Position of the Republic of Turkey for the purpose of the conference held by Forum for 21st Century on 29 November 2011 reflected in the first draft of the negotiation paper regarding the Global Cybersecurity Issues

The Republic of Turkey would like to thank Forum for 21st Century for initiating the discussion and organizing the conference on Global Cybersecurity issues and is prepared to express full support towards solving proposed topics on international level. After in-depth analysis of the draft proposed by Forum for 21st Century let us annotate it and include our suggestions as well.

In the section Notes:

- The Republic of Turkey, as member of global community, is fully aware of the importance of Cybersecurity issues solving and finds essential to create the global cooperation with related international partners in order to increase national as well as global cybersecurity capacity and capability. The Republic of Turkey utterly understands the global dependence on communication systems and sees the most important issues in establishing the coordinated approach of global society in cyberspace related issues.

- As far as the Republic of Turkey declares its effort to cooperate globally within several international organizations (ITU, IMPACT, ETSI), the European union (BEREC, ENISA), as well as within the scope of bilateral cooperation, it sees that the globally coordinated approach towards cybersecurity issues is needed.

- Information technologies, computers and various IT systems mainly, which we understand to be the main driving force of technological progress today, despite all their benefits which they naturally bring to society, at the same time create undesirable side effects that harm social systems, the right of persons and what is the most important, help criminals to commit even more sophisticated crimes as before. Moreover, rapid advance in technology affects the functions and improvement of all systems developed to increase the quality and standards of human living. Much like the majority of international actors, the Republic of Turkey is trying to cope with the problem through creating an appropriate legal and administrative substructure to minimize such criminal acts. Hereby, as far as we are concerned, the international community must inevitably devote all its effort in order to develop effective means of cyberspace control to avoid potential risk. Furthermore, the Republic of Turkey is in the conviction that countries benefiting from the Internet economy must play an active role in regards to cybersecurity related problems.

- The Republic of Turkey perceives cyberspace as borderless world and therefore agrees with Forum for 21st Century on the necessity to negotiate basic legal structure of cyberspace in order

to create stable international environment. The Republic of Turkey feels the necessity of protecting personal data, personal privacy, privacy of communication and ensuring network security against unauthorized access but equally, in order to ensure national security, public order and the smooth operation of public services finds important to set the certain limits in anonymity of Internet users.

In the section Proposals:

- Within the past decades the Republic of Turkey has witnessed and even experienced an increasing amount of cyber attacks. Prolific, ingenious, and ranging in style from large-scale worms to below the radar phishing attempts, cyber attacks have evolved to unprecedented levels of sophistication. We believe that in order to advance in the field of cybersecurity, the global society must act proactively and in synergy to change the rules of the game. Instead of being reactive to cyber attacks, the global society should become proactive and work on predicting threats and vulnerabilities and build the defense before threats materialize. The first step to do so, agreeing with Forum for 21st Century, is to create the legal basis with respect to usage and control of the Internet.

- Hereby, The Republic of Turkey would like to express full effort in creating the legal basis within cyberspace related issues. As far as the Internet usage is executed by multiple actors we propose to include public sector, private sectors policy makers, regulatory bodies, governmental bodies, international organizations and citizens into the definition of Internet users. The statutory definition should be proposed under discussion of all participants of the Conference.

- As far as the threats and attacks in the cyberspace affect not only our governmental or non-governmental organizations, but equally large masses and even more those who do not use information technologies and cause serious harm, the Republic of Turkey finds necessary to define system of sanctions for cyberspace related crimes. Firstly, we find important to discuss the definition of the cybercrime, which we perceive as every organized action or attack on any communication and information systems of our country or any private institution by taking control of their systems or web sites. Consequently, the sanctions should be defined as well. The Republic of Turkey is in the conviction that the exact definition of cybercrime sanction should be proposed under the discussion of all participants of the Conference but for the purpose of position paper and further discussion proposes following definitions of cybercriminal acts and their adequate sanctions. The Republic of Turkey perceive as cybercriminal whomever obtains program or data or another component from an automatic data processing systems illegally, whomever performs harmful activities within cyberspace with the purpose of harming anybody, whomever destroys, changes, deletes or prevents from operating an automatic data processing system, data or another component, completely or partially, for the purpose of harming anyone or deriving a benefit for himself or anybody else. Moreover, whoever whose computer is involved in committing a crime, is considered a criminal and thus shall be investigated. The

sanctions shall be graded from heavy fines up to imprisonment on the basis of cybercrime seriousness. The exact determination of fines and imprisonment shall be discussed by all the participants of the Conference.

- As a consequence of the recent large-scale and coordinated cyber attacks which were launched against government web site, the Republic of Turkey is concerned of the importance to protect its national defense systems and government bodies and therefore will consequently consider every attack of this category as an act of aggression which should be condemnable by international society. But in order to preserve the global peace we are not concerned of the retaliatory attacks or even armed forces to be needed. Instead, the agreed sanctions which shall be discussed by all the participants of the Conference should be conducted

- An internationally agreed method should be adopted for combating cybercrime as well as the unwanted actions such as the malware and spam. As far as the legal basis and terms with respect to usage and control of the Internet and local intranets is set, no exception shall be proposed to any Internet user. The Republic of Turkey is concerned that everybody, meaning every Internet user by agreed definition, is obliged to abide by the laws once they are set.

- International sharing of malevolent attacks, cyberterrorist groups within joint database is needed, equally as the workshops for experience share in order to share national and international success stories on fight against cybercrime, so that preventing a crime that occurred in any part of the globe from occurring again in other country, are needed. In order to do so, the multilateral cybersecurity exercises, such as the one which will be held in Istanbul 2012, are vital. The creation of global communication channel is needed in order to be able to get urgent information on cybercrime committed from a source in another country and so to be able to take the necessary measures.

- Furthermore we find important to protect not only national and international cyberspace related exclusively to governmental purposes of concerned parties, but our citizens as well. Therefore, we find necessary to develop legislation in fighting against IT crimes and unsecure as well as impropriate internet content. The Republic of Turkey is in the conviction that the impropriate internet content must be controlled and blocked by responsible bodies. The internet content must be supervised in order to make target groups aware of safer and responsible use of Internet. The legislation has been developed in Turkey to fight against ICT-related crime and illicit content online and as far as we are concerned, the international society must equally strengthen their law enforcement by training prosecutors and by providing the necessary means and equipment required to fight cybercrimes. Thereunto, we feel the necessity to develop international codes of conduct, under which content hosted by an Internet service provider in one country can be taken down by another country and organizations that are fighting harmful contents must play supportive role. The Republic of Turkey finds important to obligate the Internet service providers to provide secure internet usage service to their subscribers. Furthermore, the Internet

users need to be more educated of the threats and therefore the promoting of cybersecurity education is vital.

The Republic of Turkey finds aforesaid issues important to resolve and is open for further discussion.