homeland Security, the ICT regulator, etc.). For example, in Canada, responsibility for CIP and CIIP is delegated to Public Safety Canada, an agency that provides policy advice and support to the minister of public safety on issues related to public safety, including national security and emergency management, policing and law enforcement, interoperability and information-sharing, border management and crime prevention. Public Safety Canada's portfolio also includes the Royal Canadian Mounted Police (RCMP), the Canadian Security Intelligence Service (CSIS), and the Correctional Service of Canada among others.¹¹

While less common, a number of countries have also set up central management and coordination institutions (e.g. national cybersecurity councils, inter-agency cybersecurity task forces) specifically to meet cybersecurity and CIIP concerns. For example, in Japan, two central management and coordination organizations were established within the Cabinet Secretariat to deal specifically with cybersecurity issues. The Information Security Policy Council (ISPC) plays the central role in developing and reviewing the country's information security strategies and policies while the National Information Security Council (NISC) is the central implementing body for IT security issues.¹²

¹¹ For more information on the activities of Public Safety Canada, see <http://www.publicsafety.gc.ca>.

¹² For more information on the ISPC and the NISC, see <http://www.nisc.go.jp/eng/index.html>

In most countries, different cybersecurity roles and responsibilities are typically spread among multiple governmental institutions and organizations (see Box 1). Depending on their key role (e.g. defense, law enforcement, ICT development), these institutions bring their own perspective to bear on the issue of cybersecurity and shape national policy accordingly.

Box 1: Government cybersecurity framework in Brazil

Brazil has a complex and sophisticated web of institutions involved in cybersecurity. Its experience illustrates the interconnected relationships of public and private stakeholders that are an essential part of an effective cybersecurity framework.

Leadership on national ICT security issues in Brazil falls within the jurisdiction of the Institutional Security Cabinet or GSI (Gabinete de Segurança Institucional), which is part of the office of the President of the Brazilian Republic. GSI is also tasked with crisis management, intelligence, and the provision of advice for the President in military and security issues. It does not directly handle operational security issues, but works through other related organizations such as CTIR-GOV and CGSI.

CTIR-GOV (Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal) is a governmental body that deals with national security incidents that involve the Brazilian federal government.

CGSI (Comitê Gestor de Segurança da Informação) is an information security steering committee created by legislation. It comprises of representatives from every government ministry (justice, defense, health, communication, science and technology, etc). The participants discuss information security issues and through working groups define the cybersecurity policy direction of the Brazilian federal administration.

CERT.br is the Brazilian Computer Emergency Response Team, sponsored by the Brazilian Internet Steering Committee. It is responsible for receiving, reviewing, and responding to computer security incident reports and activity related to networks connected to the Brazilian Internet. Computer Security Incident Response Teams (CSIRTs) have also been established in a number of Brazilian states.

Certain methodologies for dealing with Critical Information Infrastructure Protection have been developed by the Brazilian ICT sector in cooperation with the regulator, ANATEL. These methodologies have been applied to assess the cybersecurity readiness of Brazil's ICT infrastructure.

CEPESC (Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações), a center for research and development for security in communications under the Brazilian intelligence agency, also assists and supports the Brazilian government and the GSI in all aspects related to secure communications.

Source: Adapted and updated from "International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues", TNO, 2005 available at <http://www.ists.dartmouth.edu/library/158.pdf>

In general, there are at least four overlapping typologies for how cybersecurity issues are viewed¹³:

- an IT-security perspective,
- an economic perspective,

¹³ See International CIIP Handbook 2008/2009, Center for Security Studies, ETH, Zurich available at http://www.crn.ethz.ch/publications/crn_team/detail.cfm?id=90663

- a legal or law enforcement perspective, and
- a national security perspective.

Most countries consider cybersecurity to be a national security issue of some sort. In parallel, however, they also view it from a technological, ICT viewpoint. At the same time, the law enforcement and cybercrime perspective is also found in all countries. While all typologies can usually be found in all countries, the emphasis given to one or more of them varies to a considerable degree.

In countries that view cybersecurity from a national security perspective, cybersecurity efforts are mainly led by the defense and national security establishment. For example, in France responsibility for a large part of cybersecurity falls under the general umbrella of the General Secretary for National Defense.¹⁴ Such nations have had traditionally a significant military or national security presence in the international arena and see cybersecurity as a part of cyber-warfare.¹⁵

Where cybersecurity is viewed from a law-enforcement perspective, cybersecurity efforts tend to be led by institutions that deal with law enforcement and internal security. In some countries, cybersecurity is also integrated into the overall counterterrorism effort, where the intelligence community plays a large role. For example, in the Republic of Korea the National Intelligence Service (NIS), the chief intelligence agency, serves as coordinator for the private, public, and military sectors in the event of a cyber crisis.

In countries that view cybersecurity from an economic and IT-security perspective, approaches to cybersecurity are often jointly led by the business community and government institutions involved in ICT development, such as the regulator or other institutions involved in the e-economy. In countries such as Estonia, Japan and Singapore cybersecurity is viewed as an integral part of the fostering of an information-based economy. In these countries ICT regulators play a large role not only in the implementation of cybersecurity safeguards but also in policy-making and coordination.

The establishment of these institutions and their location within government are influenced by various factors such as military and civil defense tradition, the allocation of resources, historical precedent and the general perception of where the greatest threat lies by the key policy-makers in this domain. Depending on their influence or their resources at hand, various government institutions shape the cybersecurity issue in accordance with their view of the threat.

It must be highlighted that there is no single strategic approach, organizational and institutional set up, or operational procedure that is right for every country. Between countries there are large differences in political and legal systems, economic development, and public and private sector relationships. What is important, however, is that governments adopt a flexible and adaptive approach to their cybersecurity efforts as threats to cybersecurity are constantly evolving. Sometimes this requires the periodic review and reorganization of the national cybersecurity framework (see Box 2). In adopting a flexible and adaptive approach, governments can also rapidly assimilate and adopt the latest international best practices in the area of cybersecurity without significant delay.

¹⁴ For more information, see the website of the Secrétariat général de la défense nationale at <http://www.sgdn.gouv.fr>.

¹⁵ For more information on cyber-warfare, see 'Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States', Charles Billo, Welton Chang, ISTS, 2004 at <http://www.ists.dartmouth.edu/directors-office/cyberwarfare.pdf>

Box 2: Institutional reorganization in the Republic of Korea

As a response to the large scale distributed denial of service (DDOS) attacks on 7 July 2009, the Government of the Republic of Korea confirmed in September 2009 that the National Intelligence Service (NIS) would serve as a coordinator for the private, public, and military sectors in the event of a cyber crisis.

Previously, the ICT regulator, the Korean Communication Commission (KCC), the NIS, and the Ministry of Defense shouldered responsibility separately for cybersecurity in their respective sectors.

When cybersecurity levels pass “normal” and reach “cautionary” levels, the NIS is expected to analyze the threat and implement countermeasures to contain the situation, if necessary.

Source: http://www.hani.co.kr/arti/english_edition/e_national/376585.html

3 Cybersecurity and the private sector

ICT infrastructure is for the most part owned and operated by the private sector in the large majority of countries worldwide. In many countries, the private sector is also typically the first to adopt technological changes and assess its associated vulnerabilities. As such, the involvement of the private sector is indispensable in any national cybersecurity effort.

3.1 The role of the private sector

On an individual basis, businesses are expected to implement an adequate level of cybersecurity safeguards into their business practices. Such safeguards typically involve the installation of technical solutions and the adoption of secure business processes.

Businesses in some economic sectors may be further along in adopting cybersecurity practices. For example, the financial and banking sector, with its dependency on international clearing and central banking, and its links to international financial market systems, cybersecurity concerns are accorded high priority.

On a collective level, the private sector has an important role to play in its own right and in cooperation with government in developing cybersecurity business norms, standards and codes of conduct, as well as in identifying and encouraging the adoption of good practices. By taking part in relevant forums or standards-development organizations, industry plays a critical role in agreeing on technical standards to protect security.

3.2 Cybersecurity and the bottom line

In general it has proved to be a more demanding task to focus resources on the protection of critical information infrastructure which is often subject to private ownership or control. In the competitive global business environment, businesses will necessarily be inclined to reduce or eliminate expenses that do not contribute to the bottom line, such as expenditure for cybersecurity-related systems and technologies.

Some of these business imperatives can be mitigated where government can make the case that additional security-related initiatives are a matter of overriding public concern. As

increased public awareness and government initiatives raise the profile of cybersecurity risks, businesses would be expected to take such matters into account in their operations.

Over time, cybersecurity concerns are expected to become viewed as an integral aspect of a company's product or service, as opposed to a matter of regulatory concern. As public awareness is increased about cybersecurity, consumers will increasingly expect businesses to address cybersecurity concerns in their products and services which, for example, can be seen increasingly in the software industry where consumer operating systems are more commonly being bundled with anti-spyware protection and firewall software.

4 Cybersecurity and the individual

To a large extent, consumers without significant protection against viruses and other malware prevalent in today's computer environment represent the greatest source of vulnerability to the CII. In numerous reported incidents, inadequately protected PCs connected to the Internet have been used to perpetuate cybercrime and mobilized to launch cyber attacks. At the same time, individuals are also the victims of a wide range of cybercrimes and cyber nuisances such as spam, phishing, and computer fraud.¹⁶ As both cybersecurity hazard and victim, the implementation of measures to address the vulnerabilities of individual ICT users is an important facet of any concerted cybersecurity effort.

4.1 The role of the individual

Because the technology generating cyber risks makes it very difficult to fight potential attackers in advance, the adoption of technical and procedural protective measures becomes a crucial element in ensuring security. Here, end-users are in a key position as they alone are in the position to install technical safeguards for IT security at the most basic level.

At its most basic, effective security at the level of the individual involves some degree of familiarity with cybersecurity threats (e.g. viruses, spam, etc.) and the adoption of appropriate technical safeguards (e.g. anti-virus software, firewalls, etc.). As such, a large part of governmental efforts to boost cybersecurity have focused on the dissemination of basic cybersecurity awareness. In this respect, a host of resources from government and the private sector have been made available for individuals to learn more about the role they are expected to play in cybersecurity.

4.2 The role of civil society

Society's range of interests is represented in many countries by a variety of civil society groups that take on various forms and functions. These can range from consumer rights advocacy organizations to environmental groups.

In recent years, civil society groups in a number of countries such as the United States and Canada have taken a greater interest in cybersecurity as they come to understand the range of societal issues cybersecurity raises. These can include human rights, civil liberties, privacy, and consumer protection, among others. A small but growing number of civil society not-for-profit organizations have also been established around the issue of cybersecurity and cybercrime itself.¹⁷

¹⁶ For other examples, "Cybersecurity Guide for Developing Countries", ITU, 2009 available at <http://www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdf>

¹⁷ See, for example, The Society for the Policing of Cyberspace at <http://www.polcyb.org/> and the Open Information Systems Security Group at <http://www.oisssg.org/>

In consultations with government, feedback and other contributions from such groups can serve as an important source of information to policy-makers that seek to create a holistic cybersecurity approach that takes into account interests beyond that of government and business.

5 Cybersecurity and international cooperation

Because of the “borderless” nature of the Internet and cyberspace, cybersecurity crimes, threats and attacks can originate from one country and affect another easily making investigation and law enforcement difficult. As such, there is a strong and pressing need for robust international cooperation in cybersecurity.

Cooperation in cybersecurity can take place on many levels (e.g. regional and international) and across many dimensions (cybercrime, incident response, cyber-terrorism, etc.). International cooperation can involve binding conventions and protocols or they can also involve information sharing (Box 3).¹⁸

Box 3: The ITU Global Cybersecurity Agenda (GCA)¹⁹

As facilitator for WSIS Action Line C5 dedicated to building confidence and security in the use of ICTs, ITU is working closely with key stakeholders to respond to the growing cybersecurity challenges in a coordinated manner. As such, the ITU Global Cybersecurity Agenda is designed as an international framework for cooperation and response, and for building partnerships and collaboration between all relevant parties in the fight against cyber-threats. Launched in 2007 by ITU Secretary-General, Dr. Hamadoun I. Touré, the ITU GCA is a framework for international cooperation aimed at enhancing confidence and security in the information society. The GCA is designed for cooperation and efficiency, encouraging collaboration with and between all relevant partners and building on existing initiatives to avoid duplicating efforts.

Source: Information on the Global Cybersecurity Agenda (GCA) at <http://www.itu.int/cybersecurity/gca/>

Because of the multi-sectoral nature of cybersecurity, effective international collaboration requires the involvement of all affected stakeholder groups. An example of such an inclusive approach can be found in the collaboration between ITU and the International Multilateral Partnership Against Cyber-Threats (IMPACT) (Box 4).

Box 4: The ITU-IMPACT Collaboration

Established within the framework of the ITU Global Cybersecurity Agenda, the ITU-IMPACT collaboration aims to bring key stakeholders and partners from governments, private sector companies and academia together to provide ITU Member States with the expertise, resources and capabilities to effectively address cyber-threats.

The key objectives of the ITU-IMPACT collaboration include:

- Real-time analysis, aggregation and dissemination of global cyber-threat information;

¹⁸ For a more detailed discussion of international cooperation on cybersecurity see the section on International Cooperation for Cybersecurity in the ITU Global Cybersecurity Agenda (GCA) High Level Experts Group (HLEG) Global Strategic Report, ITU, 2008 available at http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html

¹⁹ Information on the Global Cybersecurity Agenda (GCA) is available at <http://www.itu.int/cybersecurity/gca/>.

- Early warning system and emergency response to global cyber-threats; and
- Training and skills development on the various aspects of cybersecurity.

The ITU Telecommunication Development Bureau through its programmes and initiatives facilitates the development and establishment of these resources and capabilities, in line with international cooperation principles while taking into account national and regional requirements. Specific activities are being undertaken, such as:

- Developing a global framework for watch, warning and incident response;
- Establishing appropriate national and regional organizational structures and policies, such as National Computer Incident Response Teams (CIRT);
- Facilitating human and institutional capacity building across sectors; and
- Facilitating global multi-stakeholder international cooperation.

Source: <http://www.itu.int/ITU-D/cyb/cybersecurity/impact.html>

PART II:

THE EVOLVING ROLE OF THE REGULATOR IN THE AREA OF INFORMATION AND NETWORK SECURITY

6 The role of the regulator

Since the first telecommunications sector specific regulators were established, regulators have assumed a wide variety of roles that differ widely from country to country. Over time, new regulators were established with different mandates while more established regulators had their mandates changed to take into account the phenomenon of convergence and the increasing importance of ICTs to the nation.

6.1 The core duties of the regulator

Regulators in most countries, at their core, perform a traditional set of roles. As highlighted by the ITU-infoDev ICT Regulation Toolkit, the most important duties of the regulator include:

- implementing the authorization framework;
- promoting competition (including tariffs);
- interconnecting networks and facilities;
- implementing universal service/access mechanisms;
- managing the radio spectrum; and
- minimizing the burden and costs of regulation and contract enforcement.²⁰

To some extent, the early role of the regulator focused on carrying out these core economic and technical regulation duties in the context of taking the telecommunications market from monopoly to competition. During that period, the scope of these duties typically extended to telecommunications (as opposed to ICT) and was largely focused on a limited number of stakeholders, in particular the incumbent, with less attention paid to consumers and end users. Involvement in policy-making, industry development, and consumer protection were uncommon.

6.2 The evolving role of the regulator

Globally, the role of the regulator has evolved as technology has evolved, and as markets have opened to competition. Notably, this evolution has been marked by:

- A more prominent role for regulators

Technological changes have dramatically increased the usage and importance of ICTs, in turn bringing the role of the regulator into greater prominence. Regulators in many countries today play an important role in shaping ICT policy. In some cases, regulators also play an active role in managing and promoting ICT sector development.

- A widening of the regulator's scope of regulation (from telecommunications to ICTs)

²⁰ See ITU-infoDev ICT Regulation Toolkit at <http://www.ictregulationtoolkit.org/en/Section.3105.html>

Marked by the transition from analogue to digital, narrowband to broadband, voice to data, and circuit switched to packet switched, the phenomenon of convergence has led to an expansion of the regulator's core focus to include services that go beyond just voice. The markets that regulators oversee have also changed dramatically with convergence allowing previously separate industries and entirely new sectors to compete in the same newly expanded market space. The management of a transition to an e-economy has become a key function of many regulators worldwide.

- An expanded regulatory mandate to include the engagement of more stakeholders (e.g. civil society, individuals, etc.)

With ICTs becoming more accessible and indispensable to individuals, many regulators have an expanded role so as to be able to focus on issues such as capacity building, consumer protection and consumer awareness. In many countries, traditional universal access objectives have also been expanded to encompass the national objective of building of an inclusive e-society.

With the larger role regulators play in this current ICT environment, regulators have found themselves increasingly well positioned in terms of mandate, resources and experience to deal with current and emerging cybersecurity challenges.

7 The role of the regulator in cybersecurity

In Section 2.1 above, the different areas of a national cybersecurity effort where government plays significant roles were highlighted and discussed. This Section builds on that discussion by examining the roles regulators already play (or are poised to play) in those areas.

In particular, the discussion will highlight the following issues:

- What role does or can a regulator play in each particular area of cybersecurity?
- What different issues does the regulator need to consider when getting involved in these areas?
- What core competencies and resources of the regulator are critical in this process and what can be done to build the capacity of the regulator in the event it does not possess the necessary resources or competencies?

7.1 Cross-cutting competencies and prerequisites

Before embarking on an area-by-area analysis and discussion, there are a number of cross-competencies that regulators will have to demonstrate before taking an active role in any aspect of cybersecurity. These include:

7.1.1 *Institutional maturity*

Integrating cybersecurity concerns with the traditional regulatory framework may be a complex task in countries which have only recently established regulatory institutions. These institutions are already burdened with a long list of tasks associated with their core responsibilities such as licensing and interconnection. They also face a complex range of challenges that are associated with convergence and the introduction of new technologies.

In such a situation, it may be more difficult for such regulators with their fledgling status to achieve credibility in significant areas of cybersecurity given its close association with

national security policy. In many countries security issues have been the near exclusive domain of the more established military, law enforcement and the intelligence community.

Regulators in such a situation may have to define their roles carefully and identify ways that they can participate in cybersecurity activities and advise on cybersecurity policy without necessarily being the lead institution. Such regulators would be advised to look closely at the range of cybersecurity roles and responsibilities undertaken by other regulators and to decide which options and approaches are best suited to their own national context. They will need to appraise realistically what they can and cannot do and what needs to be left to others to manage and lead.

7.1.2 Engagement of the private sector

Regulators possess a well established set of mechanisms and processes to facilitate engagement of the private sector for the purposes of consultations as well as for the purposes of facilitating industry self-regulation. Across the globe, examples of regulator initiated public-private sector forums abound. Such forums deal with issues such as infrastructure sharing, interconnection and consumer protection. For example, the Malaysian Communications and Multimedia Commission (MCMC) has facilitated the establishment of a range of industry self-regulation forums focusing on issues such as access, content, consumer protection and technical standards.²¹ The same set of mechanisms and processes can be leveraged in the same way when addressing issues related to cybersecurity.

7.1.3 Technical and industry expertise

With technical regulation being a core function of regulators and technological familiarity being a prerequisite for the regulation of the ICT sector as a whole, regulators as an institution possess an in depth technical knowledge of ICTs, often employing technical experts and specialists in their staff. As cybersecurity risk factors are largely technologically driven, regulators are poised to play a leading role in identifying and explaining for cybersecurity policy makers the technicalities involved in potential cybersecurity concerns.

7.1.4 Mandate and jurisdiction

Despite the expanded role of many regulators in general, an extension of the regulator's mandate to cover issues related to cybersecurity cannot be taken for granted. Given the rapid developments in the field of cybersecurity, the cybersecurity policies and frameworks in many countries are constantly undergoing transformation. As such, in many cases there is a lack of clear jurisdictional boundaries that delineate the areas of responsibilities between the different government institutions dealing with cybersecurity issues. In such a situation, the exact scope of responsibility of a regulator with regard to cybersecurity may not be marked out clearly, leaving regulators little guidance as to their role in that field. Such a situation presents both challenges and opportunities.

In a number of countries, regulators have progressively established their role in the field of cybersecurity by building on the clear mandates that they have been given. One good example can be seen in the case of spam. Regulators in many countries have been dealing with the issue of spam as a significant consumer-protection problem and burden on the national ICT infrastructure. For example, the Dutch regulator OPTA deals with the problem of spam and malicious software - and Internet safety in general - under its wider mandate of consumer protection.²² Spam can also be a vehicle for generating BOT viruses that can lead to DDOS

²¹ For more information, see <http://www.skmm.gov.my/>

²² See, for more information, OPTA 2008 Annual Report available at <http://www.opta.nl/>.

attacks against critical information infrastructures. In this light, spam is increasingly being seen as a potential cybersecurity risk and, in turn, a link to the concerns of policy makers concerned with cybersecurity and the protection of critical infrastructure. In this way the spam issue has become an effective vehicle for regulators to become a more integral part of national cybersecurity efforts.

Similarly, the regulator's traditional role in managing communications in times of emergency and crisis can also provide a suitable avenue for its involvement in cybersecurity, particularly in efforts related to incident monitoring and cybersecurity readiness assessments (see Section 7.5.2 below). In many countries, regulators have long exercised responsibilities in the area of crisis-related communications (see Box 5). They may have had roles, at times in cooperation with other agencies concerned with emergency preparedness or national defense, in developing and implementing plans for responding to natural disasters or other civil emergencies where demands on ICT infrastructure may exceed available resources and capacity must be allocated on a system of priorities.

Box 5: Crisis communications and the Norwegian Post and Telecommunications Authority (NPT)

The Norwegian regulator, the NPT is tasked with overall contingency planning with regard to the public electronic communications infrastructure. Its wide range of responsibilities related to communications security includes the following:

- Considering investment in measures designed to increase the robustness of the telecom networks;
- Conducting inspections to see that the required measures are implemented;
- Creating awareness of communications security and contingency planning, improving the necessary related expertise, and offering guidance to operators, users and other players (e.g. through courses, seminars, company visits, establishment of forums of expertise, etc.); and
- Arranging joint exercises and developing cooperation between the operators of telecom networks.

Electronic communications providers who provide essential electronic communications services to users who have socially critical functions must notify the NPT of significant operational and technical problems that could reduce or have reduced the quality of services.

Source: NPT at <http://www.npt.no/>

As the cybersecurity takes on more national security-related overtones, the jurisdictional claims of regulators may lead to some friction with government institutions that have been more traditionally associated with national security issues. In such a situation, regulators may require a clearer mandate with regard to their cybersecurity role. Such a mandate can be granted by provisions in new cybersecurity legislation, legislative amendments to existing ICT legislation, executive decrees, internal government directives and other similar measures.

7.1.5 Appropriate resourcing

In order to carry out its roles and responsibilities effectively, a regulator has to have the appropriate financial and manpower resources. In an ideal situation, additional financial resources are given in tandem with the assumption of new roles and responsibilities either through general government appropriation or through special grants or funds.²³

²³ For example, in the United States, under the 2010 Budget, USD355 million in funding was earmarked for cybersecurity and technology R&D that will support the base operations of the National

In the absence of additional funding, regulators in a number of countries have relied on vehicles such as public-private sector partnerships to reduce the costs of cybersecurity initiatives. The consolidation of certain functions and tasks can also result in synergies and cost savings (see, for example, Box 16 below).

7.2 Engagement in international cooperation

Engagement on the part of regulators in a number of key platforms dealing with international and regional cybersecurity cooperation can greatly increase the value of their contribution to the overall national cybersecurity effort.

Through a long history of participation in a wide range of ITU activities, regulators are well positioned to engage in international cooperation and information sharing through, for example, the Global Cybersecurity Agenda which was established by the ITU following a specific mandate from WSIS (see Box 3 above).

In addition, a large number of regulators already actively participate and contribute to the ITU's global cybersecurity-related standardization activities (see Box 6).

Box 6: ITU standardization activities related to cybersecurity

ITU-T Study Group 17 is the Lead Study Group on Communications System Security and handles security guidance and the coordination of security-related work across all ITU-T Study Groups. It is responsible for studies on security, the application of open system communications (including networking and directory), technical languages and other issues related to the software aspects of telecommunication systems. It has approved over one hundred Recommendations on security.

ITU's Focus Group on Identity Management was established by Study Group 17 to facilitate the development of a generic Identity Management framework with the participation of experts on Identity Management. The Focus Group may analyze other aspects related to such a framework.

Source: ITU at <http://www.itu.int/ITU-T/studygroups/com17/index.asp> and <http://www.itu.int/ITU-T/studygroups/com17/fgidm/index.html>

Considering the core competencies possessed by regulators, in particular their ICT technical and industry expertise other regional and international cooperation platforms that may be suited for regulator participation include:

- OECD Working Party on Information Security and privacy²⁴;
- Telecommunications and Information Working Group (TEL) of the Asia-Pacific Economic Cooperation (APEC) (see Box 7) and
- Forum of Incident Response and Security Teams (FIRST)²⁵.

Cyber Security Division, as well as initiatives under the Comprehensive National Cybersecurity Initiative. More information can be found at http://www.whitehouse.gov/omb/assets/fy2010_new_era/Department_of_Homeland_Security.pdf

²⁴ For more information, see

http://www.oecd.org/departement/0,3355,en_2649_34255_1_1_1_1_1,00.html

²⁵ The "Forum of Incident Response and Security Teams" (FIRST) was established in 1990 and provides a meeting point for CSIRTs worldwide. It promotes active cooperation in incident response. It is comprised of more than 200 public and private sector CSIRTs. Other regional forums and bodies

Box 7: The Asia-Pacific Economic Cooperation (APEC)

APEC is an inter-governmental grouping comprising 21 member economies. It has no treaty obligations required of its participants. Decisions made within APEC are reached by consensus and commitments are undertaken on a voluntary basis.

On May 30, 2002, the Telecommunications and Information Ministers of the APEC economies issued the 'Shanghai Declaration' that included a Statement and Program of Action on the Security of Information and Communications Infrastructures. The Statement endorsed action by member economies to combat criminal misuse of information and instructed its Telecommunications and Information Working Group (TEL) to give special priority to work on the protection of information and communications infrastructures.

Initiatives that followed include:

- the APEC Cybersecurity Strategy, which includes a package of measures to protect business and consumers from cybercrime, and to strengthen consumer trust in the use of e-commerce;
- the TEL Cybercrime Legislation initiative and Enforcement Capacity Building Project that supports institutions in implementing new e-security laws; and
- the creation of APCERT, a regional CERT covering APEC member economies.

Source: APEC at <http://www.apec.org/>

It is also interesting to note that international regulator forums, such as the ITU Global Symposium for Regulators (GSR), as well as regional regulator groupings such as the Asia-Pacific Telecommunity (APT) and the Inter-American Telecommunication Commission (CITEL), are increasing their focus on cybersecurity issues²⁶. These international and regional efforts serve to further reinforce the core competencies of regulators in the area of cybersecurity.

7.3 Policy-making

In a large number of countries, regulators play an important part in the development of a national ICT strategy or policy. Although the responsibility for ICT policy making in general is typically delegated to a political body such as a Ministry, regulators often play a key supporting role in policy-making by virtue of their familiarity with the sector that they regulate, the resources available to them, and the processes and mechanisms that have been put in place to engage in consultations with industry stakeholders.

Roles and responsibilities

From a survey of international examples, it is possible for regulators to take on a number of roles in the policy-making area:

- The lead role in cybersecurity policy-making (see, for example, Box 8); and
- Provider of advice and inputs on cybersecurity policy (see, for example, Box 9).

promoting cooperation among CSIRTs include the European Government CERTs group (EGC), NORDUnet, CEENet and APCERT (part of the Asia Pacific Economic Cooperation or APEC).

²⁶ See, for example, the initiatives undertaken by the APT at <http://www.aptsec.org/links/NSS/Default.htm> and the ongoing work of the CITEL Rapporteur Group on Cybersecurity and Critical Infrastructure at <http://www.citel.oas.org/ccp1-tel/Cybersecurity.asp>.

Box 8: Cybersecurity policy-making in Singapore

The Infocomm Development Authority of Singapore (IDA) acts as the national ICT regulator, the ICT development and promotion agency and the chief technology office of the Singapore government.

Singapore's cybersecurity strategy is encapsulated in two Infocomm Security Master-plans launched in 2005 and 2008. These master-plans provide a national strategic roadmap for the development of ICT security capabilities. They were developed through a multi-agency effort led by IDA through the guidance of the National Infocomm Security Committee (NISC).

Source: IDA at <http://www.ida.gov.sg/>

Box 9: Cybersecurity and the National Broadband Plan of the United States

As part of a wider national cybersecurity reassessment taking place in the United States, a comprehensive draft Cybersecurity Act has been introduced for adoption. Among other matters, the Cybersecurity Act delegates the Federal Communications Commission (FCC) with new responsibilities related to its implementation of the national broadband plan that it must develop under the American Recovery and Reinvestment Act of 2009. Under the Cybersecurity Act, the FCC is required to report on the most effective and efficient means of ensuring cybersecurity of commercial broadband networks. As part of its report, the FCC is required to consider consumer education and outreach programmes.

Source: Cybersecurity Act of 2009 (Introduced in Senate) at <http://thomas.loc.gov/cgi-bin/query/z?c111:s773>:

Core competencies

In most cases, regulators are poised to play a large role in the design of a national cybersecurity strategy and the formulation of related cybersecurity policies given their core competencies:

- Establishment of the role of the regulator in providing input on ICT policy making in general

As ICT sector specialists, regulators in many countries play a vital advisory role in the formulation of national ICT policy promulgated by national governments. In many countries, such a policy advisory role has been enshrined as one of the functions regulators have been tasked to perform.²⁷ With cybersecurity being increasingly recognized as a prominent ICT-related issue, regulators with policy advisory functions will increasingly find themselves required to provide inputs on cybersecurity issues. As part of their work on Next Generation Networks, many regulators are already examining the cybersecurity dimension of their introduction.

- Availability of tools vital to policy-making

As part of their ICT market oversight role, many regulators conduct studies and research, and collect and compile important data and information of the status of national ICT

²⁷ See, for example, Section 7 of the Bahamas' Communications Act (2009) and Section 1(2) of the Danish Act on the National Telecom Agency (Act No. 395 of 10 June 1997).

development and usage.²⁸ In the context of the formulation of a national cybersecurity strategy, such information can be used to highlight the importance of ICTs to the nation, the threats and vulnerabilities posed by such reliance, and the role cybersecurity plays in mitigating the risks.

- Establishment of mechanisms, processes and relationships for consultation and feedback

As part of the regulatory process, regulators in many countries are required to engage in consultation with sector stakeholders which can include industry, civil society and individuals. With these established mechanisms and relationships in place, regulators are in a position to solicit ICT stakeholder inputs on cybersecurity policy efficiently and quickly.

Observations and recommendations

A number of issues present themselves when regulators assume a larger role in cybersecurity policy-making. In some cases, these issues revolve around concerns to be addressed before a greater level of involvement on the part of the regulator can be assumed.

- Regulator as policy-maker

A greater involvement on the part of the regulator in policy making in general may threaten the traditional separation between policy-making and regulation. In the interest of the widely accepted principle of separation of powers, situations where a regulator formulates policy, implements related regulations, and enforces its application should be avoided.²⁹

- Establishing the requisite mandates

While many regulators have been given an express mandate to provide input on ICT policy-making in general, this may not be so in the specific case of cybersecurity policy. In countries where regulators do not possess a mandate to provide input into cybersecurity policy-making, a change in the enabling legislation may be necessary. In most cases, however, such a mandate can be accommodated through the wide wording of existing provisions on the duties and functions of regulators (see, for example, the discussion on spam in the context of mandate and jurisdiction in Section 7.1.4 above).

- Building broad cross-sector expertise and establishing inter-agency relationships

An in-depth familiarity with the ICT sector addresses only one aspect of cybersecurity, albeit an important one. In order to take a prominent or leadership role in cybersecurity policy-making, the regulator also needs to be familiar with the ICT issues that affect other key sectors of the nation such as the finance sector, the energy sector, and the public sector as a whole. Such inter-sector links can be forged through the establishment of working groups, the initiation of informal collaboration on projects and other similar avenues.³⁰

²⁸ For an overview of the ICT statistics and indicators made available through the websites of regulators, see <http://www.itu.int/icteye/>.

²⁹ See, in general, the discussion on Separation of Powers in the ITU-infoDev ICT Regulation Toolkit available at <http://www.ictregulationtoolkit.org/en/Section.1269.html>.

³⁰ See, for example, the general discussion on the importance of inter-agency links in ICT development in Francisco J. Proenza, "ICT-Enabled Networks, Public Sector Performance and the Development of

- Obtaining appropriate resourcing

As with the execution of any other role or responsibility of the regulator, the regulator must be in possession of the requisite resources and staffing in order to perform its policy-advisory role competently. In the context of cybersecurity policy-making, staffing in particular may be an issue where the regulator's manpower needs in the area of strategy and policy overlap with that of the main policy-maker. Such a situation may become a strain on skilled manpower resources in developing countries. In such a case the options of training or outsourcing may need to be considered (see also Section 7.1.5 above).

7.4 Legal measures

In most countries, the enactment of cybersecurity legislation is largely the prerogative of a country's legislature. The drafting of legislation, while typically entrusted to a legal institution such as the Attorney-General's Office or the Ministry of law, necessarily also takes into account a range of inputs from relevant government institutions.

The compliance and enforcement of cybersecurity laws are entrusted to law enforcement agencies that, in some circumstances, rely on the expert advice from more specialized government institutions. In some circumstances, regulators themselves have law enforcement powers associated with their mandates.

Roles and responsibilities

Regulators have assumed a range of roles and responsibilities in the area of legal infrastructure, compliance and law enforcement. These include:

- Acting in an advisory role in the drafting of cybersecurity related legislation (see Box 10);
- Providing technical training to legislators, prosecutors, the judiciary and law enforcement on the ICT related technical aspects of cybercrime;
- Acting in an advisory role in the development of specialized national cybercrime enforcement units;
- Providing technical assistance in the investigation of cybercrimes;
- Enforcing cybersecurity laws and regulations that are within the regulator's mandate (see Box 11); and
- Participation in international anti-cybercrime efforts (e.g. the 24/7 Cybercrime Point of Contact Network).

