PARLIAMENTARY ASSEMBLY OF THE BLACK SEA ECONOMIC COOPERATION
PABSEC

INTERNATIONAL SECRETARIAT

Doc.: GA51/LC51/REC162/18

RECOMMENDATION 162/2018[1]
Strengthening Cooperation in Cybersecurity in the BSEC Member States

1. The Parliamentary Assembly of the Organization of the Black Sea Economic Cooperation (PABSEC) stresses that cybersecurity is one of the priority issues of modern times. 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.
2. The PABSEC notes that 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. Magnitude of interconnectedness, along with the dynamism of the technological development, brings concomitant cyber security concerns.
3. The PABSEC recalls its Recommendation 129/2012 "The Role of Parliaments in Enhancing Information (Cyber) Security in the BSEC Member States", which emphasizes 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. The Documents also stresses 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.
4. The PABSEC acknowledges that healthy functioning cyberspace is a beneficial for development and progress while cyberattacks may transform vulnerabilities into destructive capabilities and cause serious consequences. Safe and secure cyberspace is a

---

[1] Assembly debate on 20 June 2018 (see Doc.: GA51/LC51/REP/18, Report of the Legal and Political Affairs Committee on *Strengthening Cooperation in Cybersecurity in the BSEC Member States*, discussed in Tirana on 19 June 2018; Rapporteur: Mr. Eldar Guliyev, Vice-Chair of the Committee, Azerbaijan).

Text adopted by the Fifty First General Assembly in Tirana on 20 June 2018

complex strategic challenge that requires coordinated and focused effort from the entire society - state, private sector and people.

5. The Assembly calls for the timely implementation of necessary measures at all levels. Cybersecurity policies need to include strategies and new standards of operations in cyberspace, encompassing the full range of threat and vulnerability reduction, enhance cybersecurity and safety of information.
6. The PABSEC stresses that the BSEC Member States have intensified their activities in cybersecurity sphere and have embarked upon comprehensive measures to meet the cybersecurity challenges maintaining an environment that promotes innovation and technological development while also promoting safety and security of networks. 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, regulation and management.
7. The PABSEC appreciates the activities of the BSEC Working Group on Science and Technology, particularly the elaboration of important documents in the sphere of technological development in the framework of the existing Plan of Action. The Assembly expresses the hope that the Working Group will further develop its activities with a view to contributing to the elaboration of mechanisms for the enhancing cybersecurity.
8. The PABSEC is of the opinion that contemporary cybersecurity challenges can be addressed through international cooperation and coordinated action. It endorses the measures for elaborating policy against cyber threats taken by various international organizations.
9. The PABSEC states the importance of national cybersecurity programs in protecting citizens and national infrastructure from cyberattacks. It is also necessary to achieve unity in cybersecurity issues and unify resources to identify vulnerabilities and counteract large spectrum of cyber threats.
10. **Therefore, the Assembly recommends** that the Parliaments and the Governments of the BSEC Member States:
    i. *support* establishment of more reliable, sustainable and secure digital infrastructure;
    ii. *take measures* to strengthen interparliamentary cooperation towards strengthening national and international legal frameworks aimed at halting and preventing cybercrime;
    iii. *strengthen* regional cooperation through acceptable international legal instruments on cybersecurity and their harmonization with the national criminal code;
    iv. *ensure* effective use of mechanisms for national and international cooperation to strengthen cybersecurity by signing and implementing, as appropriate, bilateral and multilateral agreements;
    v. *facilitate* averting threats of criminal and terrorist nature, as well as ensure compliance with international law, including the principles of respect for sovereignty and non-interference in the internal affairs of other states;
    vi. *establish* a real-time system for observing, monitoring and early warning of attacks, as well as tools for responding to cyberincidents;

vii. *improve* cybersecurity strategies with the aim to ensure the preventive research and analysis of malicious codes in cyberspace with high accuracy and low level of possible misperceptions;

viii. *enforce and amend* the relevant legal measures in conformity with international norms and standards in the sphere of cybersecurity;

ix. *use to maximum extent* the available legal mechanisms for a comprehensive national cybersecurity awareness program;

x. *carry out* comprehensive measures to identify weaknesses in key resources and important infrastructure, constantly assessing potential risks;

xi. *establish* funding priorities in science, technology, and innovation in order to promote, motivate, and improve research that meets the national priorities and strategic objectives in the sphere of cyber security;

xii. *create necessary conditions* for conducting target-oriented joint research in the field of cybersecurity, taking into account short, intermediate and long-term priorities;

xiii. *promote* the establishment of multi-layer security systems that protect information resources and prevent unauthorized access to the information;

xiv. *facilitate* cooperation between public institutions and private sector, paying more attention to the solution of global problems of cybersecurity;

xv. *endorse* initiatives to establish necessary conditions for the functioning of the international network of centres for the preventing cyberattacks and developing reliable mechanisms for the safe access to and exchange of information;

xvi. *support* organisation of training courses for law enforcement and judicial personnel on cybercrime and the negative consequences of such actions;

xvii. *ensure* coordination and cooperation among the specialized national agencies within the respective ministries in order to incorporate cybersecurity as an essential element in the planning, operation, and use of information systems;

xviii. *improve* information exchange on national legislation related to preventing and combating cyberterrorism and other interrelated cybercrimes, as well as monitoring its implementation;

xix. *facilitate* creation of online platforms among the organizations dealing with cybersecurity in the BSEC Member States in several languages with the aim to exchange operational information on cyberthreats and cyberincidents;

xx. *support* the proposal to hold a "cybersecurity week" in the BSEC Member States dedicated to topical issues of safe use of social networks and protection of personal information;

xxi. *intensify* bilateral and multilateral cooperation for capacity-building and awareness-raising in the field of cybersecurity;

xxii. *organize* joint conferences and seminars on new cyber threats and cybersecurity.

11. **The Assembly invites** the BSEC Council of the Ministers of Foreign Affairs to consider this Recommendation.