Transnational Radical Party

TRP RESPONSE TO WSIS DRAFT DECLARATION AND DRAFT ACTION PLAN

The following are TRP's comments on the Draft Declaration and Draft Plan of Action dated March 21, 2003 (WSIS/PCIP/DT/1-E and WSIS/PCIP/DT/2-E).

(NOTE: In this document the original draft text is in *italics*. TRP suggested text is boxed.)

Comments on Draft Declaration

Para 22:   ***Access to knowledge****: Individuals and organisations should benefit from access to information, knowledge and ideas. The sharing and strengthening of global knowledge for development can be enhanced by ensuring equitable access to information for educational, scientific, economic, social, political and cultural activities.*

TRP welcomes this paragraph. The TRP would like to stress the importance to expose the non compliance with such a paragraph as a violation of internationally recognized human rights. For this reason the TRP recommends the following language:

> The closure of websites and/or the surveillance and/or persecution of net-surfers and on-line activists should be considered a violation of Art. 19 of the International Covenant on Civil and Political Rights (ICCPR).

To address the issue in a more comprehensive way, the TRP suggest the introduction of a paragraph 22 bis:

> The UN and its Member States should promote the adoption of a series of legislative measures to foster the right of every citizen to have access, at any moment and through a variety of means of communication including the Internet, to the proceedings of public institutions, as well as meetings of the elective and competent bodies, and to obtain public documents on and off line

Para 35:   ***Secure and reliable infrastructure****: To realise the full benefits of ICTs, networks and information systems must be sufficiently robust to prevent, detect and to respond appropriately to security incidents. However, effective security of information systems is not merely a matter of government and law enforcement practices, nor of technology. A global culture of cyber-security needs to be developed (UNGA Resolution 57/295, of 20 December 2002).*

TRP suggests introducing the principle of "technological neutrality" of legislation in Para 35 in order to avoid any discrimination against the use of any specific technology. This principle should also be extended to cover the relationship between "on-line" and "off-line" technologies. Of particular importance is the example provided by the freedom to demonstrate; in fact, a demonstration held in cyberspace – which, like a demonstration "in the real world" may also generate a certain amount of "acceptable" inconvenience – could be merely criminalised for the very fact of involving information systems. To address those concerns, the TRP recommends the following language:

> International and national laws should be based on the principle of "technological neutrality". This principle should not be interpreted solely as requiring non-discrimination with regard to the use of one type of technology as opposed to another, but also as preventing a given activity from being criminalised merely because it involves the use of such a technology.

Comments on Draft Plan of Action

13. *Access to public domain information: Information in the public domain should be of quality, easily accessible for all, including the disabled.*

14. *Open standards and open-source software: Development and deployment of open-source software and standards for ICT networking should be encouraged:*
    - Open and flexible international and interoperable standards should be promoted to ensure that all can utilize the technology and associated content and services to their maximum potential.
    - Open-source software, including UNESCO software CDS/ISIS, multi-platform and open platform as well as interoperability standards, should be used more broadly to provide freedom of choice and to facilitate access to ICTs by all citizens, at an affordable cost.
    - Standardization efforts in the field of terminology and other language resources should be intensified.

The TRP welcomes this paragraph, but would urge a more clear detailed and specific definition of what should be done in order to guarantee an open and user-friendly Internet:

> **Access to public domain information.** The information provided online must be presented not only in graphic form but also in textual mode, to enable people with sensory difficulties to use it.
> **Open standards and open-source software**. It should also be possible for all the information to be accessed also via user-friendly programs that are not dependent on proprietary software and whose use is not governed by the need for a license, patent or by any other commercial requirement.
> All information concerning citizens' civil and political rights should be provided free of charge. None of the information in possession of and/or produced by the public sector should be governed by any form of copyright that would impose an objective limit on its dissemination and re-use.

27. *Fighting cybercrime: Protection from civil and criminal offences ("cybercrime") is essential in order to build trust in information networks:*
    - A multi-pronged approach is needed to tackle cybercrime, on all fronts, with emphasis on preventive approaches, national guidelines and regional and international cooperation. At the same time, action to address cybercrime and to ensure a safe and secure Information

Society must respect the sovereignty of nations and maintain respect for the constitutional and other rights of all persons, including freedom of expression.
- Existing legal instruments, such as the Council of Europe Convention on Cybercrime, offer the international community a foundation from which to build.

In order to avoid any abuse of the international and national legislation on cyber-crime, the TRP believes it is necessary to insert the following language in Para 27:

> The obligation to regard as a criminal offence access "without right" to information systems should not be extended to activities of little or no consequence (which would not be punished if carried out "off line", i.e. without the use of new technologies) or to activities that could be regarded as a form of self-defence and/or affirmation of universal Human Rights directed against systems being used to the detriment of the norms contained in the ICCPR.