FSC-PC.DEL/2/17
23 March 2017

ENGLISH only

Permanent Mission of Ukraine
to the International Organizations in Vienna

Statement by the Delegation of Ukraine at the 64th Joint FSC-PC Meeting

(22 March 2017 at 10.00, Hofburg)
(Agenda item: Military aspects of cyber-security)

Mr. Chairperson,

The Delegation of Ukraine joins other delegations in warmly welcoming today's speakers and thanks them for valuable contribution to the discussion on the topic of "Military aspects of cyber-security".

The current massive pressure on the Ukrainian cyber space is one of the distinctive features of the crisis in and around Ukraine which was started by Russia's aggression against my country in 2014. Since that time, the competent State agencies of Ukraine have been registering a significant number of cyber-attacks on the Ukrainian State informational resources, originating from the Russia's territory. The Anti-terrorist operation related units and institutions were among the main targets of cyber-attacks. The vast experience, acquired by the Armed Forces of Ukraine, indicated a number of shortcomings in the operation of defence forces under current and potential threats, including increasing quantity and complexity of cyberattacks and cybercrimes. The cyber-security capabilities are therefore enhanced as part of Ukraine's defence reform process in line with NATO standards.

On 6 June 2016 President Petro Poroshenko enacted the Decision of the National Security and Defence Council of Ukraine on a Strategic Defence Bulletin of Ukraine that became a road map for the implementation of defence reform. The Strategic Defence Bulletin provides for participation in the implementation of the Common Security and Defence Policy of the European Union and active cooperation with NATO in the achievement of criteria necessary for the full membership in NATO. Pursuant to the adopted decisions and aiming at increasing the capability of the AFU to adequately react to the threats to Ukraine`s national security, including in cyber space, the MOD set up a Reform Committee which contains an IT-strategy and policy Group. Based on the accomplished work, the MOD Reform Committee has developed a Draft Defence Sector Cybersecurity Strategy.

We are grateful to our international partners for support in improving capabilities to counter cyber threats, including throughout setting up a Cybersecurity Incident Response Team and procuring necessary equipment and training materials.

Mr. Chairperson,
Distinguished Colleagues,

In a broader context, the activities of the MOD and AFU in the sphere of cyber defence are governed today by the Cyber Security Strategy of Ukraine enacted by the President of Ukraine on March 16, 2016.

The purpose of the Strategy is to create conditions for safe operation of cyber space and its use in the interests of people, society and the government.

Politically motivated and criminal activities of some international perpetrators in cyberspace in the form of attacks on governmental and private websites and electronic systems are today a frequent practice. The Strategy envisages a wide range of measures to ensure Ukraine's cyber security, particularly, the adaptation of the state policy up to the current situation, compliance with the EU and NATO standards, formation of a competitive environment in the sphere of electronic communications and provision of cyber defence services.

The Strategy sets the framework for deepening international cooperation and support of international initiatives in the area of cyber security, including expansion and further development of cooperation between Ukraine, the EU and NATO.

The National cyber security coordination centre started its work in June 2016. Deputy Minister of Defence, Chief of the General Staff of the AFU and Head of the Main Intelligence Service of Ukraine are among permanent members of the Centre.

Mr. Chairperson,

As threats in cyber-space have no national boundaries, we are very interested in maintaining consistent collective efforts to address security challenges in the use of information and communication technologies.

We consider that the OSCE has already developed important tools to jointly address current threats and challenges in the field of cyber security. We are pleased to recall that the first-ever set of confidence-building measures at the regional level was adopted by the OSCE Ministerial Council in Kyiv in December 2013.

We strongly support the activities of the OSCE Open-ended Informal Working Group established by PC Decision 1039 of April 2012.

Given the rapidly increasing role of the ICTs in the modern world, Ukraine is determined to actively support further progress in developing the additional set of CBMs aimed at improving the security of the global digital environment. These measures are most relevant for security of the OSCE participating States and to prevent an attack on or via cyberspace from escalating into a real-world, kinetic attack. We also look forward to discussing possible cooperative measures against other potential challenges, such as threats to energy infrastructure emanating from cyberspace.

Thank you, Mr. Chairperson.