SPECIAL EVENT ON CYBERSECURITY AND DEVELOPMENT

9 December 2011, 10:00 a.m. to 1.00 p.m. ECOSOC Chamber, United Nations, New York

INFORMAL SUMMARY

Opening session

Chair	**H.E. Mr. Lazarous Kapambwe** (Zambia), President of the ECOSOC
Setting the stage	**Dr. Hamadoun I. Touré,** Secretary-General, International Telecommunication Union (ITU) **Honourable Undersecretary Fortunato de la Peña**, Undersecretary for Science and Technology, Philippines, and Chair, United Nations Commission on Science and Technology for Development (via video link)

The opening plenary featured an opening statement by the President of ECOSOC as well as the setting of the stage for the panel discussion by Dr. Hamadoun I. Touré, Secretary-General, International Telecommunication Union (ITU) and Honourable Undersecretary Fortunato de la Peña, Undersecretary for Science and Technology, Philippines, and Chair, United Nations Commission on Science and Technology for Development via video link from the Philippines.

Cybersecurity is one of the greatest issues of our times, and it will continue to grow in importance. As more and more people use mobile phones and the Internet, it is our collective duty to ensure that ICTs are safe and secure so that the 7 billion people of this planet can reap the benefits of ICTs. Today, everything is dependent on ICTs and we are all vulnerable – cybersecurity is a global issue which can only be solved with global solutions. Cybersecurity is an area that affects each and every agency and programme of the United Nations. As we push forward the UN agenda for peace and security, we must remember that cybersecurity is part of this. The UN system's collective engagement in addressing cyberthreats is critical. ITU is leading the call for stakeholders to work together to set international policies and standards, and to build an international framework for cybersecurity.

Cybersecurity has been the topic of many reports considered by CSTD. It is a topic of importance to both developed and developing countries. Cybersecurity is essential to ensuring a vibrant information society. Concerns regarding security, reliability, privacy and fraud can prevent people from making full use of ICTs and threaten the stability of information society. New and improved ICTs are accompanied by increasingly sophisticated challenges such as phishing, Intellectual Property Rights issues, hacking, online extortion, international money laundering and identity theft. Countries must ensure safe and secure cyberspace. At its 64th session, the General Assembly adopted a resolution on cybersecurity. The resolution recognized the need for national efforts to be supported by regional and international information sharing and collaboration due to the transnational nature of cyberthreats. CSTD has highlighted that as cyberattacks proliferate, new skilled personnel are needed to combat them. National cybersecurity strategies must recognize the need for awareness raising. Advanced courses in cybersecurity should be incorporated into curriculum worldwide to cultivate a global culture of cybersecurity.

Presentations by Panelists: "An international framework to combat cybercrime and improve cybersecurity"

Chair	**H.E. Mr. Lazarous Kapambwe**
Moderator:	**Mr. Gary Fowlie**, Head, ITU Liaison Office in New York
Panellists:	**Dr. Hamadoun I. Touré**
	Mr. Anthony V. Teelucksingh, Senior Counsel, Computer Crime and Intellectual Property Section, United State Department of Justice, Criminal Division
	Ms. Cheri F. McGuire, Vice-President, Global Government Affairs and Cybersecurity Policy, Symantec Corporation
	Mr. Mohd Noor Amin, Chairman, Management Board IMPACT Malaysia
	Ms. Deborah Taylor Tate, ITU Special Envoy and Laureate for Child Online Protection, United States Commissioner, Federal Communications Commission (Ret.)
	Ms. Simone Monasebian, United Nations Office on Drugs and Crime Representative and Chief of the New York Office

In this session, the panellists gave brief introductions highlighting their respective backgrounds and identifying their particular interest in the topic for discussion.

Some key issues that were discussed included the following:

- Cybersecurity is a global problem requiring global solutions;
- The international community can build on existing mechanisms such as the Budapest Convention and develop a global convention on cybercrime;
- A human rights-based approach is indispensable when considering a global framework for improving cybersecurity and fighting cybercrime;
- While there are real differences of views on issues of culture, ideology (including on privacy), utilizing approaches from other areas such as child online protection could be a way to achieve common ground much faster;
- It is urgent to provide LDCs with technical assistance to cope with cybercrime to prevent cybercriminals from taking advantage of the weakest link;
- Lessons can be drawn from fighting other types of crimes such as human trafficking and terrorism (empowering victims to speak out, etc.); and
- A multistakeholder approach would be indispensable with a strong role for the private sector.

A brief summary of the main ideas presented by the panellists:

Partnership of the private sector and government is the key to address the cybersecurity issue. The ICT infrastructure is constantly under attack with more sophisticated and organized approaches, and the cybercrimes caused extensive damage to the society. It is impossible to resolve cybercrime issues by any one company, any one government, or any one country. Government and the private sector should work together in order to address this issue. As ICT infrastructure is primarily owned and operated by the private sector, the private sector is responsible for the protection of that infrastructure. Moreover, the private sector still needs to look for cooperative approaches, collective defences on how to protect it in best manner. Regarding the role of government, it is necessary for it to secure its own systems, provide resources to fight cybercrimes, establish critical information infrastructure protection programmes, partner with industry, write plans for responses for attacks, coordinate and conduct exercises with industry, encourage adoption of security technology, provide

education and training and support private public partnership to raise cybersecurity awareness.

