Draft WSIS+10 Vision for WSIS Beyond 2015

C5. Building confidence and security in the use of ICTs

Recognizing the central role of building confidence and security in the use of ICTs, as well as the efforts dedicated towards implementation of WSIS Outcomes, in particular related to Action Line C5, since 2003 significant progress has been achieved and several emerging trends and challenges have been identified.

Following provides guidance and priorities for implementation of WSIS Action Line C5 beyond 2015.

a) Engagement of all stakeholders, cooperation:

1. Recognize that the open nature of the multistakeholder process has proved adept at developing innovative solutions to technical and policy problems. The WSIS process should guide governments to **look beyond solely legislation and government-led solutions**, in order to both harness the existing knowledge and expertise of the multistakeholder organizations, and engage with them to enhance and improve the existing solutions.
2. **Need Multistakeholder cooperation** to foster a global culture of cybersecurity.
3. Appreciate that many confidence and security solutions are developed in **cooperation between different stakeholders including industry, academia and governments**.
4. Recognize that the **technical community and the private sector have critical expertise** that must be better incorporated into cybersecurity related policy-making.
5. Encourage **governments to work with the business sector** on a more regular basis.
6. Stress the **need for International cooperation** against cyber attack
7. Encourage **cooperation and sharing of information between the public and the private sectors and on the interregional level** in order to maintain the protection and security of networks and information systems and the protection of national cyberspace, including the application of the security measures, resilience and recovery for local networks and computer systems

This document builds upon the input/ background documents and the contributions received during the WSIS+10 High-Level Event Open Consultation Process. It has been developed for the purposes of the First Physical meeting of the Open Consultation Process.

8. Pursue greater global cooperation toward achieving **cohesive, compatible, cybersecurity policies and agreement** among governments aimed at preventing unreasonable government intrusion without appropriate oversight protections
9. Recognize that while malicious actions can undermine users' trust and confidence in the network, but **closing the Internet is not the solution**. Instead, we need to focus on ensuring the Internet is stable, secure and resilient. To do so, it is important that these **issues be addressed by all stakeholders in a spirit of collaboration and shared responsibility**. It is also important that these issues be addressed in **ways that do not undermine the global architecture of the Internet or curtail internationally recognized human rights**.
10. **Actualize enhanced cooperation**, to enable governments, on an equal footing, to carry out their roles and responsibilities, in international public policy issues pertaining to the Internet.
11. **Cooperate with the business sector**, such as manufacturers and operators, to pave the way toward the achievement of the **"security by design"** concept, where devices and products contain standard security features to reduce the exploitation of vulnerabilities

b) Frameworks addressing the issue of cyber security:

12. Strengthen and enhance the legal and regulatory frameworks.
13. Recognize the **growing importance of pursuing national, regional and international frameworks**
14. Through a programme of **multi-lateral cooperation at the legislative level**, implement comprehensive cyber-legislation in line with international treaties and conventions at the global and regional level to cover all topics related to cyberspace, in particular those related to cybercrimes, privacy and confidentiality of personal information;
15. Emphasize the need for an **international framework focused on the elaboration of norms and principles agreed at global level**, specifically in the following areas:
    - access to the Internet
    - security
    - protection of fundamental rights
    - state involvement and
    - international cooperation
16. Recognize the urgent need for **building a solid legal framework** to address existing and emerging cybercrimes at national, regional and international levels
17. Encourage stakeholders to **invest in existing fora** that work to build confidence and security in ICTs. While new national, regional, and international frameworks may be appropriate in some cases, there is already an ecosystem of entities and structures that address the issue of cybersecurity.
18. Encourage that all **frameworks must be subject to "evidence-based policy-making**" involving all stakeholders and the necessary expertise.
19. Recognize that **cloud computing is an important issue which raises both jurisdictional and investigative problems** and needs careful examination.
20. Note that more than ten year implementation of the Cybercrime Convention has brought forth a range of **measures and partnerships against cybercrime. They have to be enriched further on a global and regional level**.

