International Telecommunication Union

STATE AGENCY FOR INFORMATION TECHNOLOGY AND COMMUNICATIONS OF THE REPUBLIC OF BULGARIA

Opening Remarks 7 October 2008

ITU Regional Cybersecurity Forum for Europe and the Commonwealth of Independent States[1]

Sofia, Bulgaria
7−9 October 2008

Plamen Vatchkov, Chairman

State Agency for Information Technology and Communications, Bulgaria

Dear Ladies and Gentlemen,

Dear Colleagues,

Once again welcome to the ITU Regional Cybersecurity Forum for Europe and the Commonwealth of Independent States.

Hosting the current Forum by the State Agency for Information Technology and Communications is an expression of the will of the Republic of Bulgaria to follow steadfastly the road of information and communications technology development. At the same time it is a recognition on the part of ITU for the contribution of the Bulgarian Administration to the ITU activities as a whole.

I have talked many times about the successes we have achieved in that field, so I will not do it now. This time, however, I would like to stress that hosting the current Forum is also an expression of the commitment of the State Agency

[1] See the ITU Regional Cybersecurity Forum for Europe and the Commonwealth of Independent States (CIS) website at www.itu.int/ITU-D/cyb/events/2008/sofia/

for Information Technology and Communications to apply more efforts in the field of network and information security. I will just cast a short glance at the Agency's activity in that direction.

As of November 2006, Bulgaria became involved in the activities of the European Network and Information Security Agency (ENISA). As a result of active cooperation with ENISA and the Hungarian CERT, the establishment of a Governmental CERT in Bulgaria is underway and we hope it will start operating by the end of the year. SAITS is also taking measures to consolidate its institutional capacity in terms of information security.

We also hope that the Computer Emergency Response Team will contribute considerably in the fight against cyber crime. Presently, with the kind assistance of the ITU BDT, SAITS is conducting a campaign of self-assessment of the national cyber security. Based of the results of this self-assessment, a national strategy on cyber security will be developed.

In short, in terms of security of communication and information systems in Bulgaria we have serious achievements behind our backs, but we also have some challenges ahead of us. I believe that this Forum will greatly contribute to the successful solution of these tasks.

So, the emphasis now is not on ICTs as a whole, but on cybersecurity – an element of ICT that we have recently been increasingly aware of. Why do we have to deal with cybersecurity? Because most of us spend a lot of time online. And since this online virtual world is a reflection of the real world, just like criminals are an inevitable part of our social structure, not surprisingly, they also have populated the virtual world and they are committing cyber crimes. However, while, initially, the results of cyber crimes were felt within the virtual world, now the victims of cyber crimes are in the real world and they suffer heavy financial losses or lose credibility. And the logic is simple – since there are cyber crimes, fighting them calls for cybersecurity. And that is the reason we are here today – to find the ways and means to raise the level of cybersecurity. But cybersecurity has many aspects. And looking at the Forum Agenda, we see that all of them will receive considerable attention in the relevant sessions.

First, we will look at the different approaches to the establishment of institutional frameworks of cybersecurity and critical information infrastructure protection. Then, we will elaborate on the issue of cybersecurity culture – awareness of all stakeholders of the existing threats and the role of the governments in raising that awareness.

Bearing in mind that most of the ICT networks are private, success in cybersecurity can be ensured only by bringing together the industry and the governments in order to discuss common cybersecurity challenges. In that sense, the role and benefits of public-private partnerships will be elucidated.

Legislation and law enforcement at national and international level are important elements in preventing, detecting and responding to cybercrimes and they will get their due attention at the Forum.

Since we assume that that cyber incidents will be part of our lives, much attention is devoted to the components of efficient incident management – funding, human resources, training, technical capabilities, government-industry relations, legal framework, collaboration at all levels, etc.

Bearing in mind that cybersecurity is a process, and not just a one-off effort, then the importance of a national strategy, addressing technical, legal, financial and political issues becomes obvious, so a session is dedicated to the approaches, best practices and key building blocks for the establishment of national strategies on cybersecurity and CIIP.

There is also a session dedicated to cybersecurity solely in terms of law enforcement.

A financial perspective on cybersecurity links the efficiency of system protection with the possible obligations of individuals and companies to bear the costs of cyber incidents.

And finally, bearing in mind that the consequences of cyber crimes are global and far reaching, only a cybersecurity based on broad national and international cooperation can be successful.

In other words, we have quite an ambitious agenda of the ITU Regional Cybersecurity Forum for Europe and the Commonwealth of Independent States. And while these ambitions exclude full abolishment of cybercrime, we at least hope that we, joining our efforts, could make the Internet more or less safer, and this is a goal worth striving for.

I sincerely hope that during your stay here you will also find time to get to know more of our ancient capital city Sofia.

I wish you every success with this Regional Cybersecurity Forum and thank you for your attention.