

## CYBER TERRORISM HOAXES AND LAW ENFORCEMENT

by *Denzyl P. Dayal, South Anarkali, Delhi: Dominant Publishers  
and Distributors, 2005. Pp. 1, 336.*

JEANETTE S. ALVAREZ\*

*D*enzyl P. Dayal's work is a handy tool in enlarging a law student's perspective in criminal law. One does not need to have an extensive technical knowledge on computers in reading the book because the author used an approach that links the readers to the actual and practical scenario of the most serious abuses of the Internet or cyberspace manifested in four of its forms: Cyber Terrorism, Computer Virus, Hoaxes and Pornography, discussed below in seriatim. Even if the topic on law enforcement was discussed by the author with a background on federal laws and governance, this may be supplemented with referring to our country's pertinent laws and statutes on the matter such as The Electronic Commerce Act of 2000 (Republic Act 8792) and its Implementing Rules and Regulations, The Access Devises Regulation Act of 1998 (Republic Act 8484), Rules on Electronic Evidence, The Revised Penal Code and relevant circulars of the Bangko Sentral ng Pilipinas (BSP).

The first part of the book discusses cyber terrorism and cyber crimes. The author defines terrorism as the calculated and unlawful use of force or violence, or threat of force or violence, against persons or property to inculcate fear, intimidate or coerce a government, the civilian population or any segment thereof, in furtherance of goals that are generally religious, political or ideological. Cyber Terrorism is: the definition of terrorism with the addition, "through the exploitation of computerized systems deployed by the target." Computers have created

---

\* UST Law Review – *Business Manager*.

new risks (and rewards) concerning the discovery of information which its originator wished to remain confidential.

Cyber crimes can take the appearance of trademark or copyright violations, industrial espionage, selling a regulated medicine over the Internet without a prescription, Internet film piracy, and hacking government agencies or e-mail password of another person. With the proliferation of this new genre of crimes, law enforcement agencies and mechanisms are keeping up with the pace of their rise. The Supreme Court drafted The Rules on Electronic Evidence, which took effect on August 1, 2000, to emphasize the admissibility of evidence in electronic form subject to its authenticity and reliability. This restriction intends to safeguard against accepting evidence of doubtful character. While the Philippines does not have a CyberTerrorism team, which was suggested by the author as a first step in countering CyberTerrorism, it recognizes the vital role of Information and Communications Technology (ICT) in nation-building; \*\*\* its obligation to ensure network security, connectivity and neutrality of technology for the national benefit.<sup>1</sup> In heeding the need to combat CyberTerrorism on commerce and trade, certain acts are penalized under the Electronic Commerce Act of 2000<sup>2</sup> involving almost every illegal intrusion into any computer system, including computer viruses, and obtaining information through unlawful access.<sup>3</sup> Even if said legislation is anchored only on the protection of national commerce and trade, this is a good start for our government in fighting CyberTerrorism acts, along with The Access Devices Regulation Act of 1998<sup>4</sup> and the Central Bank's Circular regulating the electronic banking services of financial institutions.<sup>5</sup>

The second part exposes the harmful, yet seemingly innocuous hazards of Internet hoaxes and chain letters, which are e-mail messages written with one purpose – to be sent to everyone you know. It is not

---

<sup>1</sup> An Act Providing for the Recognition and Use of Electronic Commercial and Non-Commercial Transactions and Documents, Penalties for Unlawful Use thereof and for other purposes, RA 8792, §2 (2000).

<sup>2</sup> RA 8792, §33.

<sup>3</sup> RA 8792, §33.

<sup>4</sup> An Act Regulating the Issuance and Use of Access Devices, Prohibiting Fraudulent Acts Committed Relative Thereto, Providing Penalties and for other purposes, RA 8484 (1998).

<sup>5</sup> Bangko Sentral ng Pilipinas, Circular 240, April 7, 2000.

impossible that through these means, fallacious information about greater concerns, similar to those related to national security or economic crisis, will easily proliferate and wreck havoc in our country.

The third part depicts the international rise of pornography. In Canada, the government proposed a legislation that would make it illegal to view child pornography on computer screens, punishable by up to five years in prison. Sadly, the Philippines does not have a similar statute on child pornography. However, immoral doctrines, obscene publications and exhibitions, and indecent shows are condemned by the Revised Penal Code.<sup>6</sup> This provision does not directly and obviously extend to computer-related means and this is one area that should be improved by the legislature.

The last part illustrates the rapid propagation of computer viruses and how it could be a gateway for cyberterrorist acts. According to the author, "computer virus passes from computer to computer like a biological virus passes from person to person." The ease of spreading computer viruses and the lack of caution in using the Internet make them a clever tool for outsiders to hack pertinent computer systems.

In sum, the book provides a sensible, functional and opportune subject matter especially to those individuals, agencies or offices relying on a great degree on computers and Internet. We should be grateful for having such technological advancements in our time but must also be mindful of its probable adverse effects. These advancements could well be identified as power, however, with great powers come great responsibilities. It now becomes incumbent upon us to be responsible for this technology, to be on guard with the proliferation of abuses in the net or the commission of crimes through the use of computers or the illegal hacking into crucial systems. The fact that our country is a bit outdone by foreign countries in enacting legislations which parallel crime-fighting with the recent trends in technology should not totally frustrate us. The author of this book review considers our existing laws and statutes on protection of commerce and punishment of pornography as good starters, although not all encompassing. These are areas that demand enhancement by amending the provisions or endorsing supplemental laws. The writer believes that despite existing differences in every country's approach in countering cyber crimes, all of them aspire for a common goal: to stop these cyber crimes.

---

<sup>6</sup> REV. PEN. CODE, Art. 201.