PC.DEL/563/08
2 July 2008

ENGLISH only

OSCE - 2008 ANNUAL SECURITY REVIEW CONFERENCE
WORKING SESSION II
ESTONIAN STATEMENT

First of all I would like to thank chairman-in-office and other organizers for putting this important event together. I would also like to congratulate speakers of the panel for so eloquent elaboration of today’s challenges of security under OSCE framework. Security is a serious domain that affects us all and therefore it is even more important to try to find solutions and way ahead together as we have been and continue to do during those two days in Vienna. OSCE, its adherence to the CSBM’s and continuous security dialogue are and will be important elements in making our security environment more stable and predictable.

In my intervention I would like to concentrate on issue that was not covered by previous speakers but I hope that is still worth of concern, namely I would like to start with a reminder of a new asymmetric challenge we face today and what we might even more seriously face tomorrow. This challenge is connected with technology, its constant development and continuously new applications. This strive of the human mind has brought us to the situation where we have become more and more reliant on information systems and information technology for every aspect of our daily life. The reliability of those systems, and therefore their security, should be priority for all of us. We all are to certain extent, actually we do not know yet up to which point, vulnerable from the misuse or malfunction of those systems.

In terms of international security issues the acknowledgement of cyber threats as we call them, reached last year to a new level – not only because of the first coordinated cyber attack against a country, in that case Estonia, but also because of the large-scale cyber attacks against significant public and private sector information systems of many different countries of the OSCE region. And this trend in variable scale has continued.

Those coordinated cyber attacks against my government agencies, banks and media and telecommunication companies in Estonia proved that the vulnerability of a society's information systems is one of the aspects of public and state security to be addressed more thoroughly. We quickly understood that alone or with only some like-minded friends it would be very difficult to counter.

One on what we can be sure about is that those frequent cyber attacks indicate the start of a new era, where the security of cyber space acquires much wider dimension than before and needs much more attention. The protection of critical information systems could be regarded as important as that of traditional national defence and security.

The misuse of cyberspace has several angles – it can be used for terrorist purposes and criminal activity in different ways, but also for espionage or simple attacks through the wires forming a theatre of a state to state conflict. It is multifaceted and multidirectional. And the target might be a person, but also overall society, our way of life might be completely distracted and our feeling of security undermined. Imagine if one day your country or you and your neighbors find yourself in the situation where the bank machines are not working or electric system is completely paralyzed and you do not know who is behind that – a simple hacker, terrorist, worldwide corporation or some other state. Challenging is that one can be attacked through the wires by somebody and from the place never be known. So using other tools than catching the adversary is definitely more effective.

There are still so many unknowns and unexplored features in cyber security and the borders of this environment are very abstract and difficult to comprehend. Definitely they could not be described by national borders. Therefore we find it very important to have comprehensive approach to address that problem. All the tools and structures have to be used to counter the threat and neutralize the risk and we feel that OSCE can contribute.

Where do we stand at present and how to move forward?

- First, potential consequences of attacks on national and global level are not well understood and need to be discussed further to meet common understanding. All the international organizations dealing with different aspects of the security can make a difference.
- Secondly, the legal framework needs to be clarified. So far, there is very few pieces of international law on cyber security matters, and this what we have is recognised only by few of us. Clear set and widely acknowledged definitions of cyber threats and their taxonomy are missing. As part of that I would like to encourage nations who have not done it yet, to accede to and ratify the COE Convention on Cyber crime. This convention is open to everyone.
- Third, in countering the risk the cooperation is vital. In one hand cooperation between the state authorities and private sector, so called private-public partnership is needed. On the other cooperation between the nations using all international frameworks should be pursued, networking is utmost important. The private sector has an important role in securing the IT infrastructure by providing security products and adopting good security practices. But the governments also have a key role to play by supporting the development of cyber security and its technologies that underpin these products and practices.
- Fourth, it has to be understood that no nation, no person will be secure until every nation, every person takes systematic steps to enhance the cyber security. Therefore as a long-term strategy we should promote the culture of cyber security – id est education and awareness aimed at first on prevention, but which is even more important in longer term – on well-intended utilization of cyber space.

.
To conclude, Estonia hopes that cyber security issues will gain importance and receive needed attention from Vancouver to Vladivastok. Estonia is going to submit a proposal for a draft decision on information exchange with regard to the cyber security. We are willing to provide extra budgetary contribution for a workshop aimed at comprehensive addressing the issue of cyber security.