Приймак К., студентка
Національна академія внутрішніх справ
Керівник з мови: **Драмарецька Л.Б.**

COMPUTER (CYBER) CRIME LEGISLATION IN THE UK, THE USA AND AUSTRALIA

There are at present a large number of terms used to describe crime involving computers. Such terms include computer-related crime, computer crime, Internet crime, e-crime, digital crime, high-tech crime, online crime, electronic crime, computer misconduct, and cybercrime.

The global nature and rapid uptake of the Internet has resulted in enormously increased opportunities for cybercrime, criminal activity that uses the Internet for illegal purposes and criminal activity that intends to disrupt the Internet-reliance of organizations and nations. In recent times, there has been a general acceptance of a broader interpretation for the term cybercrime ([1] and [2]), making it synonymous with computer crime and many of the references, that refer to cybercrime actually relate to computer crime in the broad sense, including crimes involving stand-alone systems. Computer crime or cybercrime are increasingly becoming major threats to national and international governments in the digital era. In recent years, jurisdictions worldwide have been forced to evaluate their legal systems to deal with the growing threats of computer-related crimes. For that, we should identify the current computer crime and cybercrime legislation in Australia, the UK and the USA.

The Commonwealth of Australia is a federation of six states and two territories [3]. The Australian constitution (section 51) allocates to the Commonwealth of Australia at the national level certain topics; one of which is post and telecommunications. Another is the external affairs topic which results in the Federal Government having exclusive jurisdiction to negotiate agreements with other national jurisdictions. The main instrument in Australia for combating computer crime or cybercrime is the Cybercrime Act of 2001. Cybercrime can only be affected via a telecommunications service and as such the Cybrecrime Act 2001 is the principal enactment covering computer crime or cybercrime in Australia. In fact, the Cybercrime Act 2001 is influenced by the Computer Misuse Act 1990 of the UK3. The Cybercrime Act amends a number of statutes, including the Criminal Code Act 1995 (Cth) . The Act inserted Part 10.7, Div 467, Div 477 and Div 478, into the Criminal Code to cover computer-related offences.

In 1989, the Federal Government amended its Crimes Act with provisions to deal with computer crime [4]. Indeed, this amendment was the first article of legislation by the Federal Government regarding computer crime. In 1991, the Telecommunications Act of 1991 added sections 74 and 76 to the Australian Criminal Code. Section 74 defines ‘carrier’ and ‘data’, and section 76 discusses the criminalisation of unauthorised access to Commonwealth computer systems. It also criminalises the examination, alteration, modification and damaging of data. In 1995, the Criminal Code Act was amended to address new computer crimes such as hacking and spreading of viruses [4].

Subsequently, additional advances in technology and the Internet have led the Australian Government to update its legislation to cover new computer crime. In 2001, the Government introduced the Cybercrime Act 2001. The Act came into effect in Australia in 2002. The Act amends the law relating to computer offences and introduces the following offences to the Criminal Code Act 1995.

The United Kingdom has signed the CoE Convention on Cybercrime but has not ratified it. The legal system in the UK is based on “common law tradition with early Roman and modern continental influences” and it accepts as compulsory the jurisdiction of the ICJ, but with reservations. In 1984, the UK introduced an Act regarding the protection of data called the Data Protection Act of 1984. This Act explains how data is gathered, used, disclosed, and disposed, and deals with the procurement and use of private data.With regard to computer-related crimes, the UK was one of the first countries to have a computer crime unit, which was established in 1985. Then, in 1990, the UK introduced the Computer Misuse Act 1990 that defines the laws, procedures and penalties surrounding unauthorised access to computer systems [4]. Three years after the introduction of this Act, two UK citizens became the first people to be sentenced for violating the Computer Misuse Act [4]. The Computer Misuse Act 1990 is the only legislation in the UK which focuses specifically on computer- related crimes. The Act has introduced the following criminal offences [5]: a) unauthorised access to any program or data kept or maintained in computer; b) unauthorised access to any program or data kept or maintained in computers for the purpose of committing or facilitating further offences; c) unauthorised modification of computer contents, data or programs.

In addition, the Act covered the area of jurisdiction. Section 4 and Section 5 of the Act state that the UK courts have jurisdiction if either the offender or the targeted computer (victim) were in the UK [5]. In 2006, the UK introduced the Police and Justice Act 2006 [5]. The Police Act amended the Computer Misuse Act for three reasons: to include longer penalties under Section 1; criminalising Denial of Service (DoS) attacks; and criminalising the supply or offer to supply software/tools that could possibly be used to commit a computer crime However, the last change has created problems for researchers who use some of the dual

use tools, for the good purposes of identifying security flows. More recently, the UK government has come with guidelines that address some of the researchers' concerns. For example, in order to prosecute the owner of a tool, it needs to identify that the tools were intended to be used to perpetrate computer crime. Conversely, the guidelines have not discussed the distribution of such tools; so, it is still possible to prosecute the person who distributes such tools.

The USA is a federal country with its laws being allocated between the federal and state legislations. The legal system in the USA is a "federal court system based on English Common Law; each state has its own unique legal system". Until now, the USA has not accepted the compulsory jurisdiction of the ICJ. The main legislation in the USA concerning computer crime is the Computer Fraud and Abuse Act 1986, also known as Section 1030 of Title 18 of the USA Code (18 USC 1030). The Act covers many computer-related offences. In 2006, the USA ratified the CoE Convention on Cybercrime. In 1977, the first proposal for federal computer crime legislation in the USA was the Ribicoff Bill, which prohibits the unauthorised use of computers. Although the bill was not adopted, this bill became the model for legislation concerning computer crime and it increased awareness of computer crime around the world.

The main legislation in the USA concerning computer crimes is the Computer Fraud and Abuse Act 1986. The Act covers many offences related to computers. After the September 11th terrorist attacks in 2001, the Computer Fraud and Abuse Act was amended by the USA Patriot Act of 2001. The amendments are intended to strengthen the USA against terrorist organisations. On the 29th of September 2006, the USA joined the CoE Convention on Cybercrime, and in 2007, the Convention came into force in the USA. The Computer Fraud and Abuse Act 1986 makes the following acts as offences [6]:

- Obtaining national security information and unauthorised access to computer;
- Compromising confidentiality and obtaining information;
- Trespassing in a government computer;
- Accessing to defraud and obtain anything of value;
- Damaging a computer or information;
- Trafficking in passwords or information;
- Threatening to damage a computer.

Список використаних джерел

1.Symantec Corporation. What is Cybercrime? 2007; Available from: http://www.symantec.com/avcenter/cybercrime/index_page2.html.

2. Council of Europe. Convention on Cybercrime. 2001; Available from: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

3. Department of the Parliamentary Library. Cybercrime Bill 2001. Digest No. 48 2001; Available from: http://www.aph.gov.au/library/Pubs/BD/2001-02/02bd048.pdf.

4. Chan, N., S. Coronel, and Y.C. Ong, The Threat of the Cybercrime Act 2001 to Australian IT Professionals, in Proceedings of the First Australian Undergraduate Students Computing Conference. 2003. p. 25-33.

5.Computer Misuse Act 1990. Available from: http://www.legislation.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

6. Parker, D.B., Computer Abuse Perpetrators and Vulnerabilities of Computer Systems, in National Computer Conference. 1976: New York. p. 65-73.