





Position of the European Union for the purpose of the conference held by Forum for 21st Century on 29 November 2011 reflected in the second draft of the negotiation paper regarding the Global Cybersecurity Issues.

The European Union would like to thank the *Forum for 21st century* for summarizing the positions of participating parties to the first draft and proposing additional topics for further discussions. At the same time we express our full support towards solving the challenges and efforts aimed at safer and more effectively working cyberspace.

After an in-depth analysis of the second draft proposed by the Forum for 21st Century, the EU submits its position including its suggestions about selected topics as well.

In the Section Notes

-  The EU welcomes the standpoint of the global society towards the ensuring cybersecurity protection and highly appreciates its endeavor to cooperate in order to establish more secure global cyberspace. The members of the EU stressed significance of proposed controlling of illegal, inappropriate and illicit Internet content and consider this step very important as it would definitely contribute to peaceful cyberspace.
-  To develop ideas of ways how to determinate and regulate the inappropriate content of Internet websites, the EU proposes the following:
 - Creation of Joint Criminal Database (within the scope of newly established Cyberpol- this idea is elaborated later in the Section *Proposals*), which will provide another list of malevolent websites and IP's with illegal and harmful content (including children pornography, pictures that glorify violence and selfharm, antirasist, discriminatory and other expressions as mentioned below in the Principle Nr. 4 of Basic Cyberspace Principles and other content capable to affect physical, emotional and psychological well being of an Internet user). These websites should be blocked or the internet users should be warned by some special software before entering these websites.
 - This database should also include some information on available software designed to protect internet users (especially children) against illegal and harmful content.



- The governments of concerned parties should cooperate with private companies and other organisations (for example ESET) in developing the software tools to protect internet users and raise the awareness of internet users about them.

In the section Proposals:

- The EU would like to express its repetitive approval with the creation of basic foundations for International Cyberlaw. With this intention the member states of the EU consider the idea of broadening the Universal Declaration of Human Rights by adding the Basic Cyberspace Principles to it the right way of creating a certain control mechanism to regulations in the field of cybersecurity and cyberspace. As the Universal Declaration of Human Rights is generally accepted by all UN member states, this fact would facilitate the ratification of the amended text and at the same time its taking over to their national legislatures.

After an in-depth analysis of submitted cyberspace principles, we:


- Fully agree with the first two stated principles
- With regard to third one: The member states of the EU agree with the proposal of the *Forum for the 21st century* about the protection of personal data and the privacy of internet users. The growing phenomenon of misusing of the personal data for political and economic reasons of various companies, operators of social networks and search engines and other crimes (including wiretapping and blackmail) presents the big threat for today's society and a serious interference to their privacy. The EU is convinced about the necessity to supervise such companies that use and have access to data of personal character. This supervision should be carried out by proposed multistate holding body (consisting of state representatives and representatives of NGO's), which should also provide these companies with some internationally recognised licences (in accordance with the international standards and agreements) after proving their reliability and the purpose of collecting and using these sensitive data. The malevolent misuse of personal data by the companies and entities without the above mentioned licences should be hardly sanctioned. Moreover, the members of the EU strongly recommend that the companies, which once managed to receive these licences, should be regularly controlled in order not to misuse them. Furthermore, in order to prevent misusing this principle, the members of the EU recommend to determine the minimal software tools, which should be installed to every computer for protection. Only in the case, when the computer was provided by this software, could the complainant claim the validity of this principle.




- What the principle Nr. 4 concerns, we, the EU, propose to slightly change the text of this principle and to accurately specify the freedom of opinion and expression in Cyberspace. Taking into account the proposed determination and control of inappropriate, illicit and illegal Internet content, we consider our suggestion to legally limit this freedom as a very necessary step. The EU strongly recommends the following text of this principle:

"Everyone has the right to freedom of opinion and expression in the Cyberspace. This right includes freedom to hold any opinions excluding opinions that may disparage a person or a group on the basis of some characteristics such as race, color, ethnicity, gender, sexual orientation, nationality, religion or other characteristics, without opinions and thoughts that may incite violence or prejudicial actions against or by a protected individual or group. This freedom of opinion and expression should be reduced also in thoughts and opinions connected with organising terrorist actions and crime (in order to prevent incidents similar to the bombing of government buildings in Oslo and the mass shooting at the camp on the Island of Utoya in July 2011, which were planned on some internet websites). Moreover everyone has the right to seek, receive and impart information and ideas without interference through any media and regardless of frontiers. "

- The EU coincides with the last principle.

 The members of the EU accepts the proposed definition of Cyberspace *by Forum for the 21st Century* only partially and recommends more complex definition: „The Cyberspace is a global network, linking all people through computers, mobile and landline networks serving for communication and exchange of various information in the world. As special parts of this global network should be included intranets and special networks providing a space for exchange some secret or encoded information (like networks for exchange information between governments and their diplomatic missions abroad).“ As nowadays we always more often come into contact with cases, when government representatives misguide and overreach their governmental competences to misuse some secret information for their own purposes, we call for the need to include these special networks in the definition of cyberspace in order to also legally regulate these activities.

