"Third Draft

For the Security Section of the Forum for 21st Century"

Proposed for Respected Representatives of State and Private Corporations in Bratislava

GLOBAL CYBERSECURITY

Following is the communiqué proposed, with regard to the positions of the Respected Representatives of State and Private Corporations, by the Forum for 21st Century for the purpose of the conference on Global Cybersecurity issues held by the Forum for 21st Century on 29 November 2011 in Bratislava:

1. We, the member States and other Representatives of the Security Section of the Forum for 21st Century,

2. considering that the aim of our meeting is to achieve a greater unity between its members, recognizing the value of fostering cooperation with other States parties and Representatives, convinced of the need to pursue a common criminal policy aimed at the protection of society against Cyber Crime, considering the 2001 Budapest Convention on Cyber Crime, the 2011 Critical Terminology Foundations, the 2011 Working toward Rules for Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace and the 1948 Universal Declaration of Human Rights,

3. are determined that Cyber Attacks, which often take place to reach destabilization of international relations, should be understood as one of the major threats. Safety, protection of international cyberspace as well as the importance of international cooperation in risk management of Cyber Attacks should become the basic challenge and priority for international society in up-coming decades. With respect to these challenges, we decided to agree on following basic legal framework of Cyber Law and procedures aimed at preventing further malevolent acts as follows:

Definitions

4. **Cyberspace** is an electronic medium through which information is created, transmitted, received, stored, processed and deleted.

5. **Cyber Infrastructure** is the aggregation of people, processes, hardware and systems that constitute cyberspace.

6. **Cyber Services** are a range of data exchanges in cyberspace for the direct or indirect benefit of humans.

7. **Critical Cyberspace** is a Cyber Infrastructure and Cyber Services that are vital to preservation of public safety, economic stability, national security and international stability.

8. **Critical Cyber Infrastructure** is the Cyber Infrastructure that is essential to vital services for public safety, economic stability, national security, international stability and to the sustainability and restoration of Critical Cyberspace.

9. **Critical Cyber Services** are Cyber Services that are vital to preservation of public safety, economic stability, national security and international stability.

10. **Cyber Attack** is an offensive act conducted in Cyberspace intended to harm a designated target or to derive benefit without his consent.

11. **Cyber Crime** is the use of Cyberspace for criminal purposes as defined by national or international law by the means of Cyber Attacks.

12. **Cyber Terrorism** is the use of Cyberspace for terrorist purposes as defined by national or international law by the means of Cyber Attacks.

Basic Cyberspace Principles

13. With respect to the further development of Cyber Law, these principles shall be adhered:

14. No one shall be arbitrary deprived of having access to the Cyberspace.

15. No one shall be subjected to arbitrary interference with his internet privacy. Everyone has the right to the protection of the law against such interference (for further implementation of this principle see 18-21).

16. Everyone has the right to freedom of opinion and expression in the Cyberspace. This right excludes manifestations of:

    a) disparagement of an individual or a group on the basis of race, colour, ethnicity, gender, sexual orientation, national or ethnic origin, religion or other characteristics, without opinions and thoughts that may incite violence or prejudicial actions against or by a protected individual or group

    b) incitation to conduct violence for the purpose of achieving political motives

17. In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.

Protection of Internet Privacy

18. Each State shall adopt such legislative and other measures as may be necessary to guarantee the supervision of Cyber Services maintained by subjected private corporations and nongovernmental entities, which operate with personal information of individuals and groups.

19. Such supervision shall be limited only to the Cyber Service which operates with personal information of individuals and groups.

20. Supervision shall be conducted on the basis of regular monitoring executed by a representative of the government, subjected corporation and nongovernmental sector. Representatives shall be legally bounded to discretion with respect to operations out of their occupation.

21. Each State shall recognize subjected corporations under supervision as Internationally Secure.

Establishment of the Joint Cyber Crime Database within INTERPOL

22. Represented States and Corporations will support the establishment of Joint Cyber Crime Database (CYBERBASE) within INTERPOL and will promote the IT Crime Steering Committee as its regular operator.

23. The Content of CYBERBASE will represent reports and data on conducted or imminent Cyber Crimes, Cyber Terrorism, existing Cyberspace criminals and terrorists and malevolent sources of Cyber Attacks.

24. Represented States and Corporations will promote Best Practice Sharing as means of exchange of valuable practices specialized on prevention, deterrence or containment of Cyber Attacks.

Voluntary Internet ID Numbers

25. Each State shall adopt such legislative and other measures as may be necessary to guarantee the promotion of voluntary Internet ID numbers, which shall create a direct representation of the Internet user and his hardware used to connect on the Internet.

26. To obtain a voluntary Internet ID number, one shall request only the minimum required personal data to recognize the person on the Internet. The Forum proposes the name and ID number of an individual or a firm. This shall minimize the security risk of misuse of personal data but at the same time create the first link to a specific individual or a group.

Sanctioning and Persecution of Cyber Criminals and Cyber Terrorists

27. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the conduct of Cyber Crime and Cyber Terrorism. Further definition of sanctions and the means of persecution shall be discussed during negotiations.