Doc.: GA40/LC40/REP/12

THE FORTIETH MEETING OF THE LEGAL AND POLITICAL AFFARIS COMMITTEE

REPORT *

THE ROLE OF PARLIAMENTS IN ENHANCING INFORMATION (CYBER) SECURITY IN THE BSEC MEMBER STATES

Rapporteur: Mr. Michael EMELYANOV, Vice-Chairman of the Committee, Russia

* *Text considered by the Fortieth Meeting of the Legal and Political Affairs Committee in Athens on 17 October 2012 and adopted by the Fortieth General Assembly in Baky on 27 November 2012.*

I. INTRODUCTION

In the context of the global rise in 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. New information and communication technologies open up completely new opportunities. Multilayered strands of information encourage growth of capacity building and target higher levels of development for the benefit of millions of peoples around the world. The dependence on information technologies in almost every sphere of life is rising year by year and, at the same time, the problems related to the cyberspace get more and more globalized. Consequently, cybersecurity risks pose some of the most serious economic and national security challenges in the 21st Century.

In light of these pervasive societal implications of the technological advances and their impacts, the Legal and political Affairs Committee at its Thirty Ninth Meeting in Tbilisi on 4 April 2012 took the decision to evaluate the problem of cybersecurity in the BSEC member states from the viewpoint of the parliamentary contribution to this process.

In this respect, the Fortieth meeting of the Committee in Athens on 17-18 October 2012 is dedicated to the issue of "The role of parliaments in enhancing information (cyber) security in the BSEC member states" with a view to elaborate the Report and the Recommendation for the discussions at the Fortieth Plenary Session of the General Assembly in Baky in November 2012.

The PABSEC has been attributing substantial attention to the issue of enhancement of information society and technological development in the framework of the Assembly activities and has adopted respective reports and recommendations[1] emphasizing the importance of ensuring safe and secure scientific, technological and innovative systems, as well as sharing the responsibility to contribute to addressing the potential challenges in this sphere in order to maximize the benefits and enhance the opportunities provided by information and communication technologies to all peoples in a secure environment.

The Report benefited from the contribution by the national delegation of Georgia, Romania Russia, Serbia and Ukraine. In addition, the reference material has been obtained by the PABSEC International Secretariat through the related Internet sources and publications.

II. THE ROLE OF PARLIAMENTS IN ENSURING INFORMATION (CYBER) SECURITY IN THE BSEC MEMBER STATES

1. In the contemporary world cyberspace touches practically everything and everyone. The worldwide web is a planetary information grid of systems enabling interoperability among computer networks. New information technologies compress space and time offering lightning-fast access to the body of global knowledge and the possibility of instant exchange of information. This magnitude of interconnectedness, however, also means that problems in one place have the potential to affect computers in another place and along with the dynamism of the technological development brings concomitant cyber security concerns.

---

[1] *Report and Recommendation 45/2000 on Development of Communications in the Black Sea Region; Report and Recommendation 60/2002 on Globalization: Challenges and Prospects for the PABSEC Member-States; Report and Recommendation 66/2002 on Information Society: the Role of New Technologies; Report and Recommendation 71/2003 on Black Sea Informational Alliance; Report and Recommendation 95/2007 on Cooperation in the field of high technologies among the BSEC Member States; Report and Recommendation 121/2011 on the Role of parliaments in providing legislative support for enhancing scientific and technological progress.*

2. Societies and individuals have never been as connected as they are today. Networks of electronic information flow are embedded in nearly every aspect of life. The globally-interconnected digital information and communications infrastructure known as cyberspace underpins almost every facet of modern activities and provides critical support for the economy, civil infrastructure, public safety and national security. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that govern the functioning of the systems in the sectors of agriculture, food, water, public health, emergency services, government, information and telecommunications, energy, transportation, banking and finance, and postal services, etc. Today cyberspace represents the backbone and control system of critical infrastructures as well as a platform for innovation and prosperity.

