2010 ECOSOC General segment briefing on "Cyber security: emerging threats and challenges"

Friday, 16 July, 3:00-4:30 p.m.

Background Note

Today, information and communications technologies (ICTs) underpin just about all human activity-transportation networks, the management and provision of water supplies and power networks, industrial processes and supply chains, emergency services, healthcare, education and food distribution chains, to name just a few. Their use has become an indispensable component of political, social, economic and military life worldwide.

This dependence, however, has given rise to the need to protect against potential threats posed to the everyday lives of people and States alike. ICT networks, while connecting the world and many of the world's people, pay little attention to international borders and even international law. Cyber criminals have found ways to exploit loopholes, enabling them to attack corporations, individuals and governments worldwide. Cyber crime has now become a business which exceeds a trillion dollars a year in online fraud, identity theft, and lost intellectual property, affecting millions of people around the world, as well as countless businesses and the Governments of every nation.

The growing risk of cyber crime and cyber threats is real; no government can face this threat alone. At its 64th session, the General Assembly adopted a resolution on cyber security in which it recognized a need for national efforts to be supported by national, regional and international information-sharing and collaboration, so as to confront effectively the increasingly transnational nature of cyber threats. The resolution is attestation to the world's commitment to creating a global culture of cyber security. Most

crucially, the resolution affirmed that Governments are responsible for ensuring the security of critical information infrastructures, in coordination with relevant stakeholders. It furthermore called for a risk-based approach, whereby all stakeholders are made aware of relevant risks, preventive measures and effective responses in a manner appropriate to their respective roles.

The cross-border nature of cyber attacks and the organization of criminals necessitate international cooperation actions through justice and police systems. Countries need to take a proactive role in international initiatives, especially in the exchange of information and best practices, training and research. Capacity-building in organizational structures (including policies, roadmaps and strategies) is vital.

A briefing for ECOSOC members on these issues will take place on Friday, 16 July 2010 during the Council's General segment, from 3:00-4:30 p.m. in the ECOSOC Chamber (TNLB), and will be chaired by H.E. Mr. Somduth Soborun (Mauritius), Vice President of the Council. Its purpose will be to provide ECOSOC Members with a picture of what policies are being put into place to promote frameworks for international cooperation. The threat and challenges to cyber security can only be properly addressed through a strategy that takes into account the role played by all relevant stakeholders and existing initiatives in a framework of international cooperation. The briefing could also provide ECOSOC Member States with examples of national policies that could be adopted as well as the type of regional and international support that should be provided to successfully achieve a culture of cyber security.

Panelists:

Mr. Gary Fowlie, Representative and Head, International Telecommunications Union Office, New York

Mr. Mongi Hamdi, Head of Science, Technology and ICT Branch, Technology and Logistics Division, UNCTAD, Geneva

Ms. Gillian Murray, Officer-in-Charge, Organized Crime Section, and Focal Point for Cybercrime, Division for Treaty Affairs, United Nations Office on Drugs and Crime, Vienna