

**Secretary's speech in the Valedictory Session at One day Workshop on "International Police Cooperation against Cyber Crime" on 26<sup>th</sup> March,2009 at Vigyan Bhavan, New Delhi**

\*\*\*\*\*

Shri Ashwani Kumar, Director, CBI; Mr. Alexander Seger, Head of the Economic Crime Division, Council of Europe, Shri Ranjeet Narayan, DGP, Andaman & Nicobar Islands, Shri Rajni Kant Mishra, Joint Director, CBI, distinguished delegates and friends.

This conference has dealt with a very important concern of national and international law-enforcement agencies – that is securing the cyber world for its citizens.

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. International computer networks such as the Internet have turned the entire world into a global village, enabling communications and transactions across the globe. However, increasing use of the Internet has simultaneously given birth to innovative ways of committing crimes, taking advantage of the same enabler i.e. ICT. The IT revolution has posed several challenges to technologists, law enforcement agencies and also to users.

Today, India is increasingly acknowledged as the emerging services hub of the World with a large share of the global IT Enabled Services market. The total revenue of this sector which includes exports and domestic earnings has crossed 50 billion US dollars and this is slightly more than 5% of India's GDP. Thus, the growth of the IT/ITES sector is very important for us. Conducive IT policies and the pro-active role of Government have facilitated this growth. It is important to sustain and increase business. Instilling confidence is crucial for achieving this. Putting a legal framework in place and extending cooperation and timely help at all levels is as important as technological infrastructure.

India is one of the countries to respond early and put a legal framework in place. The Information Technology Act, 2000 defines cyber offences and prescribes punishments for them. The primary objective of the Act was to provide legal recognition for electronic commerce and E-Governance applications. The Act also created various authorities for the regulation of the Cyber World and empowered Police to investigate these offences. Further, through the Information Technology (Amendment) Act enacted on 5<sup>th</sup> February, 2009, the legal framework has been strengthened through new sections introduced for prevention of newer forms of cyber crimes. Provisions have been made with regard to breach of confidentiality and leakage of data by service providers, e-

commerce frauds through impersonation commonly known as phishing, identity theft and offensive messages through communication service etc. The amendments provide maximum punishment upto life imprisonment for cyber terrorism activities. The provisions pertaining to data protection have been strengthened. The victim whose data is leaked out or stolen will get compensation. The intermediaries who are processing and keeping the personal data will also be responsible for the leakage of data. They will have to implement International Security Best Practices in this regard. They will have to pay compensation commensurate to damage caused and are also liable to criminal prosecution.

The Indian Computer Emergency Response Team, CERT-In at the Ministry of Communications and Information Technology is a part of the international CERT community with the specific mandate to respond to computer security incidents. CERT-In handles security incidents reported from various National and International agencies including CERTs and financial institutions located abroad. CERT-In is collaborating with various IT vendors and with CERTs such as CERT/CC, US-CERT, JPCERT, APCERT, Korean CERT.

Cyber crimes, as everybody is aware, are boundaryless and can be committed from any location without physically being present at the site of incidence and such crimes are characterised by minimal risk of detection and apprehension. Crime is borderless but enforcement is constrained by borders. Therefore International Cooperation becomes essential to combat cyber crimes. The trans-national nature of cyber crimes suggests that the development of common policies on key issues should be part of any control strategy. Such common policies are important to prevent the occurrence of “data havens” in jurisdictions where certain activities have not been criminalized. In addition to this, effective measures could be pursued for improving criminal investigative capabilities in network environments, particularly in cases involving multiple jurisdictions. This includes responding to the need for operations that could be conducted quickly enough to prevent the loss or inaccessibility of evidence.

6. Therefore, for combating cyber crimes through international cooperation one needs to consider:

- Sharing of information about crime and profiling of criminal
- Common set of investigative powers
- Application of investigative powers to Mutual Legal Assistance arrangements

- Adequate and flexible MLA and extradition arrangements

But consensus on such issues is not easy. The European Convention on Cyber Crime provides an International forum to address harmonization of the national law, prosecution procedures to cope with global networks and establishment of a rapid and effective system of International Cooperation. However, declarations are not enough and must be accompanied by meaningful action on the part of all the participating countries.

The investigation of cyber crime requires the availability of staff with forensic and technical expertise and for specific procedures to be in place. This implies the formulation of training programmes and the development of investigative software tools. International training programmes should be developed and expertise should be shared between Nations. In order to investigate effectively, countries may be dependent on assistance from other nations. This includes both informal cooperation by law enforcement personnel and formal mutual legal assistance conducted through central authorities.

To be able to extend International Assistance, we also need cooperation and coordination within the country, amongst

- a) Different Enforcement Agencies of States and the Centre

- b) Law Enforcement agencies and the Private Sector IT Industry and
- c) Law Enforcement agencies and the general public.

Efforts are being made to have bi-lateral agreements with foreign countries to deal with the cyber crimes committed on foreign land but affecting Indian Computer resources.

Unlike physical crimes, cyber crimes have different characteristics. If proper measures are in place, the collection of digital evidence is far more credible, easier and analysis can lead to profiling a criminal in a much better and accurate manner than in the case of physical crimes. The issue, however, is the collection, preservation and analysis of digital evidence. Digital evidence is fragile and needs to be collected within the appropriate time and in the appropriate manner. The conditions for collection, preservation and analysis of evidence are very stringent and need to be followed strictly.

Computer crimes, in general, are being committed across nations. Systems in one country are compromised by criminals and used for launching attacks on targets. While reaching the targets, the criminal passes through many compromised systems. While analysing the evidence, the investigating agencies see the system used in the final

stage of attack on targets. The other intermediate stages can be picked up only if details and computer logs of the systems used at all stages are available. This is a major concern in the entire investigation of cyber crime. We should therefore evolve a procedure where the computer logs of the systems participating in the crime are available instantaneously to the investigating agencies. We, therefore, need to evolve a system or procedure in this direction. Such a system will go a long way in profiling and tracking down criminals.

Further, It is well known that many of the cyber crimes go unreported due either to reluctance to report or ignorance in this regard. As a result, reliable statistics on crimes may not be available for assessing the extent of the problem. However even with such limited data, the reports on cyber crimes are alarming. The trend is changing from individuals operating for mischief or profit to international organised crime groups carrying out criminal activities like terrorism, money laundering, drug trafficking, cyber based extortion and fraud, child pornography and spreading hatred. Therefore, understanding the changes in crime patterns is critical to take preventive steps. While technology provides both opportunity and capability for criminal groups, it also enhances the detection capabilities of law enforcement agencies to detect and disrupt illegal activities. Cooperation is also required

amongst the technology providers, law enforcement agencies and judicial officers for effective protection.

I thank CBI and Council of Europe for organising this Conference. This conference has provided an opportunity to members of law-enforcement agencies, service providers and other stake-holders to share best practices in international cooperation in the area of cyber crime. Today's conference has provided opportunities for participants to build networks at personal level also, which could be one way to achieve the desired quickness in response from different agencies in fighting cyber crime. It is heartening to note that the private sector, which has always been in the forefront of the ICT revolution, has taken an active part in the deliberations of this conference.

We acknowledge with thanks the support of the Council of Europe in this conference in New Delhi. I would like to congratulate Shri Ashwani Kumar, Director, Central Bureau of Investigation and his team of officers for organizing such a big conference so successfully. I once again thank the Director CBI for giving me this opportunity to be here and interact with you all.

Thank you.