RE: Developments in the field of information and telecommunications in the context of international security

CONTRIBUTION OF GREECE

The Permanent Mission of Greece to the United Nations present their compliments to the Office for Disarmament Affairs of the United Nations and, with reference to Note Verbale ODA/10-2017/CS, dated 16.2.2017, would like to submit the following information:

Within the framework of the Council of Europe, Greece has ratified by virtue of Law 4411/2016 (Governmental Gazette A’ 142, 3.8.2016) the Convention on Cybercrime (Budapest, 23.11.2001) as well as the Additional Protocol to the Convention on Cybercrime concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (Strasbourg, 28.1.2003).

It should be noted that a process for integrating the EU Directive on Security of Network and Information Systems into the national law is already in place. This directive is of paramount importance for enhancing resilience against cyber attacks at the national level and sets a number of pertinent to this end obligations for all EU member states that also include the adoption of a national strategy on the security of network and information systems.

A. According to information by the Hellenic Ministry of Defence, we mention the following:

Greece’s cybersecurity vision is to develop full range of capabilities to defend its national infrastructures and networks against latest cyber threats and cyber criminals. This includes: addressing cyber defence at the highest strategic level within our defence related organizations, further integrating cyber defence into operations and extending coverage to deployable networks. The following efforts have been undertaken at the national level to strengthen information security and promote international cooperation.

- A National Cyberdefence strategy framework is currently under development while the National Cybersecurity Strategy that regulates the general cybersecurity framework and defines the necessary actions for maintenance of the minimum requirements of cybersecurity, is becoming a law.

- Cyber defence is already part of the national defence operation plans while the National Emergency Alert System has been incorporated in most policy documents referring to Information Systems and has been integrated in all major National Exercises. Cybersecurity has been included in the operation plans for crisis periods in all public organizations.

- Greece has developed and continuously improves incident / emergency response capabilities, under the Military Computer Incident Response Center (MCIRC). “Rapid reaction teams” could deploy on short notice to help respond to and recover from cyber incidents in the military or the public networks. Recovering instructions from faults or cyber attacks, have been integrated in CIS (Computer Information Security) policy documents.

- A Cyber Security Operation Center for all National Military Defence Network Systems is under construction while at national level there are four CERTS (Computer Emergency Response Teams) responsible for the public and the private sector.

- Measures that could be taken by the international community, in order to achieve higher information security level are the following:
a) Increased Incident Response Capabilities, Network monitoring capabilities and actionable defence against cyber threats, through fully operational national Cyber Security Operation Centers.

b) Full integration of Cyber Defence into operations

c) National Cybersecurity/Cyberdefence Strategies development

d) Enhanced cyber awareness of the personnel employed in Cyberdefence and improvement of existing technical capabilities.

e) Continuous training of the personnel employed in Cyberdefence organisations

f) Harmonization of the national laws with the Global Cyber Security Laws and Directives.

B. According to information by the Hellenic Police, we mention the following:

- The mission of Cyber Crime Division of the Hellenic Police, according to article 30 of Presidential Decree 178/2014, includes the prevention, investigation and prosecution of crimes committed through the Internet or other electronic communications media. The Cyber Crime Division is an autonomous central service and is directly assigned to the chief of the Hellenic Police Headquarters.

- One of the Units of the Division is responsible for the “Security of Electronic and Telephone Communications and Software and Copyright Protection”. More specifically, the Unit investigates cases of illegal penetration of computer systems and the theft, destruction or trafficking of software, digital data and audiovisual works throughout the country.

- The Cyber Crime Division of the Hellenic Police works in close cooperation with the National CERT Authority, which is part of the National Intelligence Service. The mission of the National Authority against Electronic Attacks (CERT) is to attend to the prevention as well as to passively and actively counter electronic attacks against communication networks, data storage facilities and IT systems. In addition, the Authority is responsible for processing the data and notifying the competent authorities.