Domestic and international legislation, cooperation on the international level, and technical assistance to prosecutors, defendants, police and judges are critical to curb and prevent cybercrime. Defendants in criminal prosecutions learn everyday that laws are applied to cybersecurity space. Discussions concerning policies, norms, and agreements with respect to cybercrimes ought to be directed to strengthening and supporting the criminal prosecution capabilities in every country. The focus on efforts on the international level is in the form of bottom up support of the investigators, the police, the prosecutors, the defendants and the judges. There should be technical assistance to investigators to investigate these cases, assistance to prosecutors to train them in bringing in these cases, and assistance to judges to decide these cases. Fundamental to that mission is domestic legislation that covers very basic but broad aspects of cybercrime. The Budapest Convention on cybercrime lays out very simply the capacities that countries need to have with respect to domestic legislation on cybercrime. There are also other instruments that permit countries to support each other and to cooperate across borders with respect to cybercrime investigations. But the best cooperation internationally could not be achieved if there is a lack of domestic legislation or the capability to take necessary action. Moreover, successful prosecutions are based not only on international and national policy, but also the willingness of prosecutors, police and various countries to help. However, the important question is whether they have the necessary technical and legislative tools to do so.

The International Multilateral Partnership against Cyber Threats (IMPACT) is a platform that brings together government, industries and academia under the umbrella of the ITU, in order to address and to fight the cybercrime. With 107 partner nations and strong support from industries globally, IMPACT today is the largest cybersecurity alliance. IMPACT'S role is to translate high level policies and recommendations into concrete initiatives, that is, to translate ideas into actions. There are 4 problems currently faced by the world in the fight against cyberthreats. The first is human problems, the problem of fragmented stakeholders globally - stakeholders are not communicating with each other efficiently. The role of IMPACT is to set up unprecedented stakeholder networks. With the collaboration of ITU and UNODC, it is possible to bring traditional communities as well as law communities into the platform. The second problem is that a lot of good work and information is not reaching the right audience. IMPACT's role is to bring together key stakeholders and encourage stakeholders to exchange information on threats that are faced by each country. One of the ways to address this is by leveraging our partners. The third issue is not enough attention is given to helping those who need help the most. Last week, ITU IMPACT hosted the first cyberdrill involving 3 LDCs and other developing countries in South Asia with the help of industrial partners. The cyberdrill was able to highlight how developing nations mitigate some of the risks faced by these countries. The fourth problem is lack of uniform international legal framework, which allows effective enforcement of cyberlaws. ITU is actively engaged with Member States on these issues, and IMPACT will accordingly roll out the specific programmes to give countries options and actions to mitigate these threats.

UNODC plays a key role in the fight against cybercrime. However, more effective cooperation and additional resources are needed to assist developing countries to counter cybercrime. The transnational dimension of the cybersecurity issues due to the underlying international architecture and global services, makes effective international cooperation essential for success. UNODC is determined to work more effectively together with other players to develop simple methods of communication and information sharing between law and enforcement authorities, such as online platforms. It will also encourage international companies and subsidiaries to develop strong working relationships even in the absence of legal requirements. International cooperation is only part of the solution, more

measures are needed, such as technical solutions, education of users, legal measures and capacity building at the national level.

Child Online Protection (COP) Initiatives are crucial to full maximization of spectacular technological devices and applications for children. Online technologies benefit the society in many aspects, but they could pose potential dangers to the young generation, such as cyberbullying, Internet Addictive behaviours, geo-location tracking and even suicide. Therefore, it is important for the UN and ITU to put their efforts on promoting safety online to insure that our children reap the benefits of this new digital generation while being aware of the challenges. Possible measures could be adopted by different actors in society. For the UN and especially the ITU, they should focus on educating parents, caregivers, teachers, and children and youth regarding the dangers and providing tools and information to protect and empower them. For Leaders, they must adopt rules for cyberspace, update laws and create an environment so that the Internet can flower and flourish while at the same time, citizens have legal protections. For parents and teachers and all caregivers, they must be involved in their child's life online. For health providers, they must undertake more research, develop evidence based prevention and treatment for new diagnoses. For health care and entrepreneurs, they must build new tools and devices to protect our children. COP is working towards the goal of being a world repository of this information. It will provide the society a menu of tools and information from all parts of the globe.

Closing Session

Speaker **H.E. Mr. Lazarous Kapambwe**

The closing plenary featured a closing statement by the President of ECOSOC, who said that as cyberspace is constantly evolving and becoming increasingly important to all sectors of our society, it is imperative for the UN system and Member States to work together in partnership in order to maximize their strategic and analytical strengths to address current and emerging cyberthreats. The Council must continue to follow developments related to this issue, including through the reports of ITU and that of Council's Commission on Science and Technology for Development. Given the importance of this issue, the President expressed his hope that the Council would continue to review this issue in the near future.