Box 10: Cybercrime and the role of the Nigerian Communications Commission (NCC)

The NCC is a member of the Nigerian Cybercrime Working Group (NCWG), an inter-agency group dealing with cyber crime which has the two-fold purpose of dealing with the security of computer systems and networks as well as the protection of the critical ICT infrastructure.

The NCWG has established a cybersecurity forum intended to build consensus among existing agencies and provide expertise to the National Assembly in drafting new computer security legislation (the Computer Security and Critical Information Infrastructure Protection Bill). The working group lays the groundwork for establishing new institutional capacity in Nigeria as well as for global cybercrime enforcement through relations with the Computer

Information and Communication Technologies", 2003 available at <http://www.e-forall.org/pdf/ICTEnabledNetworks.pdf>

Crime and Intellectual Property Section (CCIPS) of the United States Department of Justice, National High Tech Crime Center (NHTCC) in the United Kingdom and the National Prosecuting Authority (NPA) in South Africa.

Source: Presentation to the ITU Regional Cybersecurity Forum for Africa and Arab States, Tunis 2009, M.U. Maska, "Building National cybersecurity Capacity in Nigeria", available at <http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/maska-nigeria-cybersecurity-june-09.pdf>

Box 11: Enforcement of cybersecurity offences under Malaysia's Communications and Multimedia Act (CMA)

Information security and the integrity and reliability of the network of Malaysia are identified as one of the ten national policy objectives in the CMA. Together with the police, the Malaysian regulator, the Malaysian Communications and Multimedia Commission (MCMC) has enforcement powers for offences relating to network security in the CMA.

Source: Malaysian Communications and Multimedia Commission (MCMC) at <http://www.skmm.gov.my/>

Core competencies

The level and form of involvement of regulators in the area of legal infrastructure, compliance and enforcement can depend on:

- The nature of cybersecurity legislation

In many countries, regulators play a key role in the review and adaptation of a wide range of cybersecurity related legislation by providing input on the nature of cyber threats and cyber crimes. The role of the regulator in providing such advice varies depending on the subjective expertise of the regulator and the cybersecurity-related law at hand. For example, regulators in general would be more familiar providing input on laws dealing with data protection and security in electronic communications (including data transmission, safe data storage, etc.) as opposed to laws dealing with computer assisted fraud.

- Existing legal mandate

A legal mandate to undertake investigations and the enforcement of legal provisions is a basic prerequisite for a regulator's involvement in the compliance and enforcement of cybersecurity laws. In this respect, supportive legislation (e.g. the granting of a wide scope of powers necessary for investigation such as the ability to enter upon premises, seize equipment and retrieve and store incriminating data) is necessary for the regulator to perform such a role (see Box 10 above).

ICT legislation in most countries grants the regulator powers of investigation and enforcement over certain areas. In many cases, these typically extend to the use and abuse of ICT networks, physical damage to ICT installations and similar offences. As highlighted before, some regulators also exercise a mandate to counter malicious activities like spyware and spam under their wider duty of consumer protection.

- Appropriate resources

Even if a regulator is empowered with a mandate to ensure compliance with cybersecurity laws, the enforcement of such laws is often difficult. Frequently, the necessary means to

investigate and prosecute misdemeanors such crimes effectively are lacking due to resource constraints.

The conduct of investigation and enforcement proceedings consumes a significant amount of the limited resources available to regulators. In complex cases, investigations may take a long time to conclude with the process for prosecution taking an equally lengthy period of time. In such situations specialized manpower resources can be tied up indefinitely. In order to avoid the perception of the lack of law enforcement in affected areas, it is therefore important to ensure that regulators have the necessary resources to undertake the enforcement roles that they assume. Regulators can also collaborate with or seek the assistance of other law-enforcement agencies that may have more specialized resources available.

7.5 Organizational structures

7.5.1 Institutional organization and coordination

While regulators are not typically established as high-level governmental institutions (e.g. at presidential or cabinet level), an independent regulator can nevertheless play a significant role in both (1) the organization and coordination of cybersecurity roles and responsibilities among appropriate government institutions and (2) the establishment of coordination and cooperation mechanisms involving private sector cybersecurity stakeholders.

Roles and responsibilities

While it is unlikely for a regulator to take the lead in the delegation of cybersecurity responsibilities among government institutions - such a role is typically reserved for the highest-levels of government - a regulator can nevertheless play a key role in the coordination of governmental cybersecurity activities such as, for example, acting as secretariat for inter-governmental cybersecurity committees or task forces established by the lead cybersecurity institution (see Box 12) or by taking the initiative to forge cybersecurity relationships directly with other government institutions (see Box 13 below).

Box 12: Singapore's ICT regulator as secretariat for cybersecurity policy and institutional coordination

The National Infocomm Security Committee (NISC) was set up to formulate policies and strategic direction for cybersecurity at the national level. With members from various government agencies, it is a platform for the government to coordinate and institutionalize considered policies and mandate strategic initiatives in IT security.

The NISC comprises representatives from the Ministry of Home Affairs, the Ministry of Defence; the Ministry of Information, Communication and the Arts; the Ministry of Finance; and the Defence Science and Technology Agency (DSTA) among others. The ICT regulator, IDA serves as the secretariat for this Committee.

Source: Infocomm Development Authority of Singapore (IDA) at <http://www.ida.gov.sg/>

Core competencies

The degree to which regulators are adapted to these roles will depend on a number of core competencies:

- Establishment of relationships with national security institutions

A coordinating role in cybersecurity requires a high level of skills in bridge building, in particular with institutions that have intelligence and national security-related portfolios. In many countries policy concerns with cybersecurity are significantly influenced by national security and intelligence policies and the coordinator will have to have significant credibility in this area. In this respect, many regulators enjoy close working relationships with law-enforcement, defense and intelligence institutions in the areas of radio-frequency allocation, legal intercept, and crisis and emergency communications.

- Establishment of inter-agency relationships

The cybersecurity coordinator must be able to bring together other ministries or departments with sector-specific oversight of different critical infrastructure services and sectors. Cybersecurity often involves sectors such as finance (e.g. finance ministries and financial services authorities), energy (e.g. energy ministries and independent energy regulators), and health (e.g. health ministries and health authorities) (see Box 13).

Box 13: Inter-agency cooperation on cybersecurity in the United Arab Emirates (UAE)

In May 2009, the UAE Telecommunications Regulatory Authority (TRA) and the Ministry of Water and Environment signed a Memorandum of Understanding (MoU) on cooperation in cybersecurity. The MoU is expected to assist the Ministry in achieving its goals of enhancing the environmental security, adopting integrated management, increasing biological security, and achieving food security.

Under the MoU, aeCERT, an initiative of the TRA, will provide specific services to enhance the security of the Ministry's ICT infrastructure through the provision of consultancy services, education and awareness; incident monitoring and response; and research and analysis.

A similar MoU was subsequently signed between the TRA and the UAE Community Development Authority (CDA) in September 2009.

Source: UAE Telecommunications Regulatory Authority (TRA) at <http://www.tra.gov.ae/>.

Regulators that have the mandate of promoting ICT adoption in the public sector may already have mechanisms in place (e.g. working groups) that allow for inter-agency coordination and information exchange.

- Experience with breaking down compartmentalization

An important task of a cybersecurity coordinator will be to break down natural tendencies to “compartmentalize” cybersecurity activities in a series of separate sectors. In cybersecurity incidents in one sector will have potential relevance in other sectors. With their experience in dealing with convergence ICT regulators are in a good position to manage issues that the different sectors may attempt to compartmentalize or exclude. Regulators are also neatly positioned as neutrals in the cybersecurity discussion, with ICT networks and technologies being the common thread that runs through the different issues involved in cybersecurity.

Observations and recommendations

- Establishing inter-agency relationships

As mentioned above, the involvement of the regulator in the organization and coordination of government institutions involved in cybersecurity requires the regulator to have established working relationships with the lead cybersecurity institution as well as other government institutions involved in cybersecurity. Where this is absent, regulators may find it more appropriate to establish such relationships by participating actively in such coordinating bodies, while over time assuming greater responsibilities, such as the role of secretariat or convener. In parallel, independent inter-agency links should still continue to be forged (see the example in Box 13 above).

- Obtaining appropriate resources

The task of organization and coordination in general will compete with other pressing regulatory priorities; therefore regulators should be first assured that they have the resources to support the role that they intend to assume in this area of cybersecurity.

7.5.2 Incident management and cybersecurity readiness assessment

As mentioned in Section 2.1.3 above, one of the most critical aspects of an overall cybersecurity program is the capability to detect, to investigate and analyze, and to respond to cyber-related incidents.

Roles and responsibilities

In the area of incident management, a number of regulators have undertaken the following roles:

- Establishing national cybersecurity incident monitoring facilities (e.g., CSIRTs³¹) (See Box 14) and
- Participating in international and regional cybersecurity incident monitoring initiatives (e.g., Asia Pacific Computer Emergency Response Team (CERT), Forum of Incident Response Security Team (FIRST), etc.).

Box 14: Establishment of the Swedish IT Incident Centre (SITIC)

In May 2002, the regulator, the Swedish National Post and Telecom Agency (PTS) established the Swedish IT Incident Centre (SITIC). Officially launched in January 2003, the SITIC supports national activities for protection against IT incidents by:

- Operating a system for information exchange on IT incidents between public and private organizations and the SITIC;
- Operating a public warning system providing information on threats to IT systems;
- Providing information and advice on security and counter measures;
- Compiling and publishing incident statistics.

Source: Swedish IT Incident Centre (SITIC) at <http://www.sitic.se/>

In the area of cybersecurity risk assessments, a number of regulators have undertaken the following roles:

- Preparing and implementing periodic cybersecurity risk assessments, audits and reviews on a national or a sector-by-sector level (e.g., financial, manufacturing, retail, etc.) (see Box 15); and

³¹ For example, in Finland, CERT-FI was established under the umbrella of the regulator, FICORA. Similarly, in the UAE, aeCERT was also established under an initiative by the regulator, TRA.

- Conducting cybersecurity exercises to test readiness and responsiveness.

Box 15: Critical Infocomm Infrastructure Surety Assessment in Singapore

Under the leadership of the Infocomm Development Authority of Singapore (IDA), the Critical Infocomm Infrastructure Surety Assessment project was established to assess the security readiness of Singapore's critical information and communications infrastructure. Initiated as a public-private sector project, it provides a platform for owners and operators of CII to work together and ascertain the adequacy of their protection measures.

Source: Infocomm Development Authority of Singapore (IDA) at <http://www.ida.gov.sg/>

Core competencies

- Crisis communications

The role of regulators in crisis related communications was highlighted in Section 7.1.4 above. Nevertheless, while responsibility for cybersecurity related emergencies may have been assumed by some regulators on the basis of their experience in this area, the nature of cybersecurity emergencies and crises are significantly different often requiring a more dedicated approach than might have been the case in the past. As such many regulators have set up CSIRTs that, while under the umbrella of the regulator, function as a specialized independent unit.³²

- Consolidation of responsibilities and resources

The establishment of a CERT or similar body requires a certain amount of resources to be expended given its round the clock monitoring function. Similarly, the responsibility of regulators to maintain round the clock responsiveness to communications related emergencies and crisis acts as a similar drain on resources. In this respect, the consolidation of all communications related emergency monitoring functions in a single institution may result in synergies that allow for lower resource expenditure (see Box 16).

Box 16: Incident monitoring and alert consolidation in Hungary

Hungary's regulator, the National Communications Authority, is responsible for the National Alert Service (NAS) in the postal and communication sectors. The NAS is based on the cooperation of designated service providers who report incidents affecting their services to the NAS. The main tasks of the NAS are to gather and distribute information based on these reports and to coordinate service provider responses in the case of natural disasters and other emergencies.

Given the significant overlap in terms of incident reporting and timely information dissemination, the operation of the NAS is assumed by the national CERT (CERT-Hungary) that is managed by the Theodore Puskás Foundation. The activities of the Foundation are funded by the private sector and the national government.

Source: International CIIP Handbook 2008/2009, Center for Security Studies, ETH, Zurich available at http://www.crn.ethz.ch/publications/crn_team/detail.cfm?id=90663

³² Ibid.

7.6 Capacity building

In Section 2.1.4 above, the importance of addressing cybersecurity awareness at the level of the end-user (i.e. individual businesses and consumers) was emphasized. In this regard, individual businesses and consumers can be empowered through a variety of means that would promote awareness and improve cybersecurity literacy and skills. Such initiatives increase the likelihood that end-users will consider cyber safety to be an integral part of the use of ICT products and services.

Roles and responsibilities

In the area of consumer awareness and capacity building, regulators can perform the following roles:

- Organization of cybersecurity awareness campaigns (e.g., media campaigns, online information resources, seminars, talks, road-shows, etc.) alone or in partnership with the private sector (see Box 17);
- Identifying cybersecurity education and training needs in the public and private sector and implementing initiatives to meet those needs; and
- Cultivate and develop a pool of cybersecurity professionals (see Box 18).

Box 17: Awareness campaigns in the United Kingdom

Get Safe Online is a public and private sector joint campaign to raise awareness of online security aimed at the general public and small businesses. Get Safe Online is sponsored by the United Kingdom Cabinet Office, the United Kingdom Office of Communications (Ofcom), the Serious Organised Crime Agency (SOCA), Microsoft, HSBC, Cable & Wireless, and Paypal.

The Get Safe Online initiative works with a range of community organizations and aims to give people the confidence to go online securely. The initiative coordinates marketing and PR activities as well as providing a comprehensive website with up-to-date advice, tools and guidance on general internet security. The website includes information on protecting individuals, families and businesses online, as well as advice on topics such as Internet shopping, social networking sites, data theft and identity fraud.

Source: <http://www.getsafeonline.org>

Box 18: Cybersecurity capacity-building in the Republic of Korea

In response to a spate of DDOS attacks in July 2009, the government of the Republic of Korea intends to train some 3,000 cybersecurity experts as part of measures to enhance Internet security. Announced by the Korean regulator, the Korea Communications Commission (KCC), the new measures, will involve the setting up of new departments in universities that will offer courses on information protection and provide support for the establishment of related research centers.

As part of the overall cybersecurity effort, the KCC will also undertake initiatives to encourage schools and companies to improve cybersecurity training and to raise awareness of Internet terrorism.

Source: Korea Communications Commission (KCC) at <http://www.kcc.go.kr/>

Core competencies

- Consumer protection initiatives

As part of the overall regulatory mandate of consumer protection, many regulators have been involved in the organization and implementation of consumer awareness initiatives that involve dissemination through a range of media (e.g. TV and newspaper advertising, websites, etc.). The same channels for dissemination can similarly be used for disseminating materials and information on cybersecurity.

- Adequate resourcing

Extensive campaigns involving media outlets such as television commercials, newspaper advertisements and online information involve a significant amount of resources that are likely to tax the resources of the regulator. To the furthest extent possible, such campaigns should be undertaken as part of a public-private partnership where resource needs can be shared between the regulator and the relevant private sector partners. Beyond resource sharing, public-private partnerships can bring significant synergies in the area of promoting end user awareness as businesses typically possess substantial experience in mounting advertising and promotion campaigns.

Observations and recommendations

- Ensuring that consumers as a class are able to have a say in cybersecurity policy

ICT regulators and policy-makers have an important role in dealing with consumers of telecom, ISP, and other ICT-related services. In particular, many regulators are tasked with an ICT consumer protection role, making them well positioned to make the case more broadly to the public and in government circles that consumers have an important role to play in developing an overall cybersecurity framework.

- Regulating to eliminate individual cybersecurity vulnerabilities

Given the significant cybersecurity vulnerabilities present at the level of the individual, the issue of whether regulations should be introduced to ensure a minimum degree of security at that level has been raised (see Box 19). This issue has also been discussed in the context of the mandatory requirement of licensing for end-users of PCs that are connected to the Internet.³³ Such an issue raises a range of policy questions that will require extensive consultations.

Box 19: Ensuring minimum security levels in Korea

Officials at the Korea Communications Commission (KCC), the country's broadcasting and telecommunications regulator, and the Korea Internet and Security Agency (KISA) confirmed they are planning to have Internet service providers, such as Korea Telecom, monitor the security levels of the computers and other devices used by their customers. The companies will limit or cut the Internet connectivity of users with less-than-required software protection, thus forcing them to upgrade their existing programs or download new ones.

³³ For an introduction to that discussion see, for example, "License PC Users? It's a Thought", available at <http://www.wired.com/politics/law/news/2001/08/46096> and "Crime expert backs calls for license to compute" at http://www.itnews.com.au/News/154129_crime-expert-backs-calls-for-licence-to-compute.aspx

Government organizations, schools, private companies and “PC-bangs” (or computer gaming centers), will be mandated to install a required level of security programs on their computers and update them when needed.

The KCC will also be granted the rights to suspend the business of software companies that fail to correct the vulnerabilities of their security programs after being ordered to do so by authorities.

The new rules will also grant government authorities the power to shut down “zombie” PCs, or computers infected with malicious software and programmed to spread the cyber attacks. KCC authorities, with the consent of the computer's owner, could inspect the device to track the routes of the cyber attack.

Source: Adapted from the article “Online security steps criticized excessive” available at <http://www.koreaitimes.com/story/5007/online-security-steps-criticized-excessive>

7.7 Private sector cooperation and industry regulation

Roles and responsibilities

A large number of regulators are in a position to lead cybersecurity coordination and cooperation activities that involve the private sector and industry having both the mandate to engage the private sector in policy consultations (see Box 20) and promote industry self-regulation, and the experience to do so.

Box 20: The Communications Security, Reliability and Interoperability Council in the United States

In 2007, the Communications Security, Reliability, and Interoperability Council (CSRIC) was formed to provide recommendations to the Federal Communications Commission (FCC) to ensure optimal security, reliability, operability and interoperability of communications systems, including public safety, telecommunications, and media communications systems. Among other tasks, its mandate includes:

- Recommending best practices and actions the FCC can take to ensure the security, reliability, operability, and interoperability of public safety communications systems;
- Recommending best practices and actions the FCC can take to improve the reliability and resiliency of communications infrastructure;
- Evaluating ways to strengthen the collaboration between communications service providers and public safety entities during emergencies and make recommendations for how they can be improved;
- Recommending methods to measure reliably and accurately the extent to which key best practices are implemented both now and in the future; and
- Making recommendations with respect to such additional topics as the FCC may specify.

Source: United States Federal Communications Commission (FCC) at <http://www.fcc.gov/>

In the technical and procedural area of cybersecurity, the regulator is poised to assume a more traditional industry regulation role. These include:

- Encouraging public-private sector efforts to develop cybersecurity standards, procedures, and codes of conduct;
- Developing or enforcing mandatory cybersecurity regulations (see Box 21); and
- Mandating or encouraging the adoption of international cybersecurity standards (e.g., ISO 27001 on Information Security Management System) and recommended best practices.

Box 21: Mandatory cybersecurity requirements in Estonia

The country's regulator, the Technical Surveillance Authority (TJA), oversees companies operating in the field of electronic communications and ensures the compliance of these companies with security requirements.

In this respect, the Electronic Communications Act defines the requirements for the availability of electronic communications networks and communications services. In the area of cybersecurity, the security requirements set out include a requirement for communications undertakings to guarantee the security of a communications network and prevent third persons from accessing the data without legal grounds.

The TJA also oversees the implementation of the Digital Signatures Act and introduces regulations in that regard. It also supervises the certification service providers that provide services under the Act.

Source: Estonian Technical Surveillance Authority (TJA) at <http://www.tja.ee/>

In some countries where governments support ICT R&D, such support may be channeled through the regulator (e.g. Singapore, Japan). In such a situation, some of that support could be channeled into the research and development of new cybersecurity technologies, techniques, standards and processes in partnership with academia and the private sector (see Box 22).

Box 22: Cybersecurity technology research in Japan

In Japan, the regulator, the Ministry of Internal Affairs and Communications (MIC), is responsible for developing the fundamental national infrastructure of Japan, including information and communications. In order to realize "secure and safe" communications as a social infrastructure, MIC promotes various policies that reinforce information security.

As part of its cybersecurity role, the MIC conducts research related to fundamental technologies related to measures against cyber-attacks and other network security issues and to the protection of personal information in the field of ICT, and carries out measures to upgrade emergency information functions in the telecommunications area.

Source: Ministry of Internal Affairs and Communications (MIC), Japan at <http://www.soumu.go.jp/english/> and International CIIP Handbook 2008/2009, Center for Security Studies, ETH, Zurich.

Core competencies

- Establishment of appropriate regulatory mandate

Ensuring the integrity of the main pipelines for delivery of ICT services is a key component of an overall cybersecurity program. With their familiarity in mandating and regulating technical standards and requirements, such as quality of service obligations,

regulators in general are well positioned to require or encourage providers of ICT backbone transmission and ISP services to adopt measures to minimize cybersecurity risks.

In a similar fashion, regulators can also play a critical role in providing a first line of defense against a range of new threats arising from the use of poorly protected PCs that are connected to the Internet (e.g. denial of service attacks using zombie PCs³⁴) by encouraging or mandating service providers to include, as part of their service offering, access to cybersecurity protection for individual users.

Observations and recommendations

- Self-regulation and soft regulation

In most cases, regulators today have the mandate to require the adoption of standards or procedures in the interest of consumer protection or even general ICT development. Despite this mandate, regulators must constantly weigh, and use with restraint, their ability to impose regulatory obligations or lead industry debates about standards. To a large extent, the issue of cybersecurity is a developing one with technical standards and operational procedures still being defined.

Regulators need to be mindful of the benefits and drawbacks involved in maintaining a balance between regulation and industry self-regulation in the area of cybersecurity. Overzealous regulatory intervention at this stage may result in the adoption of safeguards and measures that are unduly onerous on the private sector, which in turn could affect market entry and the introduction of services. Instead, regulators may be able to leverage existing cybersecurity business practices emerging in the market through public consultations, calls for contributions and forms of “soft regulation”, such as the issuance of best practice guidelines, or through self-regulation initiatives taken through public-private sector forums. Regulators in many countries, such as Switzerland, have sought to encourage private consensus building on the matter of cybersecurity standards and operational procedures, leaving decisions about implementation largely to industry.

On the other hand, the number and diversity of operators and service providers involved in certain areas of cybersecurity may be so great that the process of consensus building on certain pressing issues may take too long and regulators may instead need to consider the option of enacting new regulatory requirements.

- Participation in standards setting and coordination activities

The setting of cybersecurity standards is a relatively new field. As opposed to more traditional areas involving standards (e.g. mobile services), many regulators have yet to

³⁴ Denial of service attacks using “recruited” PCs, involve the following possibilities. The definition of denial of service as per the ITU, List of Security-Related Terms and Definitions available at <http://www.itu.int/ITU-T/studygroups/com17/tel-security.html> “1) The prevention of authorized access to resources or the delaying of time-critical operations. 2) In the context of message handling, when an entity fails to perform its function or prevents other entities from performing their functions, which may be a denial of access, a denial of communications, a deliberate suppression of messages to a particular recipient, a fabrication of extra traffic, an MTA was caused to fail or operate incorrectly, an MTS was caused to deny a service to other users. Denial of service threats include the following: denial of communications, MTA failure, MTS flooding. 3) This occurs when an entity fails to perform its function or prevents other entities from performing their functions. This may include denial of access to TMN and denial of communication by flooding the TMN. In a shared network, this threat can be recognized as a fabrication of extra traffic that floods the network, preventing others from using the network by delaying the traffic of others.”

become established participants in cybersecurity standard setting activities. Ample opportunities, however, do exist for regulators to participate in this field through the established standard setting avenues and other coordinating roles of the International Telecommunications Union (ITU) and other regional bodies such as the Commission Interamericana de Telecomunicaciones (CITEL), and the European Commission.

PART III:

CONCLUSION AND RECOMMENDATIONS

8 The ICT/telecom regulator - a key player in a national team

Looking at the larger national interest, the most effective government led cybersecurity approach would entail each government institution assuming a role to which it is particularly suited for. From the discussion above and the illustrations given by international examples, it is clear that there are a wide range of roles available to regulators in which they can play a significant, if not the lead, part in a national cybersecurity effort.

The actual role a particular regulator can and should play, however, depends in general on a number of variables. In particular, the question of how cybersecurity and cyber threats are perceived as a nation is usually a key determinant of how cybersecurity roles and responsibilities are assigned among government institutions, with a technical, technological ICT focused perception of the problem being the most favorable to a large role for regulators.

The level to which regulators are able to demonstrate a number of core competencies are also critical in determining what role a regulator plays in the national cybersecurity effort. In this respect, the following observations and recommendations can be made:

The **maturity of the regulator** will determine, to some extent, perceptions regarding its efficiency and effectiveness by other more established agencies, especially those dealing with national security, defense and law-enforcement. This in turn will affect the regulator's ability to assume a lead position in a cybersecurity policy-making or organization and coordination role.

A regulator's ICT **technical and industrial expertise** and experience must also be viewed as a core competency. Its familiarity with the technology upon which cybersecurity is built is an asset that can be leveraged in a wide range of roles, from policy-making to reinforcing the legal infrastructure.

Establishing the **relevant mandate and jurisdiction** of the regulator is a key prerequisite in its assumption of roles and responsibilities in cybersecurity. Acting from a clear position of legitimacy will boost a regulator's leadership role especially in the areas of policy-making and organization and coordination. With regards to other areas of cybersecurity such as incident monitoring or building a culture of cybersecurity, it should be recognized that many regulators already have the requisite mandates, often related to responsibilities regarding consumer protection and crisis related communications, to assume the necessary roles and responsibilities.

Ensuring that the regulator has the **appropriate resourcing** for the roles and responsibilities it intends to carry out in the field of cybersecurity is another key prerequisite. While obtaining the necessary funding from appropriations and grants is ideal, the costs of a regulator's participation in cybersecurity roles can also be defrayed by working through public-private sector partnerships and by relying on the consolidation of tasks and roles.

CYBERSECURITY: THE ROLE AND RESPONSIBILITIES OF AN EFFECTIVE REGULATOR

A regulator's mechanisms and processes to facilitate **engagement of the private sector** in consultations and partnerships must also be viewed as a core competency that will be required when assuming a role in cybersecurity. Such a core competency will be vital in carrying out the role of policy making, private sector cooperation, incident management, and building a culture of cybersecurity.

Aside from these general core competencies, a regulator must also possess core competencies related to a number of the cybersecurity roles discussed. These include:

- Policy making: Providing policy advice in ICT matters;
- Industry regulation: Mandating industry technical standards;
- Legal infrastructure: Investigation and enforcement of ICT related offences;
- Incident management and cybersecurity risk assessment: Managing crisis related communications; and
- Building a culture of cybersecurity: Promoting consumer awareness.

Only when these core competencies can be successfully demonstrated or obtained and prerequisites satisfied can a regulator assume key roles and responsibilities in the national cybersecurity effort.

Enhancing cybersecurity and improving CIIP are becoming increasingly important for developed and developing countries around the world in order to maximize societies' benefits from ICTs and manage the risks related to countries' growing dependency on these technologies. Given the changing environment and the specifics of cybersecurity and CIIP, the future role of the ICT/Telecom Sector Regulator and the Regulator's possible areas of responsibility require further discussion and analysis.

The purpose of this background paper was to provide an overview of the challenges that the ICT/Telecom Sector Regulator is facing when dealing with cybersecurity/critical information infrastructure protection (CIIP) issues and discuss how the active involvement of the ICT/Telecom Sector Regulator can positively and negatively impact the initiation, development, and implementation of a national cybersecurity strategy. We look forward to receiving your feedback on the usefulness of the material presented to provide further input and direction to ITU with regards to related activities that could be undertaken in this important and fast evolving area.

Please send any feedback you may have to cybmail@itu.int.
We look forward to hearing from you.

ICT Applications and Cybersecurity Division (CYB)
Policies and Strategies Department
Bureau for Telecommunication Development
International Telecommunication Union
Place des Nations
1211 Geneva 20
Switzerland
Telephone: +41 22 730 5825/6052
Fax: +41 22 730 5484
E-mail: cybmail@itu.int
Website: www.itu.int/ITU-D/cyb/



**BRINGING BROADBAND ACCESS TO RURAL AREAS: A STEP-BY-STEP
APPROACH FOR REGULATORS, POLICY MAKERS AND UNIVERSAL ACCESS
PROGRAM ADMINISTRATORS**

THE EXPERIENCE OF THE DOMINICAN REPUBLIC



This paper was prepared by Edwin San Roman, Senior Regulatory Expert, Indotel, Dominican Republic, for the 9th Global Symposium for Regulators (GSR), to be held in Beirut, Lebanon, 10-12 November 2009 (www.itu.int/gsr09). Peter Stern, Independent consultant, reviewed and edited this paper.

TABLE OF CONTENTS

PART I: INTRODUCTION

1. Bringing broadband to rural areas.....	5
2. Purpose of the course and this background paper.....	6

PART II: THE DOMINICAN REPUBLIC'S RURAL BROADBAND PROJECT

3. The Dominican Republic: The national context for promoting broadband access in rural areas.....	9
3.1 Geographical, political, demographic and economic overview.....	9
3.2 The telecommunications sector.....	11
3.3 Universal access and service (UAS) in the Dominican Republic.....	15
3.4 The Dominican Republic's universal access (UAF) and how it is used.....	18
3.5 The Government's policy on Information and Communications Technologies (ICTs) and the role of the regulator.....	18
3.6 The Rural Broadband Connectivity Project.....	20

PART III: METHODS AND TOOLS FOR DEVELOPING A RURAL BROADBAND PROJECT

4. The importance of local knowledge and consulting with stakeholders.....	23
4.1 Knowing the country and especially the rural areas.....	23
4.2 Consulting with public institutions and local entities.....	24
4.3 Consulting with telecommunications operators and service providers.....	25
4.4 Cooperation with NGOs and other agencies.....	26
5. The importance of a pilot project as a way of testing and demonstrating the technical and economic feasibility of a universal access and service project.....	26
5.1 Characteristics of the location of the pilot project.....	26
5.2 Involvement of local authorities.....	27

5.3 Involvement of the young.....	28
5.4 How they made it happen in the Dominican Republic.....	29
6. Overview of broadband technologies.....	35
6.1 Wired.....	36
6.1.1 DSL over copper local loop.....	36
6.1.2 Coaxial (ex. DOCSIS and HFC) and fibre optic cable systems.....	38
6.2 Wireless.....	38
6.2.1 Mobile communication.....	38
6.2.2 Broadband wireless access (WiMAX, WiFi).....	43
6.2.3 Satellite.....	47
6.2.4 End user equipment.....	48
7. Use of geographical information systems (GIS) and Google Earth in planning rural telecommunications projects.....	49
7.1 What is GIS?.....	49
7.2 Benefits of using GIS in planning rural telecommunications projects.....	49
7.3 Google Earth.....	51

PART IV: PRACTICAL MATTERS TO CONSIDER AND STEPS THAT NEED TO BE UNDERTAKEN IN DEVELOPING AND IMPLEMENTING A RURAL BROADBAND PROJECT

8. Developing a rural broadband project.....	53
8.1 Administrative matters and legal basis.....	54
8.2 Nature of licenses and issues related to spectrum.....	54
8.3 Demand analysis.....	55
8.3.1 Normal method for determining demand in rural areas.....	56
8.3.2 Approximation method used in Peru and in the Dominican Republic.....	57
8.4 The economic model.....	59
8.4.1 Method used in Peru and in the Dominican Republic.....	59
8.4.2 Determining the amount of the subsidy.....	60
8.4.3 Other considerations	60

8.5 Minimum subsidy auctions.....	62
8.6 The tender procedure (transparency and non discrimination in the evaluation of offers)..	63
8.7 The contract.....	65
8.7.1 Payment method for subsidies	65
8.8 Supervising the implementation of the project.....	66
8.9 Creation of dedicated web sites for the communities to be served.....	66
8.10 Raising awareness among the local population.....	68
8.11 Capacity-building to ensure sustainability of the project.....	69
 9. Other innovative funding mechanisms.....	 70
9.1 Public-private partnerships.....	70
9.2 Private initiatives.....	71
9.3 Private-private partnerships.....	72
 10. Sustainability.....	 73

PART V: CONCLUSIONS AND RECOMMENDATIONS

11. Challenges and lessons learned.....	75
12. Conclusions and best practice guidelines.....	76

Annex 1:

OTHER SUCCESSFUL EXPERIENCES: THE PERUVIAN RURAL BROADBAND CONNECTIVITY PROJECT

PART I: INTRODUCTION TO RURAL BROADBAND ACCESS

1. Bringing broadband to rural areas

Broadband¹, today's the principal means of delivering ICT applications, is considered by an increasing number of policy makers and regulators around the world to be a basic telecommunications service. Current universal access and service (UAS) policy for telecommunications and ICTs emphasizes the need for access to broadband applications in order to achieve the goals of economic development and social inclusion for all communities. Experience has shown that the arrival of basic telephony (in any form, such as public payphones, fixed residential or mobile lines) and broadband Internet constitutes a critical take off point in a community's path to economic and social development². The impact is even greater in rural communities where local institutions, NGOs and young people quickly become the main users of ICTs opening the way to what could be considered to be a virtuous circle of development (Picture N° 1). Yet, in most developing countries, access to broadband services is generally restricted to the capital city and sometimes to other important economic and political centres and surrounding areas.

In the communities with limited or no access to basic voice services, the Internet becomes a less expensive alternative, often serving as a substitute for the former. Generally, it costs very little to access the Internet in public Internet cafés, where a user can chat for an hour with friends and family, conduct business with people all over the world and get information on education, health, government and other matters for about the same cost as a three minute call from a public payphone.

This is why universal access and service (UAS) policies and the institutions in charge of developing and implementing UAS policies and projects are promoting and, where necessary, financing deployment of infrastructure to provide broadband access in rural areas.

¹The term is used in this document to describe high speed always on internet connections which are over 256 kbps.

² www.ictregulationtoolkit.org

This was precisely the objective of the government of the Dominican Republic and the telecommunications regulator, INDOTEL, in 2007 when they initiated an ambitious project to provide broadband access to 508 mostly rural communities in the country.

