COMMISSION ON LEGAL AFFAIRS AND INTERNATIONAL RELATIONS

5TH MEETING

ANKARA-2016

REPORT

"Combatting Cyber Crime: Development of the Legal Framework and Cooperation Among Member Countries"

INTRODUCTION

In the context of the global rise regarding the influence of information technologies the security of this field turns into a major challenge for the global community, every particular state and every particular individual. The continuous approximation and globalization of computer networks and the increased digital environment requires the awareness of new changes. The development of technology opens the door for brand new opportunities while the extended concept of crime spreads into the realm of information. The dependence on information technologies in almost every sphere of life is increasing year by year and, on a parallel with this, the problems related to the cyberspace and cybercrime become more and more globalized.

Consequently, cyber security risks pose some of the most serious economic and national security challenges. The concept of Cyber Crime becomes an important item on the agenda of countries accordingly.

In the light of the effects of technological advances and their implications, the Commission on Legal Affairs and International Relations held its Fourth Meeting on 29 April 2015 in Bishkek whereby member states of TÜRKPA decided to elaborate on the problems of combatting cyber-crime and the related legal framework from the perspective of legislation and parliamentary contribution.

In this respect the Fifth Meeting of the Commission scheduled to be organized in May 2016 in Ankara will concentrate on the theme "Combatting Cyber Crime: Development of the Legal Framework and Cooperation Among Member States" with the aim of discussing the draft Report and the Recommendations to be adopted at the Seventh Plenary Session of the Assembly to be held in Kyrgyzstan.

THE COMBAT AGAINST CYBERCRIME AND LEGISLATION AMONG TÜRKPA MEMBER STATES

1) New information technologies compress space and time while offering lightning-fast access to global knowledge and the possibility of instant exchange of information. Moreover in the contemporary world cyberspace touches practically everything and everyone. This magnitude of interconnectedness, however, also means that problems in one place have the potential to affect computers in another place and leads to issues of cyber security and concerns about cyber crimes along with the dynamism of the technological development.

2) Networks of electronic information flow take root in almost every sphere of life. The globally-interconnected digital information and communications infrastructure underpins almost every aspect of modern activities and provides critical support for the economy, civil infrastructure, public safety and national security.

3) On the other extreme, electronic computing and communication bring along some of the most complex cyber security challenges. The loose and lightly regulated digital infrastructure reaches out to many people thus increases the risk of certain vulnerabilities. Cyber attacks may transform vulnerabilities into destructive capabilities and cause serious outcomes.

4) The economies and national security are becoming more dependent upon information technology and its infrastructure. A structure consisting of networks supports the operation of all sectors of the economy, namely energy (electric power, oil and gas), transportation (rail, air, marine), finance and banking, information and telecommunications, public health, emergency services, water, chemicals, defence, industry, food, agriculture, and postal services. This structure also controls electrical transformers, pipeline pumps, chemical vats, radars, etc.

5) As all the organizations and institutions, first and foremost the state organs, have started offering many of their services on the internet environment the negative incidences faced

in this environment have the capacity to highly impact the personal, social and economic lives. The possible occurrence of such incidences may result in both material as well as moral damages. In this respect the cyber attacks to information networks could have serious outcomes on critical activities. Nowadays such ever-increasing risks set the stage for cyber crimes.

6) The existence of many concurrent initiatives in the fight against crime are carried out by various international organizations and institutions, also together with many NGO's, reveals the severity of the issue and the magnitude of the effort which needs to be exhausted in order to bring about the desired solution to the problem. Although the achievement so far is worth appreciation the necessity to gain more ground should be underlined.

7) In the studies carried out cybercrime is observed to be used as an umbrella concept emerging with the development of the information technologies or referring to the crimes committed with the utilization of IT technologies. Such crimes can be evaluated within a large spectrum including the ones directly targeting information technologies and products*(unauthorized access, damaging data or else information technologies etc.)* or committed with the utilization of information technologies*(fraud, ID, credit card etc.)* and related to content *(including storing or publishing or broadcasting child pornography or racist content etc.)*.

8) It is important to develop an innovative approach while tackling the issue of fighting against cybercrime which claims a long list. Cyber crimes and terrorism should be combatted not only on the digital front but the personal, society and political fronts as well.

9) Cyber security and policies that fight against cybercrimes include a wide array of items such as the mitigation of cyberthreats, international co-operation, urgent reaction to crimes, and legal sanctions on computer network transactions and information security which are all intertwined with the security and the stability of the global information and communication infrastructure.

10) Improving the vulnerabilities of the cyber environment and making the global community realize the full potential of the information technologies revolution are the fundamental responsibilities of governments. The governments in question should meet their economic needs and national security requirements on the one hand while investing more in research which would help to fight against crimes arising from cyber security gaps and violations of cyber security on the other. It is important to create a higher society awareness about threats and develop a holistic approach on cyber environment security.