3. On the other extreme, electronic computing and communication poses some of the most complex cybersecurity challenges. With the broad reach of a loose and lightly regulated digital infrastructure greater are the risks for certain vulnerabilities. The healthy functioning cyberspace is a beneficial for development and progress while cyber attacks may transform vulnerabilities into destructive capabilities and cause serious consequences. Countering such attacks requires the development of robust capabilities to adequately address the vulnerabilities in order to ensure that individual citizens and larger community of nations realize the full potential of the information technology revolution. To this end, enhanced cyber threat analysis is needed to address long-term trends related to the cyber threats and vulnerabilities.

4. Cyberspace security is one of the important components of the national securities. Safe and secure cyberspace is a difficult strategic challenge that requires coordinated and focused effort from the entire society - state, private sector and people. Cybersecurity policies need to include strategies, policies and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.

5. It is important to develop innovative approach to address a long list of cybersecurity priorities. Another challenge is providing better security for data flowing over various routes on the Internet. All engineering approaches to achieving security must be accompanied by methods of monitoring and quickly detecting any security compromises. Success of the cybersecurity system depends upon understanding the safety of the whole system, not merely protecting only some of its individual parts. Consequently, cybercrime and cyber terrorism must be fought on the personal, social, and political fronts together with the digital front.

6. It is the fundamental responsibility of the governments to address vulnerabilities in cyberspace and ensure that global community realizes the full potential of the information technology revolution. Without major advances in the security of these systems or significant change in how they are constructed or operated, it is doubtful that the states can protect themselves from the growing threat of cybercrimes and intrusions. The governments need to increase investment in research that will help address cybersecurity vulnerabilities while also meeting economic needs and national security requirements.

7. The governments need to integrate competing interests to derive a holistic vision and plan to address the cybersecurity related issues confronting the countries. It is important to

develop policies to mitigate cybersecurity-related risks. It is also important to develop more public awareness of the threats and risks and to ensure an integrated approach toward the need for security in cyberspace.

8. The PABSEC member states, as many other countries worldwide, embarked upon comprehensive measures to meet the cyber security challenges. They face the dual challenge of maintaining an environment that promotes innovation and technological development while also promoting safety, security and privacy rights.

9. In Romania, for example, in 2008 the Parliament passed the Law no.298 on combating information crime, however, this law was rejected in 2009 by the Constitutional Court. It was re-launched to public debate but in 2011 the Senate rejected again this law. In 2012, the Legal Committee of the Chamber of Deputies made two amendments to this law and it passed and was promulgated by the President. In its new version, Law No 298/2012 on the retention of the general or processed data by the public telephone and internet network providers, it is important that all telecommunication and Internet providers to stock all the data traffic (but not the content of the calls and messages) for six months, and on official demand to send these data to the national security authorities.

10. In order to meet the tasks in the field of enhancing information security in Russia the *Doctrine on Information Security of the Russian Federation* was approved by the President of the Russian Federation. According to paragraph 1 of the Doctrine, the Information Security of the Russian Federation means the state protection of its national interests in the information sphere together with the balanced interests of individuals, society and the state. Information security is an integral part of national security of Russia. In 2008, the President of the Russian Federation approved the *Strategy for the development of the Information Society*. Ensuring national security in information sphere is one of the priorities for the country. The scope of the management in the sphere of national security is determined by: The Federal Constitutional Law “On the Government of the Russian Federation" (art. 23), the Federal Constitutional Law “On the Judicial System of the Russian Federation”, the Federal Constitutional Law “On the Commissioner for Human Rights in the Russian Federation” (art. 24); The Federal Law “On the Federal Security Service”, the Federal Law “On Security”, the Federal Law “On the Public Prosecution of the Russian Federation”, the Federal Law “On Police”, the Federal Law “On the Accounts Chamber of the Russian Federation”, etc. The Decree of the President of the Russian Federation of 30.11.1995 № 1203 (as amended on 21.09.2011) “On Approval of the List of Information Classified as State Secret” determines the list of the information in the field of military policy, foreign policy, economic, intelligence, counterintelligence and operational-search activities of the state, which may affect the security of Russia. Measures to promote and protect human rights and freedoms, rights of organizations in the field of information are determined by the Law “On Personal Data”, the Law “On the Mass Media”, the Law on “the protection of children from information harmful to their health and development”, the Law “On communication”, the Law “On licensing certain types of activities”, the Civil Code of the Russian Federation, etc.