Picture N° 1: Young man using the Internet in a rural area of the Dominican Republic



Source: Edwin San Román

2. Purpose of the course and this background paper

This document like the accompanying ITU course, “Bringing broadband access to rural areas: a step-by-step approach for regulators”, draws primarily from the real experiences in implementing successful rural broadband connectivity projects in the Dominican Republic and, to a lesser extent, similar experiences from previous projects in Peru. It focuses on the practical aspects of these projects, including the procedures followed, the challenges encountered and the lessons learnt. While the procedures followed in the Dominican Republic were similar to those in Peru, the two countries differ significantly in the time taken from conception of a project to its implementation. In the Dominican Republic, where there is only one institution involved in the process, it takes typically less than one year from start to implementation of a UAS project. In Peru because of all the requirements in national legislation and the involvement of several government institutions in the approval process, it can easily take as long as three years. The experiences in implementing rural broadband projects in both these countries serve as the basis for the course and this background document.

While the procedures described here are applicable in most other countries, a person responsible for initiating and implementing such projects must keep in mind that particular requirements of national legislation in one country may have a negative impact on what would be a successful project in another country.

In this document and the associated course, it is presented the overall context and general aspects of rural connectivity projects, which is illustrated with examples from the Dominican Republic and to a lesser extent from Peru. The document is divided into five parts:

Part I (Sections 1 and 2) gives background information and outlines the purpose of the course and offers a brief discussion about the justifications for, and potential benefits of bringing broadband to rural areas.

Part II (Section 3) presents the context for promoting broadband rural access in the Dominican Republic and includes a brief geographical, political, demographic and economic overview of the country, its telecommunications sector, government policy on information and communications technologies (ICTs), the role of the policy maker and regulator, and the extent of their involvement in promoting and developing universal access and service. Special attention is paid to policies that promote broadband access. In this part it is presented the concept of the Universal Access Fund and how it is used. This part concludes with a brief presentation of the Dominican Republic's Rural Broadband Connectivity project.

Part III (Sections 4-7) elaborates on the general methods and tools needed to develop a rural broadband project. The importance of local knowledge and especially of rural areas and the need to consult and involve the main stakeholders is discussed in Section 4. Section 5 explains the importance of undertaking pilot projects to test and demonstrate the technical and economic feasibility of rural connectivity projects. Section 6 gives a general overview of technologies that provide broadband access. Section 7 describes the use of geographical information systems (GIS) and Google Earth and how they can be used when planning rural telecommunications projects.

Part IV (Sections 8 – 9) describes the practical steps in developing and implementing a rural broadband project and is illustrated with examples from Peru and the Dominican Republic. Section 8 elaborates on the contents of and the steps involved in the development of a rural broadband project and Section 9 discusses alternative innovative funding mechanisms. Section 10 focuses on sustainability issues.

Conclusions and best practice guidelines are summarized in Part V (Sections 11 – 12) and Annex 1 gives a brief overview of the Peruvian rural broadband connectivity project.

In addition to public and country specific information available on the Internet and cited as footnotes in this document, the two main outside references used in developing and implementing the project presented in this document and associated course are the following:

- The ITU - infoDev ICT Regulation Toolkit module on Universal Access and Service²; and
- Peter A. Stern and David N. Townsend, New Models for Universal Access to Telecommunications Services in Latin America: Lessons from the Past and Recommendations for a New Generation of Universal Access Programs for the 21st Century, a Joint Study by the World Bank, Regulatel (The Forum of Latin American Telecommunications Regulators), and the United Nations Economic Commission for Latin America and the Caribbean (ECLAC), June 2007³

³ http://www.regulatel.org/SU_Peter_31_08_07/Full_report-COMplete-June_11,2007.Edited_PAS_v.1.pdf

PART II: THE DOMINICAN REPUBLIC'S RURAL BROADBAND PROJECT

3. The Dominican Republic: The national context for promoting broadband access in rural areas

Figure N° 1: Location of the Dominican Republic



Source: Google Earth

3.1 Geographical, political, demographic and economic overview

The Dominican Republic occupies the eastern two thirds of the Island of Santo Domingo (also known as Hispaniola) bordered on the north by the Atlantic Ocean and on the south and west by the Caribbean Sea. Haiti occupies the western third of the Island. The Dominican Republic has a land surface area of 48,730 km² and a population of more than 9.5 million giving it a density of 195 inhabitants per km².

The Dominican Republic is a democratic republic divided into 31 provinces and one national district. There are three levels of government: the central government is responsible for national policies including telecommunications, ICTs, education and health; each of the 31 provinces has its own provincial government; and there are 383 local governments that include municipalities and district municipalities. Politically there is a fragmented multiparty system with three main traditional parties.

The population is made up of mixed ethnic groups (73%) and black (11%) and white (16%) minorities. During the course of their history Dominicans have emigrated to other countries in search for better economic and social opportunities. Many Dominicans today are very dependent on the remittances they receive regularly from family members living abroad, mainly in the USA. Indeed, these remittances represent about 10% of GDP.

Like most all of its neighbours in the Caribbean the Dominican Republic's economy was traditionally based on the exports of sugar, coffee and tobacco. However, more recently the services sector (mainly tourism) has overtaken agriculture as the economy's largest employer. The USA represents nearly 75% of the country's export income. The country has experienced strong economic growth since 2005. Yet according to 2007 figures, distribution of wealth is still very unequal: 10% of the population received nearly 40% of the country's GNP.

As a result mainly of the Central America-Dominican Republic United States Free Trade Agreement (CAFTA – DR)⁴, which came into force in March 2007, GDP in 2007, grew at a rate of 9% with respect to the previous year. In 2007 exports reached US\$ 7,237 million, 45% higher than in 2006. Net reserves were US\$ 2.3 billion and tax income grew at a rate of 23% that same year.

Picture N° 2: A Caribbean landscape

⁴ The Central America-Dominican Republic-United States Free Trade Agreement (CAFTA-DR) which creates the United States' second largest free trade zone in Latin America after Mexico has seven signatories: the United States, Costa Rica, Dominican Republic, El Salvador, Guatemala, Honduras, and Nicaragua. It was approved by the U.S. Congress in July 2005 and the President signed it into law on the 2nd of August of that year. The Agreement which entered into force on a date agreed upon by all parties, has been approved by the legislatures in the Dominican Republic, El Salvador, Guatemala, Honduras and Nicaragua but not in Costa Rica. Inter alia, the Agreement includes trade in services including telecommunications.



Source: Edwin San Román

3.2 The telecommunications sector

Telecommunications services have been provided by private companies since 1930. The telecommunications market which was opened to competition in 1998 has been completely liberalized for all services since 2002. Codetel (Compañía Dominicana de Teléfonos), later GTE, Verizon Dominicana and now Claro-Codetel held a monopoly until 1992 when a concession was awarded to TRICOM, which provides fixed and cellular mobile services and Internet (dial up, ADSL and cable modem) and cable TV services. TRICOM was able to start providing services only after concluding lengthy interconnection negotiations with Verizon⁵. All America Cable and Radio (AAC&R), later Centennial and now Trilogy Dominicana (commercial name VIVA), was awarded a license a short time later. By 2008 there were four competing mobile operators. Claro-Codetel and Orange Dominicana were the two dominant operators with, respectively 54% and 33% of the market share; Tricom and Trilogy Dominicana (commercial name VIVA) had together 13% of the market; OneMax and Wind Telecom, the latest entrants, started offering wireless internet and telephony services in 2008. There are also many ISPs and three submarine cable systems (Antillas-1, Arcos, FibraLink) connect the Dominican Republic to the rest of the world. The most recently

⁵ <http://nuevositio.tricom.net/historia.aspx>

completed, FibrLink Jamaica, a subsidiary of Columbus Communications⁶ has a submarine cable that connects Jamaica with the Arcos landing station at Puerto Plata.

Figure N° 2: Logos of the main telecommunications operators in the Dominican Republic



Source: INDOTEL

A new pro-competition General Telecommunications Law (Ley 153-98), promulgated in May 1998 created an independent, administratively decentralized telecommunications regulator, *Instituto Dominicano de las Telecomunicaciones* (INDOTEL), with judicial and financial autonomy and legal personality INDOTEL is the only government institution that has both the policy setting and regulatory responsibilities for the sector⁷. It is headed by a five-member Executive Council appointed every four years by the Executive Branch of the Government, coinciding with the four-year mandate of the President of the Republic⁸. The President of the Executive Council has the rank of Secretary of State.

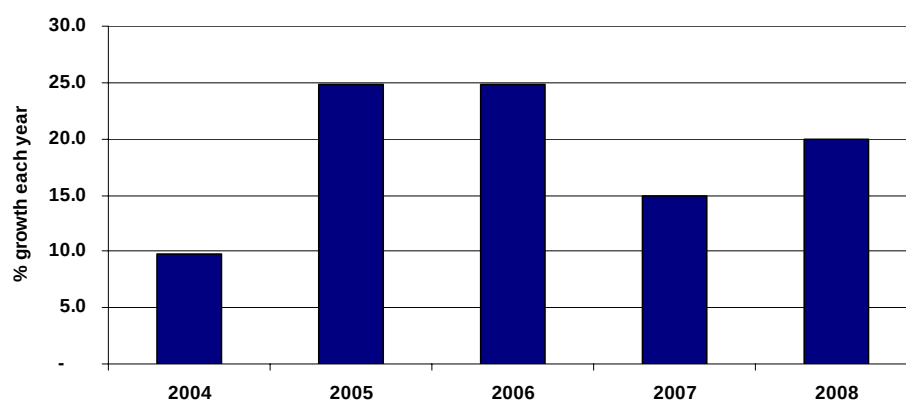
⁶ Columbus Communications is a newly established, Barbados-based company which owns Cable Bahamas, the only cable TV company in the Bahamas, the Bahamas Internet Cable System (BICS), a submarine cable system connecting The Bahamas to the USA, the Cable Company of Trinidad & Tobago (CCTT), the dominant cable TV operator in Trinidad & Tobago, and 85% of the Arcos submarine cable system.

⁷http://www.indotel.gob.do/component/option,com_docman/Itemid,587/task,doc_view/gid,66/ (article 76).

⁸ The President of the Republic who is elected every 4 years by popular vote, appoints all ministers and governors of the 32 provinces and promulgates all laws approved by the Congress, which is made up of a 150 member Chamber of Deputies and a 32 member (one per province) Senate.

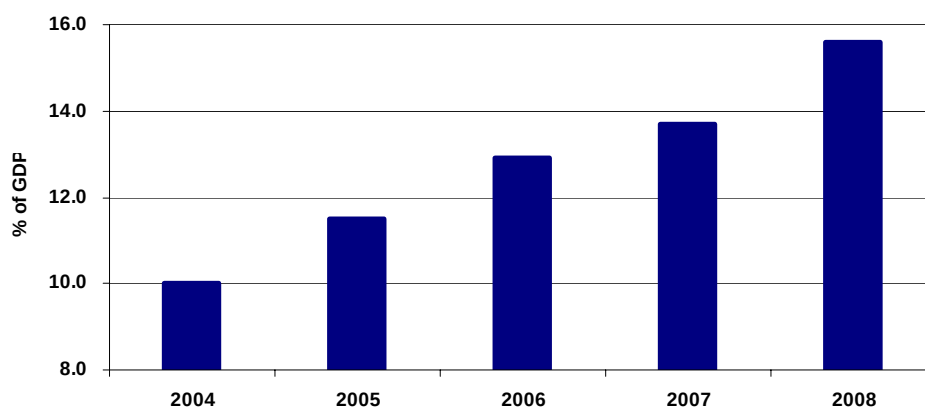
In the period since Law 153-98 was proclaimed, telecommunications has been among the sectors experiencing the highest rates of growth in the Dominican Republic. The sector has played an important role in the diversification of the economy from primary industries such as agriculture, mining and fishing, to manufacturing and services based activities such as tourism and transportation⁹. Between 2005 and 2008, the telecommunications sector grew year on year by more than 15% (24.8 % in 2005 and 2006) and represented between 10% and 15.6% of GNP.¹⁰ (Figures 3 and 4)

Figure N° 3: Growth of the Telecommunications Sector in the Dominican Republic



Source: *Banco Central*

Figure N° 4: % of GNP represented by the Telecommunications Sector in the Dominican Republic



Source: *Banco Central*

⁹ The part of GNP of primary industries (agricultural, mining and fishing) has decreased from 25% in 1980 to 15% in 2002.

¹⁰ Source: *Banco Central de la República Dominicana* (preliminary figures for 2008).

Table 1 shows the number of telephone lines, penetration rates and growth of fixed and mobile lines as of December 2008:

Table N°1: Basic telecommunications indicators

	Number of lines	Penetration rate	Annual growth rate
Fixed telephones	985,711	10.3%	8.7%
Mobile telephones	7,210,483	75%	30,8%

Source: *INDOTEL*

Eighty seven percent of the mobile lines are prepaid and it is estimated that today over 65% of the territory and over 90% of the population have access to basic telephone services through either fixed or mobile connections.

There has also been significant growth in the number of Internet users and subscribers. Between 2000 and 2008 the number of Internet users who accessed the Internet mainly in Internet cafés, universities and their work places increased by more than ten fold. During the same period the number of Internet subscribers increased by nearly five times and Internet users increased from 2.4% to close to 26.7%.

Picture N° 3: Antenna in Miches, in northeastern Dominican Republic



Source: *Edwin San Román*

Law 153-98 also established a Universal Access Fund (*Fondo de Desarrollo de las Telecomunicaciones*), which is administered by INDOTEL. Each operator of public telecommunications services contributes 2% of its gross income. Forty percent of the Fund is used to finance regulatory activities of the INDOTEL and 60%, to finance development projects which are awarded through minimum subsidy auctions. There are two types of projects which are eligible for funding: (i) Development Projects, which form part of biannual universal access and service project plans and are approved every two years by the Executive Council, and (ii) Special Projects which are of a strategic and social nature and can be approved by the INDOTEL Executive Council on an as-required basis so long as they do not surpass a defined maximum amount¹¹.

3.3 Universal access and service (UAS) in the Dominican Republic

One of the main functions of a policy maker and regulator in helping society bridge the digital divide is to be the prime enabler, facilitator and promoter of telecommunications infrastructure deployment and, especially, broadband access throughout the country. In the Dominican Republic this task is carried out by INDOTEL, the only government organization responsible for telecommunications related matters.

As part of its mandate to promote UAS, INDOTEL in 2001 issued a policy paper, *Social Policy on Universal Service and Regulations for the Telecommunications Development Fund* which, *inter alia*, proposes bi-annual plans for projects to extend universal access and service to yet unserved areas¹².

Definitions for universal access and universal service can be found in Box N° 1.

¹¹ http://www.indotel.gob.do/component/option,com_docman/task,doc_details/gid,656/Itemid,739/

¹² http://www.indotel.gob.do/component/option,com_docman/task,doc_details/gid,612/Itemid,739/

Box N°1: Definitions of Universal Access and Universal Service

Universal access is defined as “the reasonable availability of network facilities and services, on either a private or a shared, public basis, to citizens and institutions within a given community.”

Universal service is defined as being “a more absolute condition, in which telecommunications services are delivered ubiquitously to households or individuals throughout an area, and thus are both accessible and affordable, with no practical impediments to subscription and usage”.

Source: *New Models for Universal Access to Telecommunications Services in Latin America*³ and ITU - infoDEV ICT Regulation Toolkit² module on universal access/service

In addition to national strategies that promote universal access and service through broadband, it is important that the country’s legislation also addresses the financing mechanisms needed to achieve these policies including the deployment of broadband infrastructure and the acquisition and installation of terminal equipment such as computers, PDAs, smart phones and other devices that need broadband connections. In countries where by law the universal access fund does not finance the procurement of terminal equipment, changes in the law would be required.

One of INDOTEL’s primary efforts in promoting broadband and the use of computers has been directed towards the installation of local community Informatics Training Centres (CCIs¹³) and supplying them with computers since 2004. The number of computers in each CCI varies according to the population and capacity of the organization in charge of managing each CCI. INDOTEL also provides the entire technical infrastructure including hardware, software, and a backup electric supply system.

The main purpose of these centres is to train people in the use of computers. They are free of charge and open to anyone who wants to learn how to use a computer. Some CCI’s already have connections to broadband Internet, while others are being connected as the deployment of broadband infrastructure reaches their area.

¹³ *Centro de Capacitación en Informática* (CCI) are community informatics training centres, some with Internet access, and where the computers are funded through INDOTEL’s Universal Access Fund.

It is important to note here that the CCIs are administered by local people and organizations from the community in which they are located and who manage and ensure the sustainability of these centres, for example, paying instructors and all associated running costs. In planning their deployment, INDOTEL identified civil society organizations and individuals who were willing and capable of undertaking this task.

By January 2009 there were more than 867 CCIs in operation and 462 were in the process of being created. The initiative can so far be considered to have been a great success, with thousands of people throughout the country regardless of their social and economical status, age, sex and race, having learnt how to use a computer. Most centres have monthly graduation events for students who have successfully completed the standard 6-month computer training course¹⁴. INDOTEL has funded the cost of these CCIs and other universal access and universal service projects with resources from the Universal Service Fund¹⁵.

Picture N° 4: Woman and child from Rio Limpio, northwest of the Dominican Republic



Source: Edwin San Román

¹⁴ Even though all centers give training courses, only some of them have public graduation events.

¹⁵ See reference 11.

3.4 The Dominican Republic's Universal Access Fund (UAF) and how it is used

Universal Access Funds (UAFs) are commonly used as a financial mechanism to create an extra level of economic incentives for private investment in network expansion and service delivery with the objective of achieving universal access and service goals¹⁶.

In the Dominican Republic, there is a two-year planning cycle for UAF financed projects. Once projects are approved by INDOTEL's Board, their execution can begin, the first step being the elaboration of a bidding document. This document explains the purpose, objectives and characteristics of the project, as well as its technical specifications and terms of reference of the bidding process. The next step is for INDOTEL to initiate a tender, which given the characteristics of the project can be national or international in scope. Potential investors are given a certain time to prepare their bids which are evaluated according to a strict tender and adjudication procedure after the bids have been submitted. The company with the bid that meets all the technical specifications and asks for the least amount of subsidy from the Fund is awarded the project. Bids are evaluated by an INDOTEL tender evaluation team, consisting of a project manager, a telecommunications engineer, an economist, a lawyer and an assistant. Depending on the project the team may have additional support from other technical, legal or administrative sources.

3.5 The Government's policy on Information and Communications Technologies (ICTs) and the role of the regulator

Government involvement and, most importantly, political support at the highest level are essential if a country wishes to implement a national strategy to transform the current "pre-modern" into a "post-modern" society, namely, one based on information and knowledge. ICTs play a key role in this fundamental transformation. Just as important is the active participation of the public and private sectors and civil society in the design and execution of projects which promote the use of ICTs throughout society.

¹⁶ <http://www.ictregulationtoolkit.org/en/Section.3272.html>

*E-Dominicana*¹⁷ is a national strategy which has as its mission “to promote the use and appropriation of Information and Communications Technologies in the Dominican Republic by means of initiatives that create synergies between the governmental sector, the civil society, and the productive sector, to offer all its inhabitants better opportunities which will contribute to their development, by bringing them welfare and progress in the exercising of their capacities”. Its vision is “to place the country in a position that will allow it to compete in the new scenario of a globalized world, by achieving sustainable development in the economic, political, cultural, and social scope, and to assume the challenge of converting inequality and Social exclusion from the digital divide into a digital opportunity”.

Picture N° 5: Accessing internet in a CCI in Don Juan, province of Monte Plata



Source: Edwin San Román

The objectives of *e-dominicana*¹⁸ are grouped into eight thematic areas, namely, infrastructure and access, social inclusion, education, training, awareness-raising, development of contents, digital state, and industry. The objectives relating to infrastructure are to:

- i. provide access to broadband¹⁹ services for all Dominicans with a speed of at least 128 Kbps within a radius of no more than 5 km of their homes;

¹⁷ Extracted from *National Strategy for the Information and Knowledge Society, 2007-2010*:

¹⁸ http://www.cnsic.org.do/media/plan_edominicana/ObjetivosgeneralesdelaE-Dominicana.html#Topic11,

- ii. achieve an Internet penetration of 40% of the population with at least 30 % of the connections having a speed of 128 kbps or more;
- iii. achieve a penetration rate of personal computer users of at least 50% of the population.

These three objectives are to be achieved by 2010 by:

- a) developing sustainable models with prices within reach of the whole population as a means of encouraging ubiquitous access to ICT infrastructure;
- b) stimulating the ICT market and contributing to its growth through joint efforts between the government and the private sector;
- c) reducing the costs of broadband access by encouraging competition; and,
- d) promoting the use of the Internet in small companies and throughout the public sector.

3.6 The Rural Broadband Connectivity Project

What convinced INDOTEL to give a special impulse to the deployment of broadband in rural areas was the fact that in July 2007 only 62 (16%) out of the country's 383 local governments had fixed lines and broadband Internet service. Most of these are the Dominican Republic's most populated cities and their surroundings including the capital, Santo Domingo. This meant that many of the less populated municipalities and rural areas had no access of any kind despite the fact people living in these municipalities were just as anxious as their neighbours living in more populated and richer areas to have broadband services.

By May 2007 more than 400 CCIs had been established across the whole country but due to the lack of telecommunications infrastructure only a few had access to broadband. Local organizations responsible for managing these centres were unhappy with this situation and made sure that their dissatisfaction came to the attention of Jose Rafael Vargas, the President of INDOTEL, who often

¹⁹This capacity was considered as broadband at the time *e-dominicana* was launched, currently minimum speed for broadband access is 256 kbps.

attended CCI inaugurations. Vargas was besieged everywhere by demands from local authorities, residents, students and the young, for broadband and home telephone services.

Picture N° 6: A CCI



Source: INDOTEL

As a result in 2007 INDOTEL took an important decision to launch the *Rural Broadband Connectivity Project* as part of the government's *e-Dominicana* strategy. The Project has as its objective to bring residential, public telephones and broadband²⁰ services to 508 localities²¹ throughout the country that had no residential telephone connections or broadband Internet access. Broadband services were also to be made available through Internet cafés and telephony through public call centres²².

The Project included a program of awareness raising, training in the use of the telephones and computers as well as in the managing public call centres and cyber cafés. Training was proposed

²⁰ Download and upload speeds of 256/128 to 1,500 /256 Kbps under conditions similar to those found in the big cities such as Santo Domingo and Santiago.

²¹ Those 508 localities include all municipalities and districts municipalities of the country and 179 localities of the 16 poorest provinces in the country.

²² Public call centres are public places where a person can make a telephone call and pay for it in cash.

for both end users and entrepreneurs and included the development of locally generated web pages with important information about each community, such as location, how to reach it, tourist attractions, products made in the community and the names of the local authorities. To promote entrepreneurship it was also proposed that the Internet access and public call centres be managed by local entrepreneurs.

Before finalizing the tender documents for this ambitious project, INDOTEL had estimated the total cost to be US\$ 4 650 000, including all applicable taxes.

The conditions of the tender provided that as yet unassigned frequencies could be used in the project if requested by the bidder free of charge.

When the public tender was officially launched on 23 August 2007, 20 potential bidders acquired the document. Of these, five completed the initial requirements; two prequalified but only one presented a technical and economic proposal. This was Claro-Codetel, which eventually was awarded the project deposited its offer on 8 January 2008, the closing date of the tender. It requested zero subsidies and offered to complete the project in 345 days but asked for the use of 2 x 15 MHz of frequency in the 3.5 GHz band.

Following market and field studies, Claro-Codetel decided to deploy ADSL where there were fixed lines and 3G (UMTS) wireless access where there was no existing fixed-line infrastructure. By the end of January 2009, 108 of the 508 localities had been connected and it was planned to have all 508 connected by the end of September 2009.

Before launching the full scale project, however, INDOTEL decided to do a pilot project (described in detail in Section 5 below) in a small community called *Los Botados*, near the capital, Santo Domingo, to confirm that the whole project was viable economically and technically.

PART III: METHODS AND TOOLS FOR DEVELOPING A RURAL BROADBAND PROJECT

In this part it is showed why it is essential to have local knowledge and to undertake consultations with stakeholders, to present the project to them, to secure their support and involvement and then to run a pilot project to test and prove its technical and economic feasibility, essential for the regulator, operators and service providers alike. It is also showed how recent innovations in wireless technologies and geographical information systems (GIS) and Google Earth have been used for developing and implementing rural telecommunications projects.

4. The importance of local knowledge and consulting with stakeholders

4.1. Knowing the country and especially the rural areas

A thorough knowledge of the country, its geography, demography and social and economic characteristics is essential in the elaboration of any universal access and service project. Similarly, it is important to have a good appreciation of the existing telecommunications infrastructure, where it is located, its characteristics and plans for its expansion to ensure that rural telecommunications projects take into account the actual situation in the target areas. The practical way of doing this is to establish a project technical evaluation team typically composed of at least an economist and a telecommunications engineer and have them visit the target areas to gather all the essential technical, economic, geographic, social, political and other information necessary for the design of the project or projects.

In the Dominican Republic the project technical evaluation team consisting of two engineers, an economist and a lawyer drew the following general conclusions about telecommunications infrastructure in rural areas:

- Small entrepreneurs were using a variety of technological solutions including satellite and wireless and, with their own limited resources had already installed public telecentres, cyber-café's and public call centres for which the local population often paid very high prices.

- Some people had home telephones²³ installed at their own expense and without any help from the network operators, an example of what people in the rural areas are willing to do to have a telephone even if the costs are high.
- Many people already knew about the Internet and were willing to pay to have access in a public place or even at home.

Picture N° 7: Getting to know the country



Source: Edwin San Román

4.2. Consulting with public institutions and local entities

Consultations are critical to the drafting of the bidding document and should involve all or most ICT stakeholders²⁴. These consultations should have as their main objectives the gathering of information, linking stakeholders, and assessing the size of the market. Before meetings are held with operators and ISPs, the consultation team needs to have a good understanding of stakeholders' needs, expectations, current levels of connectivity and how they are currently using ICTs. For example, during the Dominican Republic's Rural Broadband Connectivity Project the

²³ Fixed telephones connected via the mobile network.

²⁴ The consultation team in Dominican Republic was the project technical evaluation team.

Ministry of Education, the Ministry of Health, and local municipalities were consulted to assess the need for telecommunications, especially Internet services and to get a better understanding of the infrastructure they currently had. The local governments were invited to support and to get actively involved in the project. These consultations revealed the degree of unanimity among stakeholders on the need for broadband access and also a general dissatisfaction not only with the lack of broadband access and services in rural areas but also with the high costs and poor quality of satellite access.

4.3. Consulting with telecommunications operators and service providers

Once the objectives of the initial consultation process have been achieved, having face to face meetings with each of the operators and, in particular, with the incumbent is an important next step. In the Dominican Republic each of these meetings started with a short presentation about the project and was followed with an open discussion about the deployment of broadband infrastructure throughout the country and the reasons for its absence in certain underprivileged areas, especially in rural areas. The operators were also encouraged to talk about their plans for expanding their networks in rural areas.

Consultations with operators should ideally be held after the technical project evaluation team has completed its field visits because it will then be possible to refer to real instances of people in rural areas asking for broadband and indicating their willingness to pay for it. These meetings have the additional benefit that they allow project team members to establish contact with the regulatory, technical and other experts from these organizations. This is very important as the project progresses through its different implementation stages where easy and quick access to these key people is essential to get quick replies to urgent requests for various types of information and data.

Consultations with operators were an integral part of the implementation of the broadband projects in the Dominican Republic, where invitations were sent by INDOTEL to the CEOs and regulatory experts of all of the major operators. At least one representative of each major company attended the meetings. Their feedback was very useful and was taken into account in

planning these projects. It greatly enhanced the projects and had the additional benefit of inciting the operators to participate in the tender process.

4.4. Cooperation with NGOs and other agencies

Establishing contact with civil society agencies and especially non-governmental organizations (NGOs) should not be underestimated because many of them work in rural areas. They are often very interested in broadband projects because they understand the benefits of high speed access and have a very good appreciation of demand for services that require broadband access. Almost all use the Internet as a working tool and want to have access available for staff situated in the rural areas.

Some CCI's are connected via VSATs but are experiencing serious delay problems, poor quality of service and high prices. Since many of these are managed and used by NGOs to provide computer training in the communities they are serving, they are willing to pay the operational expenses. Contacting these organizations was made easier because INDOTEL had all their contact information.

5. The importance of a pilot project as a way of testing and demonstrating the technical and economic feasibility of a universal access and service project

One of the most important steps in developing a rural telecommunications project is to show that it is technologically viable and sustainable. This is why a pilot project is highly recommended and why in the Dominican Republic a pilot was carried out as part of the *Rural Broadband Connectivity Project* as a pre-feasibility study to prove that it is possible to bring broadband to rural areas using low cost technologies when there is a demand.

In this section it is discussed the characteristics of an ideal location and the importance of involving local authorities and especially young people. It is also presented the *Los Botados* pilot project which was funded by INDOTEL, the local government and a telecommunications operator.

5.1. Characteristics of the location of the pilot project

The ideal location for a pilot project is one which has little or no access to telecommunications services but is situated near the capital city or a large population centre that has access to the network. In Dominican Republic's rural broadband access pilot project, a small community of 3,986 inhabitants, located 35 km or one hour from the capital, Santo Domingo, called *Los Botados*, was chosen. *Los Botados* is located in a rural area where the main economic activity is agriculture. It had minimal telecommunications services in May 2007 when it was selected for the pilot. Only 5 families had fixed WILL (Wireless Local Loop) telephone lines with a rather poor quality of service;; the rest of the community had to travel 5 km to *Yamasa*, the nearest town, 5 km to make and receive phone calls.

Picture N° 8: Municipality of Los Botados



Source: Edwin San Román

5.2. Involvement of local authorities

Given that the local authorities have a fundamental role in securing local support from the start of the project to its completion, raising awareness among them about the importance of telecommunications, especially broadband and how it will benefit the community is fundamental to the success of the project. Local authorities play a very important role in explaining and promoting the benefits to the community of access to telecommunications and its applications. In communities where local authorities are not familiar with these benefits, it is necessary to work

with other local organizations, especially young people, who will in turn bring the message to local politicians.

When the *Los Botados* pilot project was launched in November 2007, the mayor, Ramon Santos, was new to computers; however, not long after INDOTEL was able get his support, Mayor Santos rapidly gained a good understanding of the importance of ICTs, the importance of having broadband access, and the benefits this could bring to his community.

Picture N° 9: Los Botados Mayor Ramón Santos



Source: Edwin San Román

5.3. Involvement of the young

The importance of involving the whole community and especially young people should not be underestimated. It is young people who are most familiar with what the latest in technology, telecommunications and broadband Internet access can offer and will ultimately be the biggest users of the Internet and all the applications that broadband can deliver. Even though *Los Botados* had virtually no telecommunications services or training centres many of its young people had already had contact with ICTs and were using them in cybercafés and training centres in nearby towns.

Picture N° 10: Young people trying the Internet



Source: Edwin San Román

5.4. How they made it happen in the Dominican Republic

Once the target community had been selected and the support of the local authorities had been obtained, INDOTEL started examining the best technological and economic options available for providing broadband access. As part of this exercise, it contacted all operators that had infrastructure deployed in the vicinity of *Los Botados*.

INDOTEL's own study concluded that the cheapest and most feasible solution was to build a radio link of almost 25 km with a midway repeater between *Los Botados* and *La Naviza*, where VIVA had a network. It helped that INDOTEL was able to secure the involvement of the president of VIVA, who after agreeing to participate in the project, instructed his technical staff to give the pilot project his company's full support.

Under an agreement with INDOTEL, VIVA was required to build this radio link, install a Wi-Fi hot spot in *Los Botados*, and carry out initial tests on the network. For its part, INDOTEL selected and provided low-cost radio equipment.

Unfortunately the initial trial by VIVA technicians proved unsuccessful and they were not able to establish the desired point-to-point wireless link. VIVA's technicians failed to establish the link due to their lack of experience in working with low-cost equipment. They were more familiar with installing and working with more robust and powerful equipment. INDOTEL's team was, however, not convinced that the link would not function and asked the operator to let them make a final test. Due to the inaccessibility of the site and the time needed to reach it by road, INDOTEL's team hired a helicopter to transport its technicians, who succeeded in establishing the link in less than one hour. Once the link was established with equipment supplied by INDOTEL, VIVA installed a Wi-Fi hot spot in *Los Botados*, installed the link to its existing broadband network in *La Naviza* and started to provide broadband services to the community and to the CCI on 11 August 2007.

Picture N° 11: Technical team at La Naviza



Source: Edwin San Román

The enthusiasm of young people was overwhelming. It did not take long for them to put Wi-Fi cards into their computers and go online. The day that the link and hot spot were turned on, ten computers from the CCI and 11 private computers were connected to the Internet via broadband. The CCI started to operate full time and many children, young people and even adults started attending training courses. In November 2007, the graduation of more than one hundred people from a basic computer course turned out to be a great and festive community event attended by

many relatives, “godfathers” of the graduates and others. This was concrete evidence that people in rural areas are just as much at ease as their brothers, sister, cousins and friends in the cities and large urban areas in adapting to the new technology when given the opportunity.

Picture N° 12: Graduation ceremony in Los Botados



Source: Edwin San Román

The arrival of broadband in *Los Botados* changed the lives of many people in a very short time. Fredy Ortega (Yendy), is a case in point. He used to be a motorcycle taxi driver with an interest in technology, in general, and computers, in particular. Once his community had been connected, Fredy took a short training course in Santo Domingo and became an expert in assembling and repairing computers. He set up a small cyber-café where the young people of *Los Botados*, who did not have computers, could access Internet by paying a small fee. He has also become an ICT teacher in the CCI in *Don Juan*, a community some 15 km from *Los Botados*. In a very short time, Yendy went from earning a living by driving people around on the back of his motorcycle to becoming a small entrepreneur and teacher of computers and software.

Picture N° 13: Cyber-café in Los Botados



Source: Edwin San Román

It soon became evident that the ten computers at the *Los Botados* CCI were not enough to meet demand. Following the mayor's request, INDOTEL decided to provide ten more computers which, however, needed to be assembled. They were given to a group of young people who, under the supervision of the former motorcycle taxi driver, assembled them and installed Wi-Fi cards in a matter of only five hours.

Picture N° 14: Young people assembling computers for internet access



The arrival of broadband provided a big creative stimulus for other young people as illustrated by the cases of Wilfrido de Paula and Jean Carlos de León, two university students, who lived in the small community of *La Yautía*, 2 km from the *Los Botados* hotspot. Not long after broadband was available in *Los Botados*, Wilfrido and Jean Carlos, who like their friends in *Los Botados* also wanted to be able to connect from their homes, put their minds together in an attempt to figure out how they could do this. They bought a US\$ 15 Wi-Fi card and started looking for ways to get connected. Using only old kitchen pots and coaxial cables they built an antenna, which allowed them to establish a wireless broadband link with the Wi-Fi transmitter in *Los Botados*. Since they did not have enough money to build a tower, they attached their home-made antenna to a coconut tree (pictures N° 16 and 17).

