



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

ESET Slovakia would like to thank Forum for the 21st century for its summarization of topics discussed between the parties concerned and its attempt to harmonize their different views on the issues in question. ESET has performed an in-depth analysis of the newly proposed Draft and will try to evaluate its content to reflect its real-life application possibilities. ESET will also assess the newly proposed mechanisms and tactics to tackle the cyberterrorist attacks endangering the global cyberspace along with its private, corporate and governmental users.

-  As for the creation of legal basis and terms with respect to usage and control of the internet and local intranets and a subsequent definition of the terms applied, ESET does not raise any major concerns. It is of prime importance that such definitions are put in place, for the legal regulation to be effective and not objectionable by the offenders' attorneys, who will indeed attempt to find any weaknesses in the legal regulation put in place to defend their clients.
-  We believe the decision on structural concept of the organization as well as its institutional foundation administering and executing the anti - cyberterrorist agenda shall be fully in the competence of sovereign states represented in the UN and therefore ESET does not intend to interfere with such a decision process. However, as already mentioned in its first Position, any legal regulation attempts following the institutional setup of the newly formed organizational structure shall inevitably be subject to wide public debate in the international measure and discussed with the corporate sector as well - thus ensuring that every member of the international internet user community is aware of such regulation and has an opportunity to raise his concerns to an appointed representative on the national level.
-  ESET strongly opposes the notion to create a "supervision body" jointly made up by state representatives and NGO's experts to regulate the activities of the companies operating business on social networks and search engines. ESET would like to remind the international community, that it is in the nature of these companies to use the personal information provided by the users in the social networks for marketing purposes, as such companies do not run on non-profit principle. Every user accepts the terms and conditions before being allowed to create a profile on social networks in question and thus the application of marketing mechanisms listed in the terms and condition shall not be a subject to any further intergovernmental regulation. The international community may, however, focus on the campaign informing the public users of the importance to limit the amount of personal information shared, and most importantly to filter the circle of individuals allowed to view such information. It is in fact mostly the negligence of the users themselves that causes the misuse of their personal information by others.



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

On the other hand, it is true, that some of the social network providers might underestimate the importance of the prevention against the misuse of the information. ESET suggests, the international community binds such companies to include a warning message informing the user of a possible personal information misuse threat every time the user attempts to change the settings regarding the circle of people allowed to see the information shared.

- ❖ ESET agrees, that any other attempts to collect or use the private data of users other than the ones included in the terms and conditions of such entities, shall be naturally a subject to legal action and subsequent sanctions. Any individual or company attempting to collect the personal information by deceit must be aware of possible consequences of such actions. The institutional and structural model along with the typology of crimes in such regulation is again fully in the competence of sovereign states included in the United Nations and ESET will accept its organizational lay-out.
- ❖ Regarding the database on malevolent IP addresses, ESET does support the creation of such a database, however it doubts its real significance in tackling the cybercrime. The database might have a positive short-term effect, however the offenders will soon relocate their activities to another IP address. The reason for such an IP detection should be an immediate action. If it is located (based on the premise that such an IP address does not use a rerouting shield), the police force shall be dispatched to arrest an offender immediately.
- ❖ ESET believes that the idea of "Voluntary Internet ID numbers" is not necessary as their proposed functions are already being performed by commercial products invented by such companies as ESET. Such a project would not only represent an inefficient use of public financial resources, it would also destroy thousands of jobs in the private companies dealing with the internet security of private users.
- ❖ ESET still considers the introduction of cybercrime as an act of aggression into an international legislature as inappropriate. As already mentioned in the Position 1, "Cyber attacks tend to be often incredibly sophisticated, difficult to detect and most importantly they may be fabricated to be blamed on somebody else. Such a piece of international legislature might encourage certain regimes to hire top-skilled hackers to create a suspicious uncertainty and launch the uncontrolled aggression without the need of the real offender's military involvement."
- ❖ ESET supports the introduction of the topic of cyber armies, paramilitary hacker organizations and hacktivists at all points discussed.