11. The existing legal framework regulating the field of information security in Serbia includes the Law on Data Confidentiality (“Official Gazette of the RS”, No 104/09), the Law on Personal Data Protection (“Official Gazette of the RS”, No 97/08 and 104/09), the Law on Electronic Signature (Official Gazette of the RS, No 135/04), the Law on Organisation and Competences of State Authorities in Fight against High-tech Crime

(Official Gazette of the RS, No 61/05, 104/09) and Criminal Code (Official Gazette of RS, No. 85/05, 88/05, 107/05, 72/09 and 111/09). The legal framework is comprised of both the Law on Electronic Communication (Official Gazette of RS, No. 44/10) and the Law on Defence (Official Gazette of RS, No. 116/07, 88/09, 104/09). The Law on Data Confidentiality regulates the system for defining and protecting confidential data being of interest for Serbia's national and public security, defense, internal and foreign affairs, protection of foreign confidential data, access to confidential data and termination of confidentiality commitment, competences of authorities and their monitoring of the implementation of the Law, and responsibility for not performing the obligations stipulated by the Law, and other issues of importance for data confidentiality protection. The Strategy for the Development of e-government in the Republic of Serbia for the period 2009-2013, with the Action Plan for the implementation of the activities stipulated by the Strategy for the Development of e-government in the Republic of Serbia for the period 2009 – 2013 (Official Gazette of RS. No.83/09 and 5/10), as one of the e-government development principles, envisages the information security principle, and the Action Plan for the implementation of the Strategy envisages the development of the Draft Law on Information Security.

12. With regard to the cyber security issue in Turkey, who signed the Council of Europe Convention on Cybercrime on 10 November 2010, the Ministry of Transportation, Sea and Communications have prepared the draft Resolution on implementation, management and coordination of the national cyber security measures. Information Technology and Communications Authority in cooperation with the Ministry of Transport, Sea and Communications and Scientific and Technological Research Council of Turkey (TUBITAK) and with participation of other ministries every year organizes National Cyber Security Exercise events. In July 2012 in the framework of the TUBITAK-BILGEM Center of Research the Cyber Security Institute was created.

13. Viable laws and regulations concerning cybersecurity need to be adopted and modernized whenever and wherever necessary but only the adoption and implementation of the national laws is not enough to meet the contemporary cybersecurity challenges. Information and communications networks are largely owned and operated by the private sector, both nationally and internationally. Thus, addressing cyber security issues requires a public-private partnership as well as international cooperation and norms that should be a key component of strategies to secure cyberspace. The dynamics of cyberspace will require adjustments and amendments to the strategies over time.

14. The National Cybersecurity Strategy of Georgia (2012-2015) has been drafted and awaits its final adoption. The Strategy identifies steps that state, private companies and organizations, and individual citizens can take to improve collective cybersecurity and helps to reduce vulnerability to the attacks against critical information infrastructures. The Strategy implies to enhance law enforcement capabilities for preventing and prosecuting cyberspace attacks; to create a process for national vulnerability assessments to better understand the potential consequences of threats and vulnerabilities; to secure the mechanisms of the Internet by improving protocols and routing; to foster the use of trusted digital control systems/supervisory control and data acquisition systems; to reduce and remediate software vulnerabilities; to improve the physical security of cyber systems and telecommunications; to prioritize cybersecurity research and development and assess and secure emerging systems. The Strategy also places particular focus on the awareness, education, and training and international cyberspace security cooperation in order to facilitate information sharing, reduce vulnerabilities, to coordinate and redirect research

and to define and develop strategies to deter hostile or malicious activity in cyberspace. It is also important to strengthen cyber related counterintelligence efforts, to improve coordination for responding to cyber attacks, to facilitate dialogue and partnerships among international public and private sectors focused on protecting information infrastructures and promoting a global culture of security, to foster the establishment of national and international watch-and-warning networks to detect and prevent cyber attacks as they emerge, or to ensure that their laws and procedures are at least as comprehensive and to accede to the Council of Europe Convention on Cybercrime.

