Doc. GA40/LC40/REC129/12

RECOMMENDATION 129/2012[1]

The Role of Parliaments in Enhancing Information (Cyber) Security 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. This issue will continue to grow in importance, corresponding with steadily increasing dependence on information technologies in almost every sphere of life. The attendant risk of increasing interconnectivity is that information systems and networks are now exposed to a growing number and a wider variety of threats and vulnerabilities, which raise new security issues for all users.
2. The PABSEC aknowledges that cyberspace has a significant impact on virtually every individual and every aspect of life. New information technologies compress space and time, offering lightning-fast access to the vast body of global knowledge and the possibility of instant information exchange. This magnitude of interconnectedness, along with the dynamism of the technological development, brings concomitant cyber security concerns.
3. The PABSEC is aware that the widespread reach of a lightly regulated digital infrastructure carries greater risks for vulnerabilities. The safe and healthy functioning of cyberspace is beneficial for overall development and progress, but cyber attacks have the potential to transform vulnerabilities into destructive capabilities that have serious consequences. Cybersecurity is a multi-faceted phenomenon with multi-fold consequences.
4. The PABSEC recognizes that countering cyber attacks requires the development of robust capabilities to adequately address the vulnerabilities. Enhanced cybersecurity infrastructure is necessary to ensure that individual citizens as well as the global community realize the full potential of the information technology revolution.

---

1 *Rapporteur*: Mr. Serhiy Podhorny, Chairman of the Committee – Ukraine.

Assembly debate on 27 November 2012 (see Doc.: GA40/LC40/REP/12, Report of the Legal and Political Affairs Committee on *the Role of Parliaments in Enhancing Information (Cyber) Security in the BSEC Member State*, discussed in Athens on 17 October 2012; Rapporteur: Mr. Michael Emelyanov, Vice-Chairman of the Committee, Russia).

Text adopted by the Fortieth General Assembly in Baky on 27 November 2012

5. The Assembly calls on the national parliaments to take necessary security measures in cyber environment. These measures are to be implemented timely and in a manner consistent with the values recognized by democratic societies: the freedom to exchange views, the free flow of information, the confidentiality of information and communication, and the appropriate protection of personal data.

6. The PABSEC recognizes that the BSEC Member States face the dual challenge of maintaining an environment that promotes innovation and technological development while also promoting safety, security and privacy rights. It is the fundamental responsibility of the governments to address vulnerabilities in cyberspace and ensure that the 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 Member States can protect themselves from the growing threat of cybercrimes and intrusions.

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. It expresses the hope that the Working Group will further promote initiatives on the establishment of mutually acceptable terms for a functioning network of international centers to prevent and counteract cyber attacks with the aim to developing viable mechanisms for cyber security.

8. The PABSEC is of the opinion that cybersecurity issues have a transnational dimension due to the underlying international architecture and global reach of cyberspace, which makes effective international cooperation essential for cybersecurity measures. It endorses the growing international cooperation in addressing the cybersecurity challenge, and strongly supports the measures taken to develop policies that protect against the disruption of information systems and ensure cybersecurity response by the Council of Europe, the Organization of Economic Cooperation and Development (OECD), the Organization for Security and Cooperation in Europe (OSCE), the North Atlantic Treaty Organization (NATO), the United Nations (UN) and the European Union (EU).

9. The PABSEC stresses that despite increased awareness about the importance of cybersecurity and the measures taken to improve security measures, cyber risks continue to compromise information networks and systems. Unfortunately, no single strategy can completely eliminate vulnerabilities and associated threats in cyberspace. The Assembly is aware that securing cyberspace is an ongoing process, as new technologies appear and new vulnerabilities are identified.

10. **Therefore, the Assembly recommends** that the Parliaments and the Governments of the BSEC Member States:

    i. *mobilise* the support of national parliaments in strengthening inter-parliamentary regional and international cooperation to improve the national and international legal framework to curb and prevent cybercrime;

    ii. *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;

    iii. *facilitate* mutual legal assistance and judicial cooperation by signing, ratifying and implementing, where necessary, the UN resolutions relevant to cybersecurity: Resolution 56/121 “Combating the Criminal Misuse of Information Technology”; Resolution 57/239 “Creation of a Global Culture of Cybersecurity”; Resolution

64/422 “Globalization and interdependence: science and technology for development”; and Resolution 64/386 “Developments in the field of information and telecommunications in the context of international security”.

iv. *ensure* efficient use of all mechanisms for effective national and international collaboration in enhancing cybersecurity by signing and implementing bilateral and multilateral agreements as necessary;

v. *support* greater direct cooperation between judicial authorities and law enforcement agencies in the sphere of cybersecurity;

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

vii. *enhance* regional cooperation by adopting accepted international legal instruments on cybersecurity issues and harmonizing them with national criminal laws;

viii. *implement* appropriate measures to strengthen law enforcement agencies where needed and promote the effective functioning and mutual cooperation of the national agencies involved in enhancing cybersecurity;

ix. *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;

x. *maximize* the use of the available legal mechanisms to promote a comprehensive national awareness program on cybersecurity with the aim of making the benefits of technological development widely understood and supported, while minimizing and mitigating the damage from possible cyber attacks;

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

xii. *endorse* initiatives on the establishment of mutually acceptable terms for a functioning network of international centers that prevent and counteract cyber attacks, with the aim of developing viable mechanisms for safe access to and exchange of information;

xiii. *focus* on enhanced interaction and coordination among law enforcement agencies, intelligence agencies, and the judicial system, in order to adequately equip these bodies in the fight against cyber attacks and intrusions;

xiv. *facilitate* organisation of training courses for law enforcement and judicial personnel on cybercrime and the negative consequences of such actions on individuals and societies;

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

xvi. *ensure* coordinating and cooperation among the specialized national agencies under the supervision of the respective ministries in order to incorporate security as an essential element in the planning, design, operation, and use of information systems and networks.

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