PARLIAMENTARY ASSEMBLY OF THE BLACK SEA ECONOMIC COOPERATION
PABSEC

INTERNATIONAL SECRETARIAT

Doc.: GA51/LC51/REP/18

REPORT*

STRENGTHENING COOPERATION IN CYBERSECURITY IN THE BSEC MEMBER STATES

Rapporteur: Mr. Eldar Guliyev, Vice-Chair of the Committee, Azerbaijan

* *Text considered by the Fifty First Meeting of the Legal and Political Affairs Committee in Tirana 19 June 2018 and approved by the Fifty First General Assembly in Tirana on 20 June 2018*

I. INTRODUCTION

1. The challenges of the 21st century call for the development of new information and communication technologies (ICT) that open up broad opportunities for human activity. Complex, multilayer information flows contribute to the development and strengthening of human potential and aim at achieving a high-level development for the benefit of millions of people around the world. The new information technologies compress space and time and create the opportunity for broader access to global knowledge and information exchange.

2. Leading countries of the world have already shifted to the use such concepts as e-government, e-signature, digital economy, etc. Computers, smartphones, tablets and other devices are carriers and collectors of important state and confidential information, and also allow the exchange of information in a few seconds, conduct state and banking business, make purchases on the Internet, pay for services with a credit card or virtual money. These devices also carry valuable information: government documents, information, other important confidential data. Year after year increases dependence of vital sectors on information technologies practically in every sphere and therefore the problems related to cybersecurity acquire global importance.

3. Occurrence of cyberterrorism, cybercrime and cyberattacks increases every day along with the ICT development and technological progress. This generates concern of countries, large corporations and population regarding cyberterrorism, cybercrime and cyberattacks committed by unknown hackers attacking strategically important computer networks and programs.

4. Therefore, the Legal and Political Affairs Committee decided at its Fiftieth meeting in Rostov-on-Don on 25 October 2017 to address the problem of cybersecurity in the BSEC Member States. The Fifty First Meeting of the Committee is devoted to the issue of "Strengthening Cooperation in Cybersecurity in the BSEC Member States" and the preparation of the Report and the Recommendation for discussion at the Fifty First Plenary Session of the General Assembly in Tirana in June 2018.

5. The PABSEC already considered the issue of cybersecurity in 2012 at the Fortieth Plenary Session of the General Assembly in Baku, focusing on the role of parliaments in strengthening cooperation in this field. The adopted documents emphasize the importance of sharing the responsibility to contribute to addressing the potential challenges and to maximize the benefits and enhance the opportunities provided by information and communication technologies in a secure environment as an important element in achieving sustainable development. These documents also emphasize that parliaments should prioritize funding for science, technology and innovation to stimulate and expand research in order to adequately respond to these threats and to duly address them.

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

II. STRENGTHENING COOPERATION IN CYBERSECURITY IN THE BSEC MEMBER STATES

7. Cybersecurity is a combination of instruments and strategies to ensure security of information networks and data from unauthorized access. Elements of cybersecurity include: access control, training of personnel, reporting, assessment of potential risks,

penetration testing and demand of authorization. One of the most problematic elements of cybersecurity is the rapid and ever-changing nature of threats to the security of the telecommunications industry. The traditional approach concentrates resources on the most important components of information security and provides protection against threats of hacker attacks. Therefore, cybersecurity today is a necessity for further development and consolidation of the information society.

8. Cyberspace consists of global computer networks and these networks are connected and controlled through cables, fiber optic cables and wireless connections. Cyberspace interconnects the Internet and transnational networks transferring data in different areas. There are also systems that receive and control data by connecting machines through control panels and radio frequency identification, which are called Internet of Things. Threats in cyberspace are various as cyberspace is itself and it requires thorough examination and counteraction.