Picture N° 15: Antenna made of kitchen pots



Source: Edwin San Román

Their efforts made the headlines not only in national newspapers and on local television but also in the international media including UNIVISION, an American broadcaster with an international audience. Reporters visited *La Yautia* interviewed them and took note of the installations they had connected.

Picture N° 16: Home-made antenna in coconut tree



Source: Edwin San Román

In January 2009, they were honoured with the National Youth Award, and in February 2009, they received scholarships to study information technology in the *Instituto Tecnológico de las Americas* (ITLA) in Santo Domingo²⁵ and to participate in a one week leadership training course in Miami.

Picture N° 17: Home-made antenna in coconut tree



²⁵ <http://www.itla.edu.do/>

Source: Edwin San Román

VIVA is providing Internet access services to the whole of *Los Botados* for free and the community is covering all the costs of the CCI since August 2007. Since then, the support given by the telecommunication operators to the pilot has been very proactive. As a result of this pilot, the people of *Los Botados* can today choose between two companies that offer mobile telephony services and wireless Internet services, and one of them, Claro-Codetel, now also offers a connection through fixed wireless residential lines. The pilot opened the eyes of the national operators to the telecommunications demand and potential business opportunities throughout the country.

The inauguration of the pilot project in *Los Botados* was a turning point in INDOTEL's *Rural Broadband Connectivity Project*. Many guests were impressed by the project's success and coupled with the full press coverage of the event, stakeholders no longer needed to be convinced that such a rural broadband project was viable.

6. Overview of broadband technologies²⁶

Several different technologies can be used to build broadband networks. Each has a different impact on the cost, acceptability and feasibility of a rural broadband connectivity project. This section gives a short overview of both wired and wireless technologies that are currently available or that are in the process of being developed. Their use is illustrated with reference to rural broadband projects in the Dominican Republic, supported by the example of similar projects carried out in Peru.

While it is important that regulators and those in charge of promoting rural broadband projects be well informed about current and future technologies, their costs and suitability for a given application and their evolution, it is very important that no specific technology be imposed on operators and service providers who will ultimately be given the responsibility for building and operating these networks. The principles of competitive market and technological neutrality must be allowed to prevail to ensure that the best, most economical and sustainable solution is chosen

²⁶ <http://www.ictregulationtoolkit.org/en/Section.1318.html>

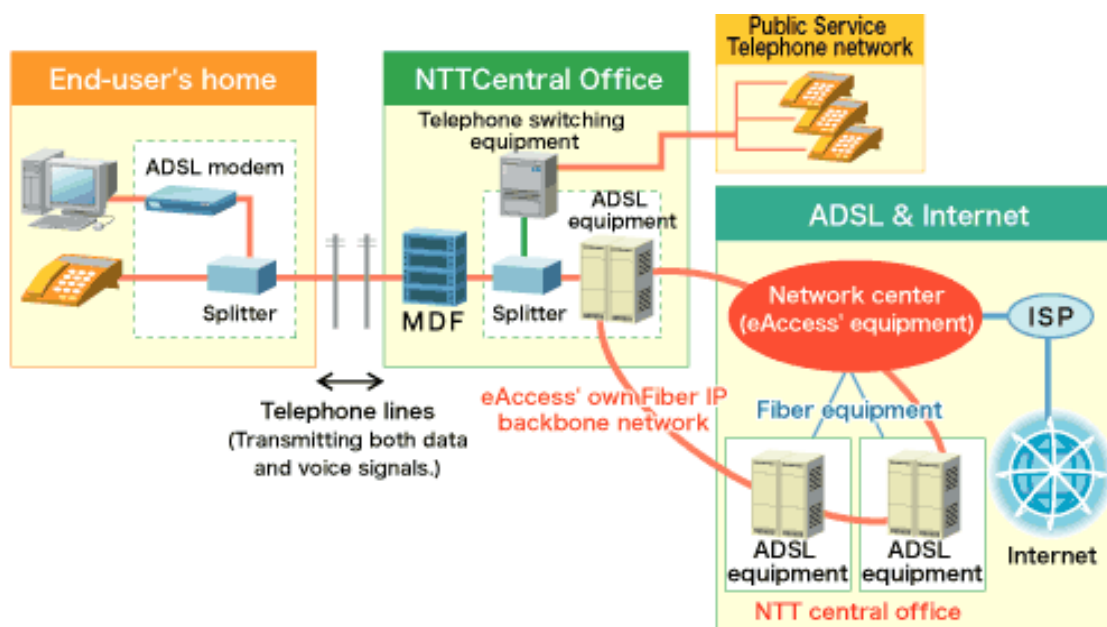
from among all available ICT technologies. Technology is neither independent of the market nor the sole determining factor for the success of a rural broadband project.

6.1. Wired

6.1.1. DSL over copper local loop²⁷

Wired digital subscriber line or DSL uses the copper local loop of the telephone network to the home or business to provide high speed data access with speeds up to 52 Mbit per second (Mbps). Data traffic is transmitted over the same copper pair as voice telephony but in a different frequency band separated using a filter or splitter. The data channel can be connected directly to a data network or to the Internet. There are several versions of DSL including ADSL (where A stands for asymmetrical) and VDSL (where V stands for very high bit rate). The most common and economic version, ADSL-Lite, can support down-link speeds of up to 1.5 Mbps and up-link speeds of up to 384 Kbps. Table N° 2 shows an overview DSL types.

Figure N° 2: ADSL Network Structure (MDF = main distribution frame)



Source: www.eaccess.net/en/company/img/etc/ttl_enterprise_sub5.gif

²⁷ See reference N°2.

Table N° 2: Overview of types of DSL

Table 2.2: The flavours of DSL
Description of selected xDSL technologies with data rate

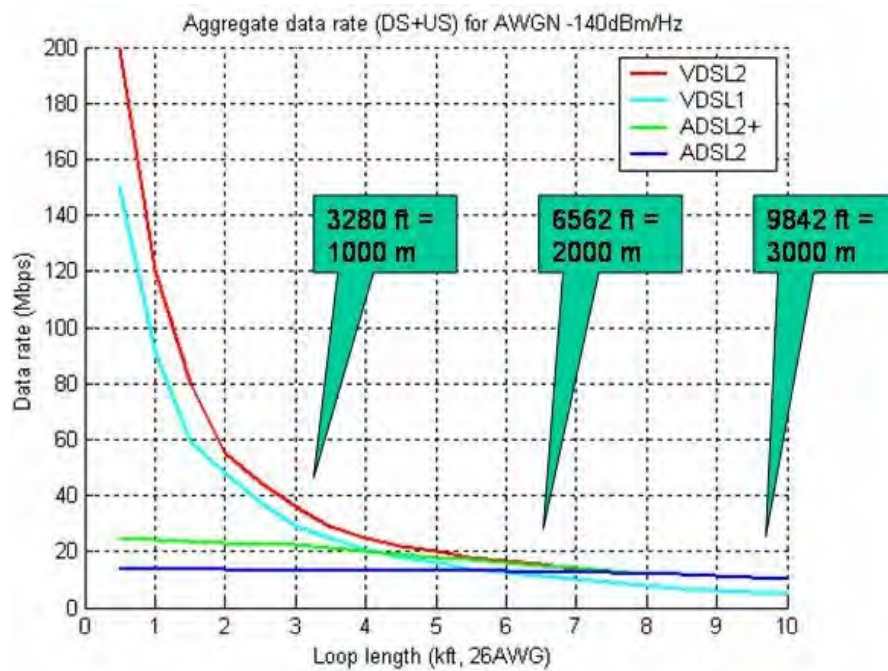
xDSL	Description	ITU Recommendation	Net data rate
SHDSL	Single-pair high-speed digital subscriber line	G.991.2	192 kbit/s to 2.312 Mbit/s
ADSL	Asymmetric digital subscriber line	G.992.1	1.5 to 6.1 Mbit/s downstream 16 to 640 kbit/s upstream
ADSL2	Asymmetric digital subscriber line	G.992.3	up to 8 Mbit/s downstream up to 800 kbit/s upstream
ADSL2+	Asymmetric digital subscriber line 2+	G.992.5	up to 16 Mbit/s downstream up to 800 Mbit/s upstream
VDSL2	Very high-speed digital subscriber line 2	G.993.2	up to 100 Mbit/s downstream up to 100 Mbit/s upstream

Source: ITU

Source: ITU

The throughput capacity of DSL depends of the length of the access loop as is shown in figure N° 6.

Figure N° 3: Data rate vs. loop length



Source: DSL Forum

DSL is used mainly in areas where a wire telephone connection exists, such as urban and sub urban areas. The deployment of DSL in such areas is easy, cost effective and considerably cheaper than other technologies.

6.1.2. Coaxial (ex. DOCSIS and HFC) and fibre optic cable systems

Coaxial cable systems, when built with Data over Cable Service Interface Specification (DOCSIS), can support downstream speeds of up to 30 Mbps and upstream speeds of 3 Mbps. Building networks with DOCSIS gives the usually unidirectional cable TV networks bidirectional capability.

Fibre optic cable systems can support speeds in the terabit per second (Tbps) range. They allow for better quality than coaxial cable because there is no crosstalk, no electromagnetic or radio interference, and they are less expensive to maintain.

In rural areas of many countries, there are small cable operators who can potentially offer a good alternative to providing broadband Internet access and telephony; however, interconnection requirements and regulatory impediments in some countries often make it too difficult and costly for them to provide the service legally²⁸.

6.2. Wireless

6.2.1. Mobile communication

According to the ITU-infoDev ICT Regulation Toolkit *“The development of mobile technologies and services in the last two decades has had massive implications on the ICT landscape. Mobile technologies enable mobility and flexibility in the use of ICT services. While these technologies have primarily been driven by voice telephony but in their development, they embrace the whole portfolio of converged services, particularly when it comes to wireless standards and the new generation mobile technologies”*²⁹.

²⁸ Many of them are already interconnected illegally, through fix-lines.

²⁹ <http://www.ictregulationtoolkit.org/en/Section.1870.html>

Second Generation

GSM (Global System for Mobile Communications) is the most popular standard for mobile telephony in the world. Since both the signalling and speech channels are digital, it has been easy to adapt this second generation (2G) mobile system to data communications (3G).

The ubiquity of the GSM standard has been an advantage to both consumers and operators who can buy equipment from any of the many vendors. The standard also offers short message service (SMS), a low-cost alternative to voice calls, which is now supported by all other mobile standards. In addition, newer versions of the standard are backward-compatible with the original GSM phones. Release '97 of the standard added packet data capabilities through General Packet Radio Service (GPRS) and Release '99 introduced higher speed data transmission using Enhanced Data Rates for GSM Evolution (EDGE). EDGE supports data speeds up to 236.8 Kbps with end-to-end latency of less than 150 msec.

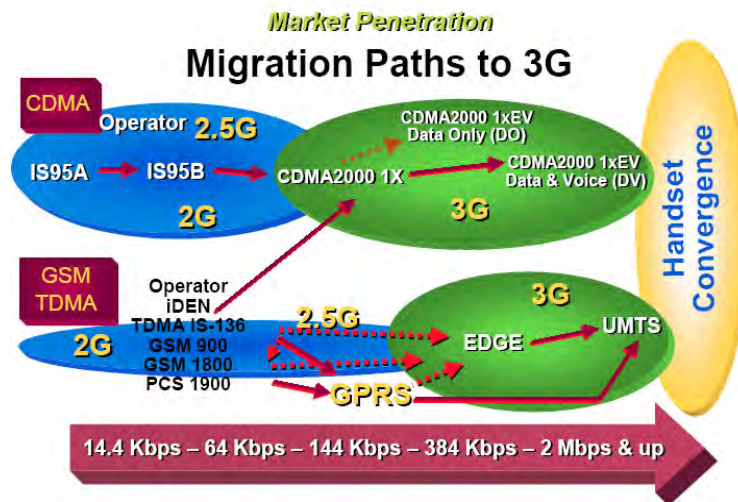
GSM operates mainly on 900 and 1800 frequency bands. In North and South America it operates also in the 850 and 1900 MHz bands.

CDMA (Code Division Multiple Access) is a spread spectrum technology with a special coding scheme (where each transmitter is assigned a code) to allow multiple users to be multiplexed over the same physical channel. CDMA (IS-95A) or CDMAOne is the second generation (2G) version of CDMA. The so-called 2.5 G version, CDMA (IS-95B), offers speeds up to 64 Kbps.

CDMA operates in the 450 MHz, 700 MHz, 800 MHz, 850 MHz 900 MHz, 1700 MHz, 1800 MHz, and 1900 MHz frequency bands.

CDMA has evolved through several steps to its third generation (3G) data only (CDMA 1x EV-DO) and data and voice (CDMA 1x EV-DV) versions. Figure N°7 shows the migration paths for CDMA and GSM to 3rd Generation mobile technologies.

Figure N° 4: GSM and CDMA Migration Paths to 3G³



Source: Stern and Townsend (2007)

Third Generation (3G) and IMT-2000

Third Generation (3G) is used to describe mobile services which provide advanced voice communications and high-speed data connectivity, including access to the Internet, mobile data applications and multimedia content. The International Telecommunication Union (ITU), working with industry standards bodies from around the world, has defined the technical requirements and standards as well as the use of spectrum for 3G systems under the IMT-2000 (International Mobile Telecommunications-2000) program, which, inter alia, requires that IMT-2000 (3G) deliver improved system capacity and spectrum efficiency over 2G systems and that it support data services at minimum transmission rates of 144 kbps in mobile (outdoor) and 2 Mbps in fixed (indoor) environments.

Based on these requirements, the ITU in 1999 approved five radio interface standards for IMT-2000³⁰. Three of the five, W-CDMA, CDMA2000³¹, and TD-SCDMA are based on CDMA (figure N° 8). In October 2007, ITU added the WiMAX air interface specification as the 6th IMT-2000 technology and modified the general naming conventions for IMT technologies: 3G technologies continue to be known as “IMT-2000”; 4G technologies will be known as “IMT-Advanced”, and collectively, all of the 3G and 4G technologies will be known as simply “IMT”.

³⁰ ITU-R Recommendation 1457.

³¹ CDMA2000 is also known by its ITU name, IMT-2000 CDMA Multi-Carrier (MC).

Figure N° 5: IMT 2000 Terrestrial Radio Interfaces



Source: <http://www.cdg.org/technology/3g.asp>

W-CDMA and CDMA2000 are two 3rd Generation mobile standards which are being used in Dominican Republic and Peru.

W-CDMA (Wideband Code Division Multiple Access), designated by the ITU to be the main technical standard for 3rd Generation or UMTS mobile communications standard, supports transmission speeds of up to 384 kbps in an outdoor environment and up to 2 Mbps in a fixed indoor environment. It operates in the 850 MHz, 1900 MHz and 2100 MHz frequency bands.

Many GSM operators in Latin America are upgrading to W-CDMA-HSPA³² which is becoming a very promising and cost effective way to provide broadband access in unserved areas with speeds up to 384 Kbps. In Dominican Republic, under the Rural Broadband Connectivity Project, more than 300 localities are being provided with broadband access via W-CDMA- HSPA.

CDMA2000 (Code Division Multiple Access 2000) or IMT-2000 CDMA MC is a hybrid 2.5G/3G CDMA standard used for digital radio, to transmit voice, data and signalling information (such as a the dialled telephone number) between mobile phones and cell sites. CDMA2000 designates a family of mobile standards that includes:

- CDMA 1x, which doubles the voice capacity of CDMAOne and delivers peak packet data speeds of 307 kbps in mobile environments;
- CDMA2000 1xEV-DO, which comes in the following versions:

³² WCDMA-HSPA, High Speed Packet Access – an extension of WCDMA to provide high bandwidth and enhanced support for interactive, background and streaming services.

- o CDMA2000 1xEV-DO Rel. 0 delivers peak data speeds of 2.4 Mbps and supports applications such as MP3 transfers and video conferencing;
- o CDMA2000 1xEV-DO Rev. A increases peak rates on reverse and forward links to support a wide-variety of symmetric, delay-sensitive, real-time, and concurrent voice and broadband data applications; and
- o CDMA2000 1xEV-DO Rev. B which provides integrated voice and simultaneous high-speed packet data multimedia services.

CDMA2000 1xEV-DO Rev. A and CDMA2000 1xEV-DO Rev. B are both backward compatible with CDMA2000 1x and CDMAOne. CDMA2000 supports data communication speeds ranging from 144 kbps to 2.4 Mbps.

There has been growing interest in using CDMA in the 450 MHz band, for rural, suburban and sparsely populated areas for both mobile and fixed applications. This is due to the relatively large cell sizes that are possible at this frequency, which makes deployment less expensive because fewer base stations are required to cover a given area as show in Table N° 3.

Table N° 3: Theoretical cell sizes that can be achieved using CDMA 2000 1x in the different frequency bands

Frequency band (MHz)	Cell Radius (Km)	Cell Area (Km ²)	Normalized Cell Count
450	48.9	7,521	1
850	29.4	2,712	2.8
1900	13.3	553	13.6
2100	10	312	24.1

Source: Response by Lucent Technologies to Questionnaire 2, usage of Lower Frequency Bands in the AP Region, 2nd Meeting of the APT Wireless Forum, Shenzhen, PR China, September 5-8, 2005.

The single, largest hurdle to the development of CDMA 450 is commercial. The low number of handset options available, their higher price, and the fact that few offer multi-band capability, has been an impediment to growth of this standard. In addition, the development of innovative approaches to rural network design and marketing by the GSM operators has limited the market

for CDMA 450. The International 450 Association³³ and a number of mobile operators have created an alliance to aggregate purchases in a bid to drive down costs of terminal equipment through bulk purchases and to nurture a market for entry-level devices.

In Peru, a small rural operator deployed the first commercial CDMA 450 network in Latin America in 2005 and has since February 2009 been deploying infrastructure for fixed broadband telephone access to more than 800 small communities across the country³⁴.

Table N° 4 indicates the year of its launch and the number of world-wide networks and subscribers for several mobile Internet and broadband access technologies.

Table N°4: Mobile internet and broadband access technologies

Technology	First commercial launch	Nb of networks 2Q2008	Nb of subscribers of mobile broadband networks 2Q2008	Data rates
CDMA 1x	1999	269 (+21*)	349 990 000 (incl. CDMA 1 × EV-DO rev.0-B)	153 kbit/s (Release 0) or 307 kbit/s (Release 1)
CDMA 1xEV-DO rev.0	2001	105 (+40*)	100 020 000	300-600 kbit/s
CDMA 1xEV-DO rev. A	2003			1.8 Mbit/s
CDMA 1xEV-DO rev. B	2005			< 4.9 Mbit/s
WCDMA	2001	182	302 840 000 (3Q2008) (incl. HSPA)	384 kbit/s
3G TD-SCDMA	2008	1	n/a	2-4.75 Mbit/s
HSDPA	2005	127 (+31*)	50 000 000	1.8-7.2 Mbit/s
HSUPA	2007	6 (+20*)		1.4-1.9 Mbit/s
WiMAX	2005	305	1 700 000	10-70 Mbit/s

Source: ITU, *Trends in Telecommunication Reform 2008: Six Degrees of Sharing*, based on data from CDMA Development Group, GSMA, UMTS Forum, GSA, WiMAX Forum, 3G Americas and other

6.2.2. Broadband wireless access (WiMAX, WiFi)

WiMAX (Worldwide Interoperability for Microwave Access) is a wireless broadband transmission standard for data, which can be used in a variety of ways including point-to-point links and portable Internet access. It does not need cables. WiMAX is based on IEEE standard 802.16 which

³³ <http://www.450world.org/>

³⁴ <http://www.televiasperu.com/>

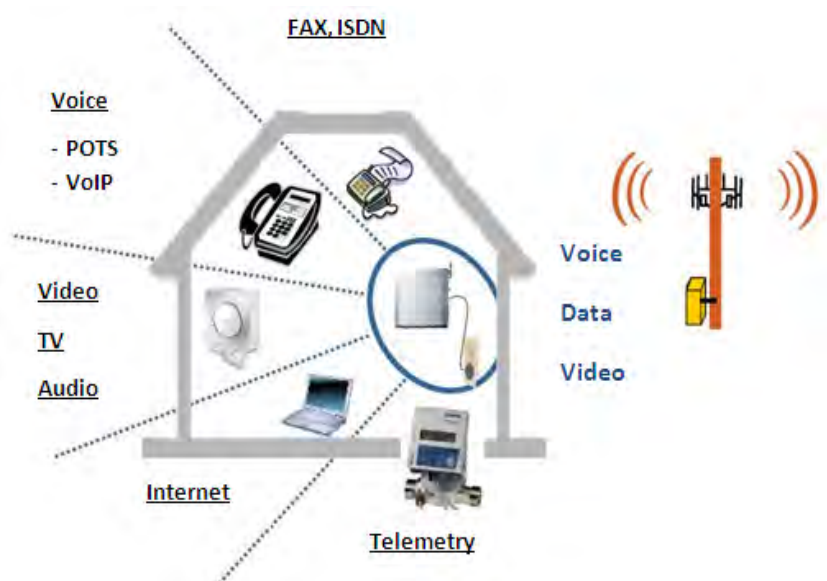
is also known as the Broadband Wireless Access (BWA) standard and provides up to 75 Mbps symmetric broadband links. It can be used as an alternative to cable and DSL for last mile wireless broadband access. See Figure N° 9.

IEEE standard 802.16-2004 or IEEE 802.16d, named after the IEEE working party that developed it, is frequently referred to as "fixed WiMAX" since it does not support mobility. IEEE 802.16e-2005, a modification of IEEE 802.16-2004, often referred to as IEEE 802.16e allows for mobility and is therefore referred to as "mobile WiMAX".

As mentioned earlier, in October 2007 the ITU Radiocommunication Conference decided to include WiMAX-derived technology in the framework of the IMT-2000 set of standards.

While there has been broad interest and enthusiasm for WiMAX technology and its potential, the business case for this standard and its ultimate success will be determined, as with other technologies, by market factors, including competition, demand, affordability of services, customer density, price and availability of end-user terminals³⁵. The current main impediment for the wide use of this technology in rural areas remains the high cost of the end-user-terminals.

Figure N° 6: Actual uses of WiMAX technology



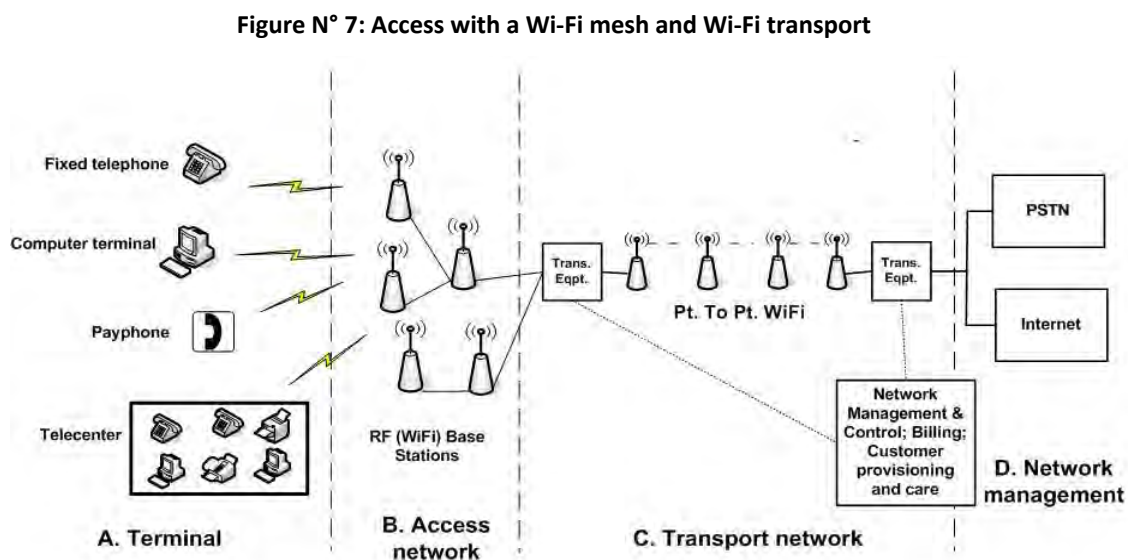
Source: *WiMAX Aplicaciones y Servicios. Siemens. Jaime Martínez.*

³⁵ See Annex 5 of Stern and Townsend, 2007.

Wi-Fi (Wireless Fidelity) is a Wireless Local Area Network (WLAN) technology and standard, which primarily provides short-range, wireless, high-speed data connections between mobile data devices (such as laptops, PDAs and telephones) and nearby Wi-Fi access points. There are several variations of the Wi-Fi standard, referred to as IEEE 802.11. The most common is IEEE 802.11b, which provides speeds up to 11 Mbps. IEEE 802.11g and IEEE 802.11a are faster versions of IEEE 802.11b with the former supporting speeds up to 52Mbps. Many IEEE 802.11g and IEEE 802.11a devices are backward-compatible with the original IEEE 802.11b.

Wi-Fi is a very good and cost effective solution for covering large areas in rural and unserved areas. Hot spots with amplifiers can easily cover ranges of up to 8 km. The low cost equipment and terminals make it affordable for low income populations. Non-mobile technologies such as Wi-Fi and wireless mesh networks built using Wi-Fi technology are well suited for small, local initiatives for which large and expensive centralized projects are not feasible. Typically, non-mobile technologies can support VoIP alternatives to 2G telephony.

Figure N° 10 illustrates a network that combines a Wi-Fi local access mesh network, with a point-to-point Wi-Fi transport link.



Source: Stern and Townsend (2007)

Wi-Fi has been deployed with success in many universal access and service (UAS) projects in rural and remote areas to provide Internet points of presence. The main advantages, especially for developing countries, are³⁶:

- i. the availability of high data throughput rates (compared with many 3G technologies);
- ii. its flexibility for small networks to develop outside of large centralized organizations;
- iii. the use of radio frequencies that are exempt from licensing in many countries where Wi-Fi frequencies are intended to be used by equipment with very limited range and indoor applications, for which interference does not need to be controlled through licensing; and
- iv. the possibilities of acquiring cheap standard equipment that is readily available and has been type approved for many countries.

Table N° 5 summarizes the basic specifications for various versions of the WiMAX and WiFi standards.

Table N°5: The basic specifications for various versions of the WiMAX and WiFi standards

Standard (technology)	Release date	Frequency Band(s)	Radio technology	Max net data rate	Max indoor range	Max outdoor range
IEEE 802.11 (WiFi)	1997	2.4 GHz	DSSS	2 Mbit/s	20m	100m
IEEE 802.11a (WiFi)	1999	5 GHz	OFDM	54 Mbit/s	35m	120m
IEEE 802.11b (WiFi)	1999	2.4 GHz	DSSS/CCK	11 Mbit/s	38m	140m
IEEE 802.11g (WiFi)	2003	2.4 GHz	OFDM, DSSS	54 Mbit/s	38m	140m
IEEE 802.11n (WiFi)	2009	2.4 GHz, 5 GHz	OFDM, DSSS	600 Mbit/s	70m	250m
IEEE 802.16d (Fixed WiMax)	2004	2 – 11 GHz	OFDM	75 Mbit/s	variable	15-50km
IEEE 802.16e (Mobile WiMax)	2005	0.7 – 6 GHz	OFDM/ OFDMA	15 Mbit/s	variable	1.5-5km

Source: ITU

³⁶ See Annex 5 of Stern and Townsend, 2007.

6.2.3. Satellite

Very Small Aperture Terminals (VSAT) are the most common satellite communication systems used for voice and Internet applications in rural and remote areas; however, the high cost of the equipment and especially the space segment compared with terrestrial radio and wireless access networks limits VSAT applications to quite remote areas. VSATs have been used successfully for providing fixed public access to telephony and broadband Internet in remote areas in many countries. Many good examples can be found in Peru, Chile, Colombia, Brazil, the Dominican Republic, Mongolia, Nepal, South Africa and other countries.

VSAT systems are sometimes also used as backbone networks for remote rural exchanges and mobile base stations (Picture N° 18).

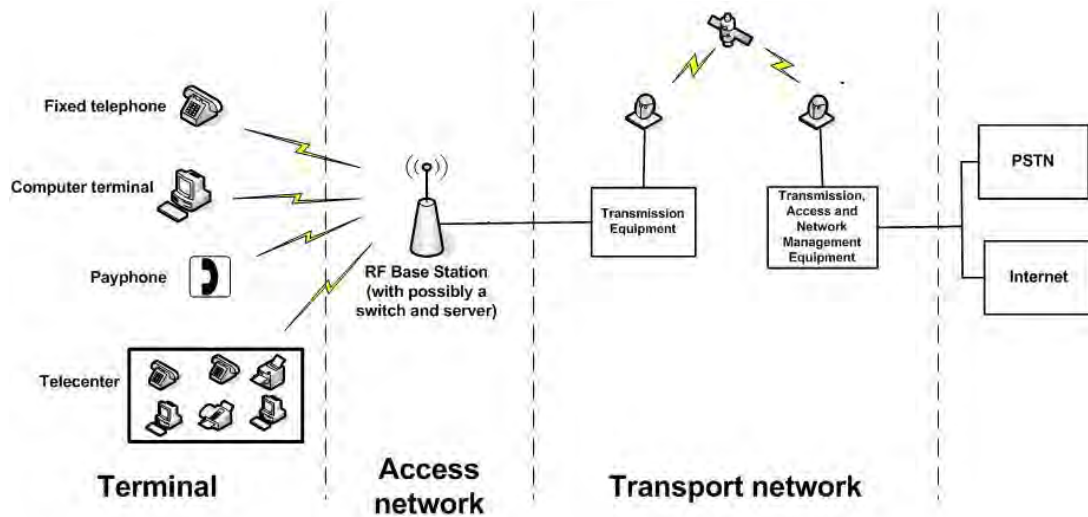
Picture N° 18: VSAT transport network infrastructure in Puno, in the Peruvian highlands



Source: FITEL

Figure N° 11 shows a Broadband Wireless Access (BWA) with satellite transport.

Figure N° 8: Broadband Wireless Access (BWA) with satellite transport



Source: Stern and Townsend (2007)

6.2.4. End user equipment

Advances in technology as well as economies of scale are lowering the costs of terminals for broadband users of which there are basically two types: (i) terminals that allow the Internet connection at home known as CPE (Customer Premise Equipment) and (ii) terminals that allow the user to use the Internet and to navigate, also known as end user devices.

The cost of CPEs is fundamental to establishing the viability of a project. It can be the deciding factor in cases where, for example, the network can be built cost effectively.

Convergence and technological advances are merging previous distinctions between types of end user devices as illustrated by the range of different devices that are available today: (i) personal digital assistant (PDA); (ii) combined phones, video cameras and music players; (iii) internet-enabled mobile phones such as Blackberry or iPhone that enable e-mail and web-browsing among other wireless services; and, (iv) powerful handheld 3G end-user devices that offer “triple-play” services: i.e. telephony, Internet and IPTV and mobile TV, such as Palm computers, PlayStation portables, etc.

7. Use of geographical information systems (GIS) and Google Earth in planning rural telecommunications projects

7.1. What is GIS?

Geographical information systems (GIS) combine hardware, software and data to capture, manage, analyze and display all forms of geographically-referenced information. Users can create interactive queries, analyze spatial information and edit data and maps. GIS is a structured geographical database that makes worldwide geographic data available in two formats:

- i. the Vector Model uses three geometric elements including points, lines or polylines and polygons, which correspond to discrete objects and therefore definite limits;
- ii. the Raster (Matrix) Model divides a given space into regular cells where each cell represents a unique value. This model focuses on the properties of space rather than the accuracy of the location.

GIS allows simultaneous spatial analysis of different layers of information representing census information, elevation, road networks, hydrographical data, infrastructure and telecommunications network elements and project information, etc.

7.2. Benefits of using GIS in planning rural telecommunications projects

GIS can be used in planning telecommunications projects to facilitate the decision-making process, including deciding where to put base stations and repeaters for a wireless project to optimize the design and coverage footprint and, ultimately, the best location for the project.

The decision-making process, which requires that data be collected, processed, and analyzed before the results can be presented and decisions can be taken, is facilitated by the fact that information from the different layers mentioned above gives an almost exact determination of the best coverage areas for deploying the project.

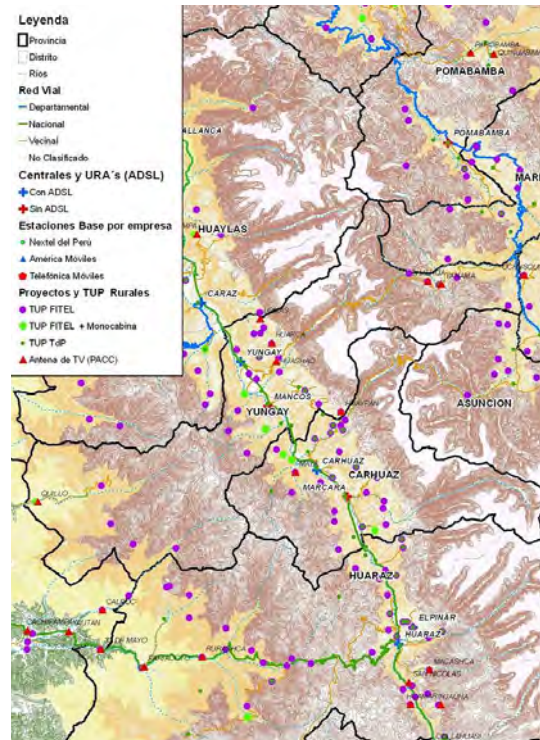
Gathering geo-referenced data such as geographical, demographic, economic and infrastructure information is, however, the most difficult task when using GIS and, if it has to be done manually, an extremely laborious task. However, in many cases there are already existing databases that can be used (government resources, national statistical offices, local authorities resources, etc.) in telecommunications projects.

GIS has been used extensively since 2001 in Peru where there are many organizations involved in gathering the required input. OSIPTEL, the telecommunications regulator, has been one of the lead users of GIS for elaborating telecommunications projects and even for calculating the walking distances to public telephones taking into account the hills and valleys that any potential user would have to cross to gain access to a telephone. In Dominican Republic, GIS is not as widely used as in Peru, even though there are several applications that do use them.

