Perry4Law
An Exclusive Techno-Legal Corporate, IP & ICT Law Firm

New Delhi, India

Critical Infrastructure Protection In India: The Problems, Challenges And Solutions

Critical Infrastructure like Oil and Gas, Power Grids, Transportation, Satellites, etc are connected to Information and Communication Technology (ICT) these days. This is so because most of the public utilities and Critical Infrastructure are connected to Supervisory Control and Data Acquisition (SCADA) Systems these days. Recently it was revealed that Internet is full of Unprotected and Unsafe Devices, SCADA Systems and Computers. This makes the Critical Infrastructures vulnerable to various forms of Cyber Attacks. India is facing serious cyber threats and Critical Infrastructure Protection must be the top priority of Indian Government.

The process of Critical Infrastructure Protection in India is still trying to tackle the sophisticated Cyber Attacks. The Cyber Security Trends and Developments in India 2013 (PDF) provided by Perry4Law and Perry4Law's Techno Legal Base (PTLB) have highlighted further Cyber Security Challenges for India. There is no second opinion that Critical Infrastructure Protection in India is needed and the sooner we ensure the same the better it would be for the National Interest of India.

Acknowledging this situation, the National Cyber Security Policy of India 2013 (NCSP 2013) was drafted by Indian Government. However, the Policy lacked on many count like Privacy Protection in India. Similarly, the NCSP 2013 has also failed to "Integrate" itself with the National Security Policy of India. Further, a National Critical Information Infrastructure Protection Centre (NCIPC) of India has also been constituted by Indian Government.

Incidences of Cyber Crimes, Cyber Attacks, Cyber Security Incidences, Cyber Warfare, Cyber Terrorism, Cyber Espionage, etc are some of the problems that are peculiar to the contemporary times. These threats are intimidating the National Security of India by striking at the Financial, Economic, Social and Political Environment of India.

Recently, Huawei was accused of breaching National Security of India by Hacking Base Station Controller in Andhra Pradesh state. The DRDO has even sought Penal Provisions

in National Telecom Security Policy of India for Telecom Companies Violating the Norms. The problem of embedded malware in imported Hardware and Software is still haunting India as the Imported Software and Hardware Testing for Embedded Malware was postponed till 1st April 2014 by India. With India being recognised as Authorising Nation under the International Common Criteria Recognition Arrangement (CCRA) this task of Hardware and Software testing may become easier in India.

Similarly, India is also facing technological issues at its Border with China. In fact, India is planning Technological Upgrade of Border Broadcast Infrastructure due to Chinese Broadcasts.

India is also trying to increase the use of E-Governance for delivery of Public Services. This is a good approach. However, along with the use of E-Governance, the Cyber Security issues would also arise. Therefore, Cyber Security of E-Governance Services in India must also be ensured. For instance, the reserve Bank of India (RBI) has suggested use of encrypted SMS based fund transfers in India. This means that in future a Robust Mobile Payments Cyber Security in India would be needed.

The Cyber Security of India must be improved further and a Robust Cyber Security Infrastructure in India is urgently needed. Further, development of Offensive and Defensive Cyber Security Capabilities of India is need of the hour.