9. In the world today, cyberspace is a concern for each and every one who is a part of global information system connecting computer networks. Interconnected digital information and communication infrastructure form the foundation of almost every sphere of contemporary life and provides significant support to economy, public infrastructure, public and national security. Hundreds of thousands of interconnected computers, servers, routers, switches and fiber optic cables support functioning of systems in the agriculture, food, water, public health, emergency services, management, information and telecommunication, energy, transport, banking and finance sectors, postal services, etc. All these require permanent examination and monitoring of these systems.

10. Social media is one of the rapidly developing sphere that gives people the new opportunities for communication and information exchange. However, here also it is equally important to ensure cybersecurity to protect systems from unauthorized use of databases and accumulated personal information.

11. Communities and people have never been so interrelated to each other as they are today. Networks of electronic information flows are rooted in almost every sphere of life. Today, cyberspace is the main system controlling vital facilities. The wide coverage of extensive and easy managed electronic infrastructure the vulnerability risks increase. In the context of the global growth of ICT influence the information security becomes the main challenge for the world community, each individual state and each individual person. Therefore, one of the main tasks is to minimize the risks in this area.

12. The existing magnitude of interconnectedness 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 cybersecurity concerns. Modern hackers have an unprecedented variety of tools and ability to apply them with maximum efficiency. Constant growth of online traffic capacity and quantity of mobile devices generates a wide choice of targets and the means for their destruction. In this case, it is necessary to build effective protection scheme against permanently developing and complicating threats. Malicious programs allow attackers to gain quick access to an unprotected device and steal data. Modern technologies allow to send and control illegal flow of finances that is the basis of modern terrorism. A modern terrorist can cause significant damage using a simple keyboard. Therefore, strengthening of cybersecurity and security of information and communication technologies is an important task for the whole world. Consequently, with the increase of terrorist attacks their prevention and elimination methods to be developed.

13. Security researchers from Cisco company published the Information Security Report for 2018, which provides data and analysis of cybercrime in recent years. According to the Report, one of the most significant trends in 2017 was the evolution of malicious software allowing penetration to data and their elimination. Researchers also draw attention to the emergence of cyberthreats that can bypass complex sandbox environment and use encryption to avoid detection. According to Cisco, as of October 2017, about 50% of global web traffic was transmitted in encrypted form. At the same time the analysis of more than 400 thousand malicious binary codes showed that as of October 2017 about 70% of the traffic was using encryption in one or another form.

14. According to the Cisco report, one of the main problems in the field of protection from cyberthreats are attacks using IoT-devices (Internet of Things) and cloud services. The document says that IoT-devices work 24 hours and can be utilised for performing malicious activity almost instantly. And as intruders increase the magnitude of their Botnets they use complex codes and malicious software that allow organization of even more advanced network DoS-attacks (Denial of Service).

15. Botnet is a computer network consisting of the devices infected with malware. A bot is a hidden program installed on the victim computer for unauthorized use. Bot-programmes are secretly installed in order to get control of a computer and are difficult to detect during routine daily work. The penetration of the bot can happen due to the insufficient attention of a user, since the autonomous program is masked under useful software. Bots run themselves unsuspected by users, they are launched and covered by shield. The protection mechanism lays in non-traditional ways of launching and replacing the system files, rebooting the machine when accessing the automatic download keys. Botnets are effective for cybercriminals and are not vulnerable, since through malicious computer devices intruders can anonymously take action from anywhere in the world.

16. Due to the increased complexity and analytical capabilities of security infrastructures, more and more researchers are suggesting the use of artificial intelligence and machine learning. According to Cisco, 39% of security professionals rely entirely on automation technology, 34% on machine learning and 32% on artificial intelligence. Guarding against cyberthreats, experts recommend constant correction and, to the possible extent, elimination of vulnerabilities, regularly taking backup copies of data and introducing advanced security technologies that include machine learning and the possibilities of artificial intelligence.

17. The healthy functioning cyberspace is a beneficial for development and progress while cyber attacks may transform vulnerabilities into destructive capabilities and cause serious consequences. Attacks on critical infrastructure sites have become more frequent. To combat such attacks, it is necessary to have broader opportunities to adequately address the problem of vulnerability.

