7th International Conference on Cyber-Crime

12 September 2007, New Delhi, India
Speech of Shivraj Patil, Minister of Home Affairs, India

Shri Suresh Pachauri, Minister of State for Personnel,
Shri Vijay Shanker, Director CBI,
Mr. Ronald K. Noble, Secretary General INTERPOL,
Distinguished Delegates,
Invitees, Ladies and Gentlemen,

It gives me immense pleasure to inaugurate the 7th INTERPOL Conference on Cyber Crime, consisting of Law Enforcement Officers from many countries, Experts in the field and representatives from the Information Technology industry. I warmly welcome you all to India, a land of great diversity and one of the ancient civilizations of the world.

In the past two decades, Information Technology has brought in a remarkable transformation in almost all walks of life. Worldwide, IT has made significant contributions in the fields of economic growth, sustainable development and good governance. It is estimated that worldwide technology and related services spending crossed 1.5 trillion US Dollars in 2006, which forms a substantial proportion of the global trade. In India, the seeds of Information and Communication Technologies were laid during the Prime Ministerial tenure of Late Shri Rajiv Gandhi, a visionary leader who had many dreams for Modernization of the country. In fulfillment of his vision, today India stands as a major force in the global IT Industry.

E-Governance initiatives have played a key role in achievement of developmental and social objectives in many countries. India has particularly witnessed many successful implementations of E-Governance projects. E-Procurement has brought in transparency in public procurement and substantially eliminated the scope for wastage. Computerization and Online delivery of public services has eliminated the scope for discretion, enhanced efficiency in the delivery systems and improved access to information and services. Adoption of E-commerce solutions even by farmers and artisans in marketing of agricultural produce and handicrafts is a testimony of wide reach of Information Technology and its significant contribution to the economic empowerment of weaker sections of the society.

Here I would like to draw your attention to the unintended consequences of the IT revolution and its implications to the law enforcement community. Until a decade ago, when the use of computers was largely confined to a miniscule portion of the population and the applications were mainly stand alone or LAN based, enforcement of discipline and order was easier. But now with proliferation of E-commerce and E-Governance applications, the situation has changed. Majority of the computers are now networked and most of the applications are online. Virtual Societies have been rapidly growing and persons from all walks of the real societies have been joining them, often transcending the national borders. Millions of cyber citizens, or in other words netizens, are being created in the process. We often hear from IT practitioners that in future social interactions through virtual world may almost equal the interactions in the real world. All this had led to an unprecedented growth of cyber crimes in the recent past.

Notwithstanding its late entrance to the arena of serious crimes, Cyber Crime today represents a wide array of offences. Hacking, Spoofing and Botnet attacks are capable of causing serious security breaches in the information systems of vital installations. The potential damage on account of such attacks to the national security is immense. Globally, instances of money laundering through e-channels for terrorist funding have assumed menacing proportions. The Internet is being used as a secure means for internal communication among terrorists and also for hate campaigns through social networking sites. Growing instances of such crimes constantly remind us the need to create a culture of cyber security awareness and the need to evolve effective preventive measures.

Many of the white-collar cyber crimes go unreported due to either reluctance to report or ignorance. As a result it is difficult to collect reliable statistics of such crimes for assessing the extent of the problem. However, analysis of the existing data presents certain disturbing trends. Earlier, amateur criminals with fun or profit motives accounted for most of the cyber crimes. But of late, organized groups of criminals have found it a lucrative means to generate huge proceeds of crime. Online Child Pornography, Online Trafficking in Contraband items and E-commerce frauds are some of the offences, which are showing rising trends. Acts of vandalism and cheating are increasingly frustrating e-Governance efforts. Needless to say, these offences are serious enough to capture the priority attention of lawmakers and members of the law enforcement agencies.

India was one of the countries to respond early to the problem. We enacted the Information Technology Act in 2000, which defines cyber offences and prescribes punishments for them. The Act has also created various authorities for regulation of the cyber world and it empowers police to investigate offences. The Ministry of Communication & Information Technology has set up a Computer Emergency Response Team for assisting the combat efforts. The Government of India has designated the Central Bureau of Investigation as the Nodal Agency for cyber crime investigation and training. Many of the State police agencies have also created their own Cyber Crime Cells. To prevent and investigate these crimes, India is one of the countries which have developed a full fledged indigenous cyber forensic software package. However, we have a long way to go and are in the process of evolving systems and methodologies to stem the menace.