 We, the European Union, fully support the suggestion to define a common systems of sanctions for criminal acts in accordance with the type of criminal or illegal activity, as presented in the second draft. The member states of the EU are prepared and obliged to abide by this joint agreement of typology, which should be legally binding and transported to national legislatures.



As cybercrime is nowadays considered the second largest criminal activity in the world, the establishment of a globally coordinated institutional framework for cooperation is more than needed. The European Union has declared its support to develop different forms of cooperation, so we also welcome the idea of *the Forum for 21st century* about the establishment of CYBERPOL. We agree that Cyberpol would be the twin-organization of apolitical character to the current Interpol. This organisation should gather the cybersecurity specialists from all over the world and representatives of private sector, who would be able to handle with international criminal activities. We are convinced about the usefulness of the creation of already mentioned Joint Cybercriminal Database as appropriate tool for prevention, detection and quickly reaction in the event of cyber attacks and cyber disruption.

The members of the European Union highly appreciate the initiative of Best Practice Sharing in which IT corporations would also be engaged. This would certainly lead to strengthening the global cooperation in fighting against cybercrime.

Recognising the need to protect communication and information systems of all structures within the EU, as well as national networks of its member states, the EU calls for the *Forum for the 21st century* to initiate the discussion about the development of minimum cyber defense requirements for communication and information systems of all concerned parties. As a strategic document that could be very useful not only for defining these requirements but also for adopting the key outcomes of the *Forum for the 21st century* regarding the Global Cybersecurity Issues, should serve the revised NATO Policy on Cyber Defence approved by NATO Defence Ministers in June 2011 and elaborated on the ground of the Strategic Concept adopted at the NATO Summit in Lisbon in 2010. Moreover, as the threats and attacks in the cyberspace affect not only our governmental or nongovernmental organizations, but even more the individuals, who in the majority of cases are not able to deal with such threats, we fully agree with the introduction of voluntary Internet ID Numbers as a useful measure of providing some help and guidance to them on cyber security and cybercrime.

Taking into account the different characteristics of the criminal acts in cyberspace we are convinced of the fact, that such cyberattacks should be considered as terrorist attacks, but of a different nature. If the main purpose of such cybercrimes is to forcefully attack national defense systems and government bodies in order to gain access to some secret and sensitive information, to disrupt public operations and economically and politically paralyse the states or to coerce them to change their internal or foreign policy or to potentially inflict on transportation, supply networks and other critical infrastructure, such attacks could be considered as acts of aggression. As the EU stands for the values as peace, prosperity and



The Model Conference Global Security Issues

Faculty of International Relations, University of Economics in Bratislava



Modelová konferencia Bezpečnostná sekcia

Fakulta medzinárodných vzťahov, Ekonomická univerzita v Bratislave

freedom, we think that such attacks should not be retaliated by military action and armed forces. Not every act of aggression is a crime against peace. It is unacceptable to react to cyberattack by using missiles and other military resources, because it could come about catastrophic mistake and serious war conflict leading to millions innocent casualties and immense material harm. Appealing to the first position proposed to the *Forum for the 21st Century*, the mandate to decide whether it is an act of aggression or not and also about the use of military action and arm forces in general, should have the Security Council of the UN and the EU will respect its decision as well as sanctions for the cyberattacks. The list of sanctions should be worked out according to seriousness of cybercrime and the level of caused harm by cybercrime specialists from all concerned parties (and has to be approved by the Security Council of the UN). On the international level, the list of sanctions for cybercrimes should include economic sanctions (fines, interruption of economic and financial relations, suspension of financial aid, embargo, etc.), but also diplomatic (interruption of diplomatic and consular relations) and communication sanctions (interruption of television, broadcasting and postal connection).

If the main "victim" of the cyberattacks are individuals, nongovernmental organisations and companies, the procedures will be taken before the national courts, which can cooperate with national courts of other states.

- Threats emanating from cyberspace – whether from states, hackers or criminal organisations, among many others – pose a considerable challenge to the global society and must be dealt with as a matter of urgency. The prompt response to cyber attack or cybercrime is required in order to avoid and decrease other possible damages. The EU supports this idea and proposes a creation of a network of Computer Emergency Response Teams in every concerned state, which will be able to cooperate with law enforcement authorities in prevention and response. The EU considers very important to strictly differentiate between "cyberarmies" as part of the national defensive units and illegal hacker organisations. The member states of the EU are open to discuss further ways of cooperation in revealing and prosecution of illegal paramilitary or terrorist activities and their culprits.