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

19. 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.

20. It is the fundamental responsibility of the governments to address vulnerabilities in cyberspace. However, 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.

21. The International Telecommunication Union (ITU) annually publishes Global Cybersecurity Index. According to the results of this survey the level of cybersecurity of the states is estimated according to five pillars: legal, technical, organizational, capacity building and cooperation. In 2017, the index included 193 countries, among them the BSEC member states took the following places (according to ascending level of threats to cybersecurity): Georgia - 8, Russia - 10, Romania - 42, Turkey - 43, Bulgaria - 44, Azerbaijan - 48, Ukraine - 59, Greece - 64, Moldova - 73, Albania - 89, Serbia - 90, Armenia – 111.

22. The PABSEC member states, as many other countries worldwide, have embarked upon comprehensive measures to meet the cybersecurity challenges maintaining an environment that promotes innovation and technological development while also promoting safety, security and privacy rights. They launch grand-scale programs and initiatives to increase cybersecurity as a response to challenges related to the protection of relevant initiatives, including a variety of activities in research and development.

23. It is important to integrate interests to derive a holistic vision and plan to address the cybersecurity related issues confronting the countries. It is necessary 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. It is necessary to enact and strengthen appropriate legislation. It is also necessary to create a network of interaction of specialists representing all interested sectors, including the government, banking, energy, transport industry, commercial facilities and telecommunications.

24. According to the Decree of the President of the ***Republic of Azerbaijan*** "On Measures to Improve Information Security Activities" of 26 September 2012 No. 708, the Ministry of Communications and Information Technologies of the Republic of Azerbaijan was instructed to conduct regular analysis of the general state of cybersecurity in the country, to inform the public, private and other structures on existing or potential cyber threats and to provide technical and methodological support in combating global cyberattacks.

25. With the aim to coordinate cybersecurity activities of information infrastructure units, to inform on existing and potential electronic threats at national level, to educate public, private and other structures in the field of cybersecurity and to provide them with methodological assistance, within the Ministry of Communications and Information Technologies of the Republic of Azerbaijan was established the Electronic Security Centre, which is a coordination structure.

26. In 2016 the Centre became a member of the Cybersecurity Alliance for Mutual Progress (CAMP). With the help of this organization and the alliances that were established to

ensure security in cyberspace, the members are rendered necessary methodological support on the issues of cybersecurity, new cyberthreats, cyberattacks, and new combating methods.

27. For the purpose of cooperation in the field of cybersecurity among the BSEC Member States it is proposed to: create an online platform in several languages among the cybersecurity organizations of the BSEC Member States in order to exchange operational information on cyberevents, cyberattacks and cyberthreats; organise a week of cybersecurity in the BSEC Member States on the topics: safety of social networks and protection of personal information; ways to limit spam; software that blocks computers and requires payment (ransomware), and ways to protect against them; conducting seminars in schools and universities; raising public awareness; distribution of booklets; organization of joint trainings with the participation of specialists from relevant departments of the BSEC Member States.

28. As a member State of the European Union, ***Bulgaria*** participates in development and coordination of the Union policies and instruments to increase overall cybersecurity. Bulgaria actively supports the proposal to set up a new European Union Cybersecurity Agency and to introduce a new European certification scheme to ensure that products and services in the digital world are safe to use. This "Cybersecurity package" was initiated during the Estonian EU Presidency and continues to be considered within the framework of the Bulgarian EU Presidency in 2018 this year. It is planned to organize a Cyber Challenge Conference in Bulgaria, which will discuss topical issues of European cybersecurity.

29. Cybersecurity standards at national level are enshrined in the EU Directive on the measures for a high level of network and information security. In the Bulgarian legislation, an interdepartmental working group was set up under the direction of the Electronic Government State Agency, which aims to incorporate the articles of the Directive into the draft of a Cyber Security Act. In 2009 by the decision of the Council of Ministers of the Republic of Bulgaria was created the post of National Cyber Security Coordinator.

