LC Paper No. CB(2)841/00-01(01)

**Wanbil W Lee**, 李雲彪

**Chartered Information Systems Engineer, Chartered Mathematician, Registered Professional Engineer (Information)**

**FBCS, FIMA, FHKIE, FounderMember HKCS, MACS**

## My View
## on the Report of the Interdepartmental Working Group on Computer-Related Crime

9:00am – 12:00 noon, 10 February 2001
Chamber of the Legislative Council Building

I commend the effort of the Working Group. Stated below are a few points that reflect my view in general:

First, I want at the outset to alert Council and the HKSAR Government to the fact that violation of computer security brings about not only criminal offences but also infringement of "civil rights". (Please see Note 1.) In this view, the report has covered the first aspect but not the second. It follows that the report, thus the ambit of the Working Group's terms of reference, is restricted and confined to address the criminal aspect. In other words, what has been done is not enough.

Second, computer crime or *cybercrime* has by itself no precise definition but its consequences can be categorised as computer abuse (a computer-related crime), computer fraud (a computer-aided crime), and software piracy. (Please see Note 2.) This should help readers of the Report by mapping the 14 chapters onto the three heads.

Specifically, while I agree with the spirit of the recommendations, I wish to express view as follows:

- "computer" and "information system" (p 13): The coverage of computer-related-crime is not adequately handled by means of these terms as it is the outcome of violation of computer security - strictly speaking, violation of security with respect to the information stored by the computer or the information in transit during process. Protection of the computer or information system really means protection of information, be it stationary in storage or in motion during transmission or operation. Therefore, the coverage should extend to pre-process and post-process stages, and includes not only the technological components and the supporting infrastructures but also all the human elements involved in all states of the information.

- "… the computer or the Internet …" (p 18, p 31, and other pages): Reference should not be restricted to the Internet; there are other networks in existence and use, for example, EBONE (European Backbone), CHINAPAC (China's new network), etc.

- E-commerce (p 21): Commercial disputes existed since the dawn of civilization, and have yet to be resolved to the satisfaction of all parties concerned. No doubt, security is a major obstacle to E-commerce applications. However, as in traditional commercial practice, risk management is a countermeasure and insurance is an effective mechanism. I suggest that it will be useful to solicit input from the insurance sector.

- Disclosure of decryption key (p 24): While encryption was claimed a useful tool in protecting confidentiality [and maintaining integrity] (p 21), it seems a contradiction to legislate disclosure of decryption keys. To do so also introduces an extra dimension of risk. Should it be the business of the law enforcement agencies to decode or decrypt any encrypted materials? This is certainly a challenge to law enforcement.

- "Much computer crime is conducted via the Internet." (p 43): This implies external invasion. However, all the statistical data testifies that the majority of crime is committed by insiders who do not have to go through the Internet. Involvement of the ISPs appears to be an extra help. But this introduces correspondingly an extra degree of risk and may infringe upon that aspect of trade practice which is to preserve anonymity of the client. I have my reservation on the involvement of the ISPs.

- "public education" (p 66) and public sector's role (p 70): Not only public awareness through educational means as recommended, but also handy reporting mechanisms and channels (like the 999 emergency call in place now) are essential. I identify here another challenge to the law enforcement agencies.

Note 1

(i) The term, Computer Security, is used in this context to embrace all references to the security aspect of the computer hardware itself, the capabilities or functions that the computer possesses (i.e., the software) and the information that is in transit or that the computer stores processes.

(ii) "Civil rights" refer to rights of a citizen to access to IT facilities (in the Image Age) in addition to political, legal and social freedom and enjoyment – denial of service.

Note 2

(i) *Computer abuse* occurs when the information stored within the computer is manipulated to the detriment of the subject (which may be an individual, a group of individuals, or an organisation) about whom that information is stored but such abusive misuse of computer resources may or may not violate criminal laws such that the perpetrator makes a gain or the victim suffers a loss, or both.

(ii) *Computer fraud* takes place when someone manipulates the computer in order to effect an offence, wilful misrepresentations with intent to deliberately deceive, directly or indirectly, such that the computer is the tool for, and the target of, the offence.

(iii) *Software piracy* is unauthorised duplication and distribution, for profit or otherwise, of copyrighted, proprietary computer software or data. It is further categorised as commercial piracy (illegal duplication of software for distribution and sale), corporate piracy (copying of software for direct financial gain) and softlifting (the software equivalent of shoplifting that occurs when a person copies a friend's software or brings a copy home from work for personal use).