15. National Security Strategy of Ukraine "Ukraine in a Changing World" ensures information security and implies creation of national cybersecurity system. Information security is one of the priority policy issues within the Law of Ukraine "On information". Activities in the field of ensuring security of information and telecommunication systems are regulated by the Law of Ukraine "On Protection of information in information and telecommunication systems" adopted in 2005. The Law of Ukraine "On State Service of Special Communication and Information Protection of Ukraine" was adopted on 23 February 2006. This body is guided by the provisions of the Model Law on informatics and information as well as of the Cooperation Agreement between the member states of the Commonwealth of Independent States in the fight against computer crimes. Ukraine has also joined the Council of Europe Convention on Cybercrime.

16. One of the six priorities in the Strategy for the Information Society Development of the Republic of Serbia by 2020 (Official Gazette of RS, No.51/10) is the information security. The ISD Strategy emphasizes that an appropriate level of information security in all forms of information and communication technologies application is one of the prerequisites for the establishment of a sustainable information society. The first priority in the field of information security is the improvement of legal and institutional framework for information security. The Law on Data Confidentiality envisages adoption of a by-law closer regulating information and telecommunication systems protection measures, but nevertheless, there is the need to regulate this issue by a law since it is necessary to establish an institutional framework and competences of some bodies, such as the accreditation of ICT systems for manipulating confidential data, issuing authorizations for cryptographic products, and for inspection surveillance in the field of information security. The conditions that ICT systems for confidential data manipulation need to meet are such that it is necessary to establish a system for ex-ante control of the conditions in order to provide a satisfactory level of their application in practice. A special working group established by the Ministry of Culture, Information, and Information Society, developed a Draft Law on Information Security aimed at enhancement of information security and regulating complete information security area, and in particular the following: Information security in ICT systems for confidential data manipulation (accreditation of ICT system for confidential data manipulation, the use of cryptographic products for the purpose of confidential data protection, protection of information and communication systems against compromising electromagnetic radiation, and deferral of duties demanding expertise in the abovementioned fields to the National Security Council Office and Ministry of Defence); Information security in other ICT systems in public authorities; Coordination of prevention of and protection against security risks in all information and communication systems in the Republic of Serbia; National communication networks (position and operation of the Academic Network of Serbia, and the position and operation of the National Communication Network); Information Security Inspection. The Draft Law is currently being harmonized with state

authorities whose scope of work involves the issues regulated by the Law. The Regulation on security and protection of information systems of state authorities (Official Gazette of SRS No.41/90) sets out organizational and technical measures to secure and protect information systems of state authorities based on the computers application.

17. At the national level the National Program of "Information Society (2011-2020)" has been adopted in Russia, which states that due to the lack of an integrated approach to the solution of the problem of the formation and development of the information society the threats to security in the field of the information society gradually increase. The priorities of the sub-program 5 "Security within the Information Society until 2015" include the following measures: to establish a system for determining and monitoring of the level of the real protection of the information society from terrorism in the field of information; to create and promote domestic safe technologies for storage and processing of large volumes of unstructured data, including the creation of domestic protected functional services and process components that provide storage and processing of large volumes of unstructured data, and their continued support and development that permits to increase the volumes of unstructured data processing; to develop and integrate with other departmental and inter-agency information control systems of the common data bank regarding the issues of the fight against terrorism; to create a national software platform (complex domestic software solutions - modules built on the basis of common technology, allowing for the development of new products by the layout and configuration of the ready modules and the development of the new ones), to develop the supercomputing and grid technologies. By the Decree of the President of the Russian Federation of 8 February 2012 №146 On Federal structures of the executive power responsible for the sphere of ensuring information security within the information systems created with the use of supercomputers and grid technologies the federal authorities to ensure the security of information in information systems associated with the use of supercomputers and grid technologies have been established – the Federal Security Service of the Russian Federation and the Federal Service for Technical and Export Control (FSTEC Russia). In the framework of the powers attributed to the "FSTEC Russia" is the function to ensure information security within the information and telecommunication infrastructure that is essential for national security in the sphere of information.