30. In 2016, the Council of Ministers of the Republic of Bulgaria adopted the National Cyber Security Strategy "Cyber Sustainable Bulgaria 2020", which envisages increase of responsibility of stakeholders in the Republic of Bulgaria to develop the national cyber system security and the achievement of an open, safe and secure cyber space. Combating cyber threats involves three phases. The first one (2016) - the institutional strengthening of the cyber defense process through the establishment of a National Cyber Security Coordination and Organizational Network (NCSCON), which includes the security services and the government institutions that are relevant to the ICT, as well as Ministry of Interior and the Ministry of Defense, the Ministry of Transport, Information Technology and Communications and the Electronic Government State Agency. The next phase focuses on adoption of urgent measures including a review of communication and information systems and the critical infrastructures of national importance. The next phase envisages the establishment in 2018-2019 in Bulgaria of the system of adequate responding to cyberattacks. In 2020 it is planned to achieve cyber sustainability at national level and effective interaction at international level in the region, the European Union and NATO. It is planned that in four years the country becomes the leader in cybersecurity in the region.

31. The Government of ***Georgia***, following the large-scale cyberattacks on the country's cyberspace in 2008, strongly supported the work to protect public IT systems. Under the guidance of the National Security Council the "National Cybersecurity Strategy of Georgia (2013-2015)" and the respective Action Plan were adopted in 2013. In 2016, the Permanent Inter-agency Commission for the Preparation of Conceptual Documents of National

Security under the Council for State Security and Crises Management developed the Cybersecurity Strategy for 2017-2018 and the corresponding Action Plan. This Strategy is focused on the further strengthening of cybersecurity. The new strategy focuses on expanding research and analysis, preparing new legislation, raising public awareness, developing education, training and international cooperation in the field of cybersecurity, with the aim of facilitating the exchange of information, reducing vulnerability, and identifying and developing strategies to prevent hostile or damaging practices in cyberspace.

32. In 2012, the Law "On Information Security" was adopted, which sets the framework for taking effective and efficient measures aimed at strengthening information security. This law establishes the Cybersecurity Bureau, whose main task is to protect the most important ICT systems of the Ministry of Defense of Georgia. Illegal access, interference with the ICT systems, malicious use of technological devices are criminalized by the Criminal Code of the country. The Law on the Protection of Personal Data was adopted by the Parliament in 2011 and is designed to protect human rights and freedoms, including the right to privacy in the processing of personal data, as well as determine the powers and responsibilities of the relevant departments. In accordance with the Law, the Data Exchange Agency of the Ministry of Justice of Georgia (CERT.GOV.GE) and the Cyber Security Bureau of the Georgian Ministry of Defense are responsible for ensuring cybersecurity in Georgia. In 2012, the Department of Cybercrime was established in the Ministry of Internal Affairs, which conducts investigations on cybercrime. Within the Department there is a 24 hours Contact Group, which is formed on the basis of the Council of Europe Convention on Cybercrime.

33. In 2013, in cooperation with the NATO Liaison Office (NLO), a working group of the Ministry of Defense, with the participation of an Estonian expert, examined the issue of cybersecurity in the defense system. As a result of this work, a roadmap was elaborated, which formed the basis for the establishment of the Cybersecurity Bureau. In 2017, an operational and technical service was created that responds to cyberattacks directed against the country's security. The Cybersecurity Bureau is actively cooperating within NATO both bilaterally and multilaterally. The Office participates in two smart defense projects - a multi-national program for the exchange of information on malware (MN MISP) and a multinational program to raise awareness of cybercrime (MN CD E & T).

