CHAPTER 13

INVESTIGATING CYBER CRIME

13.1 INTRODUCTION

Traditional investigation methods are somewhat strained and ill equipped when dealing with cyber crime. Investigators are no longer dealing with physical items situated on premises, but are required to investigate crimes perpetrated through highly sophisticated technology and sometimes through borderless information networks.

Cyber crime is of a borderless nature and conventional boundaries are no longer the norm. A virus for instance can cause widespread consequences worldwide. The gathering of admissible evidence in another country could be extremely difficult.[1] The successful investigation and subsequent prosecution of some cyber crimes will depend greatly on the co-operation between the different countries during the investigation process. The Preamble to the Convention on Cybercrime states *inter alia*:

> "Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters"[2]

---

[1] See Mark Tantam *Hacking: proving the crime* (1990) January/February Computer Law & Practice 79.

[2] Convention on Cybercrime ETS No 185, Council of Europe, Budapest accessible at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Chapter III of the Convention deals with international co-operation between the signatory countries and provides that the countries should co-operate to the widest extent possible through international agreements, treaties and domestic laws.[3] Mutual assistance to the widest extent possible in respect of the investigation of cyber offences and the collection of electronic evidence must be afforded between the signatory countries.[4] The Convention contains detailed provisions in respect of mutual assistance between signatory countries on the basis of a mutual assistance treaty[5] or in the absence of such a treaty[6]. In South Africa Interpol[7] already assists in the investigation of crime internationally and it may be appropriate that international cyber crime be investigated with their assistance.

13.2 ARREST

Arrest is but one of the ways through which an accused' attendance can be secured at court.[8] It constitutes the most drastic infringement on the fundamental rights of an individual.[9] The Electronic Communications and Transaction Act[10] contains no provisions regarding arrest and the

[3] Article 23 of the Convention on Cybercrime.

[4] Article 25 of the Convention on Cybercrime.

[5] Article 25 of the Convention on Cybercrime.

[6] Article 27 of the Convention on Cybercrime.

[7] International Police.

[8] In general see Du Toit *et al Commentary on the Criminal Procedure Act* (2003) chapter 5.

[9] Section 12 of The Constitution of the Republic of South Africa 108 of 1996 provides that every person has the right to freedom and security of the person.

[10] Act 25 of 2002.

Criminal Procedure Act[11] would therefore apply. A warrant for arrest may be issued by a magistrate on the written application of the director of prosecutions or a prosecutor.[12] In these cases the police will investigate a cyber crime and prepare a docket. The docket will thereafter be referred to a prosecutor for a decision whether to prosecute or not. If a prosecutor decides to prosecute, a written application may be made to a magistrate for the issuing of a warrant of arrest. An accused may also be summoned to appear before court in order to be criminally prosecuted.[13]

Section 40(1) of the Criminal Procedure Act 51 of 1977 states:

> "A peace officer may without warrant arrest any person-
> (a) who commits or attempts to commit any offence in his presence;
> (b) whom he reasonably suspects of having committed an offence referred to in Schedule 1, other than the offence of escaping from lawful custody;….."

Police officers, justices of the peace[14] and magistrates are all peace officers and may arrest without a warrant.[15] If a cyber criminal commits a cyber crime in the presence of a police officer, he may arrest the person without a warrant.[16]

---

[11] Act 51 of 1977.

[12] Section 43 of Act 51 of 1977.

[13] Section 54 of Act 51 of 1977.

[14] See Justices of the Peace and Commissioners of Oaths Act 16 of 1963.

[15] Section 1 of Act 51 of 1977.

[16] It is highly unlikely that this will happen, but the entrapment of a cyber criminal may result in this.

In terms of section 40(1)(b) a police officer may arrest a cyber criminal whom he reasonably suspects of having committed a schedule 1 offence. Section 1 offences include fraud, theft as well as any offence for which imprisonment exceeding 6 months may be imposed. This will include all the offences in sections 86 and 87 of the Electronic Communications and Transactions Act.

13.3 EXTRADITION

It occasionally happens that a perpetrator commits a cyber crime in a country and then flees to a different country in order to evade prosecution. The country to which he has fled may extradite the perpetrator to the country in which the crime was committed. Many countries have signed international agreements or treaties to regulate extradition. The Convention on Cybercrime also deals with the issue of extradition[17] and provides that cyber crimes should be included as extraditable offences in an extradition treaty between signatory countries.[18]

Extradition in South Africa is governed by the Extradition Act[19] that sets out in detail the procedures for extradition. An extraditable offence means "any offence which in terms of the law of the Republic and of the foreign State concerned is punishable with a sentence of imprisonment or other form of deprivation of liberty for a period of six months or more".[20] The

[17] In general see Article 24 of the Convention on Cybercrime.

[18] Article 24(2) of the Convention on Cybercrime.

[19] Act 67 of 1962.

