Project

Resolution

On Improving the Legal Framework in the Field of Cyber Security in the OSCE Region

Taking into account the intensive development of information technologies in the world, implementation of automated autonomous control systems in numerous industries, and also in the areas of strategic importance, the mass distribution of communication systems, the increase in the volume of trade and financial turnover in electronic format, the worldwide trends in the accumulation and use of information, including personal data,

OSCE Parliamentary Assembly

1. Stands for the improvement and compliance of the legal framework in the member states of the Organization for Security and Cooperation in Europe;
2. Notes the importance of cooperation to ensure and improve the legal norms (cyber-laws) in the spheres of management of machinery, servers and household electronic devices and robots, means of transport, including navigational and air means;
3. Calls for the development of a general legal framework for the security in cyberspace, which gives protection against a number of risks **when using data provided by space satellites, when using by social networks, e-mail, including state and diplomatic correspondence, and individual communication portals and chats.**
4. Declares the need to take measures to ensure protective cyber-laws related to the **health care, the defense system management, as well as the automated and programmable electoral processes**;
5. Considers it essential to urgently ensure the interaction of the OSCE countries and international structures to strengthen the **legal control over electronic financial transactions, volume of electronic commerce, Internet gambling zones.**

Recognizing the fact that violations and crimes in cyberspace have an increasing tendency, the OSCE Parliamentary Assembly expresses concern in this regard and notes the following existing risks:

1. Extortion through the use of illegal access to computers, mobile devices, accounts in social networks and public sites, etc.
2. Hooliganism, distribution of illegal materials, incitement, advocacy of violence, terrorism and calls for the acts of violence.
3. Distribution of narcotic drugs, formulae of synthetic drugs /spices/ and other drug production-related information.
4. Fraud, fraudulent transactions in movable and immovable property, precious metals and stones, antiques, etc.
5. Ponzi schemes, money laundering, illegal gambling, false lotteries, fictitious or unreal brokering fraud, the sale of securities nonexistent on the real market, etc.
6. Fake auctions, online shops nonexistent in real life, false charitable contributions.
7. Persecution, illegal collection of personal data and their use, identification of persons.
8. Illegal voice tap or tracking and viewing of correspondence, as well as photo and video materials.
9. Offer of illegal or fictitious services of fraudulent nature.
10. International, military, industrial, business, political espionage activities.
11. Spread of viruses /malware/ with malicious intent or within the frames of one or more of the above items.

Since intruders, in the exercise of almost all the listed crimes or illegal actions, partially or fully operate in the Internet space in the common chain of events, their actions often fall beyond the bounds of the criminal law that regulates the responsibility for crimes in real life due to the absence of laws related to the specific actions in the Internet or using the Internet.

In view of the existence of certain laws related to countering cyber crime in a number of OSCE countries, as well as the relevant Council of Europe Convention, the United Nations Treaty, the North Atlantic Treaty and amendments to these documents, the OSCE Parliamentary Assembly recognizes the need for detailed elaboration of cyber-laws regarding existing

risks and available crimes. It is necessary to timely develop and adopt such legislative instruments, the existence of which would regulate the crimes committed via Internet or with the partial use of the Wide-Area Network.

Stressing the essential role of the Organization for Security and Cooperation in Europe in influencing the timely adoption of legislation in the OSCE region in accordance with the requirements of the modern democratic society and the legal public conscience of the world community, the OSCE Parliamentary Assembly urges parliaments of OSCE participating States to develop a "cybercode" /a detailed legislation on cyber security/.