34. In the ***Hellenic Republic*** the Cyber Crime Division is an independent body of the Hellenic Police, which deals with Cybersecurity and for combatting cybercrime. It. Its main objective is the prevention, investigation and persecution of crimes committed using the Internet, or other online criminal behaviors. The Division consists of five departments, covering a broad spectrum of citizens' protection and cyber-security fields: Administrative support and Information Processing Department, Innovative actions and Strategy Department, Department for Electronic and Telephone Communications Security and Software and Copyright Protection, Cyber Security for Minors and Digital Investigation Department, Special Affairs and Electronic Crime Persecution Department. Cyber Crime Division successfully investigates cyber-crime.

35. Greece has transposed in domestic Law the provisions of the Council of Europe Convention on Cybercrime in the sphere of combating electronic crime. Greece actively pursues the constant exchange of criminal information based on bilateral and multilateral cooperation agreements via institutionalized information and communication channels. Existing tools and services provided by Europol's European Cybercrime Center-EC3 and Interpol Global Complex for Innovation are fully used. Close cooperation with government bodies and

institutions are conducted with the aim to ensure digital security and protection of state infrastructures.

36. The National Emergency Response Team in Cyberspace (CERT) is the body for combating cyberattacks. It controls the appearance of electronic attacks, analyzes them and ensures the information security of databases. For greater efficiency, the group cooperates with foreign CERTs, as well as with government services within the country. The Center for Security Studies of the Ministry of Interior in cooperation with the Foundation for Research and Technology (FORTH), Aristotle University of Thessaloniki and the Greek Self-Regulatory Body for the content of the Internet (Safenet) under the European Program of DG HOME AFFAIRS of the EU have created the Greek Centre for Cybercrime (GCC). This Centre is part of an emerging coordinated European effort, which has the capacity to significantly improve education on cybercrime.

37. The Government of the ***Republic of Moldova*** by its Resolution No. 857 of 31 October 2013, approved the National Strategy for the Development of the Information Society "Moldova digitală 2020" (Digital Moldova 2020) and the Action Plan for its implementation prepared by the Ministry of Information Technologies and Communications. The National Program on Cybersecurity of the Republic of Moldova 2016-2020 was approved by the Government Resolution No. 811 of 29 October 2015. These documents form the basis of cybersecurity and establish the goals for ensuring information security. To implement these goals, the government determined minimum mandatory requirements for information systems and existing information resources to ensure an adequate level of protection of information systems (Government Decision No. 201 of 28.03.2017).

38. The Supreme Security Council, in its Decision No. 01 / 1-02-05 of 07.10.2014 confirms that the provision of information security is the main element in ensuring national security, which contributes to building an information society in the Republic of Moldova based on the citizens' trust in information technology and electronic communications. In accordance with the Government Decision No. 746 of 18 August 2010 the Centre for Cyber Security (CERT-GOV-MD) was established within the Centre for Special Telecommunications in the framework of the updated Individual Action Plan for the Moldova-NATO Partnership.

39. The mandate of CERT-GOV-MD implies the provision of information security of state institutions in cyberspace, through the collection and analysis of information on cyberattacks, and the adoption of urgent and effective measures to protect the information resources of public authorities. The Centre accepts and processes information on computer incidents that have or may occur against national users of information systems and the Internet, provides recommendations on the use of information protection against computer threats, assists users and state authorities of the Republic of Moldova in investigating computer incidents, organizes and conducts trainings on information security.

40. The Republic of Moldova continues to make efforts to increase institutional capacity in the field of cybersecurity and to protect strategic communication and information systems against cyberattacks and is interested in enhancing cooperation with NATO in the field of cybersecurity and combating modern security threats.

41. ***Romania*** actively supports implementation of cybersecurity measures and according to the National Cyber Security Strategy, the National Cyber Security System (NCSS) is the general framework of cooperation gathering public authorities and institutions specialized in the field to coordinate national actions that ensure the security of cyberspace.

