"Advancing responsible State behavior in cyberspace in the context of international security"

In December 2018, the UN General Assembly adopted a Resolution on "Advancing Responsible State Behavior in Cyberspace in the Context of International Security". The Resolution requests the Secretary-General to seek the views and assessments of Member States on (a) the efforts taken at a national level to strengthen information security and promote international cooperation in this field and (b) the content of the concepts mentioned in the reports of the Group of Governmental Experts.

Greece supports the UN GGE consensus view that international law, and in particular the Charter of the United Nations, is applicable also in cyberspace and is essential for maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment. Greece also supports the continuation of the process to discuss norms for responsible state behavior, confidence building measures, and international law under the UN First Committee, and the establishment of a new GGE.

We recognize that the interconnected and complex nature of cyberspace requires joint efforts by governments, private sector, civil society, technical community, users and academia to address the challenges faced and call on all stakeholders to recognize and take their specific responsibilities to maintain an open, free, secure and stable cyberspace.

We also recognize the role of the United Nations in further developing norms for responsible state behavior in cyberspace and recall that the outcome of the United Nations Group of Governmental Experts discussions have articulated a consensual set of norms and recommendations, which the General Assembly has repeatedly endorsed, and which States should take as a basis for responsible state behavior in cyberspace.

Through our participation in international organizations such as the United Nations, the European Union, NATO, and the Organization for Security and Cooperation in Europe, we seek to establish universal rules and principles of responsible State behavior in the use of cyberspace, to cooperate, to exchange experiences and best practices, and to jointly develop appropriate means to address threats and challenges related to cyber security. Our country contributes to the fullest possible extent to the formulation and implementation of relevant decisions adopted within the framework of international organizations with the aim of increasing cooperation and transparency and reducing the risk of conflict.

Recognizing that cybercrime is a global problem, Greece has signed and ratified the Treaty on Cybercrime of the Council of Europe, also known as the Treaty of Budapest. This treaty provides an important framework both for the adoption of our national legislation and for international cooperation in the fight

against cybercrime. The treaty was ratified by Law 4411/2016. Also, in the framework of our participation in the Organization for Security and Cooperation in Europe, our country has also signed the Confidence Building Measures Agreement, aiming at Member States' cooperation on cyber security issues, transparency, stability, and reduction of the risk of confrontation in cyberspace.

Within the framework of EU commitments, Greece has incorporated in its national legislation Directive 1148 on the security of network and information systems, also known as the NIS Directive, which includes measures for a high common level of security throughout the Union, implementing cybersecurity measures, developing a national strategy, and enhancing cooperation between Member States. As a result, the protection of all critical infrastructures in our country is strengthened, while the principles of open society, constitutional freedoms, and individual rights are safeguarded. The National Authority for Cyber Security, which operates under the auspices of the Ministry of Digital Policy, bears overall responsibility for the implementation of the national cybersecurity strategy.

The key targets of our national cyber security strategy are:

- the development and consolidation of a secure and resilient cyberspace on the basis of national, European and international standards and practices
- the continuous improvement of our capabilities to safeguard against cyber attacks, with an emphasis on critical infrastructures,
- the development of a strong public and private security culture, exploiting the potential of both the academic community and the public and private actors,
- upgrading the level of evaluation, analysis and prevention of threats, towards the security of information systems and infrastructures,
- the establishment of an effective framework for coordination and cooperation between public and private stakeholders,
- the active participation of the country in international initiatives and cyber-security actions of international organizations,
- raising awareness among all social stakeholders and informing users about safe cyber space usage,
- the constant adaptation of the national institutional framework to the new technological requirements as well as to the European guidelines, and lastly,
- the promotion of innovation, research and development on security issues.