Forum for 21st century on Global Cybersecurity issues

Notes

- Transmission of information, which became the essential tool for all human activities, revealed not only its positive effects on society but on the other hand numerous negative side-effects as well. Massive expansion in technological development and increasing global interdependence reflected in multiple cultural, economic and political happenings starting with the most perceptible one, which is communication. Modern global society became so dependent on communication systems that without any protection other security strategies might lose their purpose.

- In the last decade we have witnessed increasing level of misuse, theft, modification or unauthorized access to sensitive information for various economic or political purposes. In the wake of mentioned reasons, the cyberattacks, 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 cyberattacks should become the basic challenge and priority for international society in up-coming decades.

- Moreover, war, aggression and criminal acts as we knew them in the past have largely changed in their substance. Actions, which were until recently conventional, were substituted with more unpredictable, disruptive or even destructive unconventional ones. Nowadays, the importance of having vast armed forces or even resources to wage war, which will be ultimately either expensive, unsuccessful, exhausting or in which the objectives won't be even achieved, is being pushed into the background. Similarly, criminal acts and violence on people, their property or their rights can be conducted without physical presence of the offender and can be even more harmful and vicious. One way or another, the emphasis is laid on effective, swift and precise actions, which can be carried out with minimal costs and persons involved. Consequently, there's no use for big armies anymore. There's no point in maintaining a vast network of underground connections to carry out an organized crime. Just one person seems to be enough to threaten the whole society. This is the nature of cyberwar/cybercrime in the world as we know it now and therefore the global society needs to address the mentioned risks.

- Cyberspace is currently perceived as a borderless world but so are all systems in this world, even the Internet needs certain security rules. Seeing that the states are still original wielders of power in international relations, there is a notable necessity to negotiate basic legal structure of cyberspace environment, as well as its control and usage by the states. Defining general instruments, commitments, rights and terms will create legal basis for a more transparent and

organized system without enacting tight regulations of the Internet and will moreover prevent global society from future conflicts resulting from interventions into internal affairs.

- By requiring certain limits in anonymity of Internet users as well as their actions, we intend to decrease the risk of unprecedented cyberattacks and cybercrimes and will further provide an open arena for handling inter-state cyberconflicts and cyberterrorism which currently can't be settled because of technical uncertainty and lack of legal regulation. The general idea is to defend the country's values, citizens, property and national interest in compliance with basic ethical standards and to elude possible unnecessary clashes with other countries.

- Therefore, to ensure peaceful environment for next generations, Forum for 21st Century is aware of the necessity to discuss proposed cybersecurity topics and reach common understanding.

Proposals

- Forum for 21st century calls for a creation of legal basis and terms with respect to usage and control of the Internet and local intranets (governmental, corporate and others). We propose a definition of internet users on the Internet, their rights, commitments and sanctions for criminal acts which would be accepted by the represented parties and would serve as a basis in resolving international cybernetic crimes and conflicts.

- Taking into account the significance of the destructive force of certain attacks on national defense systems and government bodies, we suggest that every attack of this category should be considered as an act of aggression and the aggrieved party can use any conventional means necessary to defend itself (e.g. retaliatory attack or even armed forces). In case a supposedly offending state declares its innocence, it should provide all assistance necessary in finding the culprit. Uncooperative behavior would be seen as an act of quiet consent and further sanctions or retaliatory actions can be conducted.

- We suggest further cooperation of engaged parties in exchange of valuable information about malevolent attacks, criminal or terrorist groups and other activity that endangers our society. An establishment of a joint database of these persons or groups with detailed information would heavily support solid foundations of a peaceful and credible cooperation between the parties concerned.