

SPEECH FOR CABINET SECRETARY (Cyber Crime Conference – 26.3.2009)

Shri Ashwani Kumar, Director, CBI

Dr. Gulshan Rai, Director, CERT-In

Mr. Alexander Seger, Head of Economic Crime Division, Council of Europe

Distinguished experts, delegates

Our friends from the Information Technology Industry

Distinguished Invitees

Ladies & Gentlemen

2. It gives me immense pleasure to inaugurate this conference on "International Police Cooperation against cybercrime", which is being organized by Central Bureau of Investigation in association with Council of Europe.

3. The digital revolution has changed the way government operates, business is transacted and national security assured. In today's environment the growth and success of nearly all organizations depend on harnessing information technology for profitable use. Hardly any walk of life has remained untouched. Leveraging IT, institutions are discovering newer ways of connecting and communicating with each other like never before. All functions are now increasingly depending on networks of critical information infrastructure, raising our dependency and rendering us vulnerable. For the law enforcing agencies around the globe, preventing cyber crimes is emerging as the most pressing priority. The emerging threat encompasses not only the crimes facilitated and driven by information technology but also the traditional crimes having technology interface. Presently even minor disruptions of the operation of information systems of critical infrastructure are going to have devastating effect on people, economies, essential government services and national security. Cyber attacks and cyber terrorism are the new looming threats on the horizon.

4. There could be attacks on critical infrastructure such as telecommunications, power distribution, transportation, financial services, essential public utility services and others. The damage can range from a simple shut down of a computer system to complete paralysis of a significant portion of critical infrastructure in a specific region or even the control nerve center of the entire infrastructure. In May 2007, for example, Distributed Denial of Service (DDoS) attack on Estonia led to the crippling of banking institutions, blocked the President, Prime Minister, Parliament and other governmental agencies from connectivity and hence brought the whole system down, crippling government and private transactions.

5. If we look at the business sense, with over 1 trillion dollars moving electronically across the Internet, it becomes a hot target for criminals. Annual “take” by theft oriented cyber criminals is estimated to be as high as 100 billion dollars and 97% of these offences go undetected. Less is known about corporate espionage, losses of proprietary information and many other modes to offend and harm computers.

6. Large scale cyber incidents may overwhelm governments, and shake public and private confidence. In today's context, ensuring safety and security of cyber space throws up new challenges and opportunities. It is a daunting task to simultaneously ensure IT enabled growth & development and at the same time prevent fraudsters and criminals from exploiting weaknesses in IT systems & networks. There are many avenues for development and creation of new products, processes & services that can help us strike a fine balance between productive growth and adequate security.

7. The Govt. of India has taken several key initiatives to enhance security of cyber space. Among these, a major initiative is towards creating a conducive legal environment and enhancement in law enforcement capabilities to enable responsible action by stakeholders and effective prosecution. In this direction, the Government has amended the Indian Information Technology Act 2000. We have provisions now to ensure that the IT Act could be technology neutral while promoting alternative technologies to authenticate electronic records; that body corporates handling sensitive data put in place procedures for their safety; that punishment for cyber offences is rationalized in accordance with comparable measures under the Indian Penal Code; and that provisions exist for examination of electronic evidence in investigations relating to cyber misuse.

8. For the law enforcing agencies across the globe, rapid detection, information exchange, investigation and coordinated response and remediation to immediately mitigate the damage caused in digital crimes should be priorities. Nations across the world are looking at preventing cyber attacks and cyber crimes and simultaneously investigating such crimes and nailing such criminals. It is in the fitness of things that we are prepared with a crisis management plan which would put processes in action when a cyber crime of any intensity is detected. The mechanisms should immediately be activated to handle the situation effectively and swiftly. Our Department of Information Technology has set up the Indian Computer Emergency Response Team (CERT-In). It operates on a 24x7 basis and is actively engaging its users with early warning alerts and advisories. CERT-In has very close cooperation with other national CERTs.

9. Our recent initiative was the establishment of a national framework for assuring compliance to international security best practices. This framework is aimed at enabling Govt. and critical infrastructure organizations to improve their security and to enhance their ability to resist cyber attacks. Govt. has mandated

all critical infrastructure organizations to implement security related best practices based on international standard ISO 27001. Nation wide efforts to facilitate research & development in security technology are on. These efforts cover basic research, technology demonstration, proof-of-concept and R&D test bed projects in advanced and front line technology areas such as encryption and digital marking. Specifically, efforts are also on towards information sharing and cooperation both within as well as outside the country. These efforts are directed towards enhancing greater international cooperation and enabling sharing of information as an aid to effective alert and warning actions. Whenever a crisis of national magnitude occurs, a Crisis Management Committee headed by me would immediately swing into action.

10. These efforts towards prevention should be coupled with effective legislation which would enable investigating and prosecuting agencies to bring cyber criminals to book. There is a need to study the old Acts and make suitable amendments in the context of information technology. There is a need for nation wide efforts to increase security education, awareness and skills. This is specially aimed at catering to the needs of critical sectors, law enforcement agencies, judiciary and e-Governance project stakeholders.

11. We need to focus on specific areas to guarantee cyber security. We must share information to make sure that we are able to trace the evidence to its origin. We must be able to preserve and protect electronic evidence. We must exchange information on a regular basis on criminals and criminal acts. We must look at our laws and determine whether there could be international standards for such laws. We must be in a position to coordinate action all over the world to deal with crises, as and when they occur. I am sure this Conference, organized jointly by the Economic Crime Division of the Council of Europe and our Central

Bureau of Investigation will deliberate on these issues and endeavour to find a way forward. I wish the Conference all success.
