Internet Society

The Internet is for Everyone

Contribution following the first Expert Group meeting

including comments on the second draft of the ITU Secretariat General's Report

Following the first meeting of the World Telecommunication Policy Forum (WTPF) Expert Group held on the 24th of June, we have prepared additional comments (see attached document) we would like to submit on the second draft of the Secretary General's Report. As requested by the ITU Secretariat General, the document also includes a proposal of a selected topic related to Convergence and Emerging policy issues. We have developed this proposal below.

ISOC wishes to voice support for the direction of many comments made several times in the development of the first draft of the Secretary General's Report and subsequent discussion: specifically that the WTPF will be more useful and effective if it narrows its focus to a pressing issue being faced by the world community.

To be specific, ISOC would support focusing on **ICT and Public Safety or Public Warning systems**. The disasters that followed the tsunami of December 26, 2004, in New Orleans in 2005, in India in 2006, in Nepal and Indonesia in 2007, as well as the recent disasters and flooding in Myanmar, several areas of China, and in the mid-western United States, to name only a few, have repeatedly challenged governments, providers of information and communications technologies to find ways to improve public warning. Warning systems must be able to alert the public about major hazards and should communicate warning messages via all available notification methods.

The following provides a brief overview of the problem and issues which we believe must be addressed urgently, and which could benefit from being adopted as the prime focus of the 2009 WTPF.

The WSIS Declaration of Principles has already highlighted the need to pay special attention to conditions that pose severe threats to development, such as natural disasters. The WSIS Action Plan goes on to make a specific call to establish monitoring systems, using Information and Communication Technology (ICT), to forecast and monitor the impact of natural and man-made disasters particularly in developing countries, least developed countries and small economies.

The need for a global and multi-stakeholder framework to allow coordination and synergy

Collaborative actions are necessary to assure that standards-based, all-media, all-hazards public warning becomes an essential infrastructure component available to all societies worldwide. To support these goals, the Internet Society (ISOC) has participated to launching the "Public Warning Network Challenge" - a call for collaborative action in order to make such public warning systems a reality. It is essential and urgent to provide an enabling environment in which stakeholders everywhere can cooperate to bring the benefits of ICT applications to the area of disaster prevention.

The goal of public warning is that people who are properly alerted will act to reduce the damage and loss of life caused by a natural or man-made hazard event. To ensure that everyone can be alerted, it is essential to leverage all available communications media. To minimize the public confusion that occurs during emergencies, the alerting system should be in routine use for all hazards, not only for rare events such as earthquakes and tsunami, but for severe weather, fire, and other threats.

In many nations, common carriers such as radio, television, and telephone networks have implemented particular public alert technologies for hazards or threats such as weather events or civil defense. From the societal perspective of public warning investments, it makes no sense to continue building a separate public warning system for each particular threat. Efficient use of funds as well as effectiveness of public warning both argue for using standards and combining the public warning requirement for all-media coverage with the requirement for an all-hazards approach.

A standards-based, all-media, all-hazards public warning strategy not only makes sense for governments who need to alert the public, it makes sense for a wide range of information technology providers and communications carriers as well. As providers of information and communications migrate to digital technologies, services are being offered that integrate radio and television with cellular and satellite telephone and with a variety of Internet-based and other network services. A service that supports all-hazard alerts and warnings is no longer a matter of designing specialized communications technology; it is a matter of simply agreeing on common standards for the content and handling of such alerts.

The content of alert messages is now being standardized across all hazard types, including severe weather, fires, earthquakes, and tsunami. In 2004, the Common Alerting Protocol (CAP) was agreed as an international standard for all-hazard alert messages. All-media distribution of CAP messages is being implemented on ever larger scales, types of alerts, and ranges of technologies. Operational systems have shown that a single authoritative and secure alert message can quickly launch Internet messages, news feeds, television text captions, highway sign messages, and synthesized voice over automated telephone calls or radio broadcasts.

However, the Emerging issue of ICT and Public warning systems requires important cautions that need to be addressed within a global and multi-stakeholder policy forum such as the WTPF 2009:

- Effective public warning involves many distinct aspects that need to be addressed in an exhaustive approach including public education, training, building codes, policy, science, and research, among many others.
- Emergency management processes should provide for human judgment between the detection of a threat situation and the issuing of public alerts, usually under control of officials with appropriate responsibilities.
- Designers of technologies supporting public warning should take into account that false alarms can be disruptive, expensive, and can degrade public confidence.
- In any system of public warning, the authentication of senders and targeted receivers is essential. Also, alerting systems can be targets for deliberate misinformation or denial-of-service attacks.
- Where alerting involves existing operational systems, any implementation of new technology will begin in parallel with current operations to assure there is no disruption of service or source of confusion.

We look forward discussing the comments submitted in the draft Secretariat General’s Report as well as the above proposal to have the WTPF usefully address a selected topic with our colleagues at the next meeting of the Expert Group to prepare the World Telecommunication Policy Forum 2009.