ITU Secretary-General, Dr Hamadoun I. Touré

Information and Communication Technologies (ICTs) have transformed modern lifestyles. These have provided us with real-time communications, borderless and almost unlimited access to information and a wide range of innovative services. At the same time, these have also created new opportunities for exploitation and abuse.

Cyber threats 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 cyber threats, cyber criminals and cyber terrorists.

ITU has been working hard to forge partnerships and support projects whose goal is to create a safe and secure cyber environment for everyone. Access to communications is useless if peace and safety online cannot be guaranteed.

That is why the ITU, as facilitator of WSIS Action Line C5 on "Building Confidence and Security in the use of ICTs", launched the Global Cybersecurity Agenda (GCA) on 17 May 2007. Designed as an international framework for cooperation and response, the GCA focuses on building partnership and collaboration between all relevant parties in the fight against cyber threats.

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. Because of light-speed communications and ubiquitous networks, cyber criminals and cyber terrorists do not need to be anywhere near the scenes of their crimes. An international response is the only answer and possible solution.

AN INTRODUCTION TO CYBERSECURITY AND ITU

Today, the Internet has become an integral part of modern societies, propelling the end user to the forefront of communication. All kinds of information is available, in all different formats and of varying topics and point of views.

The difficulty with this ever-growing multitude of resources is effectively surfing through the vast amount of information available on the Internet. How much of that information is factual, or even genuine? The real concern is not just with the dissemination of inaccurate or misleading information, but above all with malicious content. Fraud, theft and forgery exist online just as they do offline. If users are to benefit from the full advantages of the Internet, then confidence in the infrastructure is primary and of utmost importance.

Cyber threats 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.

But criminals are not the only threats to the Internet. The vulnerabilities of ICTs are a lure to terrorism and espionage. Cyber warfare and espionage have also made their appearance and can pose serious threats to critical information infrastructure.

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.

ITU: a unique global forum to discuss cybersecurity

ITU recognizes that information and technology security are critical priorities for the international community. Cybersecurity generally is in everyone's best interest and this can only be achieved through a collaborative effort. Cyber threat issues are global and therefore the solutions must be global too. It is vital that all countries arrive at a common understanding regarding cybersecurity, namely providing protection against unauthorized access, manipulation and destruction of critical resources. The ITU believes the strategy for a solution must identify those existing national and regional initiatives, in order to work effectively with all relevant players and to identify priorities.

With its 193 Member States and more than 700 Sector Members, ITU is uniquely placed to propose a framework for international cooperation in cybersecurity. Its membership includes least developed countries, developing and emerging economies, as well as developed countries. ITU is therefore an excellent forum for action and response to promote cybersecurity and to tackle cybercrime.

ITU and WSIS Implementation

The ITU, due to its long history, mandate and commitment, works hard to address cybersecurity challenges as these emerge and evolve. The ITU is promoting cybersecurity through a range of activities related to standardization and technical assistance to developing countries tailored to their specific needs. The ITU is made up of three Sectors: the Radiocommunication Sector (ITU-R), the Standardization Sector (ITU-T) and the Telecommunication Development Sector (ITU-D). At the World Summit on the Information Society (WSIS), world leaders and governments entrusted the ITU to take the lead in coordinating international efforts in the field of cybersecurity, as the sole Facilitator of Action Line C5, "Building confidence and security in the use of ICTs". In line with these developments, ITU membership has been calling for a greater role to be played by ITU in matters relating to cybersecurity through various Resolutions, Decisions, Programmes and Recommendations