For example in the case of Peru, figure N° 12 below shows the political divisions in the country (black lines), the road network (blue and green lines) and rivers (dotted blue lines). The colored dots represent the location of FITEL³⁷ and other publicly financed public phones and public Internet centers.

³⁷ FITEL (Fondo de Inversión en Telecomunicaciones) is Peru's Universal Access Fund.

Figure N° 9: Use of GIS in Peru

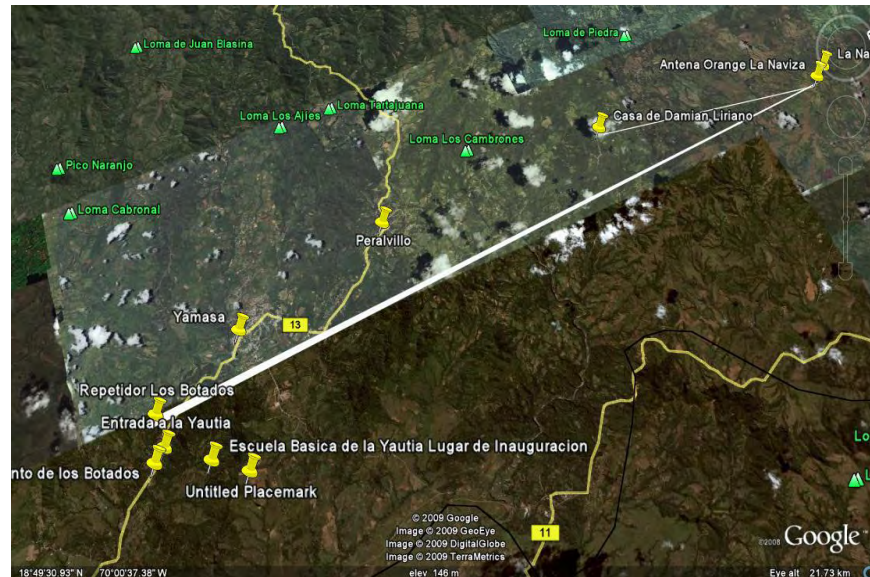


Source: FITEI

7.3. Google Earth

The Google Earth application, among many others currently available, is a powerful tool that can be used for analyzing and planning telecommunications projects. It costs nothing to use in its basic version and allows data of locations from GIS to be imported. With Google Earth it is easy to determine where the best place is to build a telecommunications network to suit a specific purpose. Depending on the degree of resolution of the Google Earth image, it is possible to identify individual houses, roads and even see existing elevations. Google Earth can provide a very good first approximation of distances and help the design engineer determine whether there is line-of-sight between any two specific points (figure N° 13). It is an ideal, first step tool for planning the required network infrastructure and coverage.

Figure N° 10: Creating lines-of-sight for wireless links between specific points in the Dominican Republic rural areas

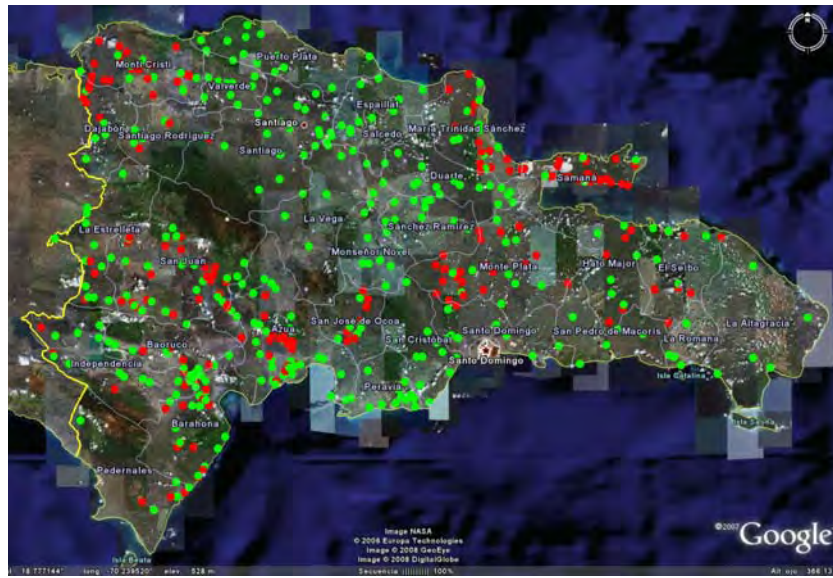


Source: Google Earth, Edwin San Román

Google Earth was used in the Dominican Republic in both the *Los Botados* pilot project and the *Rural Broadband Connectivity Project* from the development stage through to the infrastructure design stage, including the design of the transmission system and to determine coverage. In both cases the technical team designated by INDOTEL first obtained the coordinates of all localities to be covered and then overlaid these coordinates on a Google Earth image of the target area giving a view of location clusters which were within line-of-sight for wireless links. This allowed them to determine the best places for interconnections, taking into account existing transmission infrastructure.

Figure N° 14 shows the distribution of local governments (green dots) and localities (red dots) for the whole of the Dominican Republic.

Figure N° 11: Rural Broadband Connectivity Project in the Dominican Republic



Source: Google Earth, Edwin San Román

PART IV: PRACTICAL MATTERS TO CONSIDER AND STEPS THAT NEED TO BE UNDERTAKEN IN DEVELOPING AND IMPLEMENTING A RURAL BROADBAND PROJECT

8. Developing a rural broadband project

The development and implementation of a rural broadband connectivity project requires first that the administrative and legal underpinnings for the project, the nature of the licence to be awarded and the contract to be signed are well understood. It also requires that a number of practical steps be undertaken to complete the project successfully, including assessing demand, running an economic model to determine the maximum subsidy to be offered, the tender procedure, project supervision, development of dedicated web pages, awareness raising and capacity building.

Since broadband access allows not only Internet but also other services to be delivered, it is recommended that the provision of residential telephone³⁸ services be included as a requirement of the project. This enhances the potential for its sustainability because of the higher profit margins that can be derived from this service in comparison to those generated by Internet alone.

8.1. Administrative matters and legal basis

Before the bidding and contracting procedures for such a project can begin, the regulator or policy maker must ensure that the required legal and regulatory framework and administrative rules are in place before the infrastructure can be built and operated and determine the type of services to be provided.

In the Dominican Republic this framework and these rules are set out in the following documents:

- the General Telecommunications Law (No.153-98),
- the Law on Procurement and Contracts for Goods and Services, Construction and Concessions of the State (Law No. 340-06),

³⁸ Residential telephony can be provided using VoIP or any other suitable technology

- Telecommunications Universal Service Fund Regulations, and regulations on concessions, registrations and special licenses to provide telecommunications services.

In addition the social policy on universal service and the Universal Service Fund's 2007-2009 biennial budget were taken into account before the Rural Broadband Connectivity Project was started.

8.2. Nature of the licences and issues related to spectrum

Another issue concerns the nature of the licenses that will be awarded to the successful bidder(s) to operate the networks, to use certain frequencies, and to provide services. Ideally the selected operator should first be able to provide all services in the region covered by the project and then nationally under a global licence upon fulfilment of the project requirements and objectives. This is important, especially for potential new entrants, since it gives them an incentive to enter the market. Existing operators and service providers can have their existing licences modified to reflect the additional rights and obligations they have been given.

From the outset, the regulator must have a clear picture of the frequencies that can be assigned and how these are to be treated. Depending on the circumstances, the licenses and authorizations can be free or operators may be asked to pay for them.

In the Dominican Republic, INDOTEL decided that, if the successful bidder was a new entrant, it would automatically receive the necessary operating licence(s) once it had demonstrated that it met all the requirements. If it was an existing operator, its licence was to be modified automatically to reflect the added rights and obligations related to the *Rural Broadband Connectivity Project*.

With respect to spectrum, it was decided that potential bidders were to specify their requirements during the consultation phase of the project and, if successful, they would be awarded the required frequencies along with their operating licence without any additional charge. However, the successful bidder was to use these frequencies only in the coverage area of the project until completion of the project and confirmation by INDOTEL that all of the project requirements and objectives had been met. Thereafter, the company was to obtain the right to use the same

frequencies in the whole country. This was designed to be an effective incentive for the successful bidders to finalize their projects according to the specifications and within the time frame prescribed.

8.3. Demand analysis

Like their counterparts in the cities, people in rural areas want to communicate with family and friends and access information of all sorts for entertainment, work, capacity building, general knowledge and many other purposes. Communication is a vital part of their daily social, political, formative and economic activities. This creates an identifiable demand for telecommunications services.

Demand studies are used in developing telecommunications projects to determine:

- (i) the level of demand for different telecommunications services at determined prices, that the general population in rural areas can afford;
- (ii) the minimum level of investment and operating costs needed to satisfy the demand, so that there will not be high tariffs or investment deficits that could raise tariffs; and
- (iii) the potential rates of return on investments, a vital indicator for operators wanting to invest and operate in rural areas;

In addition, for rural access projects demand studies help:

- (iv) determine the level of subsidies required to incite investors to invest in rural telecommunications projects which are otherwise not viable without subsidies; and
- (v) set policies and incentives that facilitate access for operator to rural areas.

Even though demand for basic telecommunications services is predictable to a certain extent and can be measured *ex ante*, the demand for services, such as broadband, is harder to measure

because of the lack of information on usage in unserved and underserved areas. Nevertheless, comparisons can be made with localities with similar characteristics that have been connected.

8.3.1 Normal method for determining demand in rural areas

There are four basic steps in determining demand in rural areas:.

1. Collect and analyze secondary data³⁹ and information such as demographics, the economic situation of households and individuals, geography, traffic and tariffs.
2. Collect, compile and analyze primary micro-economic data on individual customers, households, companies, institutions, and others by means of questionnaires, interviews and other information gathering tools⁴⁰.
3. Use econometric modelling techniques to determine the demand functions, establish the accuracy of the estimates, and calculate elasticity and other parameters needed to quantify demand. These techniques are used for each type of service, each geographic area, each period of time, for incoming and outgoing calls, payment types, and for different socioeconomic levels⁴¹.
4. Evaluate and present the results, including an assessment of their relevance for the aspirations and objectives of the companies and/or institutions that required the demand estimates.

Although reliable, this method for determining demand is generally long, difficult and expensive, especially in a competitive sector where participants are reluctant to make commercially sensitive data, such as traffic flows on their networks, available to others, including the regulator.

³⁹ Secondary data is data previously collected by organizations such as national statistic or information agencies, census, etc. Primary data is data collected for the purposes of the rural broadband project; as such it has a special component on ICT-related information.

⁴⁰ For more information, see www.ictregulationtoolkit.org/en/Section.3335.html

⁴¹ For more information, see www.ictregulationtoolkit.org/en/Section.3341.html

Rural as opposed to urban projects are characterized by the number of obstacles to obtaining reliable demand estimates including the lack of secondary data, the difficulties and higher costs of obtaining primary data, the scarcity of traffic data, and questionable results of demand assessments for telecommunication services from rural areas. To overcome these obstacles, the regulator in the Dominican Republic, following the example set earlier by his Peruvian counterpart used a practical, less complex and quicker approximation or proxy to determine demand a method described below, which can be used in countries where there are already some telecommunications networks in rural areas, which is the case in many countries in the world.

8.3.2 Approximation method used in Peru and in the Dominican Republic

Following are the six basic steps in the approximation method used in Peru and the Dominican Republic to determine demand:

1. Select and determine the precise location of all rural communities in the country. In Peru OSIPTEL⁴² did this using the most advanced Geographic Information Systems (GIS) techniques available at the time⁴³. This required a substantial amount of information to be gathered including: demographics, number of households, availability of electricity (especially for the Internet services), accessibility to the road network, etc.
2. Using the information obtained in Step 1, identify the communities with and without telecommunication services and designate those which are to get broadband and residential fixed lines.
3. Obtain and introduce all historical information on traffic available from rural communities with telecommunication services (e.g. public telephones) into the GIS model.
4. Obtain the per capita traffic by dividing the total traffic by the total population for a representative community. For Internet access services the indicator to be used is the population of the representative community divided by the number of cyber cafés in the

⁴² OSIPTEL is the national regulator of Peru

⁴³ Arc GIS tool from ESRI. See <http://www.esri.com/>

localities that already have Internet service and the number of households that have residential Internet connections.

5. Apply the traffic structure⁴⁴ and the daily traffic per person in the community with access to the nearby unserved community. This gives a good estimate of daily traffic figures for both outgoing and incoming local, national long distance, international long distance and mobile calls. The daily traffic multiplied by the population of the targeted community and by 365 days constitutes the estimated annual demand for each service in this community.
6. For Internet access, apply the number of inhabitants per cyber café in the community with access to obtain the number of inhabitants per cyber café in the nearby community without access. With this data it is then possible to determine the number of cyber cafés per community and the bandwidth required.

In Peru, this analysis indicated that on average there is one cyber café for every 300 people in rural areas and 1 for every 500 nationally. In the Dominican Republic, a conservative estimate of 1 cyber café for every 1000 persons was made.

8.4. The economic model

8.4.1. Method used in Peru and in the Dominican Republic

Once demand has been assessed, an economic model is applied to determine the maximum amount of subsidy that can be made available. For this type of project this can simply be a cash flow analysis to determine the net present value (NPV) and the internal rate of return (IRR) of the project⁴⁵. It requires the traffic data which is obtained from the demand study. Once demand is assessed, the total number of communities and, hence, the total traffic and number of Internet cafés to be included in the project can be determined.

⁴⁴ The traffic structure is the distribution of traffic of incoming and outgoing calls for each of local fixed line calls, mobile calls and long distance calls.

⁴⁵ The ICT regulation toolkit elaborates on the quantitative socio-economic analysis using net present value (NPV) and the internal rate of return. See: <http://www.ictregulationtoolkit.org/en/Section.3349.html>

he next step is to get an estimate for interconnection charges, capital expenditure (CAPEX), operational expenses (OPEX) and profit margins. Finally, the average Return on Equity (ROE)⁴⁶, a standard industry measure which has the advantage that it takes into account the special characteristics of the country, can be estimated. ROE can serve as approximation for the cost of capital since it describes the level of profitability required for telecommunications companies to be willing to provide telecommunications services.

In the Dominican Republic this analysis was carried out separately for each of the three types of services being considered: residential telephones, the Internet cafés and public call centres.

8.4.2. Determining the amount of the subsidy

Once the ROE has been determined, a simulation of the rural operator's or service provider's revenues and expenses is done by applying prices and costs to the forecasted level and distribution of traffic. The cash flow over a specific period of time and net present value (NPV) are then calculated.

A negative NPV means that the project is not profitable. To get companies to invest the rate of return of a project has to be equal or greater than what can be achieved elsewhere. This happens when the NPV is equal to zero or, in other words, when the IRR equals the discount rate. Therefore, a subsidy that makes NPV equal to zero has to be offered to make the rural project attractive for current operators and potential new entrants⁴⁷.

In the Dominican Republic the cash flow figures were determined separately for each of the three types of services mentioned. First revenues were calculated for each and then the cost including CAPEX, OPEX and maintenance was subtracted from the total revenue to give net revenue for each service. Cash flow was determined over the five-year period that the company is required to provide the services under its contract with INDOTEL. Finally, cash flow and NPV were determined

⁴⁶ The ROE is an indicator of profitability. It is determined by dividing net income for the past twelve months by owners' equity. The result is shown as a percentage and it is interpreted as a measure of the net income that a firm is able to earn as a percent of stockholders' investment.

⁴⁷ For more information, see www.ictregulationtoolkit.org/en/Section.3347.html

on a yearly basis⁴⁸. The amount of subsidy required to make NPV zero was the maximum amount offered.

8.4.3. Other considerations

Given that the inputs into the demand study, including historical data, are obtained from neighbouring communities, the subsidy obtained is not likely to be exact. However, this is not important since the method described in sections 8.4.1 and 8.4.2 should result in a good approximation of a maximum subsidy, an amount likely to be underbid if the tender is carried out in a fair, non-discriminatory and transparent way.

In the Dominican Republic the financial assessment of the project was carried out over a five-year period which was to be imposed on the successful bidder. The five-year period was chosen because of the rapid evolution of technology and falling prices that require essential telecommunications equipment to be replaced every 4 or 5 years. Since prices in the future tend to be lower than current prices, calculating the cash flow using actual prices over a longer period may lead to a higher minimum subsidy than if a five-year period is used.

Another very important consideration results from the experiences gained with earlier rural public telephone projects in Peru, the Dominican Republic and elsewhere where an increasing number of unserved and underserved areas are being connected through rapidly expanding mobile networks and mobile telephones, which are becoming substitutes for fixed line connections and even for public telephones.

As a result, traffic from public telephones has fallen considerably. This has decreased the income of suppliers and made the projects less sustainable.

An earlier rural broadband project, the Agrarian Information System (SIA) Project in the Chancay-Hural Valley north of Lima, Peru built in 2005, is a case in point⁴⁹. Here the introduction of a 3G mobile network that also offers broadband Internet access is becoming a substitute for the fix

⁴⁸ Because the cash flow analysis was carried out on an annual basis.

⁴⁹ http://access.apc.org/images/6/61/Community_Projects_Case_Study-_Huaral_valley_agrarian_information_system.doc

wireless infrastructure deployed only three years earlier. This raises the question about cost: if providing broadband services through the 3G operators is lower than the cost of providing these same services over the fix wireless line network.

For these reasons, it is important that the life of rural access projects be spread over five years. The contract should be flexible and allow for its renewal to allow for new technical, commercial and economic conditions unforeseen at the start of the project.

The objective should be to maintain the subsidy only where competition is not providing services on a commercial basis with comparable quality and prices.

8.5. Minimum subsidy auctions

Subsidies are used when the market alone is not enough to support network deployment and service delivery and where policy concerns justify public funding or redistribution of resources. A particular type of subsidy, known as a output based aid (OBA) subsidy, is often used in the telecommunications sector and, in particular, in conjunction with universal access and service projects⁵⁰. OBA-type subsidies are intended to support investments, for example, in rural areas where the cost of construction and service provision combined with limited revenue potential makes the project commercially unfeasible. A key requirement for a one-time OBA-type subsidy is that it results in the establishment of an operation and service provision that should ultimately be self-sustaining and commercially viable.

In recent years minimum subsidy auctions have often been used in the telecommunications sector in conjunction with the economic model discussed in section 8.4 to select operators and service providers to implement universal access and service projects.

⁵⁰ OBA programs pay subsidies over a period of time, based on meeting pre-defined performance or continuous service milestones. While many OBA programs use minimum subsidy tenders, OBA projects can also be awarded and allocated using other criteria. See Executive Summary of Stern and Townsend, 2007 (http://www.regulatel.org/SU_Peter_31_08_07/Ab.Summary_v.9.PAS.pdf) and also ICT Regulation Toolkit, Module 3: Authorization of Telecommunication/ICT Services, at: www.ictregulationtoolkit.org/en/Section.507.html.

Such auctions are sometimes used in conjunction with OBA programs in which the payment of subsidies is tied to the successful bidder's meeting pre-defined performance criteria, such as the installation of a certain number of rural telephones in given areas⁵¹.

The terms of reference of the project and auction have to clearly indicate the maximum amount of subsidy which was determined using the economic method described in sections 8.4.2 and 8.4.3 above. Competing bidders for the project will ask for amounts equal to or below this maximum, underlining the importance of having the economic model prepared with much caution and getting the right input data. Bidders will need to know how much room for manoeuvre they have when determining the amount of subsidy they will need to make their operation profitable and to what extent they can underbid their competitors to win the project.

8.6. The tender procedure (transparency and non discrimination in the evaluation of offers)

Once all the tender documents have been prepared and approved, they should be published, preferably on both the regulator's and government's web sites, and in at least three newspapers with national coverage to make sure that potential investors from home and abroad are informed about the project. It is also important that this publication be accompanied by a realistic timetable which gives interested parties enough time to assess the project, do the necessary technical evaluations and prepare the bid document.

In the Dominican Republic the time allowed for the whole process was five months. Bidders were given 60 calendar days after being prequalified to prepare their technical and economic offers (Table N° 6).

⁵¹ See reference 3.

Table N° 6: Actual timetable for the Rural Broadband Connectivity Project in the Dominican Republic

Stage		Date
1	Resolution 149-07 of INDOTEL's board approves the tender	23 Aug. 2007
2	Project and tender announced (First notice)	6 Sept. 2007
3	Project and tender announced (Final notice)	10 Sept. 2007
4	Potential bidders acquire tender documents	6 - 20 Sept. 2007
5	Questions submitted by potential bidders on matters related to Envelope # 1 ⁵²	up to 22 Oct. 2007
6	Answers provided by INDOTEL on questions submitted on matters related to Envelope # 1	up to 26 Oct. 2007
7	Submission of Envelope # 1	30 Oct. 2007
8	Envelope # 1 prequalification results announced	5 Nov. 2007
9	Questions submitted by potential bidders on matters related to envelopes # 2 ⁵³ and #3 ⁵⁴	up to 20 Dec. 2007
10	Answers provided by INDOTEL on questions submitted on matters related to envelopes # 2 and #3	up to 26 Dec. 2007
11	Submission of by bidders envelopes # 2 and #3	3 Jan. 2008
12	Evaluation of bids received	up to 14 Jan. 2008
13	Envelope # 2 results announced	14 Jan. 2008
14	Opening of Envelope # 3 and announcement of winning bidder	17 Jan. 2008

Source: INDOTEL

Transparency of the tender process from start to finish is fundamental to ensure that there are a large number of bidders and a good competitive process. All bidders without exception should have access to exactly the same information at the same time. Any changes or new information must be immediately published on the relevant authority's web site and sent in writing to all those who acquired the tender document.

Bids should be evaluated by a team composed of engineers, economists and lawyers of the entity responsible for the tender if it has qualified personnel and/or specially contracted experts, so that bids are evaluated strictly in accordance with the terms of reference and other conditions of the tender. This may avoid accusations of favouritism or the use of veto powers by any evaluator, which must not and cannot be part of the process.

⁵² Envelope #1 contained administrative information of the bidders.

⁵³ Envelope #2 contained the technical offer.

⁵⁴ Envelope #3 contained the economic offer.

The evaluation process has to be completely impartial, and technical aspects have to take priority. The project has to be awarded to the bid that requests the minimum subsidy amount and at the same time satisfies all technical and legal requirements specified in the tender documents.

8.7. The contract

The contract is a legal document signed by the chosen operator and the entity responsible for developing the concept for the project, conducting the tender, and supervising its implementation. Inter alia, it commits the operator that has been awarded the project to building and operating the agreed network and providing the agreed services and it commits the responsible entity to honour the amount of subsidies offered, supervise the deployment and operation of the infrastructure, and penalize the selected operator, if required. The contract has to clearly define all the terms used in the document and the objectives of the project. It has to state the general conditions and the guarantees, the obligations of each party, the deliverable documents, the spectrum assigned as part of the project, allowable tariffs, conditions of interconnection, penalties in cases of failure to execute the project, contractual deadlines, the arrangements for supervising the project during implementation and operation, causes for rescinding the contract, validity of the contract and other relevant matters.

8.7.1. Payment method for subsidies

There are different ways of paying out subsidies. The most common is a phased approach whereby, say, the initial 20% to 40% is paid out on contract signature; the second, 20% to 40%, once the infrastructure has been completely deployed and the final portion, in regular instalments every six months over a given period of time.

In the Dominican Republic it was decided pay 20% on contract signature, 40% on completion of installations and 40% in six month instalments over a period of five years.

All of these payments must be backed up during the deployment phase by letters of credit guaranteeing the successful completion and operation of the project. These letters are not required after the infrastructure has been completely deployed. Only confirmation that the

services are being provided adequately and according to the conditions in the terms of reference and the contract are usually required. Failure to do so should result in payments being stopped.

8.8. Supervising the implementation of the project

Project implementation must be carefully supervised by the entity responsible for the project and tender, since this is the only legal guarantee that the network and facilities will be deployed properly according to specifications and in the agreed timeframe. This requires a team, the size of which depends on the scope of the project, but composed of at least three people (as was the case with the *Rural Broadband Connectivity Project* in the Dominican Republic): a team leader responsible for organization, planning and follow up of the project; a telecommunications engineer to confirm that the specified installations are deployed in each locality; and an administrator to deal with all the administrative issues of the contract. Where the size of the project requires more people, it might be necessary to contract people from outside or even outsource some of the work.

The first duty of the team in the Dominican Republic's *Rural Broadband Connectivity Project* was to visit each locality as soon as the contactor advised it that the project was ready-for-service. All installations were checked for conformity with specifications, including Internet up and downlink speeds, quality of voice on residential telephones and tariffs for telephone calls. The team also checked the training and the awareness raising programs that were being provided. Given the large number of installation that came on stream in a very short time, it was necessary for INDOTEL to temporarily increase the number of staff carrying out field supervision work by training additional technical and administrative personnel to support the base team.

8.9. Creation of dedicated websites for the communities to be served

The Internet allows each community and its residents to connect to the Information Society, to access information, generate local content, and give the rest of the world access to the community and thereby the possibility to interact with the community. This requires individuals who can create and develop local content on the community's website with information on the geographic location, how to reach it, tourist attractions, locally produced goods and the names and

information about the local authorities. The task of creating a dedicated website should not be underestimated because it will be presenting the community to the rest of the world. It has to be designed so that information can be easily and frequently updated. The objective of the exercise should be not only to develop the local content but also to train the local community in computers and Internet use and to encourage local organizations to create content related specifically to these organizations.

It is highly recommended that there be in the contract with the operator or service provider selected to carry out the project an obligation that requires it to promote and assist in the creation of appropriate and relevant web content for each locality where broadband access is going to be provided.

In the Dominican Republic the company that was awarded the project had an obligation to create a web site with the sort of information described above for each of the 508 communities in the project service area (Figure N° 15). The company also had to train local people to maintain and update the website.

Figure N° 12: Web page of the Rural Broadband Connectivity Project



Source: Claro - Codetel

8.10. Raising awareness among the local population

Raising awareness among the local population is determinant for the success of the project. It is important for the community to know about the services they will be provided with and how they will be able to access and use them. The usual way of doing this is through a publicity campaign which targets the youth of the community, since they are the ones who are most up to date with technological developments and the most inclined to use them.

For the *Rural Broadband Connectivity Project* INDOTEL decided to take the awareness raising campaign directly to high schools. The strategy was to first create awareness and interest among the younger people who understood the new technology and who in turn were to serve as conduits in raising awareness and understanding of the new technologies and services among their parents, grandparents and other adults. This awareness raising campaign for the *Los Botados* pilot took place during the deployment phase of the project as shown in Picture N° 19.

Picture N° 19: Training course in informatics in a CCI



Source: Edwin San Román

8.11. Capacity-building to ensure sustainability of the project

Capacity building and training of the local population is essential in ensuring the sustainability of the project. People in the community have to understand the importance and potential of broadband Internet as well as of the services and applications that it can deliver. Otherwise they will never adopt it. People have to be trained to become customers of the service and thereby ensure the project's sustainability.

In the Dominican Republic the establishment of more than 867 CCIs was accompanied by an important training objective. Many hundreds of people had already received computer related training in the CCIs and were ready to use Internet the day their communities were connected to broadband access. As a result, in many places where broadband is now being provided demand could not be met due to insufficient installed capacity. Consequently, the operator has been forced to expand capacity.

Once young people discover the potential and benefits of broadband they soon find ways to get a computer (which may sometimes be second-hand) and get connected. This gave INDOTEL the idea to start a new and very ambitious project called Juventec and which uses an e-learning platform to train people in assembling, maintaining and repairing computers, in Java and webpage programming, and entrepreneurship. Figure N° 16 illustrates the Juventec webpage.

Figure N° 13: Juventec Web Page



Source: www.juventec.org.do

9. Other innovative funding mechanisms

Universal access and service funds are not the only mechanisms to fund projects which bring telecommunications networks and provide services to rural, unserved and underserved areas. They were not the only mechanisms used in the Dominican Republic or Peru to achieve similar results. Other mechanisms discussed in this section included public-private partnerships, private initiatives and private-private partnerships ⁵⁵. Which one is best in a given situation depends on particular circumstances; however, whichever the regulator or other entity responsible for achieving universal access and services chooses, it is important to ensure that the desired results are achievable.

9.1. Public-private partnerships

Public-private partnership projects are ones in which the public sector, in the case of the Dominican Republic and Peru, the regulator, takes on the leadership role for the project and contracts a private operator to bring telecommunications services to a specific rural area. After first carrying out a study of the communities to be served, the regulator should contact the local authorities to discuss the project and to solicit their involvement.

Once they have reached an agreement, the regulator (or public sector entity) should contact operators who could potentially implement the project and provide the required services in the community. The regulator could propose a formula to the operator whereby the project implementation costs for a given community would be shared among the local authority, the regulator (through a Universal Access Fund, for example) and the operator.

This was the case in the *Los Botados* rural broadband pilot project where the local authority agreed to provide the land and built a supporting structure for the tower and antenna and has been providing site security. INDOTEL provided the towers and terminal equipment and the operator, VIVA, provided the radio link, the broadband hotspot equipment and Internet service as detailed in section 5.4.

⁵⁵ Other financing initiatives are also mention in chapter IV of Stern and Townsend, 2007.

Picture N° 20: Internet connection in a house in Los Botados



Source: Edwin San Román

9.2. Private initiatives

Purely private initiatives may also be used in communities where there is demand but no services are being provided by any operator. The job of the regulator in this situation is to show operators that there is demand for telecommunications services and then put them in contact with the local authorities, so that together they can work out the details of a project which will satisfy the demand and result in the installation of a network and the provision of desired telecommunications services in the community.

This is what happened, for example, in the community of *Hato Damas* in the province of *San Cristobal* where INDOTEL contacted a small telecommunications operator called Estrelatel and explained that the community had practically no access to any telecommunications services in spite of there being a significant demand for such services.

Estrelatel visited the community, contacted the local authorities and after undertaking its own evaluation became interested in building a network and providing services. After securing support of the local authorities, it built the network and is currently providing broadband access and other services. Here the operator deployed a copper local loop for fixed-lines and wireless local loop for broadband access.

Picture N° 21: Home phone installation in Hato Damas



Source: Edwin San Román

9.3. Private-private partnerships

Private-private partnerships can work where there are large private (and in some cases publicly owned) enterprises other than telecommunications companies in the vicinity of the community to be served in sectors such as mining, petroleum, and agribusiness. These enterprises usually have social responsibility programs which include, among others, the financing of some local infrastructure programs, education and health initiatives.

Here the role of the regulator is to persuade these companies to include the deployment of broadband networks in their social responsibility programs for the neighbouring communities and show them how this can promote their social and economic development. The regulator should also indicate how their support for such a project can enhance their image in these communities especially where company's activities may be having a negative impact.

Once the enterprise has agreed to be involved, the next step is for the regulator to contact a telecommunications operator that may be interested in building a network and providing services, give it the information needed for achieving the objectives of the project and, of course, put the operator in touch with the enterprise.

This type of partnership was created in the Dominican Republic for the implementation of a rural telecommunications project in *Las Salinas de Puerto Hermoso*, with Ciramar, a shipyard company located nearby and with Estrelatel, a small telecommunications company. Here, Ciramar financed a large part of the project.

Picture N° 22: Installations at Ciramar



Source: Edwin San Román

10. Sustainability

Building a network is the easy part of a rural broadband project. It is the long term technical and economic sustainability that is critical and fundamental. For sustainability to be achieved, the operator, who built the network and provides the services, has to be able to cover its costs and make a profit. If it does so, it will be encouraged to not only continue to operate and maintain the service but even expand it.

The regulator or policy maker responsible for the project must be aware of this when determining and setting tariffs, which should be based on costs and allow for a profit because otherwise the operator will have no incentive to build the network, maintain the services and or to expand it. Asymmetric interconnection rates, where more is paid to terminate calls in rural areas than in the

cities, reflecting the generally higher costs in the former, can help ensure the sustainability of rural telecommunications projects⁵⁶.

During the development phase of the *Rural Broadband Connectivity Project* INDOTEL did a comprehensive study of tariffs for similar services among different operators in the country, applied these to the economic model for the project, and then chose those that met the relevant criteria of covering costs and allowing for a profit margin.

The results were presented along with the overall project to the potential bidders with special emphasis on the proposed tariffs derived from the model. The operators provided their comments and suggestions and some of these were incorporated into the project. Tariffs derived in this way and prescribed for the operators receiving subsidies reflected commercial market realities.

It is commonly argued that tariffs in rural areas should be lower than in the cities because people in rural areas have less income than those in the cities. However, one should not overlook the main goal and objective of these projects which is long term sustainability rather than just the implementation and operation of a network and the provision of services for a limited time period. A better solution is to provide direct subsidies to individual subscribers and institutions that are not able to afford the tariffs required to achieve sustainability.

⁵⁶ For more information on asymmetric interconnection rates and other regulatory strategies to facilitate universal access and service, see: www.ictregulationtoolkit.org/en/Section.3212.html.

PART V: CONCLUSIONS AND RECOMMENDATIONS

11. Challenges and lessons learned

The following are challenges and lessons learnt in the development of rural broadband projects including from the ones in the Dominican Republic and Peru which have been referred to in this course and paper:

- It is essential that political support exist at all levels (national and local) for such a project to be successful. This was lacking in Peru whereas it was the driving force behind the project in the Dominican Republic.
- Local operators may underestimate demand, willingness to pay for telecommunications services and technological knowledge in the use of computers in rural areas. This was true in Peru and the Dominican Republic where operators whose networks covered the more populated areas found it difficult to think in terms of the technological and marketing requirements of infrastructure projects in rural areas.
- The regulator has to review the continuity and quality requirements for rural areas and modify them if necessary because providing telecommunications services in these areas with the same quality as in the cities can be very expensive.
- Instability and lack of a reliable electricity supply is a major problem for rural telecommunications projects and can add significantly to the overall cost of a project. Fluctuations of the energy supply are dangerous and often cause damage to the equipment resulting in expensive repairs and loss of service. This is an important factor to keep in mind when dimensioning the network and equipment.
- It is very important to become familiar with the social and economic situations of the targeted communities as well as their idiosyncrasies. Misunderstandings with local populations can often cause unnecessary delays in project implementation.

