HIGHLIGHTS
4 December 2008

INTERNET GOVERNANCE FORUM DISCUSSES PROMOTING CYBERSECURITY AND TRUST

On the second day of the Internet Governance Forum meeting in Hyderabad, India, discussions in two main sessions focussed on the issue of cybersecurity and trust on the Internet. More than 1,200 participants were attending the Forum, including delegates from government, the private sector, academic and research institutions, civil society and media.

Parallel workshops covered, among other issues, cybersecurity and cybercrime, multilingualism on the Internet, access to local culture and language, the future IP standard (IPv6), ways to reach persons with disabilities, Internationalized Domain Names (IDNs), bringing Internet capacity and autonomy to developing nations, and driving investment in emerging economies. Also, one Dynamic Coalition meeting concentrated on open standards, and another on climate change.

The first panel discussion this morning examined the different categories of threats and different types of illegitimate behaviours and attacks on the Internet. It also reviewed activities, resources, tools and instruments to tackle these problems, as well as cooperation in this area, in view of the increasing number and sophistication of security threats to the Internet, such as spam, botnets, viruses, DDOS attacks and malware, identity theft and other types of fraud, as well as child pornography and other content-related offences.

In the second panel, participants underlined the intricate relations existing between security, privacy and openness. They considered the different issues raised by privacy and openness, and drew attention to issues such as child protection, privacy and freedom of expression. In this respect, the right to data protection was one of the issues raised. It was stressed that the Internet Governance Forum was playing an important role in supporting the idea of an Internet Bill of Rights, which should be seen as a process, not as a negotiation of a traditional convention. Other speakers drew attention to how the Internet is impacting upon young people and their development.

The Dimensions of Cybersecurity and Cybercrime: A Mapping of Issues and Our Current Capabilities

The moderator for the discussion on the dimensions of cybersecurity and cybercrime was Bertrand de la Chapelle, of the Government of France.

The chair of the panel, R. Chandrasekhar, Special Secretary in the Indian Department of Information Technology (DIT), said heavy dependence on the Internet has also brought in its wake some unwelcome attention from people who would like to create problems in the working of the Internet, and also, by the fact that this medium is widely available, from those who want to perform acts which are illegitimate and illegal. Legislative measures are bogged down by problems of jurisdiction and geographical boundaries, and also by slow adaptability in a fast-changing technological environment.

The meeting also heard Michael Lewis, of Carnegie Mellon University, and serving as Deputy Director of Q-CERT in Qatar, and Marc Goodman of the International Multilateral Partnership Against Cyber Terrorism, who made presentations on the vulnerabilities stemming from the increasing number and range of devices, which had in turn increased the financial incentives and the interest for criminals and for terrorists. It is now fairly easy for someone to become a cybercriminal, and the rewards are quite high. Mr. Lewis stated that cybercrime is a growth industry, presenting new challenges to law enforcement, such that a comprehensive, multi-level response is necessary, and outlined mechanisms for coordinating national strategy for cybersecurity. He advocated for the creation of a "cyber security network" of trusted relations and the use of "CERT" or "CSIRT" training, utilizing the collected best practice recommendations of all relevant organizations, such as those compiled by the ITU-D's Question

22/1 on national frameworks for cybersecurity. Mr. Goodman also said that cybercrime was a global issue, and thus we need to work with our partners in the developing world to help ensure that we can have cybersecurity, cyber-peace, and cyber-trust around the world, and prevent cyber-havens.

Alexander Ntoko, head of corporate strategy at the International Telecommunication Union and focal point on cybersecurity, said the ITU had launched the global cybersecurity agenda, involving all the stakeholder groups, "because the tricky thing with cybersecurity, cyberthreats and cybercrime is that they involve so many actors."

Patrick Fälström, from Cisco, insisted on the shared responsibility of all in what is on the Internet. Because of that, it is even more important that service providers and other players on the Internet talk with each other. He also mentioned the important role of Computer Emergency Readiness Teams (CERTs).

On the issue of CERTs, the meeting also heard Jayantha Fernando, of the Sri Lankan CERT, and Gulshan Rai, Director of the Indian CERT, who both mentioned the importance of harmonization of laws, based in particular on the Council of Europe's Convention on Cybercrime.

Fostering security, privacy and openness

The panel on fostering security, privacy and openness was chaired by Shyamai Ghosh, Chairman of the Data Security Council of India (DSCI), and moderated by David A. Gross, U.S. Coordinator for International Communications and Information Policy.

Mr. Ghosh said one theme of the panel was also about the right to information, which is a building issue in India**.** It was also about conflicts between national security versus security as it relates to privacy. Mr. Gross also stressed that the World Summit on the Information Society, particularly in the Geneva phase, followed by the Tunis Agenda, set a high water mark for the commitment to free flow of information.

For his part, Stefano Rodot, chair of the Scientific Committee of the Agency for Fundamental Rights of the European Union, said there is increased awareness of the importance of data protection as regards not only the protection of the private sphere of individuals, but their very freedom. The Internet Governance Forum is playing an important role in this respect, giving support to the idea of an Internet Bill of Rights.

Abdul Waheed Khan, of the United Nations Educational, Scientific and Cultural Organization (UNESCO), underscored four fundamental principles for building knowledge societies: freedom of expression, universal access, respect for cultural and linguistic diversity, and quality education for all.

John Carr, who is the secretary of Children's Charities' Coalition on Internet Safety in the United Kingdom, said content is the first and most obvious issue we need to bear in mind when we think about children's use of the Internet. Other issues relate to the way the Internet can facilitate exchanges and benefit sexual predators; the way the Internet is facilitating insidious bullying and harassment; the way in which unscrupulous companies seek to sell to children and young people; and the question of addiction. He made a plea for a more sophisticated approach to children and young people, and to how we support families in helping their children, who are usually more Internet literate than their parents.

Jac SM Kee, member of the Association for Progressive Communications (APC) (Malaysia), introduced into the debate on privacy, openness, and security the dimension of women's human rights, saying the Internet has become a critical space for women of marginalized and diverse sensibilities toward sexuality to network, to exchange information and to be able to build communities with each other.

Joseph Alhadeff, of Oracle, said that with global information flows, information is less tied to geography. Users are now creators and publishers, and not just people who are acted upon, and generational and geographic attitudes and values are changing related to privacy.