Seoul Framework for and Commitment to an Open and Secure Cyberspace

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

All sources are identified in the foot notes at the end of this document

1. Economic Growth and Development

- The Internet is a central element of the infrastructure of the information society and a global facility available to the public.[1]The global and open nature of the Internet is a driving force in accelerating progress towards development in its various forms.[2] It is important to maintain an open environment that supports the free flow of information, research, innovation, entrepreneurship and business transformation, to ensure the protection of personal information in the online environment and to empower consumers and users in online transactions and exchanges.[3] 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.[4]

- 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.[5]

- 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.[6]

2. 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.[7]

- 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. [8]

- 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). [18]

- 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.[19] 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. [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. [21]

- Voluntary confidence building measures can promote trust and assurance among States and help reduce the risk of conflict by increasing predictability and reducing misperception. They can make an important contribution to addressing the concerns of States over the use of ICTs by States and could be a significant step towards greater international security. [22]

5. 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. [23]

- States should intensify cooperation against criminal or terrorist use of ICTS, harmonize legal approaches as appropriate, and strengthen practical collaboration between respective law enforcement and prosecutorial agencies. [24]

- States are encouraged to strengthen partnerships for technical assistance and capacity building to counter cybercrime, in cooperation with other States, relevant organizations, the private sector and civil society.[25]

- 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. [26]

6. Capacity Building

- 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 cyber security best practices and training." [27]

- 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.[9]

- Cultural diversity is the common heritage of humankind. The Information Society should be founded on and stimulate respect for cultural identity, cultural and linguistic diversity, traditions and religions, and foster dialogue among cultures and civilizations. [10]

3. Cyber security

- 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.[11] States and relevant regional and international organizations that have developed strategies to deal with cyber security 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 cyber security. [12]

- 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. [13]

- 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. [14]

4. International Security

- 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. [15]

- 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, encourage regional efforts, promote confidence-building and transparency measures and support capacity-building and the dissemination of best practices. [16]

- 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. [17]

- 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. [28]

- Capacity building is of vital importance to an effective cooperative global effort on securing ICTs and their use. Some States may require assistance in their efforts to: improve the security of critical ICT infrastructure; develop technical skill and appropriate legislation, strategies and regulatory frameworks to fulfill their responsibilities; and bridge the divide in the security of ICTs and their use. [29]

- Capacity building requires the full participation of government, business, and civil society. [30]

/End/

References

1 UNGA/RES/67/195
2 UNGA/HRC/RES/20/8
3 Seoul Declaration for the Future of the Internet Economy, 2008
4 2012 APECTELMIN Saint Petersburg Declaration, Para 25
5 OECD Principles for Internet Policy-making
6 UNGA/RES/67/195
7 UNGA/HRC/RES/20/8
8 OECD Principles for Internet Policy-making
9 UNGA/RES/67/195
10 Declaration of Principles, World Summit on the Information Society, Geneva 2003
11 UNGA/RES/64/211
12 UNGA/RES/64/211
13 UNGA/RES/64/21
14 Tunis Agenda for the Information Society
15 UNGGE Report A/68/98, 2013, Para 1
16 UNGGE Report A/68/98, 2013, Para 13
17 UNGGE Report A/68/98, 2013, Para 16
18 UNGGE Report A/68/98, 2013, Para 19
19 UNGGE Report A/68/98, 2013, Para 20
20 UNGGE Report A/68/98, 2013, Para 21
21 UNGGE Report A/68/98, 2013, Para 23
22 UNGGE Report A/68/98, 2013, Para 26
23 UNGA/RES/55/63
24 UNGGE Report A/68/98, 2013, Para 22
25 UNODC/CCPCJ/2013/RES/22/8
26 UNGA/55/63, para 1(J)
27 UNGA/RES/64/211
28 UNGA/RES/67/195
29 UN GGE Report A/68/98, 2013, para 30
30 G8 Foreign Minister statement 2013