Concept Note

International Telecommunication Union
Telecommunication Development Bureau

ENHANCING CYBERSECURITY IN LEAST DEVELOPED COUNTRIES

Location(s):	49 Least Developed Countries (LDCs)[1]
Expected duration:	24 months
Estimated Budget:	93'000 CHF per country
Implementing Agency	International Telecommunication Union (ITU)

1. Background and context

1.1 General Introduction/Context

Today, Information and Communication Technologies (ICTs) have become an integral part of modern societies and are omnipresent, constantly transforming lifestyles. ICTs provide real time borderless communication and almost unlimited access to a range of services. Technical developments have improved daily life: online banking, Mobile Data Services and Voice over Internet (VoIP) telephony are few examples.

The availability of ICTs and network-based services offer a number of advantages for the society in general. ICT applications, such as e-Government, e Commerce, e-Education, e-Health and e-Environment, are considered as enablers for socio-economic development, particularly due to their ability to deliver a wide range of basic services in remote and rural areas. In this regard, ICT applications can facilitate the achievement of Millennium Development Goals (MDGs) in developing countries, and in particular in the Least Developed Countries (LDCs).

The development of cheaper infrastructure technologies has enabled developing and Least Developed Countries to offer Internet services to more people. The popularity of the Internet and its services is growing fast: by the end of 2013 it is estimated that 39% of the world population (2.7 billion people) will be using the internet. In LDCs, the number of Internet users has increased from about 24 million in 2008 to 60 million by early 2013[2]

Today, we are more interconnected than ever before and overall reliance on the Internet continues to increase. Unfortunately, in this environment cyber-attacks occur rapidly and spread across the globe in minutes without regard to borders, geography, or national jurisdictions. Worldwide, every second, 18 adults become a victim of cybercrime, resulting in more than one-and-a-half million cybercrime victims each day[3]. Cybercrime ranges

[1] Afghanistan, Angola, Bangladesh, Benin, Bhutan, Burkina Faso, Burundi, Cambodia, Central African Republic, Chad, Comoros, Congo D.R., Djibouti, Equatorial Guinea, Eritrea, Ethiopia, Gambia, Guinea, Guinea Bissau, Haiti, Kiribati, Lao (R.D.P.), Lesotho, Liberia, Madagascar, Malawi, Mali, Mauritania, Mozambique, Myanmar, Nepal, Niger, Rwanda, Samoa, Sao Tome & Principe, Senegal, Sierra Leone, Solomon Islands, Somalia, South Sudan, Sudan, Tanzania, Timor-Leste, Togo, Tuvalu, Uganda, Vanuatu, Yemen, Zambia.
[2] ITU World Telecommunication/ICT Indicators Database.
[3] Source: Symantec.

from the stealing of private identity or child pornography distribution to the damaging and complete disruption of a country's Internet connectivity.

Consequently, it is crucial to prevent cyberspace from turning into a source of danger for users - state, business and citizen - and to build confidence and security ICTs' use: in other words to create a safe cyber environment - to ensure cybersecurity.

1.2 Problem statement

ICTs provide unprecedented opportunities to accelerate social and economic development, while at the same time, the misuse of ICTs and their vulnerabilities create new and serious threats having the potential to harm the society.

This major threat to all the developed as well as the developing and least developed countries presents a growing need to be able to communicate, coordinate, analyze, and respond to cyber-attacks across different business sectors at national, regional and global levels.

To answer the challenges imposed by the borderless nature of cybercrime and to achieve cybersecurity worldwide, establishment of national cybersecurity strategies including mechanism to identify, manage and respond to cyberthreats as well as cooperation between countries at regional and international levels is crucial.

This is particularly challenging for LDCs lacking of adequate legal and regulatory framework, limited human capacity/expertise and financial resources.

1.3 Justification

In a context of ever increasing growth of malicious cyberactivities, the project aims at replying to requests for assistance from LDCs to protect their cyberspace and critical information infrastructure as well as at building confidence and security in ICTs' use. It also aims at providing LDCs with the capacity of participating effectively in the global effort to fight cybercrime.