18. Important responsibilities in cyberspace security approaches include: developing a comprehensive national plan for securing the key resources and critical infrastructure; providing crisis management in response to attacks on critical information systems; providing technical assistance to the private sector and other government entities with respect to emergency recovery plans for failures of critical information systems; coordinating with other agencies of the government to provide specific warning information and advice about appropriate protective measures and countermeasures to state, local, and nongovernmental organizations including the private sector, academia, and the public; and performing and funding research and development along with other agencies that will lead to new scientific understanding and technologies in support of security. Coordination of state, local, and nongovernmental organizations including the private sector, academia, and the public is very important.

19. Protecting the widely distributed assets of cyberspace requires the efforts of many the countries and their citizens. The governments alone cannot sufficiently defend cyberspace. Most critical infrastructures, and the cyberspace on which they rely, are privately owned and operated. The technologies that create and support cyberspace

evolve rapidly from private sector and academic innovation. Joint actions are necessary as technologies advance, as threats and vulnerabilities change, and as the understanding of the cybersecurity issues is shaped. Coordinated efforts are necessary to identify and remediate the most serious cyber vulnerabilities through collaborative activities, such as sharing best practices and evaluating and implementing new technologies.

20. Investments in cyberspace security will foster a marketplace for more secure technologies through large procurements of advanced information assurance technologies. It will help to ensure that computer systems and networks are secure. Countries must be capable of safeguarding and defending its critical systems.

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

22. Thus, cyber attacks on information networks can have serious consequences upon critical operations. Countering such attacks requires the development of integrated capabilities in order to reduce vulnerabilities. Vulnerability assessment and remediation activities must be conducted at all times with the aim to have permanent security audit conducted by trained professionals and to create a multilayered defense and a resilient network to remedy the most serious vulnerabilities. Managing threat and reducing vulnerability in cyberspace is a particularly complex challenge. Cyberspace security requires action on multiple levels and by a diverse group of actors.

23. Despite increased awareness around the importance of cybersecurity and the measures taken to improve the capabilities, cyber risks continue to underlie information networks and systems. Unfortunately, no single strategy can completely eliminate cyberspace vulnerabilities and associated threats. Securing cyberspace is an ongoing process, as new technologies appear and new vulnerabilities are identified.

Role of the national parliaments

24. The national parliaments have to add their voice to the concerns of securing cyberspace and bring their contribution to increasing measures for ensuring information security in the BSEC member states as an important means in the pursuit of sustainable development.

25. It is a crucial task of the national parliaments to oversee government action in developing a comprehensive national plan for securing key resources and critical infrastructures, including information technology and telecommunications systems in order to prevent possible cyber attacks.

26. It is also important to continue and upgrade legal approximation of the respected legislation with the international standards in the sphere of cyber security.

27. Parliaments have to carefully set funding priorities in science, technology and innovation in order to promote, stimulate and improve research to meet the national priorities and strategic objectives in the sphere of cyber security.

28. Parliamentarians should also make maximum use of the available legal mechanisms to promote a comprehensive national awareness program to secure cyberspace in order to

make the benefits of the technological development widely understood and supported, while to minimize and mitigate the damage from possible cyber attacks.

29. It is also necessary to promote setting up of so-called system of "deep defense" composed of multilayer security systems using the measures for protecting information resources and preventing unauthorized access to the information.
30. It is also necessary to promote work on the establishment of mutually acceptable terms of functioning network of international centers for prevention and counteracting the cyber attacks with the aim to develop viable mechanisms for exchange of information and experience in cyber security field.
31. Particular attention should be paid to interaction and coordination among the law enforcement agencies, intelligence agencies, the judicial system, in order to adequately equip them in the fight against cyber attacks and intrusions.
32. Parliaments have to take lead in developing an international strategy for the integrated counteraction against the cyber threats and to elaborate common international legal mechanisms with the aim to harmonize the national criminal legislations in this respect.
33. Parliaments have to promote elaboration of the regulations with the aim to ensure that private sector is supported for well coordinated implementation of practical measures to ensure information security by means of creation and application of the most advanced technologies.
34. Parliaments have also to put effort to enhance framework for participating in the development of international standards in the field of information security for prediction, early and timely diagnostics, scientific and technological expertise, timely identification of new risk factors in order to reduce vulnerabilities and counteract the threats within the cyberspace.
35. Parliaments should also take an active role in the ratification of international instruments pertinent to sustainable development on the basis of scientific and technological progress and to incorporate their provisions in national legislation.
36. The Parliamentary Assembly of the Black Sea Economic Cooperation has to provide support to the actions undertaken by the BSEC to expand multilateral cooperation in the sphere of science and technology and to establish closer contacts with the BSEC Working Group on Science and Technology.

