Cyber Criminal Law of India: Can it cope with Cyber Terrorism?

Dr. Poolla R.K. Murti
University of Hyderabad, India
Email: prkmcs@gmail.com

K. Prasanna Rani
NALSAR University of Law, Hyderabad, India

Abstract

India has realized quite early that the easy availability of the internet does lead to Cyber Offences. Because of the unfortunate geo-political issues concerning its northern territory, India was a victim of Cyber terrorism. While there was a need to effectively combat this vexing form of terrorism unleashed from the cyber space, there was a need to have a legal framework necessary to prescribe proper punishments for such cyber offences. This is the core of the Cyber Criminal Law which found expression in Chapter XI of the Information Technology Act 2000 (IT Act).

This paper presents a critical commentary on the Cyber Criminal Law of India. The multitude of forms in which Cyber offences can occur is discussed and the provisions of relevant sections of the IT Act are analyzed to deal with the same. It is shown that exemplary punishments are prescribed in proportion to the ingredients of the crime.

After about half a decade of experience in dealing with Cyber offences, certain amendments were proposed in 2005 for an effective implementation of the law. This paper explains why such implementation is woefully poor in practice making the Cyber Criminal Law of India abysmally powerless in the face of exploding cyber terrorism enveloping the country.

The paper closes with the recommendation of effective measures to be followed learning from the experiences of the Western countries that continue to face cyber terrorism. The paper recommends an International Protocol to effectively deal with Cyber Terrorism in its various ugly ramifications