



DELEGATION OF AFGHANISTAN

STATEMENT

By Ambassador Khojesta Fana Ebrahimkhel

OSCE Asian Contact Group Meeting

“CYBER SECURITY AND CYBER DIPLOMACY”

9 March 2018

Thank you, Chair!

I wish to start by thanking Ambassador Koja and Ambassador Azzoni for their opening remarks; Ambassador Dán and Dr. Schnitzer for their introduction to the topic; and our guest from Japan, Ambassador Otaka for his excellent and very informative presentation.

I can state that we share the concerns voiced by Ambassador Otaka and we hold the view that cyber diplomacy is an area that deserves much more attention. Confidence-building measures in cyber should be established and advanced, and capacity-building efforts to strengthen co-operation on cybersecurity should be stepped up. The sustainability of capacity-building in cyber should be secured through the development of institutional capacities and specialized knowledge, which are required to deal with the highly complex cybersecurity matters in our digital environment.

Ladies and Gentlemen,

In Afghanistan, the Ministry for Communication and Information Technology is the lead agency for all cybersecurity-related matters.

In 2009, the Ministry has established a Cyber Emergency Response Team, mandated to address cyber threats and crimes and to raise awareness and provide concrete solutions on cyber issues to the government and the private sector.

In 2012, the Ministry formed an inter-ministerial committee, gathering experts also from the Ministries of Finance, Interior, Defense, Justice and Foreign Affairs, as well as from the National Directorate of Security and the Attorney General's Office, and held a first workshop on drafting a National Cyber Security Strategy. Organizational and financial support was provided by the U.S. Department of Commerce.

In 2014, the Ministry finalized and published the National Cyber Security Strategy, against the background of ICTs being widely used across Afghanistan and playing increasingly important roles in all aspects of our lives, both in the public sector, which is responsible for critical infrastructure and services like energy, health, aviation, communication and financial services, as well as in the well-developed private sector of the country. Objective number one of our National Cyber Security Strategy stipulates "to protect government ICT infrastructure, secure cyberspace for the citizens, improve and retain cybersecurity professional skills, encourage public-private partnerships, and boost and maintain international co-operation".

Similar to conventional terrorism and other transnational threats, we have to cope with the asymmetrical nature of security risks in cyber. The Government of Afghanistan is therefore committed to continuously update the country's cyber structure and systems towards a safe, secure and resilient cyber space for the public and private sectors. In doing so, we are ready to co-operate with our regional and international partners, sharing expertise, lessons learned and best practices. Before I close, let me underscore that attaining highest standards in cybersecurity and deepening of our cyber diplomacy efforts are also essential with a view to protecting rapidly increasing foreign direct investments and international trade activities in Afghanistan.

Thank you, Chair!