- The regulator and/or Universal Access Fund administrator has to be very active in promoting the development of networks and the provision of telecommunications services in unserved and underserved areas. Pilot projects are a very useful way of demonstrating to operators and other potential investors that it is possible to provide the services at costs which are lower than they may have envisaged and that there is definitely a market and willingness to pay for these.
- There are many clever and very creative people in rural communities who are already providing some forms of telephone and Internet services to others in the community. The project has to embrace their experiences and encourage them to get involved in the planning and implementation of the project in hand.
- In the absence of reliable data for estimating demand and given the high cost of conducting surveys, the regulator and/or fund administrator should consider various types of approximations (or proxies) for estimating demand when developing and designing rural broadband projects.
- Getting the large telecommunications operators to participate in tenders for rural broadband projects is often a big challenge because of they do not see such projects as viable. In this case, the regulator and/or Fund administrator has an important role to play in convincing them of the real benefits of such projects, not only for the communities affected but also for the operators themselves.
- Small broadcast cable operators in rural areas can be very good and cost effective broadband network and service providers; however, often high interconnection costs with existing networks present a barrier for them. The regulator has a role to play in bringing down these barriers.

12. Conclusions and best practice guidelines

A number of important conclusions can be drawn from the Peruvian and Dominican experiences in developing, planning and implementing rural broadband projects:

- There should be no barriers to the implementation of rural broadband connectivity projects when national policy supports such projects and when the regulator is committed to promoting them and providing its resources and facilities to demonstrate their viability and help in their realization.
- It is important for the regulator to share its vision of rural broadband projects with telecommunications operators and service providers in the country. The industry must be kept informed continuously and involved in the development of the policies for rural broadband projects and the plans for implementing projects to achieve the objectives of these policies. The views and opinions of network operators and service providers, who are potential partners in realizing these projects, have to be taken into account at all stages in the process.
- Offering available spectrum as part of the tender can serve as a useful incentive to get operators to participate in the process for awarding rural broadband licences. This has the added benefit of reducing the amount of subsidy that is requested in the minimum subsidy tenders.
- Rural areas are full of young people who are anxious to embrace the arrival of broadband and all the services that broadband can deliver.
- Given the particularities of the telecommunications sector, official public approval processes should treat projects in this sector differently from other public infrastructure projects in order to avoid unnecessary delays in implementation.

ANNEX 1: OTHER SUCCESSFUL EXPERIENCES: THE PERUVIAN RURAL BROADBAND CONNECTIVITY PROJECT

There are several good examples of the successful implementation of large rural broadband projects in Peru, where the regulator, by 2003, had already financed the installation of more than 7,000 public telephones throughout the country. OSIPTEL, the regulator, decided to implement a national rural broadband connectivity project through its Universal Access Fund (FTEL). The initial phase of this new project had as its main objective to provide broadband access to more than 3 000 localities in the country and signalled the start of a new era in rural telecommunications in Peru.

OSIPTEL had the project prepared and ready for implementation by late 2004; however, because of changes in the Peruvian legislation, the project had to go through a lengthy national public investment approval process which treats all such infrastructure projects equally, whether they pertain to road construction, sanitation, education or telecommunications.

There are no exceptions for telecommunication projects and the bureaucratic process failed to take into account of the very rapid evolution of technology in this sector and the fact that the project was to be financed from the Universal Access Fund and not from the national treasury or loans contracted by the state. Under the approval process OSIPTEL had to demonstrate basically the same social and economic benefits that it had already confirmed in preparing the project in the first place. Nothing changed in the approach but two valuable years were lost in the approval process.

There is an important lesson to be learned for governments and policy makers here. Telecommunications cannot be treated in the same way as other sectors, which may be just as important to the economic and social development of a country but which do not evolve as rapidly as telecommunications.

The goal of the project was to extend existing broadband networks beyond the cities that already had such networks to as many locations in the surrounding areas as could be covered by terrestrial

links with a maximum of up to three repeaters. These networks were to offer broadband Internet and associated services. OSIPTEL had carried out a demand study similar to the one described in section 8.3.2. The project divided the country into six areas or sub-projects with a total of 3,000 localities to be provided with broadband access. A telecommunications company bidding for a subsidy was eligible to be awarded up to three sub-projects, each of them of between 500 and 700 localities and 0.4 million and 0.5 million people covered.

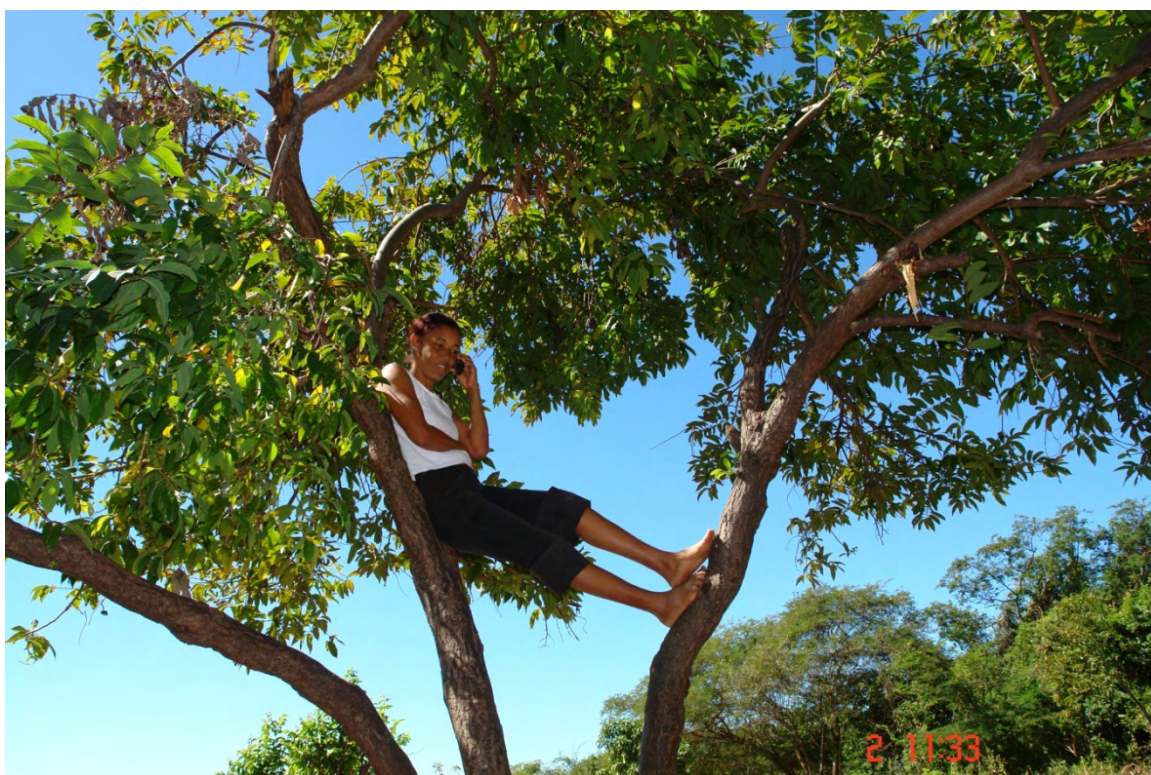
The bidding process started at the end of 2006 after all approvals had finally been obtained. There were bidders for all sub-projects and when the tender was completed in 2007, two companies ended up sharing the six sub-projects between them; however, only one, Rural Telecom⁵⁷, met all the requirements and signed a contract for 3 sub-projects. Rural Telecom's plans were to connect 1,928 towns by the end of 2009 and, as of January 2009, 669 of these had already been connected.

The Peruvian experience was very much taken into account in developing and implementing the *Rural Broadband Connectivity Project* in the Dominican Republic. The parameters for the evaluation were modified in accordance with the socio-economic and legal aspects of the country. Thanks to the lessons learned in Peru it was possible in the Dominican Republic to prepare the project, conduct the tender, and start implementation of the project in just over a year.

The experiences of Peru and the Dominican Republic with very similar types of projects show that when the political will exists and the necessary legislation is in place to develop, tender and implement such rural telecommunication projects, they can be brought on stream in a very short time. In Peru, the delay of more than two years was a result of excessive and unnecessary bureaucracy. It had nothing to do with any technological, commercial, financing or other barriers.

⁵⁷ <http://www.ruraltelecom.com.pe/>

Picture N° 23: Finding ways for communicating in Arroyo Dulce, in the south of the country



Source: Edwin San Román



TRENDS IN UNIVERSAL ACCESS AND SERVICE POLICIES: CHANGING POLICIES TO ACCOMMODATE COMPETITION AND CONVERGENCE¹

Sofie Maddens

*Senior Regulatory and Policy Advisor and Director African Affairs,
Telecommunications Management Group, Inc.*

*Senior International Expert for the ITU-EC Project to Provide
Support for the Establishment of Harmonized Policies for the ICT
Market in the ACP (HIPCAR)*

SECTION 1: INTRODUCTION

In the past, and particularly before the 1980's, the supply of telecommunications services was mainly seen as a public service, alongside other services such as water and electricity. Government controlled all such resources and sought to offer public services to people throughout the country. Since telecommunications was seen as a public service offered by government or through government intervention, policy-makers believed that a public monopoly operator would be in the best position to build telecommunication networks effectively () and that only such operators could make services available to citizens at equitable prices without siphoning off undue profits. Monopoly operators were expected to meet targets set for them, in exchange for certain benefits such as granting of periods in which they could enjoy exclusivity in the market. In most countries, the monopolistic operator was basically a state-owned enterprise, although a few countries did opt for a system of issuing licenses to private and/or state monopolies on a territorial or functional basis.

This model worked particularly well for many years in the more developed economies, where long-distance and international tariffs, which had stayed high despite technological changes, were decreasing in cost as opposed to the initial phases of their exploitation, thus enabling the development of the networks and of tele-density and the sector-specific industrial development. In these markets, cross-subsidization by monopoly undertakings generally ensured the availability of basic services, in particular connection to the fixed network and local calls.

¹ The information in this paper has been extracted from a report prepared by the ITU within the framework of an Action entitled 'Support for the establishment of Harmonized Policies for the ICT market in the ACP.' This Action was carried out with funding by the European Union.

In the less developed countries, the scenario of cross-subsidization worked less well and incumbent operators had difficulties in providing both basic and new services and in keeping up with technological changes. Although financial resources were obtained in some cases from multilateral lending or donor agencies or from bilateral government or other government-sponsored sources, this trend was not to last, thus creating the need for different method of service offering so as to provide at least some basic service to the majority of citizens..

Since the 1980's, technological advances, the perceived need to further lower tariffs to bring tariffs in line with costs, the desire to increase the range of services available to the consumers and the desire to expand businesses based on viable communications infrastructure were among the factors that started to undermine "traditional" thinking about the telecommunications sector and the funding of access to telecommunications services. Governments were faced with a situation where they had a social obligation of ensuring access to basic telecommunications to their respective populations but their power to impose such obligations on incumbents was becoming slimmer and slimmer.

It is commonly accepted that in many ways the liberalization of telecommunications markets and the introduction of convergence friendly policies, if properly implemented, has generally increased efficiency, increased the number of people who receive services, lowered prices, and improved the choice and quality of services provided. However, even in open competition environments which are properly regulated, ensuring universal access and/or service remains a challenge. Within this context, specific policy and regulatory measures as well as financing mechanisms have been introduced in many countries around the world to achieve universal access and/or service and safeguard the concept of reasonable access for citizens at an affordable price — in the light of national conditions — irrespective of income levels and geographic location

Thus, for example, with the emergence of competitive service providers and multiple technologies for the provision of telephone services, changes were introduced in universal access and universal service policies. Regulators began to introduce explicit subsidies for higher-cost services or services in remote or rural areas. These programs required a substantial level of direct, detailed regulatory intervention. Regulators now had to decide which operators or service providers had to contribute to universal service funds, how much subsidy funding should be collected and disbursed, what services should be subsidized, and which entities should receive the subsidies.

In addition, while it has been demonstrated that market forces, after liberalization and sector reform, have had the greatest impact on improvement of universal access (UA) and universal service (US) in many countries, for various reasons market gaps remained in place because of exceptionally challenging geographic characteristics combined with extremely low population densities or isolation (e.g., many islands) or extreme poverty. In other countries, markets might be able to achieve universal access (UA) or even universal service (US), but the timeframe in which this could be obtained, might be considered too long.

There is a clear need, in view of significant competitive, technological and service changes taking place in the telecommunications sector, to review traditional universal service obligations, their coverage, how they are financed and who is responsible for providing them. Indeed, universality has been achieved (to a greater or lesser extent) though a number of mechanisms,

including market reform, the imposition of universal service obligations on certain or all market players, the designation of universal service providers, the financing of universal service obligations, the creation of Universal Service Funds, as well as through innovative measures such as public-private partnerships, business-NGO partnerships, etc. Although in some cases the creation of a Universal Service Fund has been seen as one of the key requirements to achieve universal access and/or service, the sole use of such Funds is increasingly being questioned, with policy-makers realizing that there are a series of elements to be taken into consideration when considering universality issues.

SECTION 2: KEY ELEMENTS TO ACHIEVE AND MANAGE UNIVERSAL ACCESS AND/OR SERVICE

Key elements to achieve an effective framework to address universality include: defining the institutional framework for the definition and implementation of Universal Access or Service (UAS) policy and regulation; defining the scope of universal service and access, thereby ensuring that the services are available, accessible and that the price of communications is affordable; defining innovative mechanisms, including further regulatory reform, public-private partnership mechanisms, etc. to achieve UA; and, identifying financing mechanisms and selecting appropriate funding mechanism for universal access and/or service (which, as stated above, should not be limited to the creation of a Universal Service Fund).

2.1 Institutional Framework

Key questions to be addressed in relation to the institutional framework are

- *Is there a law/legal mandate to support or address the concept of Universal Access/Service (UAS)?*
- *Does the law/legal mandate direct the ministry or the regulator to develop a Universal Access/Service policy? Is the mandate clear?*
- *Is the regulator responsible for the implementation of the policy?*

Achieving universal access/service to communications is a challenge for all countries. In order to ensure that universal access/service policy is a central part of the ICT framework and not construed as simply a form of corporate social responsibility, or an act of ‘goodwill’ by investors in the ICT sector, it is important that:

- universal access/service policies are properly formulated
- universal access/service policies are given a proper space in the national policy and legislative frameworks as well as in the institutional framework for telecommunications regulation.

Universal access/service policy and its institutional framework should therefore be captured in national legislation, regulations, licenses or Ministerial policy statements (preferably a combination of all these instruments), which establish the framework and limitations within which the policy must be implemented. Such a foundation is necessary to ensure the credibility,

authority and enforceability of the policy, as well as to ensure that its terms are consistent with other national priorities and ongoing programs.

Within this context, it is also essential to ensure that the mandate of actors is clear so that they can effectively define the principle stages of a universal service and access policy, including: planning, implementation and evaluation as well as specific policy objectives for UAS and regulatory measures in ICT Policy statements. Such a mandate must be set out as clearly as possible, preferably in the law.

That being said, there is no one solution to creating an “appropriate” institutional framework for universal access/service. Universal access/service policy may be implemented by the country’s National Regulatory Authority (NRA), the ministry responsible for telecommunications and ICT, or an independent agency established to manage and administer universal access and service or even just the Fund.

In a number of countries, the ministry responsible for communications implements policy relating to universal access or service. This is, for example, the case in Colombia, Guatemala, and India. The advantage of such an approach is that the entity which defines policy also carries it out. The main disadvantage is that since such policies sometimes include special financing instruments such as a specific Universal Service Fund, which in many countries is mainly built up out of contributions from industry (which in some cases has little say in determining the level of contribution or indeed in the allocation of funds to projects), government is not perceived as being far enough removed to be an independent administrator of the finances. This is even more acutely felt where government still has any ownership interest in the industry.

In other countries, it is the National Regulatory Authority which implements universal access and/or service policies. Many recognize this as a more optimal and independent solution. Indeed, the 2005 WATRA Guidelines on Universal Access/Service state that: “ National Regulatory Authority’s (NRAs) must be established and capacitated to play a key role in implementing universal access policies first through addressing the market efficiency gap (letting the market deliver universal access/service), and second through the true access gap. NRAs should be responsible for implementing policies directed towards assuring the best quality reliable services at the most affordable prices that meet the needs of consumers—existing and future.”²

In Uganda, the 1997 Uganda Communications Act notes that the functions of the Uganda Communications Commission (UCC) will include enhancing the coverage of communications services and products in the country and expanding access to communications services in Uganda for all citizens³. In March 2005, the UCC issued Communications (Universal Service) Regulations outlining a comprehensive universal service policy for Uganda⁴. These Regulations:

² West African Common Market Project: Harmonization of Policies Governing the ICT Market in the UEMOA-ECOWAS Space, Final Guidelines on Universal Access and Service adopted by the 3rd WATRA OGM, 9 September 2005, Guideline 1.2, available at: http://www.itu.int/ITU-D/treg/projects/itu-ec/Ghana/modules/Compilation/Guidelines_final.pdf

³ Uganda Communications Act, 1997, Section 4, available at: <http://www.ucc.co.ug/ucaCap106LawsOfUganda.pdf>

⁴ Communications (Universal Service) Regulations, 2005, available at: <http://www.ucc.co.ug/regulate.php>

- ensure that the UCC has ample authority to specify and define universal service obligations for operators as well as to address services covered, that it can develop a suitable funding mechanism to support universal service, and that it has an appropriate enforcement authority
- identify the need to monitor delivery of universal service over time and review services captured in the universal service obligation, and to reassess coverage of services if need be;
- direct the UCC to establish a universal service fund to operate in concert with the already existing Rural Communications Development Fund (RCDF) which was established in 1997 by the Uganda Communications Act
- direct the UCC to both monitor and enforce the ability of the operators to carry out their universal service plans, as well as prescribing supply time and quality of service performance measurements intended to evaluate fulfillment of the universal service obligation

Having the NRA responsible for the implementation of UAS is generally seen to be a sound approach for many countries because:

- The regulator typically has the required industry sector expertise, and skilled technical, economic and financial staff;
- The regulator has a degree of independence and is perceived to be one step removed from politics; and

Once basic measures have been defined and implemented in the telecommunication sector, including opening the sector up to competition and establishing an independent regulatory agency, it is also the responsibility of policy-makers to monitor their implementation by conducting reviews at regular intervals and making any adjustments that may be needed. This is because a universal service and access strategy needs to be reviewed and fine-tuned from time to time in the light of social, commercial and technological developments, if it is to be effective.

2.2 Definition of Universal Access and Service

Key questions to be addressed in relation to the definition of Universal Access and/or Service are

- *If a law/legal mandate exists, is there a distinction drawn between universal service and universal access?*

As stated in the *Infodev* ICT Regulation Toolkit on Universal Access and Service⁵, the terms *universal access* (UA) and *universal service* (US) are used in a wide variety of contexts to describe or demonstrate objectives and policies that governments implement to ensure that all

⁵ *Infodev* ICT Regulation Toolkit, Module 4: Universal Access and Service, available at: <http://www.ictregulationtoolkit.org/en/Section.3126.html>

their citizens have access to the benefits of modern economic life. They refer to the ability of everyone, regardless of region or location, socio-economic status, ethnicity, gender, disability, or any other factor, to access services. The concepts are broadly promoted and widely accepted as the best expression of policies seeking to achieve equality and fairness of opportunity along with economic growth. Within this context, the key goal of a country's universal service/access policy is to develop the infrastructure and regulatory tools necessary to provide each member of its population with access to a point of communication.

In general, US refers to service at the individual or household level - typically a telephone in each home - whereas UA refers to a publicly shared level of service which is generally through public payphones or Internet telecentres. However, there is more to the definition of the terms than just the fact of providing a connection to every household as opposed to connectivity in every village. Indeed, the three main dimensions distinguishing Universal Access and Universal Service articulated by the ITU 2003 *Trends in Telecommunication Reform Report* are:

- **Availability:** The level of service is the same wherever a person lives or works, with no disadvantage stemming from geographic location. In particular, rural and urban distinctions do not affect a person's ability to access communication services. In the information age, the quality of services becomes even more important.
- **Affordability:** Everyone can afford service, and no one is disadvantaged by income level. Cost variations due to location, terrain or climate, which often dovetail with urban/rural factors, do not impact on one's access to ICT services. This dimension presents unique challenges with regard to addressing network expansion.
- **Accessibility:** People with disabilities can use the service; one's level of physical and mental ability does not affect access to communication services. In the information society, policy makers must look past physical accessibility and take into account the *relevance* of content and applications and the ability of users to understand it.

This has led to various definitions around the world. Under the EU Telecoms rules as set by the Universal Service Directive of 2002, for example, universal service is a safety net for achieving social inclusiveness. It ensures that basic communications services of good quality are always available at an affordable price, even if the market does not provide them under normal commercial conditions. This set of basic services, which are already available to the great majority of citizens and considered essential for participation in society, is called 'universal service'⁶. The Universal Service Directive defines universal service as "*minimum set of services, of specified quality to which all end-users have access, at an affordable price in the light of national conditions, without distorting competition*".

2.3 Scope and Enforcement of Universal Access/Service Obligations

Key questions to be addressed in relation to the scope and enforcement of Universal Access and/or Service obligations are

- *Are there key principles or goals for Universal Access/Service defined in the law or any other document (e.g., Government policy)?*

⁶ Universal Service Directive, available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0022:EN:HTML>

- *Does the law define specific services that must be provided and to whom?*
- *Does the law provide that universal service targets are reviewed on a regular basis?*
- *Does the law provide that stakeholders are consulted regarding UAS targets?*
- *Are there specific criteria for determining which operators have or are subject to Universal Access/Service obligations?*
- *Do the obligations vary from operator to operator, such as a distinction drawn between dominant and non-dominant operators?*
- *If the operator fails to meet its Universal Access/Service obligations, or contribution requirements, what enforcement mechanisms are in place to address*

The definition of universal access/service and the scope of the obligations attached to the respective definitions will differ from one country to the next depending on the economic and social context and the political will to achieve universality in terms of means of communications.

There is no fixed or standard definition for the scope of universal access/service obligations – however, currently established universal service/access policies typically seek to meet the objectives stated above: availability, affordability and accessibility.⁷ The range of the scope of UAS obligations is very broad because developed and developing countries face different market conditions and must meet different objectives in order to provide unserved and underserved rural populations with universal service/access.

In most countries, the scope of universal access and service (UAS) includes the provision of basic telephony. However, the definition of the scope of UAS is evolving to include Internet connectivity and increasingly broadband as technology develops and countries come closer to reaching their goals for voice service availability. Radio and television broadcasting has traditionally not been included in the definition of the scope of UAS, but this is also changing rapidly due to developments such as convergence, Internet broadcasting and broadcasters also offering Internet and telephony services (e.g., cable TV operators). Broadcasting policies and regulation typically have coverage requirements, though without specifics about actual access, whether by public means or for private subscribers. For example: the definitions in ECOWAS-UEMOA vary with most countries referring to voice, but a few like Ghana have considered including a wider range of services to include voice, data transmission, Internet access, access to relevant local content and broadband, in the scope of “basic.”

The scope of UAS is often specified in detail to ensure that it is fit for purpose. As mentioned above, it needs to be accessible and affordable as well as available. Features of UAS that might be specified include the following:

- Times of day when there is access to the service;
- Type of shelter for the terminals (e.g. secure building for a telecentre);
- Access to and usability of the terminal for people with physical disabilities;

⁷ Rethinking Universal Service for a Next Generation Network Environment, Working Party on Telecommunication and Information Services Policies, OECD, April 2006, p. 10.

- Convenience and pleasantness of location for all target groups of users (e.g., women might not wish to enter a bar to use a service);
- Quality of service (network reliability, fault repair times and call quality for telephony and prescribed down and upstream data rates for the Internet service).
- Payment methods (e.g., cash or prepaid cards) and for prepaid cards, availability of sales outlets; and
- Personal support for using the services.

Other services that are entering UAS policies include:

- Directories and directory enquiry services;
- Support services for Internet subscribers (e.g. help-lines, training);
- Emergency call answering facilities (dispatch of help for emergencies); and
- Special facilities to permit use by people with disabilities on par with all other facilities.

Figure 1 below shows the universal service obligations for designated universal service providers in the European Union, Uganda and India and illustrates how universal service/access objectives vary from one country to another.

Figure 1

European Union	EU Member States must ensure the following: 1) Access at a fixed location upon request, to enable users to make and receive local, national and long distance calls, fax communications, and to enable them to have functional access; 2) At least one comprehensive directory and one comprehensive enquiry service comprising the numbers of all fixed and mobile subscribers who so wish; 3) Availability of public pay phones over the whole territory; 4) Measures that ensure that the disabled have access to the same services at an affordable price. 5) <i>(since 2005)</i> Required to supply connection that provides “functional” Internet access (FIA), which is limited to a single narrowband connection and does not extend to ISDN or broadband. 6) Must respond to all reasonable requests to install a telephone line, offering the same prices irrespective of location.
-----------------------	---

Uganda	(1) Ensure universal availability of connections by every person or individual households to public communication networks through inter alia pay phones, community telecentres, tele-boutiques, kiosks, cafes or community communications internet access terminals (2) Provide the following services: (i) connection to a fixed communication network able to support voice telephony, fax and data transmission,(ii) reasonable geographic access to public call boxes across Uganda, (iii) ability of consumers to access emergency and free services, operator assistance and directory inquiry services, (iv) ability to meet needs of people with disability,(v) delivery of affordable basic communication services to all customers on reasonable request, (vi) providing customers with disabilities with the same or equivalent services as all other customers so as to have access to the same level of universal service.
India	<u>Stream I</u>: Provision of Public Telecommunications and Information Services (a) Operate and maintain village public phones (VPT); (b) after target of one VPT per village achieved, provide additional public phone in villages of 2000+ without public call office; (c) replace multi access radio relay technology public phones; (d) upgrade public telephones to public tele-information centres; (e) install high speed public telecommunications information centres. <u>Stream II</u>: Provide household telephones in rural and remote areas as determined by central government

Sources: What Rules for Universal Service in an IP-enabled NGN Environment? Background Paper, International Telecommunication Union, April 2006, pp. 5-8.; The Communications (Universal Service) Regulations of Uganda, 2003, Section 6; and Universal Service Obligation Fund, Department of Telecommunications, Ministry of Communications & Information Technology of India at <http://www.dot.gov.in/uso/usoindex.htm>.

These examples demonstrate that, despite the fact that countries have begun to adapt UAS obligation objectives to take advantage of the opportunities brought about by technological development (i.e., the Internet) and provide both voice and data communication services, most UAS obligation objectives still rely on the improvement and expansion of wireline networks to provide service and access to populations in unserved and underserved areas. Efforts to provide UAS through wireline networks have produced incremental results, but countries should consider the benefits that technologies - such as for example wireless technologies - can bring to telecommunications networks and to the fulfilment of universal service/access goals.

At present, technological change is challenging existing policies and forcing regulatory authorities to rethink the universal service obligations they impose on their carriers and establish a framework that will enable the government to carry out their universal service/access policies in a converging telecommunications sector.

2.4 Regulatory Reform and UAS

Key questions to be addressed in relation to regulatory reform and its role in addressing UAS include:

- | |
|--|
| <ul style="list-style-type: none">• <i>Does the law provide that build out requirements may be included in licenses to achieve UAS targets?</i>• <i>Does the law provide that coverage obligations (in terms of population or geographic area covered or other) may be included in licenses to achieve UAS targets?</i> |
|--|

Since markets have been opened to competition, policy makers and regulators have been using a variety of tools to achieve universal access or service. Good practice is that before using scarce public resources, governments and regulators exhaust available non-investment avenues to extend access. Often regulatory reform is one of the first steps in achieving universal access/service. This includes developing policies, regulations, and practices, including privatization design that goes beyond the more traditional framework of simply imposing obligations on designated universal service providers, which in most cases was the incumbent fixed-line operator. Such tools create incentives for the private sector to extend universal access to ICTs, as well as enacting enabling licensing and interconnection frameworks.

Establishing flexible spectrum policies as well as technology-neutral telecommunications policies that include a flexible and adaptable licensing regime can facilitate the entry and use of new and innovative technologies and provide a wider range of participants to achieve universal service/access goals. Revising universal service obligation objectives and implementing suitable mechanisms for the disbursement of universal service fund resources can also help in taking full advantage of multiple resources and technological development to better serve and benefit underserved and unserved populations.

Recently, new technologies have begun to provide unserved and underserved areas with faster service and more affordable access to communication. Mobile technologies are being used increasingly to provide rural and difficult to reach communities with fixed-wireless and mobile public payphones.⁸ In many developing countries, mobile networks have become a substitute for fixed networks because (i) they can provide wider coverage, (ii) they can usually be easily and quickly deployed at a lower cost, (iii) their management and maintenance is simpler, and (iv) pricing schemes applied by mobile operators have made access to telephony service affordable for the urban poor.⁹

As third generation (IMT-2000 or 3G) wireless technologies are deployed around the world, they can offer both voice and data services at affordable costs and thus can provide even greater access to communications services. Third generation technologies, such as CDMA 2000 and WCDMA can support both voice and broadband wireless access, transmit large amounts of traffic in a small amount of spectrum, as well as provide wider coverage. CDMA operators in India (as a result of Unified Licences being introduced) have been able to build networks quickly and are offering low price plans in underserved areas.¹⁰ In addition, operators in Brazil, China and the United States are using CDMA 2000 technology to expand and deploy Internet access across the country, including remote areas. In Peru, a clinic in the Andes is using 3G wireless voice and data equipment to communicate with medical professionals around the world to provide medical assistance to patients in this remote area of the country. The clinic, which had no connectivity of any kind until February 2006 and no fixed line communications, has been able

⁸ Mobile Operators: Their Contribution to Universal Service and Public Access, January 2003, pp. 7.

⁹ UMTS Forum Report "Benefits of Mobile Communications for Society", June 2004, Report No. 36.

¹⁰ Opportunity for All: Using Wireless to Provide Universal Access to Telecom Services, pp. 2-6.

to treat over 3,000 residents in the area. In the same manner, EV-DO high-speed wireless technology is being used in the Democratic Republic of the Congo to access vital patient information quickly and to notify doctors in case of emergency.¹¹

Other technologies such as Voice over Internet Protocol (VoIP), very small aperture terminals (VSAT), and broadband over power-line (or power-line communications) which are not as widely used at present, are also options that can provide connectivity inexpensively and effectively to rural areas, and can help countries achieve universal service/access.¹²

Given the importance of new technologies in reaching unserved and underserved rural populations, regulatory authorities are modifying their universal service/access policies by incorporating new technologies and relying on them to reach rural populations. Forward-looking telecommunications policies can foster the use of new and innovative technologies and can be instrumental in helping countries to achieve their universal service/access goals.

- ***Technology Neutrality***

A critical factor in establishing progressive policies for achieving universal service/access is technology neutrality. In other words, when establishing universal service/access policies, countries can maximise the opportunities for achieving their universal service/access goals by not limiting technological choice.¹³ By avoiding traditional paradigms that rely only on wireline operators to achieve universality, countries can encourage the use and application of innovative technologies and foster a more competitive and dynamic market that can further support universal service obligation goals by introducing technology-neutral policies. In turn, such policies will be conducive to a universal/access policy that will better answer the needs and demands of a country's rural population.

- ***Licensing***

As telecommunications markets have liberalised, countries have moved away from restrictive individual licensing regimes, which can limit the scope of technologies and services that an operator can offer, to a variety of more progressive licensing options such as service or technology neutral licensing regimes. Unified (converged) licences, which can be described as a license that allows an operator to offer a panoply of services under one authorisation,¹⁴ seem to be well-suited for countries trying to expand their telecommunications networks to reach as much of the population as possible. This type of regime opens the scope of technologies and services that can be offered by one operator and thus increases participation of new market entrants, encourages the introduction and use of new technologies, and also facilitates the process of obtaining a license. Countries such as India, Australia, individual member states of the European Union, Japan, Kenya, Malaysia, Mali, Mauritius, Singapore, Tanzania, and

¹¹ 3G Creating Digital Multimedia Access Opportunities Around the World, 3G CDMA Wireless Technologies Benefiting Society.

¹² A New Model for Rural Connectivity, Development Through Enterprise, Al Hammond and John Paul, May 2006.

¹³ What Rules for Universal Service in a an IP-enabled NGN Environment? Background Paper, International Telecommunication Union, April 2006, p. 20.

¹⁴ The Challenge of Creating Policy and Regulation in a Converged ICT Era, Ernest C. A. Ndukwe, Telecom World Africa Conference 2005, Capetown, South Africa, p. 7.

Uganda¹⁵ have all introduced some form of converged licensing regime based on the characteristics and needs of their markets.

Regulators should follow a strategy of aggressive all-service licensing of operators willing to provide services in currently uncovered areas. In some countries, operators are expressing a preference for alternatives, such as accepting reasonable rural build-out targets in their licence, or negotiating ex-ante specific rural universal access and service (UAS) targets with the regulator in exchange for relief from UASF levies or taxes.

In establishing the framework necessary to provide universal service/access to rural populations, a country also should consider a licensing regime that will allow it the flexibility to take advantage of technological development and convergence. Build-out targets are increasingly used in licensing procedures as an important factor to evaluate applications alongside the bid price. Thus, for example, in Uganda, the Second National Operator's bid evaluation criteria included a network rollout plan in addition to the bid price. In India, the regional local fixed operator bid evaluation criteria gave weight to rural coverage plans, but only 15 percent compared to 72 percent weight of the amount of license fee offered.

Under these models, investment in the sector, rather than short-term fiscal benefits, is treated as a major or primary consideration—ensuring a higher rate of investment over the long run (Dyiamond, Juntunen, and Navas-Sabater 2000). At the same time, licenses need to be designed carefully to ensure that the investments encouraged under the scheme will actually help meet access targets.

Brazil is an example of a country that, although it has developed a funding mechanism, generally achieves its universal objectives through coverage obligations imposed on its licensees. In fact, one could argue that Brazil's coverage obligations are more effective at achieving universal service goals than any of the special telecommunications development funds that have been created to fund or subsidize telecommunications projects. Because the Brazilian legal framework uses a variety of tools to achieve universal service, it took advantage of the new licenses being issued for third generation (3G) mobile services and imposed more expansive coverage obligations on those new 3G licensees than obligations previously imposed on mobile licensees. In so doing, Anatel recognized that imposing coverage obligations through licenses brings more immediate benefits to the population than other funding mechanisms. To this end, during the last tender for 3G mobile licenses, areas of low demand were not licensed in their own right, but were included as coverage obligations along with the more populous licenses.¹⁶ For example, winners of the São Paulo metropolitan licenses (in the southeast of the country) are obligated to provide coverage in the northern states of Amazonas, Amapá, Pará, Maranhão and Roraima.