11) TÜRKPA member states take measures, like in many other countries, in order to ensure cyber security and fight against cybercrimes. Here, member states are in a paradox of supporting safety, security and right of confidentiality on the one hand and protecting an environment that promotes innovation and technological development on the other.

12) Turkey, which has undersigned and ratified the European Commission's "Convention on Cybercrime", has prepared a draft "Resolution on the Execution, Management and Coordination of the National Cyber Security" with the efforts of the Ministry of Transport, Maritime and Communication. National Cyber Security Drills are carried out each year with the participation of Information Technologies and Communication Institution, Transport, Maritime and Communication Ministry and Turkish Scientific and Technical Research Institute (TÜBİTAK). "Cyber Security Institution" was established in July 2012 under the roof of TÜBİTAK-BİLGEM (Informatics and Information Security Research Centre).

13) When the current legislations on crimes committed in the field of information and internet are evaluated it is observed that the cyber security legal infrastructure in Turkey is supported by various laws and their related regulations such as the "Turkish Penal Code" numbered 5237, "Law on the Regulation of Publications and Broadcasting on the Internet and Combating Against Pertaining Crimes" numbered 5651,and the "Law on Electronic Signature" numbered 5070.

14) The Republic of Azerbaijan ratified the European Council's "*Convention on Cyber Crime"(Budapest Convention)* on 30 September 2009 and this went into effect with the signature of the President. Moreover, the country has become a signatory party of the European Commission's "Convention on the Protection of Individuals with regard to the Automatic Processing of Personal Data" dated 1981 and adopted with the law numbered 209. Moreover, laws on "Electronic Signature" and "Government Security" are other important legal frameworks in this field.

15) There are certain provisions in the Azerbaijan Penal Code which are directly related with cyber crime. (Section30, Articles 271, 272, 273) The Code includes provisions regarding unauthorized access, harmful content and the publication of programs. The same Code also involves penalty provisions related to insult, damage and defamatory publications pertaining to the Internet environment (Article 147 and 148). Moreover the 16th Section of the Law on Administrative Offence includes articles on "Utilization exploitation, distribution and protection of information within the framework of offense against the utilization, publication and protection of information". In addition to these, the law contains other articles about the violations conducted during the utilization of technology.

16. The new Penal Code of the Kazakhstan Republic signed by the President and which came into effect on 1 January 2015 has a separate section on punitive responsibilities pertaining to cybercrime. These include unauthorized access to computer data, illegal procurement, deletion or distortion of data, the dissemination of program and data which could be harmful for the society. Moreover, there are articles in the Penal Code that cover distribution of defaming and insulting information. Along with this, cooperation in combatting the cybercrime is carried out within the framework of the Commonwealth of Independent States (CIS) as well as other documents signed at the international level.

17. The Penal Code of the Kyrgyz Republic includes three articles regarding the "Crime on Information Technologies" (Section 28). Also within the framework of the Law on

Administrative Responsibilities of the Kyrgyz Republic, Section 21 concentrates on "Violations on the operations and utilization rules of telecommunication network and communication".

18. The adoption and implementation of national laws is not sufficient nowadays in order to combat cyber problems. Permanent laws and regulations should be adopted to fight against cyber crime and they should be amended when required. The reason for such laws is that information and communication networks is mostly under the ownership of and operated by the private sector both at the national and international level. In this respect public-private partnerships as well as international co-operations and norms will be the key elements of developing a strategy in order to be used for tackling the issues of cyber security problems.

19. Parliaments should raise their voice regarding their concerns about the cyber environments and combatting cyber crimes and contribute more to the increase of measures regarding cyber security which is an important means of sustainable development.

20. They should utilize the current legal mechanisms up to the highest level in order to create an extensive national awareness on cyber security and cyber crimes in an attempt to minimize and mitigate the damages of cyber attacks on the one hand and enable different circles to understand the benefits of this technological development on the other.

21. Special attention should be paid to develop mutual interaction and co-ordination between security institutions and judicial authorities in order to substantially support the related institutions in combatting cyber attacks and interventions.

22. The parliaments of the member states should pioneer the development of an international strategy for a holistic contra-action against cyber threats and cyber crimes and tailor a common international legal mechanism in order to harmonize the national penal codes in this respect.

23. It is important for laws on cyber security to be harmonized within the scope of international standards. Moreover it is also vital for them to play an active role in the approval of international agreements related to sustainable development based on scientific and technological advances.

International Activities

The global issues of cyber information and network security and the related crimes can only be tackled by an international co-operation strategy encompassing fundamental stakeholders and the creation of a cyber security culture. There is absolutely no denying the necessity of an international dialogue and co-operation to fight against cyber crimes that impact many countries concurrently.

