

RESOLUTION

On the Fight against Cyber Crimes

The Baltic Assembly

notes that cybercrime is a dangerous example of contemporary asymmetrical threats to society and any country which relies extensively on information and communication technology may fall victim to cybercrime,

underlines that in the future, cyber attacks may become a considerably more widespread and dangerous weapon to security, because they may destabilize the society, jeopardize the availability of public services and the functioning of vital state infrastructure,

stresses that international community should step up its efforts to defeat cybercrime, taking into account the requirements of the Convention on Cyber crime of 2001 of the Council of Europe and eventually building to the development of a globally negotiated and comprehensive law of cyberspace,

recognises the essential role of co-operation between all parliaments, governments and international the community in order to successfully cope with modern security risks,

welcomes the decision of NATO to establish the Cooperative Cyber Defence Centre of Excellence in Estonia,

calls on parliaments and governments of Estonia, Latvia and Lithuania and international organisations:

- to increase co-operation and information exchange in the field of cyber security, because only through joint and coordinated efforts it is possible to effectively respond to the threats originating from cyber space,
- to condemn cyber attacks similarly to human trafficking or intellectual property piracy, and to create universal rules of conduct in the cyber space,
- to develop and adopt international principles of combating cybercrime by developing, adopting and implementing national action plans on cyber security to prevent security incidents, to increase the security awareness of information and communication technology users,
- to revise the existing legal acts concerning cyber security and to develop supplementary means, including the harmonisation of the relevant legislation of states, to enhance information exchange on relevant experiences and best practices, also involving relevant actors from the private sector and civil society, and to establish public-private-partnerships in this regard,
- to increase public awareness on cybercrime and cyber security,
- to strengthen international co-operation in this field.

