CHAPTER 2

CYBER CRIME DEFINED

It is essential firstly to establish what *computer crime*, *cyber crime* or *information technology crime* entail. Differently stated: which actions can be described as *cyber crime*; which devices will be included in this description; and how to define the different actions that will be prohibited.

2.1 COMPUTERS AND DATA

The concept *computer* was defined in section 1(1) of the Computer Evidence Act[1] as

> "any device or apparatus, whether commonly called a computer or not, which by electronic, electro-mechanical, mechanical or other means is capable of receiving or absorbing data and instructions supplied to it, of processing such data according to mathematical or logical rules and in compliance with such instructions, of storing such data before or after such processing, and of producing information derived from such data as a result of such processing".

The Computer Evidence Act[2] was repealed in its entirety by the Electronic Communications and Transactions Act[3]. A detailed

[1] Act 57 of 1983.

[2] Footnote 1 *supra*.

[3] Section 92 of Act 25 of 2002.

description of *computer system* is found in the Financial Intelligence Centre Act[4]:

> "'computer system' means an electronic, magnetic, optical, electrochemical or other data processing device, including the physical components thereof, and any removable storage medium that is for the time being therein or connected thereto, or a group of such interconnected or related devices, one or more of which is capable of –
> (i) containing data; or
> (ii) performing a logical, arithmetic or any other function in relation to data."

The same definition is found in the proposed Computer Misuse Bill in the South African Law Commission's Report on computer-related crime.[5] It is interesting to note that the Convention on Cybercrime[6] used the terms *computer system*[7] and *computer data*[8] and appears to limit the application of the Convention to computers, computer systems and computer-related data. *Computer hardware* refers to the mechanical components of a computer system and is physical in nature.[9] *Computer software* refers to the instructions given to a computer in order to function in a certain

---

[4] Act 38 of 2001.

[5] SA Law Commission Discussion Paper 99 Project 108 *Computer-related crime: Preliminary proposals for reform in respect of unauthorised access to computers, unauthorised modification of computer data and software applications and related procedural aspects* (2001) 64.

[6] Accessible at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[7] *Computer system* means "any device or group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data" *Article 1a of the Convention on Cybercrime*.

[8] *Computer data* means "any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function" *Article 1b of the Convention of Cybercrime*.

[9] A J Ebden *Computer Evidence in Court* (1985) SALJ 687.

way.[10] These instructions consist of electronic data and are incorporeal in nature.

The Electronic Communications and Transactions Act[11] do not deal with the concepts *computer* or *computer system* but rather with the concept *data*. In fact the terms computer and computer system are not defined in the Act at all. *Data* is defined as "electronic representations of information in any form"[12] and widens the scope of the application of the Act, because it is not limited to only computers. This is advantageous since this would include information systems, large computer networks, the Internet and cyberspace. Information technology necessitates the use of the term *data* rather than the term *computer*. One of the main purposes of the Act as stipulated in the preamble is to prevent abuse of information systems. The term *information system* is defined in the Act as "a system for generating, sending, receiving, storing, displaying or otherwise processing data messages and includes the Internet".[13] The Act defines the *Internet* as "the interconnected system of networks that connects computers around the world using the TCP/IP and includes future versions thereof".[14] The legislator expressly makes provision for any future forms of information networks such as the Internet.

It is further important to note that computer components are used not only in computers but various other devices.[15] The programming and functions

[10] Ebden (footnote 9 *supra*) 687.

[11] Act 25 of 2002.

[12] Section 1 of Act 25 of 2002.

[13] Section 1 of Act 25 of 2002.

[14] Section 1 of Act 25 of 2002.

