UNITED NATIONS ECONOMIC AND SOCIAL COUNCIL

ECOSOC

SPECIAL EVENT ON CYBERSECURITY AND DEVELOPMENT

9 December 2011, 10:00 a.m. – 1:00 p.m., ECOSOC Chamber

ISSUES NOTE

Chair **H.E. Mr. Lazarous Kapambwe**, President of ECOSOC and Permanent Representative of Zambia to the United Nations

Moderator **Mr. Gary Fowlie**, Head, ITU Liaison Office in New York

Panelists **Dr. Hamadoun I. Touré**, Secretary-General, International Telecommunication Union

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 & 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

BACKGROUND

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, public information and financial services, 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. The economic impact and consequences of cyberattacks against critical infrastructure that increasingly depend on ICTs (dams, aviation and air control, electricity grids, pipelines, factories with dangerous or sensitive production processes, the banking system, national health systems, essential government and industry databanks, etc.) could be extremely high. The disruption of trade, economic and social activities can retard countries' progress towards achieving the MDGs and particularly in combating poverty. Furthermore, the threats posed to security of countries' borders, infrastructure and trade and the potential for triggering inter-state and other conflicts can put the entire development process at considerable risk.

Furthermore, cyber criminals have found ways to exploit loopholes, enabling them to attack corporations, individuals and governments worldwide. Cybercrime 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. Most developing countries, already affected by weak institutional mechanisms, weak infrastructure and relatively weak surveillance capacity are very vulnerable to such breaches.

The cross-border nature of cyberattacks and the organization of criminals necessitate international cooperation among governments and close cooperation of a range of private stakeholders. 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. As well, consideration should be given to the need for an international code of conduct or cooperation framework to address such threats.

OBJECTIVES AND OUTCOMES

The objectives of the Special Event will be to:

(1) build awareness at the international policy level by providing ECOSOC Members with a picture of the current situation and challenges concerning cybersecurity and its links to development;

(2) identify a range of best practice policies and initiatives in place around the world to build a culture of cybersecurity; and

(3) explore options for a global response to rising cybercrime.

The ideas discussed could contribute to the elaboration of the global response and/or framework to deal with cybersecurity and cybercrime.

ISSUES AND CHALLENGES

Cyberthreats have become one of the biggest global issues of our time. The proliferation of always-on connections has created a global network of open conduits. Whilst this brings untold benefits in terms of access to information and knowledge on an unprecedented scale, it has also led to vast quantities of malware and spyware circulating freely on the Internet, and an alarming rise in the number and scale of cyberthreats, cybercriminals and cyberterrorists.

Cyberthreats such as malware and attacks are becoming extremely sophisticated. This is especially true with the increased presence of organized criminal groups online. The Internet has ceased to be the domain of the technically competent. User-friendly software and interfaces have enabled all types of users, including children and novices, to interact remotely. This new territory contains a gold-mine of valuable information and potential victims. The complicated infrastructure of the Internet also makes it more difficult to track down criminals.

Cybersecurity and cybercrime are multidimensional issues, involving a number of different disciplines, skills and technologies. The disparity between developed and developing countries could generate “safe havens”, where cyber criminals can make use of the legal loopholes, and the lack of strong security measures present sometimes in developing countries to perpetrate cybercrimes.

While national efforts to strengthen cybersecurity are necessary, they are not sufficient. Cyberspace is global, and many of the threats to its security transcend borders. The lack of international principles, agreed globally, for governing behaviour in cyberspace, might allow cyberattacks among countries; Cyberspace could become the ground for new warfare paradigms, shifting the usage of conventional weapons to cyberweapons. The risk of massive coordinated cyberattacks to a country is now seen as an integral part of a wider military strategy.

Cybersecurity is one of the most critical concerns of the information age. It forms the cornerstone of a healthy, connected world. It is a global issue, demanding a truly global approach. Strengthening security in the information society is therefore a shared responsibility in which all stakeholders (governments, private sector, international organizations and civil society) have vital roles to play. Because of light-speed communications and ubiquitous networks, cybercriminals and cyberterrorists do not need to be anywhere near the scenes of their crimes. An international response is the only answer and possible solution. The transnational nature of cyberthreats and cybercrimes can only be met through global cooperation which must call for new and innovative ways to make sure that public and private technical community, regulators, ICT Ministries and the IT industry properly synergize. Such cooperation need to involve not only governments, but also intergovernmental and international organizations, able to act as catalysts for dialogue and discussions and global level.

ADDRESSING THE CHALLENGES

Even though national measures are being taken, cyber threats remain an international problem. Loopholes in legal frameworks are being exploited by perpetrators and harmonization between existing laws is far from satisfactory. Coupled with the absence of appropriate organizational structures, there is a genuine problem in responding to cyber threats.

This is without counting on the constant evolution and sophistication of such threats and the vulnerabilities in software, and more recently hardware, applications. With the phenomenal growth in mobile ICTs and new trends such as cloud computing and virtualization, it is increasingly likely that cyber threats will spread to new levels.