In addition, specific coverage obligations were also detailed in the licenses, according to the following chart:

¹⁵ Licensing Approaches in an Era of Convergence, Global Symposium for Regulators, Geneva, Switzerland, 8-10 December, 2004.

¹⁶ *Edital de Licitação* ("Bidding Terms") No. 002/2007. The tender was concluded in Dec. 31, 2007 and the 3G licenses were signed and published on the Brazilian Official Gazette in Apr. 29, 2008.

Table 1 – 3G Licenses Coverage Obligations

Target	Threshold population	Coverage Obligations
I.	Without cellular service	Licenses will have the first 2 years to provide mobile services to 25% of the municipalities of each area acquired that still does not have cellular service.
II.	Less than 30,000	Licenses will provide 3G coverage to 15% of all municipalities within 5 years, and reach 60% coverage in all municipalities within 8 years.
III.	30,000 – 100,000	Licenses will provide 3G coverage to 50% of all municipalities within 5 years.
IV.	More than 100,000	Within 1 year, licenses must cover 50% of state capitals and municipalities with more than 500,000 inhabitants; within 2 years licenses must cover 100% of state capitals and municipalities with more than 500,000 inhabitants; within 3 years, licenses must cover 50% of municipalities with more than 200,000 inhabitants; within 4 years, licenses must cover 100% of municipalities with more than 200,000 inhabitants; within 5 years, licenses must cover 100% of municipalities with more than 100,000 inhabitants.

Source: Anatel.

2.5 Multi-pronged Approach to achieving UAS

- **Key questions to be addressed in relation to the introduction of a multi-pronged approach to achieving UAS:**
- *Does the law provide for a multi-pronged approach to addressing universal access/service challenges and opportunities?*
- *What complementary strategies to meet the objectives targets are set out? Do they include:*
 - a. *micro-credit programmes;*
 - b. *‘build, operate and transfer’ (BOT) or ‘build, transfer and operate’ (BTO) arrangements;*
 - c. *cooperatives and community-owned networks;*
 - d. *regional operators;*
 - e. *telecentres and multi-purpose community centres (MPCCs)?*

Complementary strategies can be applied to ensure that objectives and targets are met through a mix of tools. As stated in the 2005 WATRA Guidelines: “Member States shall design universal access/service policies, regulations and practices in order to create incentives for the private sector to extend universal access to communications services.” The Guidelines also provide that: “ Member States shall use a multi-pronged approach to addressing universal access/service challenges and opportunities. That is, rely on complementary strategies to meet the objectives targets that have been set out.”

The 2005 ITU West African Harmonization Report on Universal Access and Service Report¹⁷ provides that:

“Over the years, given the economic case for universal access/service, there has been a shift towards seeing universal access and service schemes not as “burdens” but as opportunities from a commercial perspective. This policy choice, between setting mandates and providing incentives, is often captured in the term “pay or play.” That is, an operator can either pay to support universal access/service or undertake to provide it itself. The strategy of incentivising operators to provide universal service does not diminish governments’ role in addressing universal access/service. Governments retain the responsibility to set overall policies which will facilitate private-sector contributions to universal access/service.

A common approach of engaging operators and allowing them to “play” is to provide incentives for operators to provide telecommunications in less profitable areas. Such incentives could include purely commercial mechanisms (not necessarily directly related to the telecommunications sector and therefore requiring consultation with other government departments) aimed at targeting the operators’ bottom line, such as tax concessions, removal of duties on telecommunication equipment targeted at rural and remote areas, or lifting of foreign exchange restrictions.

Other ways in which universal access/service may be promoted include:

- micro-credit programmes;*
- ‘build, operate and transfer’ (BOT) or ‘build, transfer and operate’ (BTO) arrangements;*
- cooperatives and community-owned networks;*
- regional operators; and*
- telecentres and multi-purpose community centres (MPCCs).”*

Bangladesh is a good example of a country where telecommunication access to most of the rural areas is mainly being provided not by government mandate but through Grameenphone’s¹⁸ Village Phone Program.¹⁹

¹⁷ Available at: http://www.itu.int/ITU-D/treg/projects/itu-ec/Ghana/modules/FinalDocuments/Universal_Service.pdf

¹⁸ Grameenphone is a joint venture enterprise between Norway’s Telenor (62%) and Grameen Telecom Corporation (38%), a not-for-profit subsidiary of Grameen Bank, a micro-credit pioneer and “internationally reputed bank for the poor”. See [http:// www.grameenphone.com/About Grameenphone/Shareholders](http://www.grameenphone.com/About%20Grameenphone/Shareholders).

¹⁹ Grameenphone was founded by three visionaries: (1) Iqbal Quadir, Muhammad Yunus, founder of the Grameen Bank, and Khalid Shams. See Grameen Telecom’s Village Phone Programme in Rural Bangladesh: A Multi-Media Case Study, Final Report, March 17, 2000, available at <http://www.telecommons.com/villagephone/contents.html>.

The Telecommunication Act 2001 does not provide for the regulator, the Bangladesh Telecommunications Regulatory Commission (BTRC) to establish a universal service project or universal service fund. However, it does provide the BTRC discretion to include a compulsory obligation in the operator's license requiring them to provide the licensed services to rural and sparsely populated areas, although not exceeding ten percent of the licensee's capacity.²⁰ No universal service fund has been established and there is no specific funding mechanism for providing universal service.²¹ Currently, fixed line operators and mobile operators have obligations to provide universal access/service, which is generally done by providing 5 percent of their network capacity to rural areas.²² The result is that telecommunication access to most of the rural areas is mainly being provided not by government mandate but through Grameenphone's Village Phone Program.

The National Telecommunications Policy of 1998 (NTP) states that it is the Bangladesh government's goal to "facilitate universal telephone service throughout the country, and where there is demand, all those value added services such as cellular mobile telephone, paging, data services, access to Internet (including electronic mail), voice mail and video conferencing". Universal service is defined to include services to both urban and rural areas of Bangladesh. Services included in Bangladesh's definition of universal service include both fixed line private residential service and individual mobile cellular services. Under the NTP, universal service obligations for basic telephone services are to be included in the licenses of all network operators.

The BTRC, which began operation January 31, 2002, had the following mission:

- Increase the teledensity to at least 10 telephones per 100 inhabitants by 2010;
- Establish a phone in every village by 2006;
- Promote ICT applications to support socio economic development;
- Create an enabling environment and customer choice for ICT services;
- Encourage joint Public-Private cooperation in ICT development; and
- Encourage ICT applications which stimulate poverty reduction.

The Village Phone Program, started in 1997, is the initiative of the Grameen Bank, an NGO with an extensive rural banking network and an expert in microfinance programs that assists poor villagers in rural areas by providing loans to them under a micro-credit program for rural income generating activities. To implement the Village Phone Program, the Grameen Bank created an independent not-for-profit subsidiary called Grameen Telecom, which then established a for-profit company, Grameenphone, to fund the Village Program in Bangladesh with the profits it earns as a nationwide cellular mobile telephone provider. Grameen Telecom administers the Village Phone Program with the help of Grameen Bank, trains the operators, supplies them with handsets and handles all service-related issues.²³

The Village Phone Program is able to provide modern digital wireless service to rural areas through Grameenphone's GSM network in Bangladesh. The program provides loans to Grameen Bank members, who are most often female, to purchase a mobile phone under the

²⁰ Bangladesh Telecommunication Act of 2001, Chapter V, par. 37.

²¹ *Id.*

²² *Id.*

²³ Grameenphone website/About Grameenphone/Shareholders/Grameen Telecom Overview, at <http://www.grameenphone.com>.

lease-financing program of Grameen Bank. These villagers then become Village Phone operators and earn money by offering telephone service to other people in their village. Each Village Phone operator is responsible for providing telephone services (sending and receiving calls), collecting call charges according to prescribed rates, remitting payments to Grameen Bank, and ensuring proper maintenance of the telephone. The Village Phone operator's income results from the difference between charges paid by customers and the airtime charges billed to the operator by Grameen Telecom, as well as a flat charge for incoming calls. Grameen Telecom buys airtime in bulk at a discounted rate from Grameenphone, which enables Grameen Telecom to pass on savings to the village operators.²⁴

The initial goal of the Village Phone Program was to install 40,000 village phones by year end 2004. According to Grameenphone's 2006 Annual Report, there were over 280,000 village phone operators by year end 2006 and 300,000 operators as of May 2007.²⁵

According to data from the International Telecommunication Union (ITU) ICT Eye Survey on Universal Service, the total telephone subscriber per 100 inhabitants in 2007 in Bangladesh was 22.41, of which 0.75 were fixed telephone line subscribers and 21.66 (or 96.7 percent of total telephone subscribers) were mobile cellular subscribers.²⁶ This low fixed line penetration rate is partly due to the fact that the state-owned Bangladesh Telegraph and Telephone Board (BTTB) had a monopoly in the telecommunications sector until 2004 and failed to increase its subscriber base because of capacity constraints, inadequate investments, and corruption within the state system.²⁷ The majority of villages across Bangladesh still do not have access to a landline²⁸ and where access has been fulfilled, it is provided by mobile phone networks.

Grameenphone obtained a national mobile operator license in November 1996, and commenced operation in March 26, 1997. It is currently the largest telecommunications services provider in Bangladesh, with a subscriber base of 19.58 million (out of a total of 42.04 million mobile subscribers) as of May 2008.²⁹ In comparison, the number of PSTN phone subscribers in May 2008 was only 1.26 million. Since it began operations in 1997, Grameenphone has also built the largest cellular network in Bangladesh, installing over 10,600 base stations in more than 6100 locations, bringing nearly 98 percent of the country's population under its network coverage area.³⁰

²⁴ Grameen Telecom's Village Phone Program in Rural Bangladesh: A Multi-Media Case Study, Final Report (Mar. 17, 2000), available at <http://www.telecommons.com/villagephone/finalreport.pdf>. See also Grameen Telecom information at <http://www.grameen-info.org/grameen/gtelecom/index.html>.

²⁵ Grameen Foundation, Village Phone Direct Manual: Enabling Microfinance Institutions to bring Affordable Communications to the Poor (2007).

²⁶ *Universal Service Profile, Bangladesh* (2004), accessible at <http://www.itu.int/ITU-D/ICTEYE/Regulators/Regulators.aspx#> under "Country Reports".

²⁷ M. Iqbal Ahmed and Erin C. Lentz, Enhancing the Livelihoods of the Rural Poor: The Role of Information and Communication Technology (Feb. 2007) at pp.8-9.

²⁸ *Id.* at p. 9.

²⁹ Bangladesh Telecommunication Regulatory Commission website data, Mobile Phone Subscribers (May 2008).

³⁰ Grameenphone website at <http://www.grameenphone.com>, "CEO Announces Q1 results, talks about new brand campaign", Press Release (April 2008).

Apart from Grameenphone, other private operators such as Peoples Telecommunication and Information Services (PeoplesTel) and Integrated Services Limited (ISL) were also given licenses to provide fixed line PSTN services to rural areas in Bangladesh.³¹

The initiatives of private companies like Grameenphone and Grameen Telecom's Village Phone Program in Bangladesh demonstrate the possibility of successfully extending universal service and access to remote rural villages by means other than a universal service fund.

Furthermore, the Bangladesh Village Phone Program is also an example of the emergence of mobile technology as the dominant and preferred method to providing universal service/access, particularly in developing countries where mobile penetration rates are higher than fixed line penetration rates.³²

2.6 Funding of Universal Access and Service

2.6.1 Financing of Universal Access/Service

Key questions to be addressed in relation to the financing of UAS include

- *Does the law establish some sort of financial mechanism to support provision of UAS?*
- *Does the law provide that funding or subsidies provided must be targeted and determined and delivered in a manner that is transparent, non-discriminatory, inexpensive, and competitively neutral?*
- *Does the law establish an explicit funding arrangement for UAS or does it assume implicit (hidden) funding through fees and other indirect sources?*
- *Are there monies taken from a general government budget to support Universal Access/Service goals?*
- *Is there rate setting above cost to provide some mechanism of "support"? If so, which services have above-cost rates? Which services or infrastructure receives the support from these above-cost revenues?*
- *Are there other sources of implicit funding such as inter-carrier compensation fees? If so, which services or infrastructure receives the support from these implicit subsidies?*
- *Where government decides to fund operators through UAS programmes, are the subsidies 'smart subsidies' meaning that they are used to encourage operators to enter the market and not to create an unending dependency on subsidy?*

³¹ PeoplesTel was previously Bangladesh Rural Telecom Authority (BRTA) and ISL is the successor of Sheba Telecom's rural telecommunication license.

³² GSM Association Report, Universal Access: How Mobile can Bring Communications to All, at http://www.gsmworld.com/documents/universal_access_full_report.pdf

The financing of Universal Access and Service has gone through various stages, ranging from the application of revenues from cross-subsidies to finance non-profitable areas under a monopolistic scenario, to the creation of Universal Service Funds funded solely from operator levies so as to be able to finance universality projects in a competitive market. Obviously, there are a range of other solutions between these two solutions. Important is that countries do not focus solely on the creation of a Universal Service Fund and that they do not see it as the only way in which universality will be achieved, but that such Funds are seen as a tool amongst tools, and that in order to achieve universality, a variety of tools (as described throughout this document) are needed. Other public finance mechanisms such as loan guarantees and public private partnerships (PPPs) to enhance and target investments into priority areas in need of special finance may be applied and achieve universality more effectively.

Recently, such alternatives to Universal Service Funds have gained momentum around the world. Thus, for example, in September 2009, the European Commission adopted Guidelines on the application of EC Treaty state aid rules to the public funding of broadband networks. The Guidelines provide a clear and predictable framework for stakeholders and will help Member States to accelerate and extend broadband deployment by outlining the rules and conditions on how public funding could be provided to build broadband networks in line with the EU state aid rule. The Guidelines also contain specific provisions concerning the deployment of Next Generation Access networks, allowing public support to foster investment in this strategic sector without creating undue distortions of competition³³.

The main aim of the Guidelines is to facilitate a rapid deployment of such networks in Europe by providing to all stakeholders (including local and regional authorities, as well as network operators) a clear, predictable and comprehensive framework for the public financing of such networks. In particular, the Guidelines explain how public funds can be channelled for the deployment of basic broadband networks as well as Next Generation Access ("NGA") networks to areas where private operators do not invest. The Guidelines outline the distinction between competitive areas ("black" areas), where no state aid is necessary and unprofitable or underserved areas ("white" and "grey" areas) in which state aid may be justified, if certain conditions are met. This distinction is then adapted to the situation of NGA networks (whose deployment is still at an early stage) by requiring Member States to take into account not only existing NGA infrastructures but also concrete investment plans by telecom operators to deploy such networks in the near future. A number of crucial safeguards (such as detailed mapping, open tender, open access obligation or technological neutrality and claw-back mechanisms) are laid down in the Guidelines in order to promote competition and avoid the 'crowding out' of private investment.

The Commission provided that although investments for high speed and very high speed broadband networks should primarily be driven by private operators, state aid can play a crucial role to extend broadband coverage in areas where market operators have no plans to invest. The primary objective of the Broadband Guidelines is to foster a wide and rapid roll-out of broadband networks while at the same time preserving the market dynamics and competition in a sector that is fully liberalised. The Guidelines also ensure specify that whenever state aid is

³³ European Commission Rapid Press Release of 17/09/2009: "State aid: Commission adopts Guidelines for broadband networks", Reference: IP/09/1332, available at: <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/1332&format=HTML&aged=0&language=EN&guiLanguage=en>

granted to private operators, the aid must foster competition by requiring the beneficiary to prove open access to the publicly funded network for third party operators³⁴.

2.6.2 Universal Access/Service Funds

Key questions to be addressed in relation to the establishment of UAS Funds include

- *Does the law clearly provide for the establishment of a fund?*
- *Does the law clearly identify who is responsible for the management and operation of the fund and ensure the independence of this entity through clear regulatory provisions?*
- *Does the law provide that all licensed entities must contribute to the fund?*
- *Does the law provide that the percentage, flat fee or other formula used to calculate an operator's contribution to the fund is clearly defined in the Law and is applied in a non-discriminatory manner to all similarly-situated service providers?*
- *Are fees not excessive and assessed on revenues from telecommunications services?*
- *Are payments into the fund on an annual or quarterly basis?*
- *Are operators required to file revenue reports that the fund manager uses to calculate contributions on an annual basis?*
- *Are there other reporting requirements for operators?*

A further mechanism used to help achieve the goal of universal access/service is the creation of universal service funds. These funds are being used increasingly in competitive markets to supplement market-based policies, and address access gaps and market failures in remote and under-served locations. However, there are some legitimate and understandable concerns regarding UASFs, fuelled mostly by a few unfortunate examples. Also, there have been concerns raised over the complexity of establishing and managing a UASF. Negotiating fair UAS contributions for all operators, which are equitable between all and accepted as fair, is not necessarily an easy feat.

Brazil is an example of a country which has struggled with its Fund. Although established in August 2000, the FUST has been unable to achieve its goals. FUST was first established with the purpose of creating a financial resource that could complement the deployment of universal obligations of the fixed line operators, but in reality the cost of expanding services is being borne directly by the operators. FUST's most critical challenge is that it is not technologically neutral. It favors fixed service operators over other telecommunications providers as the funds can only be applied towards fixed service projects. However, all telecommunications service providers are required to contribute thus indicating favoritism of one service over another. Acknowledging that this is not the best approach for a funding mechanism, the Ministry of Communications, in its recent public consultation on Reforming the Brazilian Telecommunications Framework, called attention to this fact and proposed that the FUST should be, at the very least,

³⁴ Commission Press Release IP/09/1332, State aid: Commission adopts Guidelines for broadband networks, 17 September 2009, available at: <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/1332&format=HTML&aged=0&language=EN&guiLanguage=en>

technologically neutral in its distribution mechanism. In addition, the Ministry is also considering a variety of other ways to distribute funds and to determine appropriate projects. As operators have continued to build out their networks according to their roll-out obligations, the government has collected a significant amount of FUST funds, but has only implemented one project and has no clear strategy on how to use the rest of the funds, which amount to seven billion Reais (US\$ 4.31 billion).

Mechanisms need to be put in place to make universal service funds accessible to a wider range of telecommunications service providers. Limiting access of funds only to a specific category of licensee or to licensed operators, for example, can create barriers that continue to support existing conditions (i.e., the expansion of wireline networks to provide universal service/access) and discourage the implementation of new technologies to provide service in unserved or underserved areas. In Peru, telecommunications services providers with concession contracts for final public services (fixed line, including pay phones, and mobile) and value added services (data services including broadband Internet access) can access FITELE funds. If the entity/company requesting the funds does not have a concession contract for the area for which it is requesting the funds, the entity/company needs to request the appropriate expansion of the concession contract from the Ministry of Transportation and Communications.³⁵ Letting a variety of entities have access to universal service funds allows countries to benefit from a greater number of possible resources to help it achieve its universal service goals. In addition, these resources can sometimes provide innovative solutions for small-scale projects that would not normally be considered profitable.

In addition, the development and presentation of project proposals for universal service funds consideration should not be restricted only to the fund authority or to telecommunications providers, but instead should be open to all entities with an interest in contributing to the fulfilment of universal service/access. In Chile, project proposals can be presented by telecommunications service providers, regional/provincial/municipal authorities, universities, non-governmental organisations (NGOs), neighbourhood communities and others. SUBTEL, the entity responsible for administering and managing the country's universal service fund, uses these project proposals to design and develop the fund's annual project agenda.³⁶ A system where multiple parties can submit project proposals allows all interested parties to contribute in achieving universal service obligation objectives. Having multiple sources for project proposals can provide a more realistic vision of the needs and conditions of the market, such as what type of service is required by localities and which technology is best suited, and are more likely to result in creative and resourceful project solutions.

The Universal Service Fund should not only support a country's present universal service objectives, but also be able to adapt to the demands and trends of a converging telecommunications sector by fostering the use of new and innovative technologies to achieve future universal service obligation goals. The advantages and benefits of wireless technologies require that countries reconsider their universal service obligation objectives and establish

³⁵ OSIPTEL Board of Directors Resolution # 025-2005-CD/OSIPTEL, May 2005.

³⁶ SUBTEL decree approving the Guidelines for the Telecommunications Development Fund (Fondo de Desarrollo de las Telecomunicaciones), December 28, 2001.

universal service fund disbursement mechanisms that will support the implementation of new technologies to serve rural populations.

In order to encourage the use of new technologies in achieving universal service/access, countries first have to revise present universal service fund objectives. Given the importance mobile technologies are playing today in providing affordable access to previously unserved or underserved areas and the increasing usage of other new technologies in similar efforts, universal service funds should consider integrating and supporting the application and deployment of new technologies to meet universal service obligation requirements. In Colombia, South Africa and Uganda, mobile payphones and public access businesses have already been used to fulfil regulatory obligations or to meet universal service fund competition requirements.³⁷ Because wireless technologies can usually be deployed faster and more affordably, incorporating them into universal service fund programs can provide countries with the means necessary to meet universal service obligation priorities more efficiently and effectively.

To ensure the smooth incorporation of new technologies into universal service fund programs, and guarantee the equal participation of all telecommunications sector participants, countries also need to make certain that the purpose of the universal service fund and the role of the universal service provider is well-defined. When Peru's FITEC fund was established, it was determined that the fund would provide populations in rural areas and localities considered of "preferred" social interest with greater access to telecommunications services. In addition, the fund's administration and management regulations stipulated that FITEC would not finance past or future network expansion obligations imposed on telecommunications operators by the government. Thus, the incumbent operator was excluded from accessing FITEC funds to finance its rollout obligations.³⁸ In Uganda, RCDF funds are only used to improve and service rural areas. In addition, "serve or lose" clauses have been included in main operator licences with regards to rural areas motivating main operators to effectively comply with universal service obligation, but also providing new market entrants with an opportunity to provide those services if the main operator fails to do so.³⁹ In India, the universal service fund is currently facing problems because, aside from being eligible for universal service funds, the incumbent operator receives Access Deficit Charge (ADC) revenues (that have been reduced from 30 to 10 percent, but that come from the country's universal service fund) to cover its deficit for providing fixed lines in rural and urban areas. This gives the incumbent operator a "favoured" position in comparison to other telecommunications service providers that have access to the fund.

³⁷ Universal Access and Universal Service Funds: Insights and Experience of International Best Practice, Intelcon, July 2005.

³⁸ OSIPTEL Resolution No. 48-2000-CD/OSIPTEL approving Regulations for the Administration and Management of the Fondo de Inversion de Telecomunicaciones (FITEC), October 2000; and Aprueban Normas Complementarias al Reglamento de Administracion y Funcionamiento de FITEC y su Exposicion de Motivos, OSIPTEL Resolucion de Consejo Directivo No. 025-2005-CD/OSIPTEL, May 2005

³⁹ The Challenge of Universal Access – African Solutions for Africa, Country Case: Universal Access in Uganda, Patrick F. Masambu, March 1-4, 2005.

Telecommunication Development Sector

Study Groups



**Fourth Meeting of ITU-D Study Group 1
Geneva, 7-11 September 2009**

**Document 1/251-E
21 July 2009**

Original: English

For action

Question 10-2/1: Regulation for licensing and authorization of converging services

SOURCE: Rapporteur for Question 10-2/1

TITLE: Draft Final Report on Question 10-2/1: Regulatory trends for adapting licensing frameworks to a converged environment

Action requested:

The Rapporteur for ITU-D Question 10-2/1 submits this contribution for consideration of the Rapporteur's Group for ITU-D Question 10-2/1 during the Study Group 1 meeting in September 2009.

Abstract:

This contribution is submitted as the draft final Report on Question 10-2/1. It is substantially based on input contributions to the Rapporteur's Group for Question 10-2/1, as well as ITU-D SG 1 Document 1/123 and licensing information extracted from the ITU World Telecommunication Regulatory Database. The guidelines and principles were developed and agreed to during the Rapporteur Group meeting in March/April 2009.

1. Introduction

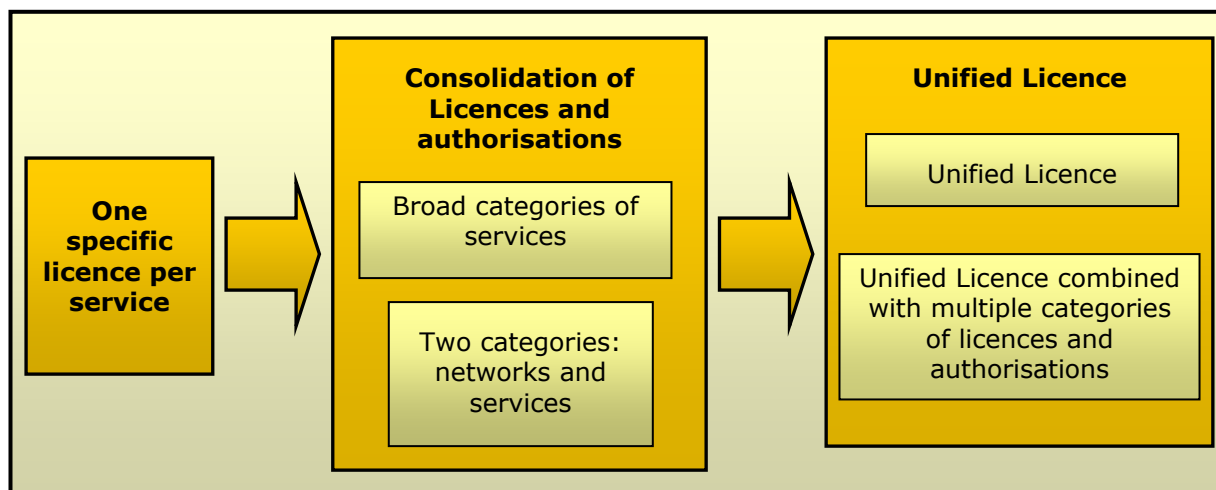
With the advent of convergence in telecommunications and broadcasting markets, diverse countries have been modifying their telecommunications regulations to support the development of convergent services and the expansion of markets and competition, with the objective of promoting the provision of new and innovative services, the reduction of prices and an increase of efficiency in the provision of services, as well as increasing the variety of offerings for subscribers.¹

Traditional regulatory systems focused primarily on the specific means of telecommunications or on the specific service provided by the operator. Regulatory frameworks were often based on wireline, wireless or broadcasting services or were divided into local and long distance markets. Now with converged networks, such distinctions are no longer practical. Therefore, reforms directed at adapting traditional regulatory systems to convergence have consistently focused on two key elements: the introduction of the principles of technology and service neutrality, and the establishment of greater flexibility in key aspects of their existing regulatory frameworks.

These reforms have followed similar tendencies around the world which have had great impact on diverse aspects of telecommunications regulation, but above all on service licensing and the rights and obligations of providers, including interconnection, numbering and universal service, and spectrum use.

Service licensing reform towards convergence has followed two main trends that have been implemented both separately and jointly. The first consists of simplification of licences that traditionally have been established for individual services, which would generally mean that a single telecommunications operator would have to hold as many licences as the different services it provided. Simplification involves the consolidation of different services in a generic categorisation or the unification of all services under a single licence or concession, what is often called a unified licence.

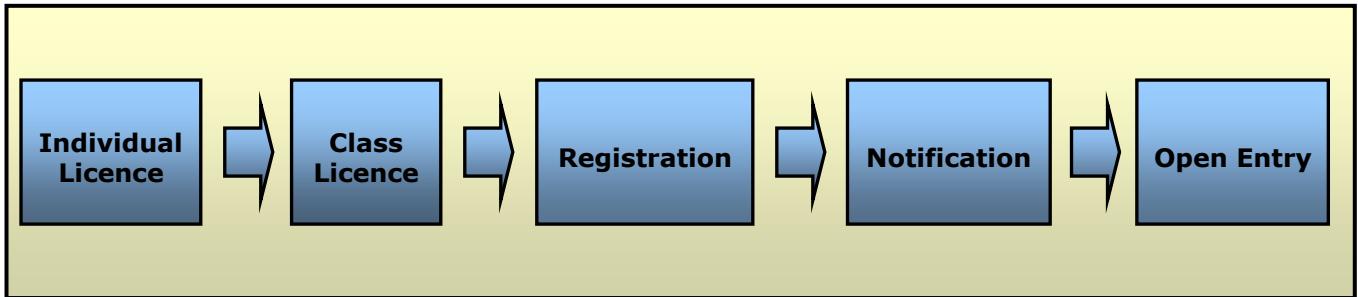
Figure 1: Simplification of Licences²



The second has consisted of the reduction or elimination of the administrative and formal requirements to enter the market and provide a service. This trend involves modifying the general authorisation category to allow more services to be provided or the establishment of notification or registration systems that replace licences or general authorisations altogether, therefore simplifying the process of obtaining them and, in some cases, making it automatic. Finally, some countries have opted for deregulation of services, which comprises the elimination of licences or concessions and even of the need to notify or register with the regulator.

¹ For more information, see *infoDev/ITU, ICT Regulatory Toolkit, Module 6, Legal and Institutional Aspects of Regulation, Chapter 4 Impact of Convergence* (2006), available at <http://www.ictregulationtoolkit.org/en/Section.1254.html>. See also, Mindel De La Torre and Sofie Maddens, "Transitioning Regulation From Old to New" in the ITU's *Trends in Telecommunications Reform 2004/2005: Licensing in an Era of Convergence* (December 2004).

² Document 1/123, *Regulatory trends for adapting licensing frameworks to a converged environment*, 11 September 2007.

Figure 2: Models for Reduction of Administrative Requirements³

Usually, both trends are combined in order to achieve greater simplification and flexibility. It is important to note that any modification must be managed to minimise inconsistencies between new and existing rules. Also, licensing reforms are most effective in addressing the challenge of convergence if the guiding principles of technology neutrality and flexibility are applied to the rights and obligations of the telecommunications operators as well as to the other essential elements of the regulatory framework, including, interconnection, numbering, universal service, and spectrum use.

The increasing implementation of converged licensing frameworks has been a recognition of two key trends, as noted by the GSM Association: convergence is enabling disparate technologies (including fixed, cable and mobile) to offer competing services, and the increase in competition has been shown to deliver such services at a lower cost and higher quality, as well as encouraging introduction of new services.⁴

2. Approaches to Authorisations

In light of the regulatory issues that flow from convergence and the transition to a next generation network (NGN) environment, regulators have begun to adapt the traditional, service-specific approach to authorisations.⁵ There are now three broad approaches to authorisations in the information and communications technology (ICT) sector:

- **Service-specific authorisations:** these authorisations allow the licensee to provide a specific type of service. Usually, the licensee is required to use a specific type of network and technological infrastructure. However, some service specific authorisation regimes are technology neutral (e.g., the fixed and mobile services authorisation regime in Saudi Arabia and the Canadian basic international telecommunications services licences). These types of authorisations are sometimes issued as individual licences (particularly in developing and transitional economies) and sometimes issued as general authorisations.
- **Unified (or global) authorisations:** these authorisations are technology- and service- neutral. They allow licensees to provide all forms of services under the umbrella of a single authorisation, using any type of communications infrastructure and technology capable of delivering the desired service. In most countries, unified authorisations are issued as individual licences. However, in some countries, the process for issuing the unified authorisation blends aspects of general authorisation processes and competitive licensing regimes. These hybrid processes can best be described as non-competitive individual licensing processes: while applicants do not compete for a limited number of authorisations, they must meet a variety of criteria to qualify for a licence and their applications are subject to close regulatory scrutiny.
- **Multi-service authorisations:** these authorisations allow service providers to offer multiple services under the umbrella of a single authorisation, using any type of communications infrastructure and technology capable of delivering the services in question. Like unified authorisations, multi-service authorisations are technology neutral. However, multi-service authorisations are more limited than unified authorisations; licensees are permitted to provide any of a designated set of services, but not any and all services. Multi-service authorisations are sometimes issued as general authorisations and, in other cases, are issued as individual licences. It is not uncommon for a country to have both

³ Document 1/123, *Regulatory trends for adapting licensing frameworks to a converged environment*, 11 September 2007.

⁴ Document RGQ10-2/1/008, 10 December 2007.

⁵ Document 1/178, *Licensing practices in a converging ICT environment*, 28 August 2008.

general authorisation regimes and individual licence regimes for their multi-service authorisations. Individual multi-service authorisations are often issued using a non-competitive individual licensing process.

3. Overview of Legislative Frameworks

3.1 Simplification of Licences

3.1.1 Consolidation of Licences

The consolidation of licences involves the reclassification of existing telecommunications services into different categories based on technology neutrality. As a result, the number of licences is reduced and the services included in each expanded. This has been the option followed by many countries, including Malaysia, Tanzania, Uganda, and Singapore.

In Malaysia, the previous regulatory system recognised a total of 31 different licences based on networks and services, such as operators of international and national networks, mobile communications, trunking, Internet service providers, value-added services, broadcasting, etc. To adapt its licence regime to convergence, Malaysia reduced these 31 licences into the following four technology neutral categories:⁶

- Network facilities provider includes all network infrastructure operators of any nature (satellite earth station systems, fibre optics, mobile communications systems base stations, etc.)
- Network services provider covers those that provide basic connectivity and broadband to support applications. These licences allow connectivity and backhaul among different networks.
- Application service provider is assigned to those operators that provide functions such as voice, data, content and electronic commerce services, among others. Generally, applications services are understood as the functionalities and capabilities offered to the end users.
- Content application service provider includes the traditional broadcast services (radio and television) and new services such as information services.

Within these four categories, two types of licences exist: individual licences are granted for activities with a high degree of regulation (e.g., the need to grant rights of use for spectrum) and registration, which is renewed yearly and recorded in the registry administered by the Communications and Multimedia Commission of Malaysia. Furthermore, lesser activities within each category are exempt from the requirement of obtaining a licence.

As in Malaysia, Tanzania also simplified its licence regime with the introduction of the Converged Licensing Framework (CFL) in February 2005. The CFL includes the same four categories of licences as those established in Malaysia, namely, Network Facility Licence, Network Service Licence, Application Service Licence and Content Service Licence.⁷

Uganda has also developed a new streamlined technology-neutral licensing regime that was implemented in January 2007. Under the regime, there are three categories of licences: (i) public service provider licence; (ii) capacity provider licence; (iii) infrastructure provider licence; and (iv) general authorisation (Chart 1).

