**<Attachment I>**

**(Draft) Seoul Principles and Guidelines for Open and Secure Cyberspace**

In the preparatory stage of Seoul Conference on Cyberspace 2013 and the Conference itself, the following principles and guidelines, inter alia, are identified for an open and secure cyberspace:

1. **Economic Growth and Development**

* Internet is a central element of the infrastructure of the information society and a global facility available to the public. (UNGA/RES/67/195). The global and open nature of the Internet is a driving force in accelerating progress towards development in its various forms. (A/HRC/RES/20/8). States maintain an open environment that supports the free flow of information, research, innovation, entrepreneurship and business transformation. States ensure the protection of personal information in the online environment and empower consumers and users in online transactions and exchanges. (Seoul Declaration for the Future of the Internet Economy, 2008) It is necessary to continue to work together towards ensuring a trusted, secure and sustainable environment in partnership with multiple stakeholders, including international organizations and the private sector. (2012 APECTELMIN Saint Petersburg Declaration, Para 25
* More ubiquitous access to and use of broadband Internet networks, which are available in a competitive market and at affordable prices, is essential to foster innovation and drive the growth of the Internet economy and of the economy in general. (OECD Principles for Internet Policy-making)
* The information and communication technologies have the potential to provide new solutions to development challenges, particularly in the context of globalization ,and can foster sustained, inclusive and equitable economic growth and sustainable development, competitiveness, access to information and knowledge, poverty eradication and social inclusion that will help to expedite the integration of all countries, especially developing countries, in particular the least developed countries, into the global economy. (UN A/RES/67/195)

1. **Social and Cultural Benefits**

* The same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.(UN A/HRC/RES/20/8）
* Stakeholders including business, civil society, the Internet technical community and academic institutions, make an essential contribution to the ongoing development of the Internet and the enrichment of society using the Internet. (OECD Communique on Principles for Internet Policy-Making)
* The international management of the Internet should be multilateral, transparent and democratic, with the full involvement of Government, the private sector, civil society, academic and technical communities and international organizations.(UN A/RES/67/195)
* Cultural and linguistic diversity online is important to enable people to exercise their individual, social and cultural rights”. (A/RES/67/195 and ICESCR).

1. **Cybersecurity**

* Governments, business, organizations and individual owners and users of information technologies(cyberspace) must assume responsibility for and take steps to enhance the security of the information technologies(UNGA/RES/64/211) States and relevant regional and international organizations that have developed strategies to deal with cybersecurity and the protection of critical information infrastructures are encouraged to share their practices and measures that could assist other Member States in their efforts to facilitate the achievement of cybersecurity. (UNGA/RES/64/211).
* The Security of critical information infrastructures is a responsibility Governments must address systematically and an area in which they must lead nationally, in coordination with relevant stakeholders, who in turn must be aware of relevant risks, preventive measures and effective responses in a manner appropriate to their respective roles.（UN A/RES/64/211）Note: It may be redundant with the above
* States affirm the need for a common understanding of the issues of Internet security, and for further cooperation to facilitate outreach, the collection and dissemination of security-related information and exchange of good practice among all stakeholders on measures to combat security threats, at national and international levels. (Tunis Agenda for the Information Society)

1. **International Security**

* International law, and in particular the UN Charter, is applicable and is essential to maintaining security and stability and promoting an open, secure, peaceful and accessible cyberspace (ICT environment). (UN GGE REPORT A/68/98, 2013, Para 19)
* The application of norms derived from existing international law relevant to the use of ICTs by States is an essential measure to reduce risks to international peace, security and stability. Common understandings on how such norms shall apply to State behaviour and the use of ICTs by State requires further study. Given the unique attributes of ICTs, additional norms could be developed over time. (UN GGE REPORT A/68/98, 2013, Para 16)
* States have repeatedly affirmed the need for cooperative action against threats resulting from the malicious use of ICTs. Further progress in cooperation at the international level will require an array of actions to promote a peaceful, secure, open and cooperative ICT environment. Consideration should be given to cooperative measures that could enhance international peace, stability and security. These include common understandings on the application of relevant international law and derived norms, rules and principles of responsible behaviour of States.(UN GGE Report, A/68/98, 2013, Para 11)
* State Sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory.（UN GGE Report 2013, Para 20)
* States must meet their international obligations regarding internationally wrongful acts attributable to them. States must not use proxies to commit internationally wrongful acts. States should seek to ensure that their territories are not used by non-State actors for unlawful use of ICTs.(UNGGE Report , A/68/98 , 2013 para 23)
* Voluntary confidence building measures can promote trust and assurance among States and help reduce the risk of conflict by increasing predictability and reducing misperception. (UN GGE REPORT A/68/98, 2013, Para 26)
* The United Nations should play a leading role in promoting dialogue among member states to develop common understandings on the security of and in the use of ICTS. (UN GGE Report, A/68/98, 2013，Para 13)
* State efforts to address the security of ICTs must go hand- in-hand with respect for human rights and fundamental freedoms set forth in the Universal Declaration of Human Rights and other international instruments. (UNGGE Report, para 21, A/68/98)

1. **Cybercrime**

* Law enforcement cooperation in the investigation and prosecution of international cases of criminal misuse of information technologies(cyberspace) should be coordinated among all concerned States. (UNGA/RES/55/63)
* States should intensify cooperation against criminal or terrorist use of ICTS, harmonize the legal approaches as appropriate, and strengthen practical collaboration between respective law enforcement and prosecutorial agencies (UNGGE REPORT A/68/98, 2013, Para 22)
* States are encouraged strengthen partnerships for technical assistance and capacity building to counter cybercrime, in cooperation with other States, relevant organizations, the private sector and civil society.(UNODC/CCPCJ/2013/RES/22/8)
* The fight against the criminal misuse of information technologies requires the development of solutions taking into account both the protection of individual freedoms and privacy and the preservation of the capacity of Governments to fight such criminal misuse (A/55/63, para 1(J))

1. **Capacity Building**

* Capacity building is of vital importance to an effective cooperative effort on securing cyberspace. (UN GGE REPORT, A/68/98, 2013)
* Capacity building requires the full participation of government, business, and civil society. (G8 foreign minister statement 2013)
* States need to enhance efforts to close the digital divide in order to achieve universal access to information and communications technologies and to protect critical information infrastructures by facilitating the transfer of information technology and capacity-building to developing countries, especially the least developed countries, in the areas of cybersecurity best practices and training.” (A/RES/64/211)
* Information and communications technologies present new opportunities and challenges and there is a pressing need to address the major impediments that developing countries face in accessing the new technologies, such as insufficient resources, infrastructure, education, capacity, investment and connectivity and issues related to technology ownership, standards and flows, and in this regard calls upon all stakeholders to provide adequate resources, enhanced capacity-building and technology transfer on mutually agreed terms, to developing countries, particularly the least developed countries(UNGA/RES/ 67/195).

/End/