World Telecommunication Development Conference (WTDC-14)
Dubai, 30 March – 10 April 2014

Document WTDC14/20-E
28 January 2014
Original: French

SOURCE: Dem. Rep. of the Congo
Ministry of Posts, Telecommunications and New Information and Communication Technologies

TITLE: Establishment of computer incident response teams (national CIRTs) in developing countries

COD/20/1 **Objective 3**

Summary

New information technologies constitute a highway which allows for tremendous expansion of the Web. This leads to an improvement in living standards, but at the same time calls for the exponential enhancement of cybersecurity.

Who is protecting whom?

In the interests of good governance, all stakeholders are expected to protect everyone at all levels.

It is necessary to deploy IT infrastructures and cyberservices that are reliable, maintainable, robust and secure, while respecting basic human rights and the rights of States. The need to protect systems and valuable information has to coexist and be made compatible with the parallel protection of the rights and digital privacy of individuals.

Developing countries need to enter the information society without exposing themselves to excessive risk, building on the experience acquired in the developed countries and avoiding the danger that a new factor for their exclusion arises in the form of cybersecurity. In my country, the Democratic Republic of the Congo, which had no policy for protecting data, either personal or at the level of infrastructure, a draft law on data protection has been put forward for promulgation.

Introduction

IT and telecommunication security, or cybersecurity, touches on the security of the digital and cultural wealth of people, organizations and countries.

The challenges involved are complex, and meeting them requires that there be the political will to devise and implement an overall strategy for the development of digital infrastructures and services (e-services) which includes a coherent, effective, verifiable and manageable cybersecurity strategy. The cybersecurity strategy must be part of a multidisciplinary approach, with solutions in place at the educational, legal, management and technical levels. A strong response, with priority attention to digital infrastructure security needs, can build confidence and generate welcome

Contact: Name/Organization/Entity: Kasongo Uba Makosho Joackim Kascky, Delegation of the Dem. Rep. of the Congo, Dem. Rep. of the Congo
Phone number: +243 898931095
E-mail: kascky@yahoo.fr

economic growth benefiting all of society, while at the same time giving effect to WTDC-10 resolutions and recommendations.

Mastery of digital information wealth, distributing intangible goods, adding value to content, and bridging the digital divide are all problems of an economic and social nature, which call for something more than a one-dimensional, strictly technological approach to cybersecurity.

1 What protection measures do we need to take?

It is necessary to understand the concept of cybercrime and propose measures to combat cybercrime targeting ICT operators and their users.

- **Cybercrime and culture**

A people's culture is a feature for their identity and cohesion. National cultures are being reshaped to suit the globalization revolution. These effects, particularly evident on the population, are compounded by the extraordinary progress in the ICT sphere.

Developing countries are faced with the problem of needing to join the information society without ignoring the risks of becoming dependent on technologies and technology providers.

Telecommunication infrastructures and the services and activities that they make possible can enhance the characteristics of developing countries.

The speed of data exchanges has considerably raised the hopes of organizations/associations within the sector.

Proposed measures

- **Legislation**

We believe that each developing country must take all possible action to adopt suitable cybercrime legislation. We must never cease impressing upon governments that combating cybercrime is a crucial matter.

- **Training**

Training takes place at two levels. On the one hand, at the "macro" level: training and exchanges of experiences for legal and technical staff, in order to equip them with the required competencies in relation to cybercrime. And on the other hand, at the "micro" level: creating a network of trainers and focal points to educate and raise awareness among associations, organizations or groupings of persons on the use of new technologies, while drawing their attention to the dangers and threats it entails.

- **Entities**

Governments must encourage the creation and implementation of entities, organizations or agencies that will combat this scourge and effectively manage incidents.

We encourage the establishment of administrative agreements between Member States and ITU for the creation of national computer incident response teams (CIRTs).

_____