Cyber crime investigation is different in many ways from the conventional crimes and presents serious enforcement challenges. There is no physical contact between the victim and the perpetrator of the crime and, quite often, they are situated in different countries, thousands of miles apart. This practically rules out availability of eyewitness account. Availability of presentable documentary evidence rapidly diminishes over time, which calls for a quick incidence response. Cyber laws are still in the evolving stage. Most of the agencies associated with criminal justice administration face knowledge and capacity constraints. Majority of offences require investigations abroad, which involve compliance of time taking procedural formalities.

In view of the special challenges involved in the cyber crime investigations, which I have just mentioned, creation of more and more facilities on a stand-alone basis is definitely not an optimal solution. As Pandit Jawaharlal Nehru once said, “Highest type of efficiency is that which can utilize existing material to the best advantage”. In the context of cyber law enforcement, unless domestic efforts are leveraged with instruments of international cooperation, combat efforts will be ineffectual. Also, harmonization of international efforts, in the field of law making, investigation, prosecution and sharing of forensic technologies, is another prerequisite for effective control of offences.

International cooperation operates at various channels. The most prevalent and formal mechanism is through diplomatic missions making use of the multi lateral and bilateral instruments of cooperation. However, the second channel of police to police cooperation is equally, if not more, important in dealing with a cyber crime situation. By the very nature, Cyber crimes need quick response and data preservation, which is possible only through peer-to-peer cooperation. I am happy to note that INTERPOL has been taking right steps in fostering such cooperation and I must say such steps are commendable and deserve wholehearted appreciation. I suggest that these efforts can be advanced by organizing more training programmes and joint efforts by all the multi lateral agencies for working out a comprehensive international convention on Cyber Crime.

Enormous contributions made by the Information Technology solutions in transforming the lives of poor and needy are too precious to be frittered away. Similarly, no sovereign nation can afford to leave vulnerability in their technology apparatus, which can be exploited by terrorists, and organised crime syndicates. It is, therefore, the bound duty of every one concerned with law enforcement to ensure that Information Technology gains are not nullified by a handful of criminals. In this regard, persons like you can contribute a great deal. Here I am reminded the words of Mahatma Gandhi - “Strength does not come from physical capacity, it comes from an indomitable will”. In the fight against cyber crime it is the belief in the cause and the will to make dedicated efforts that enhances your strength and not the availability of material resources or the technological capabilities. I would like to suggest some simple steps for the enforcement efforts at the individual level and the national level.

First and foremost, we must realize the need to honour and quickly respond to the INTERPOL references and bilateral requests for information sharing and data preservation. Second, there should be a liberal sharing of forensic technology for achieving standardization of expert efforts. Third, there should be more cross-country training exchange programmes. Fourth, timely alerts should be provided by the affected countries to others regarding new forms of crime and new modus operandi.

Collaboration between Public and Private Entities is another essential facet of investigation cooperation. Private Internet Service providers are often the victims of cyber attacks and frauds and they need a quick response from enforcement authorities. Enforcement authorities, in turn, require quick response from the service providers for network monitoring, provision of traffic data, data storage and forensic support. I am told that Industry representatives are also going to interact with the delegates. It would definitely provide a good platform for interaction.

I commend the INTERPOL Secretariat and Central Bureau of Investigation for organizing this conference on such a large scale. This would not have been possible without the dedicated efforts of the staff of both the organizations. Conferences like this enable practitioners and experts to keep abreast of the latest developments at the global level. They also provide an opportunity to the delegates to get acquainted with each other and foster sustainable working relations. I am happy to note that you have a comprehensive agenda which touches upon almost all the main issues of concern to the cyber crime enforcement officials and paves the way for achieving the desired objectives.

I wish the conference a grand success. I wish you all an enjoyable and comfortable stay in India.

Thank you.