



The Republic of India would like to thank the Forum for 21st Century for initiating the discussion and organizing the conference on global cybersecurity issues. The Republic of India highly appreciates your invitation and would like to acknowledge its will to participate in the discussion and come up with potential solutions. It is of great significance that the common challenges in the sphere of information security should be dealt with through international cooperation and in the spirit of mutual respect. Regarding considerable progress achieved in developing and applying the latest information and telecommunication technologies, the Republic of India highlights its objectives of maintaining international stability and security. After a precise analyse of the draft proposed by the Forum for 21st Century let us annotate it and express our propositions.

During the past decade, the world has witnessed a clear escalation in the number of politically motivated cyber attacks, often including hackers from around the world in regional disputes. Political conflicts that have led to attacks on cyber systems present a variety of forms and may include cyber attacks by terrorist groups, sympathizers of the terrorists or by hackers with general anti-sentiments of certain States. Level of sophistication of cyber attacks lacking any particular political motivation are increasing rapidly as well. The Republic of India struggles against cyber attacks permanently. The tension between India and Pakistan over the disputed territory Kashmir have hit Indian sites especially hard. Pro-Pakistan hackers have used cyber tactics to disrupt Indian information systems and disseminate propaganda. The number of pro-Pakistan defacements of Indian web sites has risen markedly over the past years and sensitive information has been downloaded. Previous and ongoing global conflicts indicate the vulnerability of critical infrastructure systems to cyber attacks and the increasing willingness of groups to target sensitive systems during political conflicts. For the reasons mentioned above the Republic of India recalls for mutual cooperation among the State representatives and international organisations.

The Republic of India underlines the significance of close cooperation between the state institutions and private sector. The most important development in IT sector, numerous innovations and progress in science and information technology in the context of international security have been reached by private IT corporations and institutes. It is desirable to understand the roles and responsibilities of information and communication private sector in order to facilitate the creation of a culture of information security and the protection of critical information infrastructures.

The Republic of India underlines the need for enhanced bilateral, regional and international coordination and cooperation among States in combating the criminal misuse of information technologies and highlights the role that could be played by international and regional organisations. At the same time The Republic of India



suggests to promote the establishment of a multilateral and transparent international management of the Internet to ensure an effective cooperation among the engaged parties and expresses its full support to create a joint database as mentioned in draft.

- The cyber space offers a high level of anonymity and is controled with difficulties. Creation of unified mechanism defining main crimes in cyber security is difficult also in national level. Closer cooperation on international level and definition of proper and functioning legal framework is urgently required. The Republic of India stresses the necessity of global legal base, formulation of international norms and peacefull settlement of international disputes with respect of fundamental human rights defining free access to information and free diffusion of information on Internet. Importance of legal protection of personal rights and transactions in cyber space are respected as well.
- The Republic of India would like to take advantage of the conference held by the Forum for 21st Century and discuss closer cooperation between India and NATO member countries Turkey and the United Kingdom. Israel is involved in NATO's Mediterranean Dialogue. There is a growing need for nations and organisations to cooperate more closely in many other areas such as cyber attacks and piracy in Indian ocean which compel nations to search additional frameworks which allow them to talk together and especially to work together. Cyber attacks can be conducted on borrowed infrastructure that is stored anywhere in the world and carried out by a small number of computer professionals. The technological sophistication and expertise to conduct cyber attacks is closer to the expertise required to conduct piracy. As national viewpoints on international piracy interconnected with cyber crimes are quite opposite, the Republic of India would like to formulate a more inclusive legal framework on cybercrime and maritime piracy laws.

Regarding the goals the Republic of India proposes:

- To enhance the security of Communications and Information Infrastructure through proactive action and effective collaboration among countries at the regional and international level. Creation of international information society and joint database of cyber criminals based on a clear statement of political will.
- To implement an efective law system defining cyber crime, cyber attack, penalties and other terms related to cyber security.
- To increase a private investment in infrastructure development and closer cooperation between state and private sector.



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

- ☛ To define a legal framework on cybercrime and maritime piracy laws as there is a existing cohesion between both issues.

Conclusion

The Republic of India recognizes a need of policy enactments and necessary investments to fight the menace of rising cyber crimes. Assurance of institutes, industry and government have to be guaranteed to protect the economic prosperity which is highly depended on Information Technology. Underlining that outsourcing becomes more widespread and communication security is one of the decision making factors for companies that decide which provider to cooperate with, it is of high importance to improve privacy standards for the outsourcing companies and use powerful safeguards. All together we have to find a way to cooperate so that the cyberspace remains a driver of economic prosperity of nations and a space where people from all countries can safely interact and exchange goods and services.