42. CERT-RO, Romanian National Computer Security Incident Response Team, is an independent institution aiming to prevent, identify and respond security incidents that threaten the national cyberspace. The team operates an Early Alert System based on alerts received and has a database on processed cyber security alerts. CERT-RO carries out awareness campaigns, provides consulting services and cooperates with other authorities in Romania, the European Union and beyond, in order to increase the level of information on cyber threats and the level of response to incidents. CERT-RO is coordinated by the Ministry of Communications and Information Society and is financed entirely from the national budget.

43. In the framework of the Directive on security of network and information systems (NIS), adopted by the European Parliament in 2016, the Ministry of Communications and Information Society, with the support of CERT-RO, has drafted a transposition project of the Directive, which was published and submitted to the public consultation and currently is in the process of approval. This project establishes primarily the institutional framework, cooperation mechanisms at national level and with European partners for facilitating and implementation of strategic objectives of information exchange.

44. In the framework of the Europe 2020 Digital Agenda, Romania has defined four priority directions: (1) e-Government, Cyber Security, Cloud Computing, Open Data, Social Media; (2) ICT in Education, Health, Culture; (3) e-Commerce, Research, Development and Innovation in ICT; (4) Broadband and Digital Services Infrastructure.

45. In the ***Republic of Serbia***, the Law on Information Security ("Official Gazette of the Republic of Serbia" No. 6/16 and 94/17) is in force, which regulates measures for use of information and communication systems and strengthening information security. The Law specifies a competent authority for information security in the RS is the Ministry of Trade, Tourism and Telecommunications. The Law also establishes the National CERT (Regulatory Agency for Electronic Communications and Postal Traffic) and the CERT of public authorities (Government Office for Information Technology and E-Government). At the same time, the Law on Organisation and Jurisdiction of Government Authorities for Combating High-Tech Crime ("Official Gazette", No. 61/05 and 104/09) determines competence of special departments of the Republic Public Prosecutor's Office and the Ministry of Internal Affairs for Fight against High-Tech Crime

46. The Government of the Republic of Serbia adopted the Information Society Development Strategy in the Republic of Serbia from 2017 to 2020 ("Official Gazette of the RS", No. 53/17). The Strategy lays down priority areas of information security development in the Republic of Serbia: (1) security of ICT system; (2) information security of the citizens; (3) fight against high-tech crime; (4) information security of the Republic of Serbia and (5) international cooperation. The Government of the Republic of Serbia formed the Coordination Body for Information Security Affairs, which consists of representatives of relevant institutions in the field of information security. The Coordination Body rganises cooperation between the respective bodies in the field of increasing information security and taking preventing measures towards strengthening of cybersecurity.

47. The Republic of Serbia cooperates with other states and international organisations in the area of high-tech crime. The Republic of Serbia participates in the in the work of the International Telecommunication Union and the Organisation for Security and Cooperation in Europe (OSCE). To this end, it is suggested to expand cooperation in cybersecurity between the PABSEC member states through exchange of information, knowledge and

experience of national and international centres for prevention and elimination of atacks on information systems.

48. In ***Turkey***, the Cybersecurity Strategy includes the following main areas: cyber-defense and cyber-prevention operations; combating cybercrime; crisis management; Internet network management; coordination of actions between the relevant institutions. The main goal of the government is to integrate cybersecurity into the national security system of Turkey.

49. One of the most important steps regarding cybersecurity policy was the Decision of the Council of Ministers, in June 2012, No. 3842, "On the implementation, management and coordination of work to ensure national cybersecurity". In accordance with this decision, the Committee on Cybersecurity (SGK) was formed to prepare a cybersecurity policy, strategy and action plan. The Ministry of Transport, Shipping and Communications is responsible for ensuring cybersecurity in the country. In 2013, the National Centre for Cyber Incident Response (USOM) was established by the Decision of the Committee on Cybersecurity.

