JAWATANKUASA PEMBAHARUAN UNDANG-UNDANG MALAYSIA
BAHAGIAN HAL EHWAL UNDANG-UNDANG
JABATAN PERDANA MENTERI

THE LEGAL CRITIQUES OF THE COMPUTER CRIMES ACT 1997 IN REGULATING CYBERCRIME

RESEARCH MANAGEMENT INSTITUTE (RMI)
UNIVERSITI TEKNOLOGI MARA
40450 SHAH ALAM, SELANGOR
MALAYSIA

ASSOCIATE PROFESSOR DR ZAITON HAMIN
HARTINI SARIPAN
RAFIZAH ABU HASSAN

NOVEMBER 2011

Contents

3. Report

3.1 Proposed Executive Summary

From the practical legal perspective and engaging at the instrumental and normative levels, this research attempts to focus on the legal critiques of the Computer Crimes Act 1997. In particular, on the question of what is cybercrime, why is reform needed to the substantive provisions of the said Act and what changes are sought for as well as the rationales in reforming the said Act. Issues affecting the degree or kind or both that drive the need for reform of the 1997 Act will be also be discussed.

In line with the approach of common law jurisdictions, in particular the United Kingdom and Singapore as well as the Cybercrime Convention 2001, the research will examine the problems of substantive law, specifically the provisions that may be inadequate to cover certain cybercrimes such as distributed denial of service and the provisions that may in fact cover too wide an area of conduct. Also, from the theoretical level, philosophical issues involved in cybercrime, in particular the problem of identifying legal interests and emerging legal interests will be examined.

Adopting a doctrinal and library-based research approach with content analysis as the research design, this current research proposes to scrutinise the 1997 Act in comparison with its Singapore and the United Kingdom counterparts, Computer Misuse Act 1993 and the Computer Misuse Act 1990 respectively. A cursory look at the Communications and Multimedia Act 1998 would also be necessary to examine if the former statute have adequately supplemented the 1997 Act. The Council of Europe Cybercrime Convention 2001, a significant piece of international instrument, which is broadly aimed at harmonizing cybercrime laws around the world, will also be critically examined to determine the extent to which the 1997 Act in its current form is in keeping with this Convention.

In its outcome, this research would primarily offer a critical analysis of the 1997 Act and comparisons with the relevant laws in the above-mentioned jurisdictions, which will provide evidence of the flaws and weaknesses in some of its provisions. The research will also recommend several legislative drafting of the relevant provisions that require amendment as well as the inclusion of several new provisions which are currently non-existent. In the long run, these recommendations would, in some ways, provide some lessons and guidance for the policy-makers in reforming the law. Besides, it would

contribute and add to the existing and the extant literature and knowledge on cybercrime and its legislation.

3.3 Introduction

The 1997 Act was drafted in early 1997 and was modeled after the Computer Misuse Act 1990 of the United Kingdom (the 1990 UK Act). In contrast to the 1990 UK Act, the creation of the Malaysian 1997 Act was not preceded by a Law Commission report. The Computer Crimes Bill was tabled together with the Digital Signature Bill during the parliamentary session on March 25, 1997. The then Energy, Telecommunication and Post Minister, Datuk Leo Moggie, presented it for the first reading and the House of Representative passed the bill on May 5, 1997. Typical of the Malaysian law-creation practice, there was a lack of discussion and consultation with the public on the policies underlying the law. Any discussion of the social or legal implications of the proposed cyber laws was also lacking. Hence, its creation was shrouded in controversy, not so much from its criminalizing implications but from the secrecy in which it was introduced in Parliament (D.L Beatty 1998).

Despite the primariy aim at criminalizing hacking activities, which inevitably was intended to prevent and punish the perpetrators of computer crime (Dr Mahathir Mohammad 1997) the wider objective of the 1997 Act and other other cyberlaws created since 1997 was to establish Malaysia as a leader in the development of cyber laws (Dr Mahathir Mohammad 1997). Also, towards this aim, Dr Mahathir had proposed that other ASEAN countries adopt the cyber laws that Malaysia had enacted (Dr Mahathir Mohammad 1997).

This computer-specific law created four new offences of simple unauthorized access (section 3), unauthorized access with intent (section 4), unauthorized modifications (section 5) and disclosing passwords, code etc (section 6). Instrumentally, the legislative excess of the CCA 1997 includes the definition of computers, the criminalization of mere hacking in section 3 that was criticized as too harsh on young computer hobbyists (The New Straits Times April 24, 1997) and too wide leading to the criminalization of accidental unauthorized access (The Star, April 1, 1997). Whilst the vagueness of *mens rea* requirement in section 6 is a problem (Julian Ding 2000), the unexplained policy reason for the difference in the concept of authority for unauthorized access and unauthorized modification is another (Hamin 2003). The restricted scope of unauthorized modification to the contents of computer such as program or data only as opposed to any computer that does not extend to acts that prevent or hinder access or impair the computer systems is another cause for concern (Hamin 2003).

This is due to the fact that new cybercrimes such as denial of service attacks would not be covered by the current ambit of section 5. Such crime is now covered by the UK Computer Misuse Act 1990, which has since been amended to replace unauthorized modification with unauthorized acts with intent to impair computer operation (Fafinski 2008). Normatively, in contrast to the position in the UK and Singapore, the 1997 Act does not provide for many offences such as the offence of the offence of unauthorized obstruction of use of the computer, data interception, data theft, network interference, network sabotage, virus writing and computer-related forgery and fraud (McConnell Report 2000).

In view of these legislative inadequacies and breadth, it is imperative that the 1997 Act be reformed and amended as the said Act in its current form is struggling to deal with new emerging threats and risks of cybercrimes that were non-existent, unknown and unforeseen at the time of its inception in 1997. Since 2006, the 1990 Act, on which the Malaysian counterpart is based upon has been amended to deal with these new threats and to keep pace with changing times. However, for the last fourteen years we have adopted the English position of justification for the criminalization of unauthorized access and their approach in sentencing cybercriminals, and has consequently brought and adopted whatever problems of the 1990 Act that have occurred in the UK to Malaysia. Change is long overdue.

In conducting this research, the authors attempt to address these issues: What are the legislative deficiencies and excesses that could be elicited from the substantive provisions of the Computer Crimes Act 1997? How could these issues be rectified and the provisions be improved? What lessons could Malaysia learn from the Singaporean law, the law in the United Kingdom and the recommendations of the Cybercrime Convention? It is a truism that in the contemporary modern society, the dynamic nature of the Internet and technology will give rise to different types of computer crimes and the law must remain vigilant to keep up with such innovations and criminal activities which are the inevitable consequences of these developments.

The next part of the report elucidates the literature review briefly, after which the research methodology will be explained. The findings and discussion will be explicated through the instrumental critiques on the inadequacies and the excesses in the substantive provisions as well as the normative critiques of the 1997 Act prior to the recommendation and conclusion of this report.