CYBERCRIME in the Greater China Region
Lennon Yao-Chung Chang
Edward Elgar (2012)
ISBN 978-0-85793-667 -7

Book review by Sally Ramage

We are reminded that the Internet was built for research and not for commercial purposes and its founding protocols 'are inherently insecure. (See Lessing, 2000). The world's total population is over 7 billion and the Internet plays a major part in the life of many people on this planet, from giant organizations to a bare-footed schoolchild in a developing country.

In this monograph, Professor Chang of Hong Kong University has studied China's internet system and the 'hacking' that takes place in China and in Taiwan. He claims that this activity is mostly political but admits that commercial interests are not included.

Although this book is not directly related to any other country, it is an important study that reveals the culture in China and the secrecy in those spheres and the almost impossibility of penetrating that secrecy. This gives us a flavour of a macro situation that can assist in learning about any micro cybercrime situation.

Cybercrime can only be known about by its impact thereafter. It cannot be revealed without digital evidence and the term 'digital evidence' encompasses any and all digital data that can establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its perpetrator.

The application of forensic science principles is used in the location, recovery, and examination of digital evidence. Digital evidence is evidence that is stored on or transmitted by computers play a major role in a wide range of crimes. Though an increasing number of criminals are using computers and computer networks, few investigators are well versed in the evidently, technical and legal issues related to digital evidence. How computer networks function; how they can be involved in crime and how they can be used as a source of evidence,; criminal profiling; understanding criminal motivations, is very necessary knowledge in order to understand the law related to cybercrime.

Cybercrime is the use of computers for criminal activity. Cybercrimes such as e-mail defrauding, harassment in chat rooms, 'spoofing' and 'cracking' of computer networks are activities that leave digital evidence which can be gathered with minimal distortion and used legally for prosecution in a court of law.
Chang's book in only concerned with terrorist cybercrime when computer experts illegally interrogate the whole computer systems of a country's government.
This includes automatic data-mining techniques being developed to find these crimes in large databases.

References

Lessing, L.(2000) Code and other laws of cyberspace, London: Basic Books.