[15] Computerised machinery; a cellular phone also contains data.

of these computerised devices are in the form of data. A cellular phone for instance also contains data in that it stores information in electronic format. A *smart card* is a plastic card with a microprocessor chip embedded in it.[16] The microprocessor chip enables it to store data and to process information. A smart card has computer intelligence and can perform various functions in respect of the stored data.[17] Traditional credit and debit cards are issued with magnetic strips that contain data. Bank account numbers and expiry dates are encoded on the magnetic strips through means of computer technology. These magnetic strips may also be the subject matter of the crimes discussed in the chapters below. South African banks, however, are moving towards the use of microprocessor chips embedded in credit and debit cards.[18] It is possible that various crimes could be committed in respect of the smart card itself as well as the functions and data contained in the microprocessor chip, which will make the various crimes discussed below equally applicable to smart cards. Al these devices essentially contains data that involves some form of computer and information technology and it is submitted will all fall within the scope and ambit of the Act. It is therefore submitted that it is clear that the Electronic Communications and Transactions Act will also be applicable where criminal acts are perpetrated in respect of data in smart cards, computerised devices and cellular telephones.

---

[16] In general see Kevin O'Conner *Smart Cards, Privacy Issues* (1994) Journal of Law and Information Science Vol. 5 No. 2 248; W Faul *Die 'smart' kaart – hoe werk dit?* (1989) 1 SA Mercantile Law Journal 381 and Stephen Saxby *EFT Fraud Report* (1985) 3 Computer Law and Security Report 2.

[17] Faul (footnote 16 *supra*) 382.

[18] In a promotional advertisement published in the Sunday Times (12/10/2003) it is advertised that Absa bank is the first South African bank to use chip technology in respect of debit and credit cards.

2.2 CYBER OR INFORMATION TECHNOLOGY CRIME

There is no *consensus* amongst authors and scholars as to what exactly the term *computer crime* entails.[19] Wasik states that computer crime is a rather diffuse topic and it is hard to agree on definitions.[20] According to Chen the absence of clarity in respect of a definition on computer crime results in confusion when deciding whether one is dealing with a computer crime and hinders the development of effective and consistent solutions to the computer crime problem.[21]

2.2.1 International definitions

According to Van der Merwe the American author Donn B Parker defined *computer crime* as: "any intentional, malicious act associated with computers as objects, subjects, instruments or symbols in which a victim suffered a loss and a perpetrator made, or may have made, a gain".[22] The definition was later widened to "an illegal act where perpetration, investigation, or prosecution requires a knowledge of computer technology".[23] The problem with the former definition is that the requirement of gain and loss in respect of computer crime places a limit on the type of actions that are criminalised which disregards reality. Some malicious acts may cause harm but hold no advantage to the

[19] See Christopher D. Chen *Computer crime and the Computer Fraud and Abuse Act of 1986* (1990) Computer Law Journal Vol. X, No. 1 72; Colin Tapper *"Computer Crime": Scotch Mist?* (1987) The Criminal Law Review 4 *et seq*.

[20] Martin Wasik *Crime and the Computer* 1991.

[21] Chen (footnote 19 *supra*) 72.

[22] Dana van der Merwe *Computers and the Law* (2000) 166.

[23] Footnote 22 *supra*.

perpetrator.[24] The latter definition is also far too wide since it would include investigations by means of computers that are not necessarily limited to computer crime.[25] For instance one can use computer technology to investigate and solve a murder mystery.

According to Sieber the term *computer crime* was defined by the OECD[26] as "any illegal, unethical or unauthorised behaviour involving automatic data processing and/or transmission of data".[27] The wideness of the definition according to Sieber is advantageous.[28] However, this definition is in my view far too wide since unethical behaviour may not necessarily entail a criminal action punishable in terms of criminal law.

Sloan also advocates a broad definition.[29] He distinguishes between *computer abuse*[30], *computer crime*[31] and *computer-related crimes*[32]. Wasik refers to the Scottish Law Commission's report on computer crime's[33] use of the term *computer abuse* that avoids the debate in respect

---

[24] A virus for instance may cause damage but holds no benefit for the perpetrator.

[25] Van der Merwe (footnote 22 *supra*). Also see D P van der Merwe *Computer crime – recent national and international developments* (2003) 66 THRHR 34.

[26] Organisation for Economic Co-Operation and Development.

[27] U. Sieber *New legislative Responses to Computer-Related Economic Crimes and Infringements of Privacy* in *Computermisdaad en strafrecht* (1986) 76; Ulrich Sieber *The International Emergence of Criminal Information Law* (1992) 5.

[28] Footnote 27 *supra*.

[29] Irving J Sloan *The computer and the law* (1984) 2.