The project will be implemented in the framework of the ITU mandate[4] to enhance security and to build confidence in the use of ICTs applications.

In particular, it will build on the activities implemented with the International Multilateral Partnership Against Cyber Threats (IMPACT) for the deployment of solutions and services to address cyberthreats worldwide as well as on the ITU partnership with the European Union to "Support the establishment of Harmonized Policies for the ICT Market in the ACP[5]", encompassing wide range of legal, regulatory and technical aspects related to cybersecurity.

[4] ITU Plenipotentiary Conference, World Telecommunication Development Conference (WTDC), World Telecommunication Standardization Assembly (WTSA) and World Summit on the Information Society (WSIS).
[5] African, Caribbean and Pacific Group of States.

2. Description

2.1. Objectives

The "Enhancing Cybersecurity in LDCs" project aims at supporting LDCs in strengthening their cybersecurity capabilities to better respond to cyberthreats to ensure enhanced protection of their national infrastructure, including the critical information infrastructure, thereby making the Internet safer and protecting Internet users, to serve national priorities and maximize socio-economic benefits in line with the objectives of the World Summit on the Information Society (WSIS) and the Millennium Development Goals (MDGs).

2.2. Expected results

The expected results of the Project include:

- Enhanced national expertise on cybersecurity including, among others, technical, legal and regulatory, institutional and organizational aspects;
- Online and/or face-to-face workshops and training activities on cybersecurity aspects/topics implemented;
- Improved national preparedness in identification, prevention, response, and resolution of cybersecurity threats/incidents.
- Customized guidelines on national cybersecurity legislation, regulation and technical aspects ;
- Relevant equipment and solutions delivered to Ministries for subsequent distribution.
- Training curricula developed on cybersecurity national, regional and international legislation, regulation and technical aspects;

2.3. Implementation strategy/methodology

The following main activities will be undertaken:

a. ***Launch of the project in selected LDCs:*** Personalized communications to LDC Member States will be undertaken to identify and select beneficiary countries and to formalize full commitment and participation of respective ICT Ministries and Regulatory Authorities involved in cybersecurity in the project.

b. ***Assessment of the situation:*** At the initial stage of the project, information gathering and assessment of the existing situation in each beneficiary country will be carried out to identify the national cybersecurity challenges to be addressed. The study will cover, among others, technical, regulatory and legal as well as institutional and organizational aspects of cybersecurity. Material produced by ITU and by other organizations/institutions on these subjects will be collected and reviewed.

c. ***Development of guidelines:*** From the situation analysis, guidelines on cybersecurity legislation, regulation and technologies which would facilitate implementation of electronic protection system on national level will be developed. These guidelines will help beneficiary countries in enhancing their cybersecurity in order to adequately react on cyber threats.

d. ***Equipment and solutions distribution:*** According to the situation assessment and the developed guidelines, relevant sets of equipment and software will be delivered to the beneficiary countries and then deployed by responsible agencies.

e. ***Capacity building:*** Training material will be developed and curricula prepared on national, regional and international cybersecurity legislation and regulation, as well as technology aspects. Through a train-the-trainer approach, the project will deliver face-to-face capacity building workshops in conjunction with virtual (distance) learning sessions to selected national experts from ICT Ministries and Regulatory Authorities involved in cybersecurity. These sessions will be conducted with the support of the ITU Academy e-learning platform and the regional Center of Excellence.

2.4 Sustainability

The project will be conducted to ensure that, after its closure, the beneficiary countries have the capacity to sustain it on their own. Particular attention will be put on beneficiary ownership as it remains a key element of sustainability. National experts will receive adequate training and will be encouraged to share the acquired knowledge with their colleagues having not participated in the capacity building training sessions (train-the-trainer approach).

3. Contact information

PSB Division
PSB-RM@itu.int