[20] Section 1 of Act 67 of 1962.

principle of *double criminality* means that the extraditable offence must be a crime in the country to which the perpetrator is extradited as well as the country that is extraditing the perpetrator. This principle can be very problematic in respect of cyber crimes since there are still countries that have not criminalised cyber crimes. South Africa has criminalised cyber crimes and will therefore be in a position to extradite cyber criminals to countries that have similar offences. A period of imprisonment exceeding 6 months or more may be imposed in respect of contraventions of sections 86 and 87 of the Electronic Communications and Transactions Act as well as the common law crimes of theft and fraud. These types of cyber crimes are therefore extraditable offences.

It is clear that a perpetrator will only be extradited for a serious offence and a perpetrator that merely gained unauthorised access to a system without causing damage, might not be extradited.[21]

13.4 SEARCH AND SEIZURE[22]

A police officer may search on authority of a search warrant.[23] A police official may also search (without a warrant) any person, container or premises for the purposes of seizing an article referred to in section 20, if the person or owner or occupier consents to the search.[24] In terms of section 22(b) of the Criminal Procedure Act a police official may search a person, container or premises for an article referred to in section 20, if he

---

[21] Barrie Gordon *Internet Criminal Law* in Buys(ed) *Cyberlaw @ SA* (2000) 444.

[22] In general see Du Toit *et al Commentary on the Criminal Procedure Act* (2003) chapter 2.

[23] Section 21 of Act 51 of 1977.

[24] Section 22(a) of Act 51 of 1977.

believes on reasonable grounds that a search warrant will be issued to him if he applied for one and that the delay in obtaining the warrant would defeat the object of the search. The context in which the word premises are used implies physical structures or items. A computer is a physical item but the information contained in a computer is of an incorporeal nature. Similarly is an information system or network incorporeal in nature. The Electronic Communications and Transactions Act provide that the concepts *premises* and *article* will also include information systems and data messages.[25]

It is very easy to delete data and information contained in a computer or system. A perpetrator can simply press the *delete* key and everything that he had been busy with, is erased. Data contained on disks can just as easily be erased. It is sometimes imperative that a search be done immediately and without prior notice to prevent the destruction of evidence and to preserve the integrity of data.

Computer components and disks can sometimes be very small and can easily be hidden on a person. In terms of the Criminal Procedure Act a person may be searched when premises are searched. An arrested person may also be searched.[26]

A further problem an investigator may be faced with is the searching of computer and information networks. It may be difficult to pinpoint the location of data and the location may then not be specifically mentioned in the search warrant. It may happen that a network spans over several

[25] Section 82(4) of Act 25 of 2002.

[26] Section 23 of Act 51 of 1977.

magisterial jurisdictions or that information is in more than one magisterial jurisdiction. Which magistrate should issue the search warrant then? It may happen that the location of the information may be in a different country. International co-operation will be necessary to legally seize that information.

Information or data may be protected by passwords, encryption and other security measures. May the police officer attempt to overcome these security measures? What methods may be used in order to overcome security measures?

The Criminal Procedure Act provides that the following articles are susceptible to seizure:

- articles which are concerned in or are on reasonable grounds believed to be concerned in the commission or suspected commission of an offence, whether within the republic or elsewhere;
- articles which may afford evidence of the commission or suspected commission of an offence, whether within the Republic or elsewhere;
- articles which are intended to be used or are on reasonable grounds believed to be intended to be used in the commission of an offence.[27]

Physical computers, devices, disks and printouts are examples of physical items that may be seized. The question arises whether incorporeal data and information are susceptible to seizure. Section 20 of the Criminal Procedure Act states that an *article* may be seized. An article implies an object of a physical nature capable of being physically seized. However in terms of the Electronic Communications and Transactions act an article

[27] Section 20 of Act 51 of 1977.

will include data messages.[28] Data may therefore be seized provided the requirements in section 20 of the Criminal Procedure Act are met.

A person's constitutionally protected rights to privacy[29] and property[30] are infringed upon during a search and seizure. These rights however are limited[31] due to the public's interest in the investigation and prosecution of crimes. What may be of concern during the search of a computer or information system is that private data unrelated to the offence may be observed. This information may contain trade secrets.

13.5 CYBER INSPECTORS

A controversial chapter in the Electronic Communications and Transactions Act is the appointment of cyber inspectors.[32] The Director-General of the Department of Communications may appoint an employee of the Department as a cyber inspector.[33] The Act does not stipulate the qualifications that a cyber inspector should have. A certificate of appointment must be provided to a cyber inspector[34] and this certificate must be shown to concerned parties when a cyber inspector performs his

[28] Section 82(4) of Act 25 of 2002.

[29] Section 14 of Act 108 of 1996.

[30] Section 25 of Act 108 of 1996.

[31] A fundamental right may be limited in terms of the provisions of section 36 of Act 108 of 1996.

[32] See in general Wim Mostert *The good things about the Electronic Communications & Transactions Bill…* (2002) Without Prejudice Vol. 2 No 3 1; Jacques Jansen *A new era for e-commerce in South Africa* (October 2002) De Rebus 20; Adv B Gordon *A new tool for cyber crime fighters* (2002) May Servamus 32.

[33] Section 80(1) of Act 25 of 2002.