International cooperation

37. One of the major instruments in enhancing international cybersecurity is the 2001 Council of Europe Convention on Cybercrime. It provides guidance on how national legal frameworks should be harmonized and on the elements of international cooperation in fighting cybercrime. The importance of this legal instrument is both practical and political. As it sets guidelines for developing respective national legal frameworks against cybercrime, it is a useful tool for exporting European norms on the issue. Furthermore, accession to the Convention also facilitates international cooperation on operational matters – including extradition of cybercriminals. The political importance of the Convention lies in the fact that it is the only binding international agreement on cybersecurity issues, and accession to the Convention shows that a country is ready to harmonize its internal laws and to take the fight against cybercrime seriously. The Council of Europe, together with the private sector and Member States, has launched a Global Project on Cybercrime to promote the Convention worldwide. The increasing

number of countries joining this Convention provides for a significant deterrence to criminal groups and governments sponsoring cyberattacks through proxies on their territories.

38. The Organization of Economic Cooperation and Development (OECD) intergovernmental Working Party on Information Security and Privacy (WPISP) develops policy recommendations and reports on the information society and resilience building. Through its network of experts from government, business and civil society, it monitors trends and facilitates information exchange. The OECD issues regular reports analyzing the impact of technology on information security and privacy. The OECD report on CIIP practices among its Member States is one of the best comparative documents in the field, comprising analyses of best practices, organizational structures and the regulations of the most advanced economies. The OECD has started a research series on "Global Shocks" with a report on "Reducing Systemic Cybersecurity Risks". As cybersecurity in the OECD context has predominantly been a sub-category of economic and technology policy, the rise of cybersecurity as a subject for national security has somewhat reduced its importance for the OECD's agenda. The OECD's contribution to collecting and exchanging the best practices in building national information infrastructure resilience could be useful for the countries who are searching for the right model for their respective national cybersecurity organizations.

39. The Organization for Security and Cooperation in Europe (OSCE) started discussions on cybersecurity in 2008. Since then, the states participating in the OSCE have held several high level meetings on cybersecurity, where central themes of the discussions have included raising cybersecurity awareness, a need for countries to build their capability to fight against cybercrime and terrorism, as well as determining responsible state behavior in cyberspace. OSCE countries have very different interests and angles in approaching the subject of cybersecurity, and consensus has not emerged on what the exact role of the OSCE will be in the debate. The Joint Meeting of the OSCE Forum for Security Cooperation and the OSCE Permanent Council held in June 2010 decided that discussions will continue on strategic cybersecurity issues.

40. The UN General Assembly has adopted the resolutions relevant to cybersecurity. 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 Cybersecurity" were adopted. Both resolutions stress the importance of international cooperation, the need to eliminate safe havens for cybercriminals, to encourage law enforcement cooperation, as well as to enhance general awareness of cybersecurity issues. Resolution 64/422 "Globalization and interdependence: science and technology for development" also included the CIIP self-assessment survey for UN countries to advance 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 cybersecurity. The UN resolution 64/386 "Developments in the field of information and telecommunications in the context of international security" adopted in 2009 proposes to continue discussions on cybersecurity in the context of international security and to convene a group of experts that would issue further recommendations. In 2010 the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security produced a report that calls on countries to collaborate to improve information security and international cooperation. The report offers recommendations for further dialogue among states to reduce risk and