[30] *Computer abuse* is "any intentional act involving a computer where the perpetrator made or could have made a gain and the victim suffered or could have suffered a loss" (Sloan; footnote 29 *supra* 3).

[31] *Computer crime* is "the common term for illegal computer abuse and implies the direct involvement of the computers in the committing a crime" (Sloan; footnote 29 *supra* 3).

[32] *Computer-related crime* is "any illegal act for which a knowledge of computer technology is essential for successful prosecution" (Sloan; footnote 29 *supra* 3).

[33] 1987.

of the term *computer crime.*[34] Wilson writes that the recent trend is to use the term *computer-related crime* that encompasses "any illegal act for which knowledge of computer technology is essential".[35] It is submitted that computer technology may also be an investigative tool but is not always indicative of a computer crime. *Computer-related crime* has also been defined as "those crimes in which a computer has played an active rather than a passive role".[36] This definition has merit and would eliminate instances where the computer is merely an investigative tool or played an unimportant role in the commission of the offence.

Jonathan B Wolf distinguishes between instances where the computer is the target of the crime (e.g. hacking and viruses) and those where the computer is used as a tool to commit a crime (e.g. fraud by means of the Internet).[37] The United States Department of Justice distinguishes between crimes where a computer is the object of the crime (such as theft of computer hardware or software); crimes where a computer is the subject of the crime (such as hacking and viruses) and instances where the computer is an instrument used to commit traditional crimes in a more complex manner (such as Internet fraud).[38] Forst proposes a very wide definition and states that: "cybercrime encompasses all of those proscribed (i.e., illegal) activities that are committed by or with the aid of

---

[34] Martin Wasik *Law Reform Proposals on Computer Misuse* (1989) The Criminal Law Review 257.

[35] Darryl C Wilson *Viewing computer crime: Where does the systems error really exist?* (1991) Computer Law Journal Vol. XI No. 1 267. Also see Steve Shackelford *Computer-Related Crime: An International Problem in Need of an International Solution* (1992) Texas International Law Journal Vol. 27 No. 2 483.

[36] Edwards, Savage & Walden (editors) *Information Technology & The Law* (1990) 142. The mere theft of a computer will constitute a passive role.

[37] Jonathan B Wolf *War Games Meets the Internet: Chasing 21st Century Cybercriminals With Old Laws and Little Money* in American Journal of Criminal Law (2000) Vol. 28 No. 1 95.

[38] Shani S Kennedy & Rachel Price Flum *Computer crime* American Criminal Law Review (2002) Vol. 39 No. 2 274 *et seq*.

computers or information technology, or where computers are the target of the criminal enterprise."[39]

2.2.2 South African definitions

South African authors Credo and Michels defined computer crime as: "computer crime encompasses the use of a computer as a tool in the perpetration of a crime, as well as situations in which there has been unauthorised access to the victim's computer, or data. Computer crime also extends to physical attacks on the computer and/or related equipment as well as illegal use of credit cards and violations of automated teller machines, including electronic fund transfer thefts and the counterfeit of hardware and software."[40] This definition is quite old and as pointed out by Van der Merwe does not include the advent of computer viruses.[41]

Van der Merwe in the first edition of his book defined computer crime as an illegal act where perpetration involved a computer.[42] In the second edition, the author had changed the definition to: "computer crime covers all sets of circumstances where electronic data processing forms the means for the commission and/or the object of an offence and represents the basis for the suspicion that an offence has been committed".[43]

---

[39] Martin L Forst *Cybercrime: Appellate Court Interpretations* (1999) 1.

[40] Credo and Michels *Computer crime in South Africa* (1985) 2.

[41] Dana van der Merwe *Computers and the law* (2000) 187.

[42] See D P van der Merwe *Computers and the law* (1986). See footnote 43 *infra*.

[43] Dana van der Merwe *Computers and the law* (2000) 188.

According to Gordon computer crime involves any criminal activity where a computer is involved.[44]

Jonathan Marshall recently emphasised the importance to distinguish between instances where computers are the object or "victim" of a crime and those instances where a computer is the instrument or tool with which the crime is committed.[45] He is of the view that the use of a computer as an instrument to commit the crime is not much different from using a gun to commit a murder.[46] In my view what establishes a cyber crime, whether information technology and/or a computer is the target or object of the crime or a tool or method with which the crime is committed, is the fact that a computer and/or information technology play an *active* role in the commission of the offence.

