



*World Telecommunication  
Development Conference 2006  
The Doha Action Plan*

*Cooperation on Cybersecurity  
including combating spam*

Alexander NTOKO

Chief, E-Strategies Unit

ITU Telecommunication Development Bureau



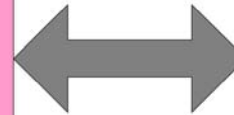
# Istanbul Action Plan Programme 3 and the WSIS Plan of Action

## Plan of Action C.5

WSIS Plan of Action  
December 2003

IsAP Programme 3  
WTDC March 2002

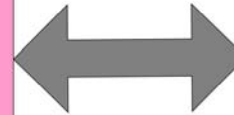
**C5) Building confidence and security in the use of ICTs** 12. Confidence and security are among the main pillars of the information society.



Enhance security and build confidence in the use of public networks for e-services/applications.

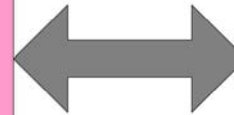
**b)** Governments in cooperation with the private sector, should prevent, detect and respond to cyber crime and misuse of ICTs...

**e)** Take appropriate action on spam at national and international levels.



Provide assistance to Member States in developing laws and model legislation for e-services/applications, prevention of cyber crime, security, ethical issues and data privacy.

**f)** Further strengthen the trust and security framework with complementary and mutually reinforcing initiatives in the fields of security in the use of ICTs...



Identify security requirements and propose solutions for the development of secure IP infrastructure for e-services/applications on various types of networks using relevant technologies.

**g)** Share good practices in the field of information security and network security and encourage their use by all parties concerned.



Develop tools to facilitate the exchange of best practices on IT security, legal issues related to the areas of activity of this Programme.

**i)** Encourage further development of secure and reliable applications to facilitate online transactions.



It is necessary to address the security concerns in order to leverage the potentials of public networks as vehicles for delivering affordable value-added e-services/applications



# What is our strategy?



Identity Management as vital component for cyber security.

ICT applications should be built on secure the trusted platforms to increase their benefits to the population.

A holistic approach to cyber security addressing the needs of all sectors.

Appropriate policies and legislation taking into account the balance between enforceable legislation and technology neutrality.



## *Concretely, what do we do? – Deliverables*

- **Projects:** Coordinating the design, development and implementation of projects on Cybersecurity for securing ICT applications.
- **National Policies:** Assisting Member States in addressing technology and policy issues for Cybersecurity for ICT applications.
- **E-legislation:** Providing guidance in the development of laws and model legislation for the prevention of cyber crime, security and data privacy.
- **Publications:** e.g., Cybersecurity guide for developing countries, Report on legislation for Cybersecurity and cyber crime.
- **Awareness:** Building basic awareness amongst the population on the potentials of secure ICT applications for the delivery of services in various sectors.



# WSIS Declaration of Principles Paragraph 35

## *Some important points on Cybersecurity*

- Cooperation with all stakeholders is key.
- Take into account level of socio-economic development.
- Respect the development-oriented aspects of the information society.
- Prevent the use information resources and technologies for criminal purposes.
- Spam and Cybersecurity to be deal with at appropriate national and international levels.



# WTDC2006 – Doha Plan of Action

## *Some key decisions on Cybersecurity including spam*

1. Primary responsibility to Programme 3 for Action Line C5 – *Focused approach where cooperation and collaboration are vital.*
2. Stronger and broader mandate on Cybersecurity, spam and cyber crime.
3. Develop common understanding on issues of spam and cyberthreats and act as facilitator for regional and interregional cooperation.
4. The importance of standards but more needed to address the development-oriented aspects of the information society.
5. Actions should be Membership driven and supported by interested Member States.



# What NEXT?

1. Invite Member States and Sector members to send proposals/contributions.
2. Organize meetings on Resolution 45. First meeting scheduled for 31 Aug – 1 Sep 2006 at ITU HQ.
3. Meetings will focus on discussing mechanisms for cooperation and not substantive discussions on this subject.
4. Emphasis is on *interested* Member States. Resolution 45 is not aimed at building consensus amongst **all** ITU Member States.
5. Report the results of these meetings to Plenipotentiary Conference 2006.



# For Further Information:

## **E-Strategies Unit**

**Telecommunication Development Bureau (BDT)**

**International Telecommunication Union (ITU)**

**Place des Nations**

**CH-1211 Geneva 20**

**Switzerland**

**Fax: +41 22 730 5484**

**Web: <http://www.itu.int/ITU-D/e-strategies>**

**Email: [e-strategies@itu.int](mailto:e-strategies@itu.int)**