IGF Daily Highlights - 23 October 2013 P.M.

For information media • not an official record

IGF sessions zoom in on Managing Risks of Cyberspace Era

Bali, Indonesia - Aiming to produce takeaways on legal and other frameworks for addressing the complex problems of spam, hacking and cyber-crime, the Internet Governance Forum (IGF) devoted an afternoon focus session to examining the impact of these security issues. Consistent themes addressed by the discussants centered on the need for international capacity building, sharing best practices, international and regional cooperation modalities, and continued discussions around the Budapest Convention on Cybercrime. Recommendations from the session included the possibility that the IGF offer training -- as part of the concerns around capacity building.

One part of the discussion focused on capacity-building activities being undertaken at an international level to help address spam, based on successful initiatives to reduce and control unsolicited commercial e-mail. Some speakers emphasized that spam should be defined more broadly to include other unwanted electronic messages, particularly as some are linked to broader malicious activities (including phishing, malware, and identity theft).

A poignant example from Mexico was the increasing use of spam from criminal organizations to jam police emergency service call lines, which the commissioner of Mexico's telecommunications regulatory body described as an issue of "public and national security" that requires an "international strategy" that is "part and parcel of international telecommunications regulation." In response, the coordinator for cyber issues of the U.S. State Department said that while international cooperation was needed to deal with these threats, law enforcement issues can be addressed separately by "strengthening capabilities" without necessarily becoming the "subject of an international telecommunications regulatory scheme."

Questions from participants included a request for expert advice on whether developing countries should prioritize combating cyber-crime, protecting data, or combating spam.

The search for a reasonable balance between national interests in protecting citizens' security in cyberspace and upholding citizens' rights was the subject of a morning workshop on "Cybersecurity: Throwing Out Preconceptions", in which some speakers advocated a "risk management" approach as opposed to the belief that online security can be guaranteed. The discussion which followed highlighted the ever evolving nature of the term 'cybersecurity' and the importance of continuously learning about online risks since total 'security', in practical terms, is very difficult to achieve.

On a related theme, the “Cybercrime Treaty: Advantages for Developing Countries” workshop looked at what happens when cybersecurity issues cross national borders and examined the global and borderless nature of cybercrime. It specifically addressed cybercrime issues from a legal perspective and examined ways in which developing countries can overcome domestic and international cybersecurity and cybercrime challenges by participating in existing international and multilateral treaties. Some of the key points brought out in the discussion included the need for laws and policies to work with the architecture of the internet and not against it, relating particularly to copyright and intellectual property policy.

As well as looking at technical issues such as internet Infrastructure and terminology, a number of workshops concluded proceedings of Day 2 of the forum by looking at the power of the internet to help those who need to have their voices heard most. In this regard, the workshop on “Oppression Online: Rights and Restrictions on the Network”, looked at the social and economic impacts of national level ICT legislation and regulation as well as international telecom practices on human rights, particularly freedom of expression and privacy, including the impact of government and private sector practices at the national and international level.

The “Network Neutrality: from Architecture to Norms” workshop picked up on the human rights and freedom of expression on the internet discussion, in the context of recent trends by telecommunications operators to manage traffic flows in ways which may aim to block, filter and throttle different data flows in order to prioritise or impede access to specific applications, services or content. Participants in the discussion warned that without scrutiny or oversight these trends risk jeopardising open access to information and user's ability to send and receive the content they want using the applications or services of their choice.

Concerns raised around the use of intrusive traffic management techniques resonated with those discussed in the “State surveillance online: which principles and safeguards?” workshop, which looked at efforts that are being made to counter invasive surveillance from human rights, technological and other perspectives. The discussion centred around key principles of legality, legitimate aim, necessity, adequacy, proportionality, due process and judicial oversight, and ho
w
these can provide a framework in which governments and other stakeholders may assess how current or future laws on surveillance can comply with international human rights standards.

Looking towards the future, a workshop on the Internet of Things (IoT) highlighted the social impacts, economic opportunities and public policy issues of managing an environment in which an estimated 50 billion physical objects will be linked to the Internet by the year 2020.

For more information
visit: www.intgovforum.org/cms/ follow @intgovforum #IGF2013