⁶ See *Malaysia Communications and Multimedia Act 1998*, available at: http://www.mcmc.gov.my/mcmc/the_law/ViewAct.asp?cc=31478525&lg=e&arid=900722.

⁷ For further details of the CFL, see the contribution of Tanzania to this Question 10-2/1, *Tanzania's Experience in Licensing of Communication Operators under Converged Licensing Framework*, Document RPGQ10-2/1/006-E (May 31, 2007).

Chart 1: Uganda's new licensing regime⁸

Type of Licence	Services Covered Under Licence
Public Service Provider Licence	Category 1: Public Voice and Data - Cellular, Fixed voice, GMPCS, Internet access (including IP telephony + Virtual Private Networks), Internet exchange services, Virtual Private Networks (VPNs) that are not provided over the Internet Category 2: Capacity Resale - Local and international capacity resale, calling cards
Capacity Provider Licence	Category 1: Licensees already permitted to install infrastructure of the type they have already invested in, for example Internet Access Providers with wireless networks Category 2: Persons whose core business is not in telecommunications but who possess private communications facilities with surplus capacity and wish to resale this to third parties Category 3: New entrants in the Internet Access market operating their networks using the Industrial, Scientific and Medical frequency (ISM) band, e.g., 2.4 GHz and 5.7 GHz bands
Infrastructure Provider Licence	Public Infrastructure Provider Private Network Infrastructure
General Authorisation	Category 1: Public Pay Communication Services (e.g., Internet Cafés, Payphones, telephone bureaus, etc.) Category 2: Private Networks

Finally, in Singapore, the simplified licensing system is composed of only two types of licences:

- Facilities-based operator (FBO) and
- Service-based operator (SBO).

The first is awarded to those telecommunications services providers that deploy their own infrastructure, such as operators of fixed and mobile telephone networks, trunking, etc. The second type is awarded to those operators that provide services over a third party's infrastructure, as for example, resellers of services, providers of virtual private networks, Internet access, etc. While the FBO always takes the form of an individual licence, the SBO may be awarded via an individual licence or general authorisation or notification, depending on the service.

Other countries, such as India or Kenya, have also adopted proposed simplification plans and reductions in the number of service licences as a stepping stone to a unified licence system, as addressed in the following section.

3.1.2 Unified Licence

A second trend consists of introducing a unified licence system, in which a single licence is created that covers an extensive range of services, although definitions vary by country. This trend has been adopted, or is being adopted, with certain variations, in many countries, including Argentina, Botswana, EU member states, Hong Kong China, India, Jordan, Kenya, Nigeria, Peru, Trinidad and Tobago, and Uganda.⁹

In this regard, in 2000, Argentina introduced a unified licence that authorises the provision, to the public, of all telecommunications services, whether fixed or mobile, wireline or wireless, national or international,

⁸ See UCC, Communications Licensing Application Guidelines, available at www.ucc.co.ug/licensing/default.php.

⁹ Document 1/178, *Licensing practices in a converging ICT environment*, 28 August 2008. Tanzania has been included in the previous category as the system that has been adopted is one of consolidation of licences.

with or without infrastructure.¹⁰ If spectrum is required for provision of service, the corresponding authorisation and/or permit must be obtained as well.

In the European Union, the new regulatory framework¹¹ created a system similar to that of a unified licence, although refined by means of simple notification, which eliminated the division of the different licences by networks and services. The unified licence only requires a prior notification, as further addressed in the following section. The unified licence also allows the provision of any kind of telecommunications service and the deployment and operation of any telecommunications networks. Similar to Argentina, the assignment of spectrum rights requires a specific permit independent of the single licence.

The Telecommunications Regulatory Authority of India (TRAI) has proposed the adoption of a hierarchical unified licence regime that can be represented as an inverted pyramid, in which the major licence comprises all the services, while the minor licences cover a smaller number of services.¹² It should be noted that under the TRAI proposal, broadcasting services are to be offered through a stand alone or autonomous licence. The proposed system includes the following classification of licences:

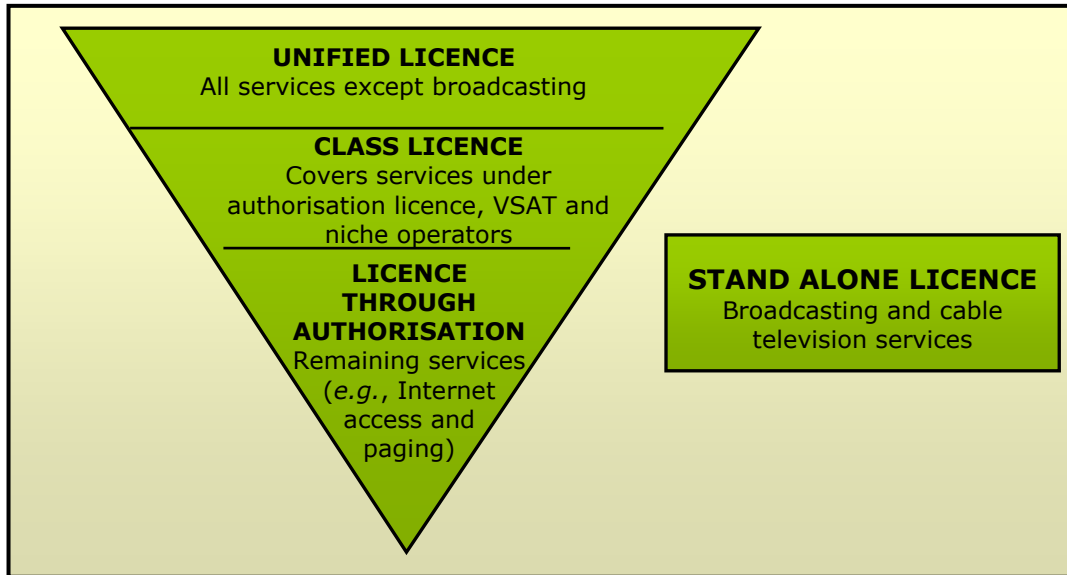
- Unified (Single) licence
- Class Licence
- Licence by authorisation
- Stand alone licence for broadcasting and cable television services

The unified (single) licence allows for the provision of all the telecommunications services, including those authorised services through the remaining categories of licences (class licence and licence by authorisation). The class licence covers the services granted under the licence by authorisation, VSAT services and niche services (services in rural zones with teledensity lower than one percent). The licence by authorisation includes the remaining services, among them, Internet access and paging. Finally, for the case of the broadcasting and cable television services, the licence system requires a stand alone licence.

¹⁰ Telecommunication being defined as any transmission, emission or reception of signs, signals, writings, images, sounds or information of any nature, by wire, radio electricity, optical mediums and/or any other electromagnetic systems. Article 3 and Article 5.1 of the Telecommunications Services Licence Regulations. This definition is almost the same as the ITU definition of telecommunication.

¹¹ Official Journal of the European Communities, *Directive 2002/21/EC of the European Parliament and of the Council of March 7, 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)*, available at http://ec.europa.eu/information_society/topics/telecoms/regulatory/new_rf/index_en.htm#reg.

¹² According to TRAI's "Consultation Paper on Licensing Issues relating to Next Generation Networks" issued on January 27, 2009, the government has not accepted TRAI's recommendations for the unified licensing regime. (Consultation is available at <http://www.trai.gov.in/WriteReadData/trai/upload/ConsultationPapers/163/cpaper27jan09no3.pdf>). As of Mar. 24, 2009, TRAI has posted the "Comments of Stakeholders received on Consultation Paper on Licensing Issues related to Next Generation Networks (NGN)" (available at http://www.trai.gov.in/ConsultationPapers_content.asp).

Figure 3: Hierarchical system of unified licence proposed in India¹³

The Nigerian Communications Commission (NCC) in March 2006 introduced a unified licensing regime covering several telecommunications services. The licence is issued as an individual licence under Nigeria's communications law.¹⁴ Specifically, Nigeria's Unified Access Service Licence covers fixed telephony (wired or wireless), digital mobile services, international gateway services, national long distance services, and regional long distance services. The NCC also set criteria which existing licensees must meet in order to transition to a unified licence.¹⁵

3.2 Reduction and elimination of administrative and formal requirements for obtaining licences

As previously explained, the second trend followed for adapting licensing regimes to convergence consists of the reduction or elimination of the formal and administrative requirements for the provision of services. This trend follows various stages, from enhancing the scope of general authorisations or implementing a notification or registration system to the deregulation of services. The registration or notification system replaces the process of granting licences or general authorisations, making the process for obtaining licences simpler and, in some cases, automatic, while the deregulation of services eliminates the requirement of obtaining a prior licence or concession. Each of these stages has the following characteristics.

Individual licences include the specific conditions of the service, specifying the rights and obligations of the licensed service. In addition, each individual licence is approved on a case by case basis for a particular service and licensee. General authorisations, however, establish a general system of rights and obligations that applies to all the operators by means of the same authorisation, and the process of awarding them is more straightforward, not requiring an exhaustive examination of the request as in the case of the individual licence.

The registration system implies a step beyond the authorisation, where general service conditions are applied to operators that only require the registration of their request to provide the service. The analysis and approval of the operator's request is minimised to almost a mere formality.

Finally, notification is the last step prior to deregulation of the service. In this stage, an operator does not even have to wait for the administrative agency's approval to provide service, being free to provide the

¹³ See TRAI *Recommendations on Unified Licensing* (January 13, 2005), available at <http://www.trai.gov.in/trai/upload/Recommendations/13/recom13jan05.pdf>. See also, Document 1/123, *Regulatory trends for adapting licensing frameworks to a converged environment*, 11 September 2007.

¹⁴ Nigerian Communications Act of 2003, available at <http://www.ncc.gov.ng/index4.htm>.

¹⁵ See Nigerian Communications Commission, *Licensing Framework for Unified Access Service in Nigeria*, <http://www.ncc.gov.ng/RegulatorFramework/unifiedLicensingFramework.htm>.

service as soon as the notification has been filed. The service terms and conditions are also of general application.

As detailed above, the majority of the simplification and unified licence systems limit the individual licence to specific services often including use of spectrum, and expand the services that are granted by means of a general authorisation. In some cases, as in Malaysia and Singapore, some services just require a notification.

In other countries, such as the EU member states, a complete registration and notification regime has been established for the provision of telecommunications services. In the European Union, the provision of electronic communications services as well as the deployment or operation of networks is subject to a notification to the corresponding national regulation authority under a general authorisation regime. General authorisations for the provision of electronic communications networks or services replaced individual licences in 2002.¹⁶ Although an entity may be required to submit a notification, a national regulator may not require an entity to obtain explicit approval prior to beginning operations. However, there continues to be a special scheme for issuing rights to frequencies, numbers and other scarce resources as well as provisions for the designation of certain universal service functions.

Finally, there are countries that have effectively eliminated authorisations as well as notifications and registrations for the provision of certain services, arguing that such services are beyond the regulator's scope of jurisdiction or, merely, based on an explicit decision of the regulator exercising its discretion not to regulate a specific service. In general, this is the approach followed in the United States with regard to Internet access, which has been classified by the FCC as an information service not regulated under the Communications Act, with the purpose of promoting the continuous development of the Internet.¹⁷

4. Evaluation of Telecommunications and Competition Regulator Experiences

4.1 Experiences with converged licensing

According to the survey responses incorporated into the ITU World Telecommunication Regulatory Database, in addition to the cases noted above, 11 countries have introduced unified licensing for at least some services: Botswana, Bhutan, Egypt, Equatorial Guinea, Latvia, Maldives, Mali, Mauritania, Namibia, Senegal and Slovenia. In addition, 81 respondents reported use of individual licences, 28 reported use of general authorisations or class licences, and ten allow some services to operate on a licence-exempt basis. These categories are not mutually exclusive; regulators may use a mix of different licensing methods depending on the service and the relevant legal framework. Further, as noted above, definitions of unified licensing vary among countries.

The following sections highlight the experiences reported by telecommunications and competition regulators with respect to licensing frameworks for converged services.

4.1.1 Democratic Republic of Congo¹⁸

In the Democratic Republic of the Congo (DRC), licensees have the right to use the technologies and equipment of their choice to provide telecommunication services. This principle serves to make the licensing system flexible so as to be able to adapt to rapid technological change in the sector.

With regard to next-generation networks, the current law makes no mention of licensing for converging services. In practice, however, convergence is being accommodated de facto in the licensing process, through the granting of WiMAX and 3G licences, which is currently underway. Indeed, the current philosophy is based on service convergence (telephony, Internet, data, multimedia, etc.), moving from

¹⁶ Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) and Directive 2002/20/CE of March 7, 2002, on network and electronic communications services authorisation (Authorisation Directive).

¹⁷ 47 U.S.C. § 230 (b). Also see, with regards to cable modem and wireline broadband services: (i) *In Re Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities and Internet Over Cable Declaratory, and Appropriate Regulatory Treatment for Broadband Access to the Internet Over Cable Facilities*, and *Appropriate Framework for Broadband Access to the Internet Over Cable Facilities*, Declaratory Ruling and Notice of Proposed Rulemaking (NPRM), GN Docket No. 00-185, and CS Docket No. 02-52 (FCC released March 15, 2002); and (ii) *In Re Appropriate Framework for Broadband Access to the Internet Over Wireline Facilities; Universal Service Obligations of Broadband Providers; and associated dockets*, Report and Order and NPRM, CC Docket No. 02-33, CC Docket No. 01-337 et al. (FCC released September 23, 2005).

¹⁸ Document RGQ 10-2/1/020, 2 March 2009.

triple-play to quadruple-play in a single offering with a single customer connection, thus tending towards a unified market.

DRC has granted two WiMAX licences on the basis of the principle of a negotiated contract, in the absence of a formal procedure. A draft for the sale of the 3G licence had already been initiated through a public consultation for which a number of operators had already expressed their interest.

Regarding the procedure for granting this type of licence, the regulator is considering a regulated procedure based on either a call for bids or an auction, or possibly a beauty contest.

At the government level, a draft national ICT policy document is under development that will pave the way for setting target indicators and objectives that may serve as a basis for the licensing of converging services. Not all these steps have been able to be completed as yet, on account of a number of difficulties encountered, such as lack of an overall government policy.

4.1.2 Republic of Guinea¹⁹

In 2005, the Republic of Guinea adopted several new communications and radiocommunications regulations that sought to liberalise the ICT sector and promote the development of advanced and convergent technologies.²⁰ The Ministère des Télécommunications et des Nouvelles Technologies de l'Information (MCNTI) reformed the communications framework to favour convergence by establishing a regime of licences and authorisations. The telecommunications law established a licensing regime of four categories:

- Licences;
- Authorisations;
- Declarations; and
- Unregulated services.

Under the law, licences must be obtained for the:

- Establishment and/or operation of public telecommunications networks or services;
- Establishment and operation of independent networks using the public domain (rights of way over public land) and utilising radiocommunications systems; and
- Provision of Internet access.

The MCNTI issues licences upon the recommendation of the Autorité de Régulation des Posts et Telecom (ARPT). The general conditions in the licences provide the licensees' rights and obligations and are uniformly applied to all licensees in the same network or service category to ensure equitable treatment of all operators. The operators are required to uphold the principles and rules, including those regarding non-discrimination, confidentiality and technology neutrality and non-interference with others' networks and services. Dominant operators have further obligations including contribution to universal access and provision of free-of-charge emergency call services.

There are currently five telecommunications operators in Guinea – Sotelgui, Areeba, Intercel, Orange and Cellcom – as well as a dozen Internet access providers. The government plans to reduce poverty and meet the objectives of the U.N.'s Millennium Project by improving equitable and non-discriminatory access to services by all populations. The government also seeks to reduce the digital divide by increasing penetration rates of the following ICT services:

- NGNs from 0.5% to 25%
- Telephone service from 7.6% to 25%
- Radio coverage from 75% to 95%

¹⁹ Document RGQ10-2/1/023, 19 March 2009.

²⁰ *La loi L/2005/018/AN portant modification des dispositions de la loi L/92/016/CTRN relative à la Réglementation générales des télécommunications; La loi L/2005/019/AN du 08 septembre 2005 portant modification des dispositions de la loi L/95/018/CTRN portant réglementation des radiocommunications en République de Guinée.*

4.1.3 Republic of Korea

The Republic of Korea submitted a case study on mobile voice over IP (VoIP) regulation, presenting information on the current status of regulation and the service and business classifications in use.²¹ Korea uses three business classifications for telecommunications providers: facilities-based telecommunications business (responsible for installation of telecommunications lines), resale business (uses lines provided by facilities-based telecommunications businesses and installs telecommunications facilities within buildings), and value-added communications businesses (leased line telecommunications facilities from facilities-based telecommunications providers). In terms of telecommunications services, Korea uses two classifications: facilities-based telecommunications services and value-added communications services. Facilities-based telecommunications services include telephone and leased line services, wireless services with spectrum allocations, Internet connection services, VoIP and other services. Value-added services include all other telecommunications services.

While VoIP was first introduced as a fixed-line service, technological advances have made it feasible to introduce mobile VoIP (*i.e.*, VoIP over wireless Internet or broadband wireless networks). This development made it incumbent upon Korean regulators to determine how to address the entry of mobile VoIP providers into the existing mobile service market. At the time of Korea's contribution to the Rapporteur's Group, regulators were considering different scenarios for regulation of this converging market.

The Republic of Korea also provided a case study on IPTV and the various barriers to its adoption in Korea, including the regulatory environment.²² In Korea, demand for regulation regarding IPTV differs between telecommunications operators and broadcasters, and between telecommunications regulators and broadcast regulators. Telecommunications regulators and telecommunications operators perceive IPTV as a total service, *e.g.*, a new converged service that is different from existing ones, thereby calling for light regulation. Meanwhile, broadcasting regulators and broadcasters see IPTV as being identical to the existing cable service, citing the scheduled television programs contained in IPTV as evidence of this, thereby calling for the same regulation as that applied to the cable service in accordance with the principle of applying the same regulations to the same services.²³ Moreover, they insist that since a satellite broadcasting provider and digital cable TV operators provide video on demand (VOD) service only after obtaining approval from the broadcasting regulators, a telecommunications operator seeking to offer VOD service should also obtain approval as a broadcasting operator.

With respect to the regulatory agencies involved in a converged environment, Korea's regulatory organisations were somewhat complicated until the establishment of the Korean Broadcasting and Communication Commission (BCC) in February 2008. Prior to the BCC, authority over the broadcasting and communications sectors were shared among ministries and agencies. The Ministry of Internal Affairs and Communication (MIC) and the Korea Communications Commission (KCC) regulated communications while the Ministry of Culture and Tourism was responsible for some broadcasting policies and the right to permit and approve broadcasting business. This unintegrated regulatory environment hindered the development of converged technologies such as IPTV since, structurally speaking, it was very difficult to discuss and reach agreement on the agenda concerning the convergence of telecommunication and broadcasting.

4.1.4 Liechtenstein²⁴

The European Union Telecommunications package of 2002 (Framework Directive, Authorisation Directive, Universal Service Directive, Access Directive, Directive on privacy and electronic communications, Competition Directive and a decision on management of frequency spectrum) was adopted in the Communications Act of 2006 and the relevant national regulations in Liechtenstein.

The objective of the Communications Act is to provide a technology neutral framework for the electronic communication and entire electronic communications networks and services, whether in fixed and mobile

²¹ Document RGQ10-2/1/009, 13 December 2007.

²² Document RGQ10-2/1/010, 13 December 2007.

²³ The telecom sector names IPTV as a broadband convergence service, and the broadcasting sector as a fixed multimedia service.

²⁴ Document RGQ10-2/1/014, 5 January 2008.

communication networks, satellite and broadband networks or terrestrial mobile networks and the services offered.

The innovative changes in the new framework of electronic communications require no licensing regime, and the new services and activities in the electronic communication industry could be offered without a licence, however these must be registered with the national regulatory authority.

4.1.5 Lithuania²⁵

According to the 2002 Law on Telecommunications, licensing of telecommunications activities has been abolished since 1 January 2003. The right to engage in these activities is granted without an individual authorisation, following the requirements laid down in legal acts. According to the General Terms and Conditions for Engaging in Telecommunications Activities, all undertakings intending to engage in the provision of the public fixed telephone network and/or services, the provision of the mobile public telephone network and /or services, as well as the provision of leased lines services, must submit a notification about the commencement of telecommunication activities only. Lithuania was one of the first EU countries to abolish the licensing system and move to the general authorisation system in the telecommunication sector.

Since the liberalisation of Lithuania's public fixed telephone networks and services market in January 2003 and the introduction of the new law, Lithuania's telecommunication sector has undergone a quick and successful transformation. It should be noted that low administrative charges created preconditions for the low service prices on the retail market.

The 2004 Law on Electronic Communications came into effect on 1 May 2004. Its key objective was to transpose the 2002 EU Directives on the New Regulatory Framework for Electronic Communications and Associated Services into national legislation. The Law introduced technological neutrality as an objective in regulation.

With respect to broadcasting, in 2006, the Law on Provision of Information to the Public regulating broadcasting activities was amended to end the licence requirement for certain broadcasting activities, *i.e.*, the Law does not require licences for activities not intended for programme broadcasting and/or re-broadcasting or for broadcasting for non-commercial purposes. Further adaptation of the regulatory system to convergence conditions is envisaged with transposition of the modernised 2007 EU legal framework for audiovisual media services (Directive 2007/65/EC). The aim of the new directive 2007/65/EC is a modernised and flexible framework for television broadcasts, including other linear (scheduled) audiovisual media services, and to introduce a set of minimum rules for non-linear (on-demand) audiovisual media services.

With respect to spectrum, when liberalising radio frequency usage conditions, the Communications Regulatory Authority of the Republic of Lithuania (RRT) is striving to encourage market participants to provide the widest range of modern wireless services and use the available limited national resources as efficiently as possible. As markets and new technologies evolve under convergence conditions, the regulation inevitably tends towards becoming more liberal and technology/service neutral.

The general authorisation regime implemented since January 2003 has produced favourable results in market development. Those segments to which the general authorisation system has not yet been fully applied will be regulated under this system in the future once the relevant amendments to the legal acts are finalised. Since technology-neutral regulation, as witnessed by the traditional telecom services sector, fosters market incentives to invest and develop advanced technologies, users are provided with the best service offers in terms of price and quality. This also helps to better ensure user interests and increases overall economic competitiveness.

4.1.6 Tanzania²⁶

In February 2005, the Tanzania Communications Regulatory Authority (TCRA) introduced the Converged Licensing Framework (CLF) after the end of the exclusivity period granted to the incumbent fixed line operator. Under the Communications (Licensing) Regulations (2005), the CLF encompasses technology and service neutrality and seeks to ensure regulatory flexibility, efficient utilisation of network resources, and market entry of small scale operators.

²⁵ Document RGQ10-2/1/016, 21 February 2008.

²⁶ Document RGQ 10-2/1/021, 25 February 2009.

As shown in Chart 2 below, the Schedule to the Regulations provide services in four market segments – international, national, regional and district – for the following four licence categories:

- Network facility: authorises licensees to install, own, control and provide access to electronic communications facilities such as fixed links, radio communications transmitters, satellite stations, submarine cables, fibre/copper cable, towers, switches, etc.;
- Network services: authorises licensees to operate and maintain public electronic communications networks using any technology such as GSM or CDMA;
- Application services: authorises licensees to provide electronic communications services to end users via private facilities or reselling services from licensed facilities/network service providers; and
- Content services: authorises licensees to provide content services for broadcasting.

Between December 2005 and June 2008, TCRA issued over 150 licences under the CLF, which has been embraced by both existing licensees (who have migrated into the CLF) and new entrants who have decided to venture into the communications sector.

In addition to the increase in operators, the number of subscribers has increased from 3,118,157 in 2005 to 9,523,392 in March 2008, which the TCRA attributes to the increased number of telecommunications licensees.

A number of lessons may be learned from Tanzania's CLF which may be useful to countries intending to introduce converged licensing procedures.

- Flexibility: TCRA engaged stakeholders, especially operators, in dialogue and gave a flexible timeframe for implementing the CLF. Although the initial grace period for existing communication operators to migrate to the CLF was 12 months, TCRA extended the grace period another six months since operators were unclear about which licence category to pursue. TCRA held several meetings with operators to educate them about the CLF and explain its advantages to them. Further, licensees are required to submit roll-out plans as an appendix to their licence, and a licence condition allows the plan to be reviewed annually, giving licensees an opportunity to change roll-out plans to accommodate new technologies and services.
- Incentive Regulations: Migrating operators were given incentives by excluding application fees and initial licence fees, and by offering longer licence durations – specifically that the term of the new licence would begin from the licence issuance date regardless of the remaining duration of existing licences.
- Slow Pace in Deployment of Converged Network: Although the CLF was introduced over four years ago, deployment of converged networks, particularly NGN, has occurred slowly. One possible reason is the lack of understanding of the CLF, the migration path to the NGN.

The CLF has also faced a number of challenges. The most critical challenge is to ensure that the prices of communication goods and services are affordable so as to meet consumers' expectations. Another challenge is for TCRA to maintain a clear, comprehensive and transparent licensing framework. Finally, after introducing competition and the CLF, it became more critical to ensure that spectrum is assigned to applicants with sound business and technical plans, as well as with the financial and technical capability to provide communication services.

Chart 2: Number of Licensed Operators under Tanzania's CLF (30 June 2008)²⁷

	Type of Licence	Market Segment	Number of Licences Issued
1.	Network Facility	International	4
		National	8
2.	Network Services	International	4
		National	8
3.	Application Service	International	12
		National	41
		Regional	5
4.	Content Service	National Television	5
		National Radio	5
		Regional Television	1
		Regional Radio	6
		District Television	18
		District Radio	30
		Community Television	0
		Community Radio	2
		Support services for satellite content services by subscription	3

4.1.7 United Kingdom²⁸

To prepare the United Kingdom for the challenges of converged communications between information technology and broadcasting, the Government introduced the Communications Act of 2003. The Act addressed the convergence of telecommunications and broadcasting by reforming the regulatory frameworks, including the introduction of a single regulator for the entire electronic communications sector. The Act sought to create a future-proof framework by creating a regulator that collaborates with stakeholders and accommodating the rise of convergent services in communications and broadcasting. The Act provided for:

- The Office of Communications (Ofcom), the single regulator combining the roles of five previous regulators (Of tel, the Independent Television Commission, the Radiocommunications Agency, the Radio Authority, and the Broadcasting Standards Commission).
- Ofcom to apply the powers of the Competition Act and other competition legislation to the communications sector.
- Freedom for new entrants to provide communications networks and services without having to apply for a licence.
- Trading of radio spectrum.
- A new and more coherent system for regulation of broadcasting.
- Greater freedom for public service broadcasters to regulate themselves.

²⁷ Document RGQ 10-2/1/021, 25 February 2009.

²⁸ Document 1/048, 6 September 2006.

Complementing trading and liberalisation policies, the United Kingdom pursues market mechanisms in spectrum management by seeking to make licences more flexible by liberalising licence terms to allow licence holders to change the use without applying to the regulator. Ofcom is working on defining licences to be flexible and technology-neutral while protecting other licensees against interference.

As a light-touch regulator, Ofcom seeks to move away from central management and increase the use of licence-exemption. Licence-exemption is being carefully examined in particular for low power devices and will be implemented as much as practicable as it is a key area for innovation and growth.

4.2 Future plans for converged licensing

4.2.1 Bangladesh

According to its contribution to the Rapporteur's Group,²⁹ Bangladesh plans to migrate to a technology-neutral and service-neutral licensing regime in 2011, which would allow operators to incorporate new technological developments and be more flexible and creative in developing communications services. Currently, the Bangladesh Telecommunication Regulatory Commission (BTRC) has no plans to issue converged licences, but it will consider convergence for a new licensing regime in the future. In the meantime, Bangladesh will look to the ITU for guidance on a smooth migration from the present licensing regime to a converged licensing regime.

4.2.2 Cameroon³⁰

The government of Cameroon recognises that its telecommunications laws and regulations must be revised in order to adapt to and promote convergent technologies. Such reforms will require the cooperation of various ministries and agencies, including Ministère des Postes et Télécommunications (MINPOSTEL), Ministère de la Communication (MINCOM), Agence de Régulation des Télécommunications (ART), Agence Nationale des Technologies de l'Information et de la Communication (ANTIC) and Conseil National de la Communication (CNC). Cameroon must also harmonise its legal frameworks and regulations with the Communauté Économique et Monétaire des Etats de l'Afrique Centrale (CEMAC).

The 1998 telecommunications law began the process of liberalisation in Cameroon by establishing ART as an independent regulator responsible for the regulation and control of the telecommunications sector, including management of radio frequencies for telecommunications.³¹ Although ART manages radio frequencies for telecommunications, it does not have the authority to regulate spectrum. Instead, MINPOSTEL retains the authority to regulate spectrum for telecommunications while the authority to regulate broadcast spectrum is granted to MINCOM.

The licensing regime is contained in Cameroon's telecommunications law and provides for three categories: concessions, authorisations and declarations.

- Concessions grant entities the right to establish and/or operate public telecommunications networks.
- Authorisations allow entities to establish telecommunications networks with a view to offering a public telecommunications service other than basic telecommunications services, such as Internet and value-added services. Such authorisations require licences so that operators may have several types of licences.
- Declarations permit entities to establish private, low-range and low-capacity networks

4.2.3 China³²

A significant challenge to China's telecommunications regulation is how to adjust itself to the convergent market environment. With the development of new technologies and services, convergence has become the main trend in the telecommunication industry of the world. It includes the convergence of the fixed and mobile networks; the telecommunications, Internet and broadcasting and television networks; and the next generation network's industries.

²⁹ Document RGQ 10-2/1/022, 18 March 2009.

³⁰ Document RGQ 10-2/1/012, 18 January 2008.

³¹ *La loi N°098 du 14 juillet 1998 régissant les télécommunications au Cameroun.*

³² Document 1/036(Rev.1), 29 August 2006.

The Chinese government has placed much importance on the convergence of three networks. In 2001, the fourth meeting of the National People's Congress, ratified as the "10th 5-year plan guidelines," put forward that the nation would promote the convergence of the telecommunications, television and computer industries. In 2005, the "11th 5-year plan" mentioned that the accommodation capacity of information infrastructure should satisfy the requirement of the informatisation, the universal service capacity will be significantly improved, the convergence of the three networks can be essentially obtained, and the preliminary mechanism of information sharing can be established.

With regard to China's regulatory system, there are two independent authorities. The Ministry of Industry and Information Technology (MIIT) is responsible for constructing, operating and managing telecommunications and Internet networks and was established by the 2008 National People's Congress, which merged several former ministries. The State Administration of Radio Film and Television (SARFT) is responsible for content in the broadcasting and television services.

In China, some new services, such as IPTV and mobile television, have been employed in certain cities, and MIIT has played an active role to encourage the deployment of these new applications.

4.2.4 Nepal³³

The main agencies in Nepal that regulate the telecommunications, broadcasting and information technology sectors are the Nepal Telecommunication Authority (NTA) for telecommunications, Ministry of Information and Communications (MOIC) for broadcasting, and the Ministry of Science and Technology (MOST) in the IT sector. Though NTA is the autonomous regulating body, in practice the MOIC has been the principal actor in the telecommunications sector. The MOIC is also the highest body responsible for formulating broadcasting policies in the country. Thus, MOIC and NTA share responsibility for governing telecommunications providers, while the MOIC has sole authority over radio and television broadcasters.

Regarding spectrum management, there is a high level committee comprising officials from different ministries and NTA under the umbrella of the MOIC. As a consequence, the administration of radiofrequency spectrum is not governed by a single agency.

In Nepal, convergence has raised several debates about classification of certain telecommunications and broadcasting services. As the lines between data transmission, broadcasting and voice transmission are eroded, regulators are faced with the tasks of how best to classify the converging segments of the communication sector. The regulatory system in Nepal is therefore experiencing difficulties with the trend of convergence. Since the division of the regulatory responsibility and jurisdiction is based on the distinction of whether the provider is primarily a telecommunications, broadcasting or IT service provider, the government is less than effective in regulating activities which are not easily categorised. This situation clearly indicates the need to overhaul the regulatory system and the organisation of the communications sector in Nepal.

5. Guidelines and Recommendations

The implementation of unified and multi-service authorisation regimes requires careful planning. Regulators must address many issues, including:

- whether a unified or multi-service authorisation regime is appropriate for the local ICT market;
- whether to adopt a unified or a multi-service authorisation regime;
- the categories of authorisations in a multi-service regime;
- the licensing procedures for issuing the new authorisations;
- the terms and conditions attached to these authorisations; and
- how to transition existing licensees to the new licensing regime.

Depending on the nature and scope of the authorisations, regulators and policy makers may have to grapple with the issue of which regulatory agency should administer the new forms of authorisations. Since many countries have traditionally distinguished between telecommunications (*i.e.*, transmission-based) services and broadcasting, or content-based services, it is not uncommon to have different regulatory agencies administer telecommunications and broadcasting services. In these countries, the inclusion of broadcasting and content-based services within the scope of a unified or a multi-service authorisation thus raises the question of which regulatory agency should administer the authorisation.

³³ Document 1/014, 5 July 2006.

Regulators must also carefully consider the procedural dimension of implementing a new unified or multi-service authorisation regime. In order to promote transparency and confidence in the process, best practices suggest that regulators should consult with industry stakeholders prior to implementing the new authorisation regime.

Regulators are encouraged to consider the following principles when transitioning to and adopting a converged licensing framework:

- Fostering technology neutrality;
 - Ensuring flexibility to allow the new licensing regime to accommodate future technological and market changes;
 - Simplifying the number of licence categories;
 - Reducing administrative burdens and fees on market players;
 - Applying incentive mechanisms that encourage existing operators to transition to the converged licensing framework, *e.g.*, fee holiday;
 - Ensuring transparency with regard to converged licensing responsibilities;
 - Fostering close collaboration amongst appropriate entities with regulatory and oversight responsibilities regarding a converged licensing framework; and
 - Referring to international best practices and international regional organisations to help harmonise licensing approaches.
-



Documents of the Global Symposium for Regulators (GSR)
10 – 12 November 2009 – Beirut, Lebanon

Document

*Policy Paper "Lebanon at Horizon 2013, General Rules for the Regulation of Telecommunications
Services in Lebanon Including a Change-Reform-Repair-Plan of Action"
(English, Arabic)*

H. E. Eng. Gebran Bassil, Minister of Telecommunication,

Not available

Pas disponible

No disponible