CYBER CRIME
A COMPARATIVE LAW ANALYSIS

by

SANDRA MARIANA MAAT

submitted in part fulfilment of the requirements for the degree of

MAGISTER LEGUM

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROF D P VAN DER MERWE

NOVEMBER 2004

SUMMARY

The Electronic Communications and Transactions Act, 25 of 2002, eradicated various *lacunae* that previously existed in respect of cyber crimes. Cyber crimes such as *inter alia* hacking, rogue code, unauthorised modification of data and denial of service attacks have now been criminalised. Specific criminal provisions in relation to *spamming*, computer-related fraud and extortion have also been included in the Act. It is argued that theft of incorporeal items such as information has already been recognised in our law, but has not been taken to its logical conclusion in our case law. However, there are instances where neither the common law nor our statutory provisions are applicable and where there is still a need for legislative intervention. The Act sufficiently deals with jurisdiction, the admissibility of data messages, the admissibility of electronic signatures and the regulation of cryptography. Cyber inspectors are a new addition to law enforcement.

KEY TERMS

Cyber crime

Hacking

Rogue code

Denial of service attacks

Unauthorised interception

Computer-related fraud

Theft of information

Cyber inspectors

Cryptography

Digital signatures

TABLE OF CONTENTS

CHAPTER 4

UNAUTHORISED MODIFICATION

CHAPTER 5

DENIAL OF SERVICE ATTACKS

CHAPTER 6

UNAUTHORISED INTERCEPTION

CHAPTER 7

DEVICES

CHAPTER 8

CYBER OBSCENITY

CHAPTER 9

EXTORTION

CHAPTER 10

COMPUTER-RELATED FRAUD

CHAPTER 11

THEFT

CHAPTER 12

JURISDICTION

CHAPTER 13

INVESTIGATING CYBER CRIME

CHAPTER 14

PROVING CYBER CRIME

CHAPTER 15

PREVENTING CYBER CRIME