Organization for Security and Co-operation in Europe

NATIONAL WORKSHOP ON CYBER/ICT SECURITY IN THE CONTEXT OF REGIONAL AND INTERNATIONAL SECURITY, USE OF THE INTERNET FOR TERRORIST PURPOSES, AND CYBERCRIME

20– 21 May, 2015

Opening remarks by Ben Hiller, Cyber Security Officer, OSCE

Ladies and Gentlemen,

Dear colleagues,

Allow me to welcome you to this National Workshop on Cyber/ICT Security In The Context Of Regional And International Security, Use Of The Internet For Terrorist Purposes, And Cybercrime co-organized by the National Police Academy of Uzbekistan and the OSCE.

It is truly a pleasure for us to be here in Tashkent, and I want to thank the Uzbek authorities for their wonderful hospitality!

I am the OSCE Cyber Security Officer, and with me here today are my colleagues representing different entities in the OSCE, as well as a number of renowned international experts in their respective fields.

Our goal today and tomorrow is to review the most pressing threats emanating from cyberspace as well as effective responses to these threats.

In as much as this workshop is a stock-taking exercise, we also see this event as another meaningful step in our co-operation with Uzbekistan in tackling transnational threats, and in particular in the area of cyber/ICT security.

We look forward to sharing our experiences with you, and we are very keen to learn more about the steps Uzbekistan has taken to enhance cyber/ICT security.

A principal objective, especially during tomorrow's session will be to identify potential future joint activities - in one or all of the areas the three thematic sessions will touch upon.

But before we start, I wanted to make a couple of observation which I hope will set the scene for our discussions.

First up, why are we conducting this workshop?

There is no doubt, the growing dependence on information communication technologies (ICTs) and the interconnection of critical infrastructure have made a secure cyberspace vital to the functioning of a modern state!

ICT infrastructure have become the very fibre that connects us in the modern world, and made a positive impact on all our lives! They are a principal driver of economic and social growth.

On the flipside, if our communication networks are compromised, misused or attacked, so is life as we know it. This is a concern that all States share, no matter what their stage of development.

Cyber-attacks are a quintessential 21st century threat. Global in nature, virtually untraceable, eminently deniable, with perpetrators that can be state actors or not, many or few, acting directly or indirectly, and stationed anywhere.

Advances in the ICT sector have presented terrorists and other criminals with new opportunities and attack vectors.

In addition, this technology has added a complex dimension to interstate relations.

But when we talk about cyber threats what exactly are we talking about?

The answer to this question is trickier than one would think. There are few international policy fields where terms and concepts represent such obstacles to effective co-operation and have been so divisive.

Terms and concepts are often used interchangeably, and different meanings are attached depending from which part of the world you are from.

Hence for our discussions today and tomorrow, I would like to propose that we distinguish between three main categories, recognizing that these are not cast in stone:

- The first category is “cybercrimes” or “computer crimes”. Here we distinguish between crimes that either target computers directly such as viruses; or crimes facilitated by computer such as fraud and identity theft. More often than not when it comes to cybercrimes there is a financial incentive.

- The second category relates to “the use of the Internet for terrorist purposes”. As we know terrorists use the Internet to incite, to radicalise, to recruit, to showcase atrocities or to finance activities. The recruitment of foreign fighters is a particular concern at the moment.

- The third category refers to how States make use of ICTs and cyber/ICT security. Here we are particularly concerned about how to reduce the risks of conflict stemming from the use of ICTs through misunderstandings and/or how to enhance national resilience to cyber attacks on critical infrastructure.

While perpetrators in the first two categories are likely to be non-state actors, in the third category we are very much talking about state actors, or state proxies.

However, the key message I would like to convey is that while the motivations might differ between the various perpetrators - be it for making money, ideological reasons or to gain a strategic advantage - the methods employed are often very similar.

Consequently, threats should not be viewed in isolation, especially from a technical perspective, though from a policy side motivations do matter since it determines which national authority will deal with a particular threat.

The key to successful national and international cyber/ICT threats is co-operation - co-operation between the various stakeholders dealing with different cyber threats, both from the technical- and policy side, and to move forward in a complementary fashion.

National strategies therefore need to be inclusive and take into account all kinds of threats and actors – be it within a single and comprehensive strategy; or through a compilation of strategies related to specific threats.

However, there needs to be a thread that binds all components together; establishes clear areas of responsibilities and fosters information exchange between authorities, the private sector and civil society.

It is with this approach in mind that we drew up the agenda for our meeting today and tomorrow: While different sessions will address different threats, it will offer a platform for multi-stakeholder discussions, thereby offering a comprehensive platform to reflect on national responses in this field.

Incidentally, this way of thinking is also at the very heart of OSCE efforts in this field!

While different OSCE entities deal with particular cyber threats, they do so with the understanding that their efforts are part of achieving a larger goal - namely comprehensive cybersecurity. An approach that strengthens,

- tackles cybercrime;
- inhibits terrorist use of the Internet;
- enables authorities to protect a wide spectrum of targets including critical infrastructure;
- while at the same time safeguarding the Internet as a space for free expression and assembly.

With its inclusive approach the OSCE represents a bridge between different national, sub-regional, regional and international approaches to tackling different cyber threats thereby enhancing co-operation and capacities.

In addition, by prioritising and adopting the first ever set of confidence building measures to reduce the risks of conflict stemming from the use of ICTs, the OSCE has led the way in enhancing cyber stability between States and the trust infrastructure that underpins it.

I very much hope this workshop will be able to demonstrate the unique platform the OSCE has to offer in this field and underline the OSCE’s role as platform for formulating practical measures towards global cyber stability.

Thank you for your attention.