50. The National Cyber Strategy and Action Plan for 2013-3014 takes into account the main factors influencing the policy of Turkish national cybersecurity and sets the following goals: adoption of additional laws in the field of cybersecurity and improvement of existing ones; creation of a group of counteraction to cyber threats (SOME) under the control of USOM; the development of reliable backup mechanisms to determine the source of cyberattack and its impact; strengthening security of public information systems and providing new technologies; increasing human capacity in cybersecurity and organization of activities to increase awareness, development of local technologies to ensure cybersecurity and expansion of the scope of work in the institutions responsible for national cybersecurity.

51. To combat cyber threats more effectively, it is necessary to intensify bilateral and multilateral cooperation for building capacity and raising awareness in the field of cybersecurity. It is proposed to draw attention to the following areas within the framework of cooperation between the BSEC member states: exchange of information on the legal framework of national cybersecurity; organization of working visits; exchange of experts; exchange of intelligence information on counter-threats; organization of joint exercises in the field of cybersecurity; organization of joint conferences and seminars on cybersecurity.

52. The recently adopted Law of ***Ukraine*** "On the Basic Principles of Cyber Security of Ukraine" defines the main legal and organizational bases for ensuring the protection of vital human, public and state interests, Ukraine's national interests in cyberspace, the main objectives, directions and principles of state policy in the field of cybersecurity, responsibilities of state bodies, enterprises, institutions, organizations, individuals and citizens in this sphere.

53. Within the framework of the project of the Council of Europe and the European Union "Cybercrime and the Eastern Partnership" the draft of amendments are elaborated to the Code of Criminal Procedure of Ukraine with a view to ensuring proper implementation of the Convention on Cybercrime. It is proposed to improve the procedural mechanisms for collecting evidence in electronic form and to introduce a special procedure for removing information from telecommunication channels by the court decision during pre-trial crime investigation. It also implies the procedure of urgent fixing and storage of electronic data. Also the mechanism of blocking a certain (identified) information resource (information service) is defined. It is expected that this Law will also regulate the relationship between

law enforcement agencies and providers, as well as between law enforcement, intelligence and counterintelligence bodies.

54. A number of working meetings were also held between the representatives of the National Police of Ukraine, the Security Service of Ukraine, the Ministry of Justice, the National Commission implementing state regulation in the field of communication and information, during which the proposals for amendments to the legislation were discussed and comments and suggestions were made for their further improvement. In addition, a working meeting was held with the participation of the experts of the Association "Telecommunications Chamber of Ukraine". In order to take measures to restrict the participation of any business entities in activities to ensure information and cyber security, in particular to strengthen state control over the state of cryptographic and technical protection of information and restrict the use of products, technologies and services of such entities, the National Police elaborated the regulation "On the organization of measures for the implementation of the Cybersecurity Strategy of Ukraine".

55. Important responsibilities in cybersecurity approaches include developing a comprehensive national plan for securing the key resources and critical infrastructure; 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 cybersecurity.

56. Protecting the objects of cyberspace requires the efforts of many the countries and their citizens. The technologies that create and support cyberspace evolve rapidly while threats and vulnerabilities changed. 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.

57. The economies and national security are becoming more dependent upon information technology and the information infrastructure. Global cuberspace 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. Therefore, cyber attacks on information networks can have serious consequences upon critical operations. Countering such attacks and reducing vulnerabilities require development of integrated capabilities at different levels.

International Cooperation

58. One of the major instruments in enhancing international cybersecurity is the 2001 Council of Europe Convention on Cybercrime, which entered into force in 2004. 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. The Convention is supplemented by the Protocol concerning the Criminalization of acts of Racist and Xenophobic Nature Committed through Computer Systems, which entered into force on 1 March 2006 *(all BSEC Member States signed and ratified the Convention except Russia; all the BSEC Member States signed and ratified the Protocol except Azerbaijan, Bulgaria, Georgia, Russia; Turkey signed, but did not ratify the Protocol).*

59. 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 behaviour in cyberspace. The confidence-building measures adopted within the OSCE are one of the basic tools for ensuring international information security. Confidence measures are aimed at reducing the risks of conflicts when using information and communication technologies. The Organization has an informal working group established in accordance with OSCE Permanent Council Decision No 1039 of 2012. In 2016, the Decision No 1202 was adopted on "Confidence Building Measures within the OSCE to reduce the risks of conflict arising from the use of information and communication technologies".