Recently Van der Merwe wrote that the data and information contained in a computer are key concepts and that *information technology*[47] *crime* would be a better term to use.[48] The use of the term computer is outdated and the revolution in information technology necessitates a different approach. Criminal behaviour is no longer only directed at a computer,

---

[44] Barrie Gordon *Internet criminal law* in Buys(ed) *Cyberlaw @ SA* (2000) 423. Also see Adv B Gordon *Computer crime – An introduction* (2002) Servamus 34.

[45] Jonathan Burchell *Criminal Justice at the Crossroads* (2002) SALJ Vol. 119 at 585. Also see Debbie Collier *Criminal Law and the Internet* in Buys(ed) *Cyberlaw @ SA II* (2004) 322 *et seq*.

[46] Burchell (footnote 45 *supra*) 585.

[47] A definition of information technology is found in section 1 of the State Information Technology Agency Act, 88 of 1998: "Information Technology means all aspects of technology which are used to manage and support the efficient gathering, processing, storing and dissemination of information as a strategic resource".

[48] D P Van der Merwe *Computer crime – recent national and international developments* (2003) 66 THRHR 31. Also see D P van der Merwe *Computers* in W A Joubert(ed) LAWSA Vol. 5 2; Martin Wasik *The role of the criminal law in the control of misuse of information technology* (1992) 8 Computer Law and Security Report 27 *et seq*.; Ulrich Sieber *The International Emergence of Criminal Information Law* (1992) 11 *et seq*.

but involves computer systems, information networks, the Internet and cyberspace. In modern times it would be more appropriate to use the term *information technology crime* to describe all the illegal activities in respect of computers and information technology. The term *cyber crime* is wide enough to encompass all illegal activities in respect of computers, information networks and cyberspace. Watney uses the term *cyber crime* ("*kubermisdaad*") and defines cyber crime as all illegal activities pertaining to a computer system, irrespective of whether the computer is the object of the crime or the instrument with which the crime is committed.[49] In my view both *information technology crime* as well as *cyber crime* are suitable to classify this specific group of illegal activities and crimes.

2.2.3 A proposed definition of the terms *cyber crime* or *information technology crime*

It is essential to distinguish between computer technology that is used to investigate crime in general and cyber crimes. The essence of a certain type of crime is to be found within the crime itself and not necessarily the manner in which it is investigated. Cyber crime is no longer restricted to computers and the focus has moved to data and information technology. The first leg of the definition should include unauthorised access to data (i.e. hacking)[50], unauthorised modification of data (i.e. viruses and worms)[51] and unauthorised interception of data[52]. The criminalisation of

[49] M M Watney *Die strafregtelike en prosedurele middele ter bekamping van kubermisdaad (deel 1)* (2003) 1 TSAR 56.

[50] See chapter 3 *infra*.

[51] See chapter 4 *infra*.

[52] See chapter 6 *infra*.

the dealing and possession of devices used to commit cyber offences should also fall within the first leg of the definition.[53] In other words the first leg of the definition encompasses all the new types of crimes that surfaced with the advent of the computer and information technology. The computer or data is generally the target of the crime.

Computer-related extortion[54], computer-related fraud[55] and theft of information, credit and data[56] should fall within the second leg of the definition. These types of crimes have existed for ages and are now perpetrated by means of sophisticated technology. Computers and information technology play an active roll in the commission of these offences. Child pornography should also fall within this leg of the definition since computers and the Internet are now tools through which child pornography is manufactured and distributed.[57]

In my view *cyber crime* or *information technology crime* can be defined as follows:

> Cyber crime encompasses all illegal activities where the computer, computer system, information network or data is the target of the crime and those known illegal activities or crimes that are actively committed through or with the aid of computers, computer systems, information networks or data.

---

[53] See chapter 7 *infra*.

[54] See chapter 9 *infra*.

[55] Computer-related fraud would include Internet fraud. See chapter 10 *infra*.

[56] See chapter 11 *infra*.

[57] See chapter 8 *infra*.