21. Develop appropriate **national legal and regulatory framework for privacy protection, e-transactions and cybersecurity**
22. Leverage **enhanced cooperation to develop solid legal frameworks and operational processes** to address security, cybercrime, spam and related abuses at the national, regional and international levels
23. Highlight that any emerging international framework focused on the **elaboration of norms and principles in the area of access to the Internet** will need to address public access if we are to ensure that everyone in the information society is catered for.
24. Establish special regional structure in order to build confidence in using ICT within the region.
25. Recognize the need for an **international agreement to cooperate on security matters** and to avoid unilateral assertions of national laws and to avoid extra-territorial actions. In this context, all countries should acceded to the 2012 ITRs and should consider the principles posted at "necessaryandproportionate.org", both when developing or revising national legislations, and as a possible new Resolution or Statement.
26. Need Institutional and regulatory framework for the **protection of personal data at cross-border level.**

c) Technical and procedural measures:

27. Recognize the **importance of the concept of "security by design", especially amongst the business sector** when providing products and services.
28. Outline standards and adopt novel and innovative methodologies on how to develop **safe and reliable e-services and applications resilient to external risks and threats**, including necessary mechanisms to maintain the privacy and confidentiality of personal information with special focus on the Arab region specificity in general and the development Arabic-enabled tools in particular
29. Develop and integrate technology, protocols and standards improvements that introduce **native capability for Internet** security while maintaining stability and interoperability.
30. Promote the **use of e-signature methods**, with enhancing the confidence and security in using such technology, which could be done through adopting efficient legislations and using different mechanisms as developing USB-based authentication token for multiple applications and network services.
31. Develop an **effective and efficient equipment certification process** and ensure adherence to global standards benefits both the industry and users, as it protects the integrity of the telecom networks, guarantees that consumers get standard equipment that works and prevents frequency spectrum interferences.

32. Facilitate the **introduction and expansion of electronic transactions** over the Internet and the development of efficient security systems in this regard.
33. Adopt a strict hierarchical architecture for the **public key infrastructure (PKI)** set up as it is becoming central to efforts to protect digital identity for individuals and organizations, enabling advanced e-business, e-government and e-commerce activities.
34. Recognize the **urgent need to introduce cyber risk analysis and risk management** and Develop a **better understanding and analysis of the threats and actors involved**; this would allow for more tailored and proportionate policy responses.
35. Recognize the increasing importance of **proactively identifying vulnerabilities** in critical resources, infrastructures and key priorities relying as part of a cyber security plan involving all stakeholders
36. Promote World Standards Cooperation
37. Focus on security in **mobile devices and the Cloud**, security of **critical infrastructures**., computer security for **national defense**

d) Organizational Structures

38. Realize the need to establish strategies and capabilities at the national level to ensure protection of national critical infrastructures, while enabling prevention and prompt responses to cyberthreats. Also the **establishment of Computer Incident Response Teams (CERTs) with national responsibilities** and national cybersecurity frameworks are key elements towards the achievement of cybserecurity.
39. Encourage with appreciation the growing deployment of national Computer Incident Response Teams.
40. Encourage and **support Security and Emergency Response Team at the Government and Business level**.
41. Establish ISMS (**Information Security Management system**) in each organization
42. Create **alert centers** in those countries that do not have one
    a. Enhance alert centers in those countries that have one
    b. Promote the interconnection of the alert centers
43. Establish the **NISC (National Information Security Center) within the government to promote measures relating to information security**. The NISC establishes basic strategies on information security, promotes and assists measures on security for the government.

e) Capacity Building:

44. Recognize that prevention represents an important stage in the fight against attacks in cyberspace. It is a broad category encompassing the elaboration of standards as well as practical steps such as: constant provision of information about the opportunities and the risks of the Internet; formation of special skills and behaviour of users and especially of young people; distribution of sufficient materials; organization of campaigns; promotion of good models and practices, etc.

45. Emphasize the importance of accounting for the "**human element" as priority**.
46. Recognize the **urgency to build human capacity**, to improve the skills and expertise of security professionals and increase the awareness of the general public
47. Build **national and regional capabilities** in the field of Cyber-Security. There is a need to continue building national and regional Computer Incident Response Teams.
48. Promote **Education for safety and security** of Internet usage. Raise **public awareness in regards to online safety** at large for all segments of users with various aims.
49. Encourage **campaigns by the governments and other stakeholders** to promote people's awareness about the importance of confidence, safety and security in cyberspace and empower them to protect themselves against the threats.
50. Promote **dialogue on confidence and security issues between all stakeholders**. The security of the individual must be further prioritized.
51. Contribute to the **building of a "national culture of cyber security"** through proper awareness and education campaigns regarding online risks particularly those affecting children
52. Enhance ICT literacy that includes **knowledge on information morals and information security**
53. Encourage the education and training institutes to develop related programs on cyber security to ensure the **availability of qualified human resources**.
54. Provide **assistance to countries needing help** in setting up national cybersecurity strategies and the creation of national Computer Incident Response Teams (CERTs). This could be provided in a number of ways **including by bilateral assistance from those countries that have already set up national strategies and CERTs**.
55. Aim to **educate government officials on non-legislative solutions available to them**, and facilitate bringing together technical experts - from the business community and civil society - and policy makers in developing countries. As the issues faced by the stakeholders engaged with Internet security develop rapidly it is difficult for legislation to keep up with the pace of technological change. Engaging with, and benefiting from, international best-practices and policies developed by the multistakeholder organizations can be a more effective way to enhance security for all stakeholders.
56. Enhance regulatory requirement and institute an **effective assessment mechanism on the ISP's security capability**; Encourage **industry self-discipline on content management**; Awareness-raising for Internet users

f) Privacy, Data protection, Intellectual property:

57. **Protect the privacy and personal data** in the various processes of information processing in the public and private sectors
58. **Protect intellectual property and copyright**
59. Raise the **awareness on the IPR and related rights.**
60. Promote **respect for privacy in the digital age**. Business and government should work together in developing practices aimed at ensuring protection for personal data in a manner that not only provides effective protection of personal data and privacy, but

also enables the data flows that are needed by new technologies and business models to foster both economic growth and societal benefits.

61. Promotion of **personal data utilization and circulation considering privacy protections** etc.
62. Clarify rules regarding utilization of personal data that considers the **balance between free circulation of information and protection of privacy**
63. Enhance utilization and circulation of information that contains personal datum that crosses over borders through network
64. Recognize the **contradictions between surveillance and security**, with one undermining the other.
65. Note that **Public confidence in the privacy of personal data has been shaken** by a) the increasing use of personal data by commercial enterprises to maximise business revenues, with **limited control available to individual users over their own information**; and b) recent revelations concerning the extent of mass surveillance of personal data and communications, including internet use, by government agencies. These two factors threaten public confidence in ICTs and especially the internet, and could in particular inhibit the use of cloud computing. They also raise the risk of data becoming available to criminal organisations and so increase the vulnerability of electronic commerce.
66. Concern about the **importance of data privacy and data protection**, resulting from changes in the capabilities of technology, the depth and intrusiveness of analysis of data now undertaken by commercial businesses, and recent revelations concerning surveillance by governments. These are likely to be **exacerbated by the spread of cloud computing and the advent of the internet of things**. Public confidence in ICTs and the internet depends on data privacy and data protection, which should be given greater emphasis in this Action Line.
67. A new concept of **data protection under the conditions of cloud computing to be formulated** and **cross-border instruments for investigation** be elaborated.

g) Human Rights, Freedom of Expression:

68. Recognize that **Freedom of expression and the media can be crucial tools** for attaining all enlisted goals and the media can be a valuable partner in the fight against cybercrime and other cyber offences and risks. Freedom of expression on the one hand can boost positive attitude and on the other help in exchanging relevant information and good practice.
69. **Concern for the catch-all approach to the issue of cybersecurity and the use of invasive and disproportionate policy responses** that can imperil human rights and economic development
70. Attention to cybersecurity needs to **balance the protection of individual citizens with the protection of ICT and internet access and services for society as a whole.**

h) **Protection of the vulnerable**

71. Emphasize the urgency to **ensure that the child online safety element is imbedded in the work stream of Action Line C5**

72. Need **special protection against harmful and inappropriate behaviour on the net**. With regard to this **children and the most vulnerable have to be particularly protected and educated** how to communicate in the new information environment.
73. Emphasize that it is **critical to provide parents and children with the information they need** to navigate cyberspace in order **to create a trusted environment** that will encourage children to go online.
74. Encourage **broad cooperation between national authorities and social partners** (including the owners of the servers and Internet portals, foundations, etc.) in order to protect children from the illicit content.
75. Encourage **Governments, educators and industry together to help parents and children** understand how to maximize the benefits and minimize the risks of being online.
76. Develop responsible practices, clear information, robust education and coordinated law enforcement efforts that can greatly improve the level of safety children experience online.
77. Emphasize that **special protection should be offered against cyberbulling and cyberattacks on women.**
78. Prioritize **Digital literacy among girls and women** .
79. Governments and private sector should commit to provide a safer ICT services particularly internet for child and family to fulfill their obligations based on the UN Convention on the Rights of Child and its optional protocols.
80. Encourage all stakeholders to work to establish Child Online Protection (COP) frameworks to promote and harmonize the necessary activities to provide safer internet for child at regional and national level.
81. Develop **policies to guide child online protection**.
82. Emphasize the **need to protect children from accessing undesirable content, including child pornography**.
83. Highlight **violence against women online** which presents a serious threat and inhibitor for women's use of ICTs; privacy issues.

i) Spam

84. Promote measures against spam mail