60. Global issues of cybersecurity, which affect the interests of almost all countries in the world, are being discussed under the auspices of the United Nations. The UN General Assembly has adopted resolutions on cybersecurity. The UN Resolution 64/386 "Developments in the field of information and telecommunications in the context of international security" adopted in 2009, suggests continuing discussions on cybersecurity in the context of international security and creating an expert group that will prepare 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. Attaching importance to international information security as one of the key elements of the international security system, the UN is working to develop a Convention on Cybersecurity.

61. 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 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 cyber-component to the defense planning process and accelerating information sharing and early warning capabilities. In 2017 the NATO Cooperative Cyber Defence Centre of Excellence was set up in Tallinn (Estonia) which became the flagship initiative of European cybersecurity. The Centre annually conducts the

world's largest cyber defence exercise "Locked Shields" for experts in the field of cyberdefense. The Centre is developing a doctrine on cyberdefense - a single algorithm of actions, which the countries will follow in case of an attack. It is expected that the new doctrine will be approved by NATO in 2019. NATO and the EU are conducting parallel coordinated exercises to test their ability to respond to modern cyber threats.

62. The Digital Agenda for Europe (DAE) was launched by the European Commission in May 2010 to support economic growth in Europe and provide assistance to citizens and businesses in Europe to maximize the impact of digital technology. In 2013, the European Union formulated and approved a Cybersecurity Strategy. The aim of the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace is to increase the resilience and capacity building in the field of cybersecurity of the EU member states (strengthening the fight against cybercrime, building an effective security infrastructure, elaboration of principles of international policy in the area of cybersecurity). In 2017, it was decided to make the existing strategy more up-to-date so that it takes into account all new challenges and technologies. The European Commission has proposed a number of measures to strengthen cybersecurity, among them the creation of the EU Cybersecurity Agency. The Agency will build on the existing European Agency for Network and Information Security (ENISA), which will assist the EU countries in the fight against cyberattacks. A key tool for protecting critical information infrastructure is the Computer Emergency Response Teams (CERT). These teams exist in the EU states and are intended to be the main providers of security services for the state and citizens, as well as engage in educational activities. Member States, in their turn, ensure that they have the necessary level of national capacity and resources to ensure cybersecurity.

III. CONCLUSIONS

63. 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.

64. Safe and secure internet system is crucial for economies and societies. 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 who intends to misuse it. Ensuring cyber security is now a central challenge for the states, business and society both at national and international level.

65. Each country needs to 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. Global culture of cybersecurity needs to be encouraged, promoted, developed and vigorously implemented.

66. Laws and regulations on cybersecurity need to be enacted and continuously updated since only adoption and implementation of national laws is not enough to address contemporary cybersecurity challenges. Cybersecurity issue calls for the partnership between public and private sectors, as well as international cooperation and norms that should become a key component of cybersecurity strategies.

67. 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 the Internet and other digital resources is a shared responsibility. It is necessary to remember that the cybersecurity starts with each individual user's responsible behaviour in the cyberspace.

68. It is very important to strengthen efforts for stronger cybersecurity, to improve coordination of the response to cyberattacks, to promote partnerships in protecting information infrastructure and to promote the establishment of national and international systems for monitoring and preventing cyberattacks as they emerge. Vulnerability in cyberspace is a real, serious and rapidly escalating problem.

69. Today, global informatization is a key trend in the development of society. In this context, security in information and communication technologies is becoming one of the main issues on the international agenda. Cybersecurity issues consolidate the world community and, through the strengthening of a common understanding of the real danger of cyber threats the agenda is shaped to create a truly reliable and safe information environment.