protect critical national and international infrastructures. It should also be noted that on 12 September 2011 the Permanent Representatives of China, Russia, Tajikistan and Uzbekistan to the UN sent a joint letter to UN Secretary-General with the request to circulate the draft of the "International Code of Conduct for Information Security". The main task of the Regulations is to elaborate the code of responsible behavior of the states in the sphere of the international information security with due regard to the military, political, criminal and terrorist challenges and threats. The document implies the counteraction towards use of information and communication technologies with the aim not corresponding to the tasks of establishing the international stability, peace and security. It also envisages observance of human rights and fundamental freedoms in the information space, respect of sovereignty, territorial integrity and political independence of all states as well as establishment of multilateral transparent and democratic international mechanism of regulation of the Internet. The Russian Federation in its capacity as one of the elaborators of the project calls on all interested parties to take active part in the discussions on this issue. This initiative may become a first step towards elaboration of the universal document of the UN – a Convention, which will focus on providing a comprehensive international information security, implying to the greatest extent the interests of the world community.

41. NATO developed its first Cyberdefense Policy in 2007, which constitutes the basis for other strategic documents and activities in the field. NATO was the first international organization to adapt quickly to the new strategic environment, and recognized that non-traditional security threats are central to the national security of the Allies. NATO's 2007 Cyber Defence Policy set objectives for bolstering the cyberdefense capabilities of NATO's own networks, and established initial mechanisms for consultations with Member States in cyberdefense issues. The NATO Computer Incidence Response Capability Technical Centre serves as a central technical authority on operational cyberdefense issues. The cyberdefense MOU-s facilitate regular consultation, information sharing, and describe how the NATO Rapid Reaction Teams can support individual Allies in case of cybercrises. The new NATO Strategic Concept adopted at the Lisbon Summit in November 2010 stresses that NATO must accelerate efforts to respond to the danger of cyberattacks. The Lisbon Summit commits NATO and the Allies to address the new security challenges and, among other objectives, draws a very ambitious roadmap for the cyber agenda of the Alliance. It includes bringing all NATO military and civilian bodies under central protection, introducing the cybercomponent to the defense planning process and accelerating information sharing and early warning capabilities. In June 2011 NATO Defence Ministers approved the NATO Policy on Cyber Defence that sets a vision for efforts in cyber security and associated Plan of Action. At Chicago in May 2012 Heads of State and Government took decision to bring all NATO networks under centralized protection under the NATO Computer Incident Response Capability (NCIRC).

42. The EU has approached the issue of cybersecurity in a fragmented manner, where parallel policies have sometimes been launched with different overlapping themes. Most of these initiatives have direct or indirect relevance to EU Members' preparedness to withstand serious cyberattacks, as they address the means and methods of cyberattacks, as well as the consequences of these attacks. In 2007, the European Commission issued the communication "Towards a general policy on the fight against cyber crime" that sought to improve operational law enforcement cooperation, political cooperation and coordination among Member States. It also promoted political and legal cooperation with

third countries as well as awareness -raising, training, research and a reinforced dialogue with industry for possible legislative action. “Counter-radicalization”, i.e. the ability to monitor and address violent ideological material, has long been a focus of the EU counter-terrorism strategies. In December 2009, the “Stockholm Program” was accepted, which represented a significant step in the “internal security” agenda of the European Union. Besides calling for a European Internal Security Strategy, the program made a number of references to cybersecurity, including: the need to develop better and more resilient network information security measures, a better ability to deal with cyberattacks, the importance of all Member States ratifying the Cybercrime Convention, and the importance of information exchange, both between governments as well as with the private sector. Adopted in October 2010, the new EU Internal Security Strategy aims to raise the level of security for citizens and businesses in Cyberspace and attempts to deal with cybercrime issues head-on. Three specific proposals in the strategy include the establishment of an EU cybercrime Centre by 2013, the establishment of a network of Computer Emergency Response Teams (CERTS) in all EU institutions by 2012 (as well as the cooperation of these institutions with law enforcement), and the launching of a European information sharing and alert system (EISAS) by 2013. In 2010 the Council agreed on a Cybercrime Action Plan that also called for Europol’s European Cybercrime Platform (ECCP) to be strengthened, for better support for cross-border education of law enforcement agencies, and for better coordination internationally. Europol has often featured as the focus of many of the new Council decision and recommendations, and the ECCP has recently been upgraded to a full-time initiative, with a number of subordinate initiatives. An important organizational initiative, the European Cyber Crime Centre, has been proposed and agreed upon a number of times since first being discussed around 2007. An agreement was reached in June 2010 to set up the European Union Cybercrime Task Force as a precursor organization to the actual establishment of the Centre.

