# Final Communiqué

For the Security Section of the Forum for 21st Century

Adopted by Respected Representatives of State and Private Corporations in Bratislava

# GLOBAL CYBERSECURITY

Bratislava, 29 November 2011

## Introduction

The fifth ordinary session of Representatives of State and Private Corporations of the Security Section of Forum for 21st Century was held in Bratislava, Slovak Republic, on 29 November 2011 under the chairmanship of Mr. **Tomáš Jurka**, current Chairman of the Security Section of Forum for 21st Century.

The following Representatives of State and Private Corporations attended the session:

The Honourable **Jana Jánošková**, High Representative of the Union for Foreign Affairs and Security Policy, European Union

The Honourable **Katarína Chovancová**, External Affairs Minister, Republic of India

The Honourable **Viliam Ovsepian**, Minister of Foreign Affairs, State of Israel

The Honourable **Nóra Szikorová**, Minister of Foreign Affairs, People's Republic of China

The Honourable **Miroslav Janečka**, Minister of Foreign Affairs, Russian Federation

The Honourable **Alica Lacová**, Minister of Foreign Affairs, Republic of Turkey

The Honourable **Renáta Zuščáková**, Secretary of State for Foreign and Commonwealth Affairs, United Kingdom of Great Britain and Northern Ireland

The Honourable **Peter Pilz**, Secretary of State, United States of America

Mr. **Lukáš Grega**, Global Chief Executive Officer, Eset

**Following is the Communiqué adopted by the Respected Representatives of State and Private Corporations at the end of the session for the purpose of the conference on Global Cybersecurity issues held by the Forum for 21st Century on 29 November 2011 in Bratislava:**

We, the member States and other Representatives of the Security Section of the Forum for 21st Century, have come to a mutual agreement on following Cybersecurity issues:

1. The security and protection of national and international Cyberspace is strongly required by Global Society and therefore we perceive the necessity to achieve a greater unity between the respective parties concerned.

2. We recognize the value of fostering cooperation with other Parties and Representatives and are convinced of the necessity to pursue a common criminal policy aimed at protection of society against Cyber Crime and Cyber Terrorism, considering the 1948 Universal Declaration of Human Rights, 2001 Budapest Convention on Cyber Crime, 2011 Critical Terminology Foundations and 2011 Working towards Rules for Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace.

3. Cyber Attacks, which often take place to reach destabilization of international relations, should be understood as one of the major threats to global security. Safety, protection of international Cyberspace as well as the importance of international cooperation in risk management of Cyber Attacks and Cyber Crime should become the basic challenge and priority for international society in the up-coming decades.

4. In order to lay solid foundation for peaceful and credible cooperation with all respect to the challenges proposed, we decided to agree on following basic legal framework of Cyber Law and procedures focused on prevention of malevolent acts.

## Definitions

To address immediate challenges faced by the global society, we commit to coordinate our actions and policies. Each State shall adopt such legislative and other measures as may be necessary to guarantee the firm implementation of following mutually agreed definitions:

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

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

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

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

9. **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.

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

11. **Cyber Attack** is an offensive act conducted in Cyberspace intended to harm a designated target by Cyber Weapon *(for further definition of Cyber Weapons see Appendix 1).*

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

13. We affirm our commitment to move towards a similar agreement on the definition of Cyber Terrorism.

## Basic Cyberspace Principles

We have made progress in defining basic principles which shall be adhered by each State in further legislation and implementation of Cyber Law. We assume these principles should be the cornerstone of transparent and just laws regarding Cyberspace, which will defend basic human rights within the Cyberspace and protect individuals against arbitrary measures. We have all agreed on following:

14. No one shall be deprived of having access to the Cyberspace unless it's justified by the national or international Law.

15. 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

    c) illicit, illegal content subjected to national Law *(People's Republic of China and Republic of Turkey reserve their right for the modified implementation of this article as following: "inappropriate, illicit, illegal content subjected to national Law"*).

16. 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 17-19).*

## Protection of Internet Privacy

We are determined to strengthen the protection of individuals and reduce the misuse of personal data for malicious purposes. Convinced of the essential role of transparency, we recognize the importance of monitoring the operations of non-state actors related to the processing of crucial information of private nature. Not only they can influence the everyday life of every individual, they are a frequent target of Cyber Attacks as well.

We have decided following:

17. 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 independent experts, which operate with personal information of individuals and groups.

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

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

## Establishment of the Joint Cyber Crime Database within INTERPOL

At this critical time of vast threats in the Cyberspace, it is important to stress the practical cooperation of States in tackling Cyber Crime and Cyber Terrorism and avoid possible mismanagement of cooperative initiatives. Being aware of its apolitical and international nature, we are confident that Interpol as a highly regarded international organization with second biggest membership will be a suitable candidate for handling and gathering sensible data. We have agreed on following *(United Kingdom of Great Britain and Northern Ireland reserves the right to withdraw from this agreement and statement)*:

20. 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.

21. 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 *(State of Israel reserves the right to cooperate within CYBERBASE strictly only with its closest allies).*

22. 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 within INTERPOL.

## Voluntary Internet ID Numbers

Noting that significant action has already been taken at national levels to offset the missing link between the Internet user and his hardware used to connect on the Internet, we will further promote development of such measures, which will tackle the often misused anonymity on the Internet. Represented States and Private Corporations value both protection and privacy of their citizens and clients very highly, therefore:

23. 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.

24. 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 basic link to a specific individual or a group.

25. International Community stresses the securitization of Internet ID cards and economic feasibility of technical implementation.

## Sanctioning and Prosecution of Cyber Criminals and Cyber Terrorists

We have made significant progress in defining Cyber Attacks, Cyber Crime, Cyber Terrorism and the environment in which these acts are conducted. Although these terms were defined, due to the complicated nature of finding the culprit behind these acts, we decided to firstly press on the creation of the link between users and connected machines to the Cyberspace. With respect to the grave importance of this matter, further negotiations were requested.

We thank Forum for 21st Century for hosting the successful 5th Session of the Security Section. By signing this document, the signatory Parties express their will to implement agreed proposals within the time framework set:

In Bratislava, 29 November 2011

| | | |
|---|---|---|
| ..... | ..... | ..... |
| European Union | Republic of India | State of Israel |
| ..... | ..... | ..... |
| People's Republic of China | Russian Federation | Republic of Turkey |
| ..... | ..... | ..... |
| United Kingdom of Great Britain and Northern Ireland | United States of America | Eset |

## Appendix 1

A general list of Cyber Weapons proposed:

- keyloggers, IP spoofing, sniffing
- viruses, worms, malicious code, root kits, trojan horses, spyware, logic bombs, video morphing
- botnets, back-doors, trap doors
- spamming, software vulnerability exploitation, info-blockades
- Denial of Service (DoS), Distributed Denial of Services (DDoS)
- Directed Energy Weapons (DEWs), high energy microwaves (HEWs), high power microwave (HPWs) and transient electromagnetic devices (TEDs)
- electronic countermeasure, defence shields against electronic attack, transient electromagnetic devices
- infrared decoys, angle reflectors, false-target generators
- autonomous mobile cyber weapons