24. One of the instruments in enhancing international cyber security is the 'Convention on Cybercrime', which was drafted by the Council of Europe, signed on the 23 November

2001 in Budapest and went into effect on 1 July 2004. The Convention provides guidance on how national legal frameworks should be harmonized and on the elements of international cooperation in fighting against cyber crime. This legal document is important both practically and politically. The Convention is an important tool regarding the European norms as it puts forth guidelines for developing respective national legal frameworks against cybercrime. Furthermore, accession to the Convention also facilitates international cooperation on operational matters, including extradition of cybercriminals. The Council of Europe, together with the private sector and Member States, has initiated a Global Project on Cyber crime to promote the Convention worldwide. The increasing number of countries joining this Convention forms a significant deterrence factor to criminal groups and governments sponsoring cyber attacks through proxies on their territories.

25. The Organization of Economic Cooperation and Development (OECD) inter-governmental Working Party on Information Security and Privacy (WPISP) develops policy recommendations and reports on the information society and resilience building. The governments monitor trends and facilitates information exchange through its network of experts from government, business and civil society. The OECD issues regular reports analysing the impact of technology on information security and privacy.

26. The Organization for Security and Cooperation in Europe (OSCE) initiated discussions on cyber security in 2008. Since then, the states participating in the OSCE have held several high level meetings on cyber security which focused on the main themes raising cyber security awareness, need for countries to build their capability to fight against cybercrime and terrorism and determining responsible state behaviour in cyberspace. The discussions held have not yielded a common point of view of what the exact role of OSCE will be as countries have varying interests and perspectives in approaching the subject of cyber security.

27. The UN General Assembly has adopted the resolutions relevant to cyber security. Under the UN Social and Economic Committee resolutions 56/121 “Combating the Criminal Misuse of Information Technology” and 57/239 “Creation of a Global Culture of Cyber security” were adopted. Both resolutions underline the importance of international cooperation, the need to eliminate safe shelters for cybercriminals, to encourage cooperation in law enforcement practices, as well as to enhance general awareness of cyber security issues. Resolution 64/422 “Globalization and interdependence: science and technology for development” also included the CIIP self-assessment survey for UN countries related to their cyber-protection. These initiatives have drawn attention to rising concern over cyber threats and helped to raise global awareness as well as encouraged UN countries to adopt the necessary measures to advance their national mechanisms for cyber security.

III. CONCLUSIONS

- ✓ It is evident that nowadays information related to people, institutions and organizations has soared tremendously both in volume and in diversity. Most of our information asset has been digitalized which has indeed facilitated public as well as

private business processes. This makes new services possible which were non-existent before. Besides all these facts, however, it is explicit that cyber security and cybercrimes pose a major problem and necessary measures be implemented fastidiously.

- ✓ In cyberspace borders have marginal importance. The vulnerabilities of the cyberspace due to its global dimension take place before the eyes of the world and can be accessed by anybody who has the adequate capability to exploit. Governments should emphasize certain facts that most of the time the cyber attacker and victims are in different countries, thus international inter-operability mechanisims are gaining importance to fight against cyber crimes and ensure security and that there is a necessity to increase coordination and co-operation between states together by emphasising the role which could be undertaken by international as well as regional organizations.

- ✓ Governments are in a paradox of supporting safety, security and right of confidentiality on the one hand and protecting an environment that promotes innovation and technological development on the other. Safeguarding cyber security is a fundamental problem for governments, businesses and the society both on a national and an international level.

- ✓ As a consequence of increasing number of attacks targeting cyber networks the development of legal regulations and legislations is pivotal in order to create a safe, secure and resilient cyber space and to support cyber security information and innovations in this respect. Transpositioning of international legal norms followed by their ratification at the national level is necessary step towards systematizing the fight against cyber crimes

- ✓ Public-private sector participation in the legislation preparation phase is the key factor. Public–private sector participation could take different formats when pursuing activities regarding awareness building, education, technological development, elimination of vulnerabilities and regeneration.

- ✓ The participation of professional experts from different disciplines like legal experts, technical people, various social scientists such as sociologist-psychologist etc. in the preparation of legislations for cyber security and the fight against cyber crime is important to ensure legal and technical infrastructure harmonisation.

- ✓ Our member states are ~~badly~~ in need of training more experts on cyber security. In this respect universities and education institutions providing opportunities for certification and thesis works will ensure great benefits and contribute considerably to the sound execution of the process. Legal and technical regulations should be prepared urgently without any discrimination between the public or private sector in order to protect the critical infrastructure. Supporting scientific research carried out in this respect will be highly beneficial,

- ✓ The promotion of cyber security culture should be promoted, supported and stringently implemented in order to combat cyber attacks on a global basis.

- ✓ TÜRKPA member states should work on the improvement of legal framework to fight against cyber crime and also closely co-operate in order to develop a mutual activity to protect information networks.