[34] Section 80(2) of Act 25 of 2002.

or her functions.[35] Any person who falsely holds himself out to be a cyber inspector is guilty of an offence[36] and upon conviction may be sentenced to a fine or imprisonment not exceeding 12 months.[37] It was recently reported that although the Act has been in operation for almost two years, no cyber inspectors have been appointed by the Department of Communications.[38]

A cyber inspector has wide powers and these include the power to monitor and inspect any web site or activity on an information system in the public domain and to report illegal activities to the authorities.[39] A cyber inspector also has powers in respect of cryptography service providers, authentication service providers and critical database administrators and to ensure that these service providers comply with the relevant provisions of the Act.[40]

Section 81(2) of the Act provides that "any statutory body, including the South African Police Service, with powers of inspection or search and seizure in terms of any law may apply for assistance from a cyber inspector to assist it in an investigation". The body must apply to the Department of Communications for such assistance and the assistance may be subject to certain conditions.[41] The South African Police Service

---

[35] Section 80(4) of Act 25 of 2002.

[36] Section 80(5)(b) of Act 25 of 2002.

[37] Section 89(1) of Act 25 of 2002.

[38] *SA has no 'cyber cops' to police cyber traffic* The Citizen 30/01/2004 page 4.

[39] Section 81(1)(a) of Act 25 of 2002.

[40] Section 81(1) of Act 25 of 2002.

[41] Section 81(2) of Act 25 of 2002.

employs experts in the fields of forensics and technology. The police may also request the assistance and expertise of cyber inspectors in their investigation of cyber crimes. According to Watney the requirement that the requesting body must have the power to search and seize could mean that cyber inspectors are only there to assist in an advisory capacity.[42]

A cyber inspector has wide powers to enter any premises or access any information system that has bearing on an investigation in order to search and seize, but are limited to the extent that a warrant is required.[43] A search and seizure may be performed at any reasonable time during the day[44], without prior notice. A judge or a magistrate may issue a warrant on request of a cyber inspector, subject to the provisions of section 25 of the Criminal Procedure Act. [45] This means that the magistrate or judge on the basis of information under oath must have reasonable grounds to suspect that a crime has been committed or is in the process of being committed or will be committed upon premises in its jurisdiction. A judge or a magistrate may issue a warrant where the offence has been committed in South Africa, the perpetrator is a South African citizen or resident or present in South Africa when the warrant is applied for.[46] A warrant may also be issued when "information pertinent to the investigation is accessible from within the area of jurisdiction of court".[47]

---

[42] M M Watney *Die strafregtelike en prosedurele middele ter bekamping van kubermisdaad (deel 1)* (2003) 70.

[43] Section 82(1) of Act 25 of 2002.

[44] Section 83(5) of Act 25 of 2002. A warrant may be executed during the night if it is authorised by the issuing judge or magistrate.

[45] Section 83(1) of Act 25 of 2002.

[46] Section 83(2) of Act 25 of 2002.

[47] Footnote 45 *supra.*

This provision is helpful when information is located in a network that spans over several jurisdictions.

The warrant must identify the premises and information system that may be entered and searched.[48] The warrant must also specify which actions can be performed by a cyber inspector in respect of the information system.[49] A person must first enter premises in order to gain access to the computer. The cyber inspector will then access the computer, information system or network. A cyber inspector may perform various actions subject to what is specified in the warrant.[50]

One of the main criticisms against the appointment of cyber inspectors is the possible infringement of the constitutionally protected right to privacy and property. According to Collier the appointment of cyber inspectors, who have extremely wide powers, to assist the police, who actually are the persons that should investigate cyber crime, is an unwarranted extension of the powers of the Department of Communications.[51]

The provisions of section 82(1)(f) of the Act is interesting since provision is made for the investigation of cyber crime when the cyber inspector has reasonable cause to suspect that computers, networks or equipment on the premises may have been used in the commission of any crime. This may happen when a cyber inspector searches the premises on authority of a warrant and discovers computers that he reasonably suspects may have

[48] Section 83(3)(a) of Act 25 of 2002.

[49] Section 83(3)(b) of Act 25 of 2002.

[50] Section 82(1)(a) – (h) of Act 25 of 2002.

[51] Buys(ed) *Cyberlaw @ SA II* (2004) 335-336.

been used in the commission of a different offence.[52] The cyber inspector may then proceed with his investigation at the premises without obtaining a warrant. In this case the time lapse that will occur when a warrant is obtained may lead to the destruction of evidence.

The Act contains no provisions in respect of arrest by a cyber inspector and the provisions of the Criminal Procedure Act would therefore apply. At the time of writing cyber inspectors have not been classified as peace officers and if they arrest a cyber criminal the provisions relating to arrest by a private person will apply.

Any person who hinders or obstructs a cyber inspector in the performance of his or her duties is guilty of an offence[53] and upon conviction punishable with a fine or imprisonment not exceeding 12 months[54].

[52] Watney (footnote 42 *supra*) 71.

[53] Section 80(5)(a) of Act 25 of 2002.

[54] Section 89(1) of Act 25 of 2002.