



CONVENED BY THE UNITED NATIONS SECRETARY-GENERAL

10 – 13 November 2015, João Pessoa, Brazil

Lack of trust in the internet, a key driver of the global economy, can adversely impact the achievement of [the recently adopted sustainable development goals](#). Recognizing the crucial need to enhance cybersecurity and build trust, the 10th Annual Internet Governance Forum (IGF) in João Pessoa held valuable discussions with stakeholders coming from the government, private sector and the civil society to give them an opportunity to share their views on the challenges, and provide recommendations for addressing the issue of digital trust.

“Given the segregated nature of the internet, trust is central to the operation and continued growth of the internet. Each of us must have faith that the data stored in the cloud will remain secure, and that common status transacted online is based on enforced contracts,” stated Raul Gosain, Director of DeitY, Government of India, at the main session on “Enhancing Cybersecurity and building Trust” at the IGF.

Ambassador David Gross, partner at the Wiley Rein Firm, noted that millions of people are discouraged from going online for fear of facing cyberattacks. World-wide, every second, 18 adults become a victim of cybercrime, resulting in more than one-and-a-half million cybercrime victims each day.

David Van Duren of the Global Forum on Cyber Expertise stressed the crucial role of the internet, providing the example of his country, the Netherlands, where 80 per cent of the population do online banking, 60 per cent do internet shopping and 95 per cent use social media.

Participants at the session discussed the challenges found in tackling cybercrime and building trust on the internet.

“A key challenge is the fact that cybercrime doesn’t have any borders. This makes it difficult for law enforcement to be able to address cybercrimes,” noted William Check, Vice President of National Cable and Telecommunications Association (NCTA).

Advancements in technology have made the world smaller and have blurred boundaries, making it difficult to determine territorial jurisdiction. Additionally, the internet by nature is not static and evolves on a daily basis, therefore making a standard model for addressing cybersecurity unfeasible.

Another factor is addressing the issue of cybersecurity in an equitable manner to ensure that the freedom of expression as well as the growth of internet are not negatively impacted.

The general consensus coming of the session was that cybersecurity is everyone’s problem. Everyone should understand that the cyber world is a dangerous place and take action to make the internet safe. Moreover, a need for a comprehensive approach to tackle cybercrime and build trust, such as the introduction of security elements when developing cyber products and services, was highlighted.

There were many calls for multistakeholder participation in tackling cybercrime. The involvement of the government, private sector, civil society and other stakeholders in terms of sharing best practices, results of critical assessments and identifying globally accepted standards of cybersecurity was seen as fundamental. Participants also stressed the critical role that education plays in addressing cybercrime issues and noted that education should be expanded to involve all levels of society.

Capacity-building was cited as an indispensable driver for cybersecurity.

“Capacity-building is one of the most important components, while establishing information infrastructure. In order to establish a capacity-building programme for a nation, it is important to manage this through cybersecurity, through national cybersecurity strategy,” Zmarialai Wafa, Head of the Cybersecurity department of the Ministry of Communications in IT in Afghanistan.

On looking at the broad scope of cybersecurity, Mr. Wout de Natris, one of the moderators for the session, concluded that it was important for the participants present to undertake more active outreach to encourage the engagement of new stakeholders.

Chris Painter, Head of Cyber Issues of US State Department acknowledged that more countries are developing programmes, for example in Brazil, to get the local populations to understand the issue of cyber threats. He added that a cybersecurity awareness month in the US in October was also held. This culture of cybersecurity, while a long term process, is expected to contribute to greater awareness and help build trust in the internet, an engine for growth and development.