Third Meeting for WSIS Action Line C5
Thursday 22 May 2008

SESSION 4

Global Challenges requires Global Solutions: are any in the pipleline?

Professor Solange Ghernaouti-Hélie
www.hec.unil.ch

Global challenges don't mean to answer them only by global answers!

1- A large range of issues

Because ICT security has a global dimension and deals with a large range of issues as:

- ICT uses or misuses;
- Technical measures;
- Economic, legal and political issues;

It is important to develop a global approach to master ICT related risks and threats.
Challenges can be seen at global level because all ICT resources are interconnected and interdependent and because cyberthreats are global and also because information technologies are under the same kind of threats.
But as the same time, technologies and ICT uses are different and need specific organizational and technical security measures to prevent and react to incidents.
So a global and unique security answer to different technologies, services, uses or needs is not relevant.
However, a global answer is needed to master ICT related risks at international and regional levels and mainly rely upon international cooperation.

2 - Specific national actions and international cooperation

To be effective, international cooperation relies upon national levels.
Specific actions should be taken at national level, to raise or build cybersecurity capacities of various actors in order to be able to deal with national and international cybersecurity issues.
Awareness efforts, as previously mentioned by ENISA, have to be done to educate and train all the actors of the information society: from decision makers to citizen, including children and older people
Awareness is difficult to achieve and awareness programs are costly.

3 - Awareness is not enough

Awareness is not enough to empower the end-user in a way that he could be able to adopt a safe behaviour when dealing with ICT technologies. At the same time, efficient, simple and cost effective security measures should be operational.
For that, financial, technical, organizational and human resources should exist.
As capacity building activities take place at national level, resources should be found at specific national level. Nevertheless, global actions to support cybersecurity are important as for example:

- Development of standards;

- Definition of model, guidelines related to legal framework, framework for international cooperation;
- Etc.

But we must keep in mind that most of the operational works is done at a national level!

ICT level of penetration or internet uses can vary from country to country even if cybersecurity problem could be similar, the way to deal with them is dependant of local culture, context or of national legal framework for example.

4 - Answering a global challenge

Global challenges don't mean to answer them only by global answers!

So any global strategy has to be adapted to local needs. Even each country is different, some countries at regional level, could have the same level of Internet penetration and have similar cybersecurity needs. So sometime, having a regional answer could be relevant in specific contexts. In this case, a regional answer could be seen as a global answer!

A global answer could be perhaps effective if the international community wants to focus on the need to use more reliable ICT technologies. That means that technologies should be less vulnerable!
To achieve this generic goal, the market has to integrate security requirements into ICT products or services life cycle development at the very beginning of the product life cycle and also during all the life cycle toward the product implantation, integration in every day activities.
So the question of ICT products distribution, of economic model is raised.

Perhaps a global will and a global approach involving all the industrial and economics actors could help to deal with the compromise that should be done between:

- Product delivery;
- Cost;
- Profitability;
- Security effectiveness;
- Vulnerability reduction.

A global answer could also be relevant if the focus is done on a defence in deep security approach.
That means that security must exist at several levels of any information infrastructure.

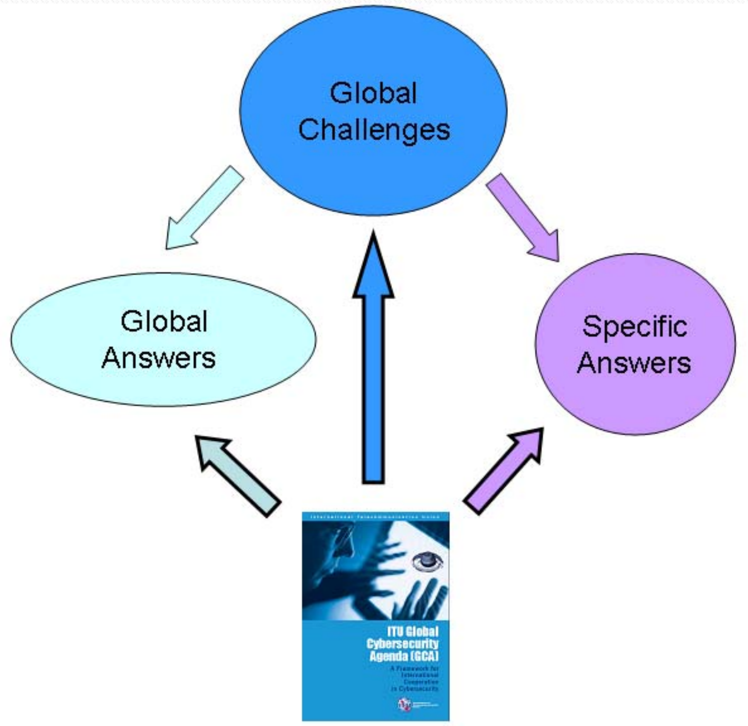
Security should exist at the following levels:

- Operational system, software, applications, services, contents levels;
- Hardware level;
- Network level;
- End-user level.

Every element of the ICT chain should has is security hardened in order to "raise the bare" in a way to significantly decrease the level of threats or the level of ICT risks impacts.
In this context, security in deep can be equivalent to global security because security in deep has also to take into consideration the organizational and managerial dimensions of cybersecurity.

5 – An innovative approach

With the Global Cybersecurity Agenda, ITU proposes a unique framework to consider cybersecurity issues in a holistic and systemic approach, a unique model to deal with the global challenges of building confidence and security into the use of ICT.


Global Challenges
Global Answers
Specific Answers
ITU Global Cybersecurity Agenda (GCA)
A Framework for International Cooperation in Cybersecurity

ITU: an innovative approach to answer a global challenge

ITU proposes an innovative and efficient interdisciplinary framework from which global, schedulable and specifics answers could be developed, by relevant players in order to be effective in international collaboration and well prepared to face the challenge of building an inclusive information society.

The development of my point of views could be found in my publication "Information Security for Economic and Social Development" UNESCAP – 2008 – Link http://www.unescap.org/icstd/policy/

- **Recent publications**

"Protecting the information is a crucial issue to take into consideration in the Information Society. Developing and least developed countries may face significant challenges in meeting the requirements of the global market place without information security. The lack of technology development in information security, therefore, may constitute a serious infrastructure deficiency that is widening the digital divide. This publication is aimed at the major players of the information society, especially policymakers for information economy. It deals with key economic, legal, and social issues related to information security. The purpose is to help countries get prepared to face issues and challenges linked to information and communication technologies (ICT) deployment, uses and misuses."