III. CONCLUSIONS

43. In the past few years, threats in cyberspace have risen dramatically. Given the growing reliance on cyberspace in almost every sphere of life, countries and the international organizations have started to develop policies designed to protect against the disruption of the operation of information systems and ensuring cyberspace security response.

44. As world rapidly becomes dependent on the Internet, the commitment to the development of more secure cyber environment becomes imperative. There are endless possibilities of the World Wide Web in private and professional environments. The internet is used to communicate, to do research, to trade and to work. At the same time, industrial control systems, used in vital sectors of economy, are also linked to the internet. This adds a new dimension to the internet dependency: safety and security.

45. A safe internet system is crucial for economies and societies. Information flows continuously. The infrastructure that makes up cyberspace is global in its design and development. In cyberspace national boundaries have little meaning. Because of the global nature of cyberspace, the vulnerabilities that exist are open to the world and available to anyone, anywhere, with sufficient capability to exploit them.

46. Countries face the dual challenge of maintaining an environment that promotes innovation and technological development while also promoting safety, security and privacy rights. Ensuring cyber security is now a central challenge for the states, business and society both at national and international level.

47. Each country needs to determine relevant state behavior in cyberspace, invest in skills and education to build capacity of people working in information security area, and ensure cooperation among the public, private and academic sectors. It is imperative to apply cybersecurity threat and vulnerability reduction programs as well as cyberspace security awareness and training programs.

48. In order to protect the Internet and other ICT networks from threats and vulnerabilities and for further cooperation at national and international levels, the national parliaments have to promote the need for enhanced coordination and cooperation among the states in combating criminal misuse of information technologies, and, in this context, stress the role that can be played by the international and regional organizations.

49. The growing number of attacks on cyber networks has become one of the most serious security threats that challenge to keep civilian networks secure and to secure the cyberspace. That calls for the need for a safe, secure, and resilient cyber environment, and promotion of cybersecurity knowledge and innovation.

50. Public-private engagement is a key component to secure cyberspace. Public-private engagement can take variety of forms to address the problems of awareness, training, technological improvements, vulnerability remediation and recovery operations. Activities should also support research and technology development that will enable protection of networks and systems, indications and warnings, and protection against organized attacks.

51. It is imperative to ensure confidence and security in the use of information and communications technologies that represent the main pillars of the information society. Global culture of cyber-security needs to be encouraged, promoted, developed and vigorously implemented.

52. BSEC member states have to cooperate closer in order to develop a common legal framework for combating cyber crime but also a joint action for the protection of information networks and BSEC member states that are not members of the EU should adopt a common legislation with the BSEC member states that are EU members.

53. Countries have to invest in the cutting-edge research and development necessary for the innovation and discovery to meet the digital challenges of our time; to make proportional investments in network security, technical training, cybersecurity awareness and digital literacy.

54. The increasing volume and sophistication of cyber security threats, such as scams, data theft, and other online vulnerabilities, demand that users remain vigilant about securing their systems and information. It is important that each user understands the risks as well as the actions to help protect information networks and cyber systems.

55. Within an interconnected world in which there are myriad of devices, such as computers, smart phones, tablets, everyone share the same communication channels, and every particular consumer has its role to play in securing their part of cyberspace. Protection of Internet and other digital assets is a shared responsibility of every user of every type. As people enjoy the Internet and appreciate the benefits it brings to their lives, it is necessary to remember that the cyber security starts with each individual user’s responsible behavior in the cyber world.