

**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

SUMMARY.....	I
---------------------	---

KEY TERMS	ii
------------------------	----

TABLE OF CONTENTS.....	iii
-------------------------------	-----

CHAPTER 1

INTRODUCTION

1.1 THE ELECTRONIC FRONTIER	1
1.2 DEFINING THE PROBLEM	4

CHAPTER 2

CYBER CRIME DEFINED

2.1 COMPUTERS AND DATA	12
2.2 CYBER OR INFORMATION TECHNOLOGY CRIME	16
2.2.1 International definitions	16
2.2.2 South African definitions	19
2.2.3 A proposed definition of the terms <i>cyber crime</i> or <i>information technology crime</i>	21

CHAPTER 3

UNAUTHORISED ACCESS

3.1 INTRODUCTION	23
------------------------	----

3.2 WHAT IS HACKING?.....	24
3.3 SHOULD HACKING BE CRIMINALISED?	27
3.4 COMPARATIVE LAW ANALYSIS IN RESPECT OF HACKING.....	29
3.4.1 United States of America.....	29
3.4.1.1 Federal laws	30
3.4.1.2 Individual States.....	34
3.4.2 United Kingdom.....	36
3.4.3 Germany.....	41
3.4.4 Greece.....	42
3.4.5 Australia	43
3.4.6 Singapore and Malaysia	45
3.5 INTERNATIONAL RESPONSES BY THE COUNCIL OF EUROPE.....	46
3.6 SOUTH AFRICAN OFFENCES BEFORE THE ENACTMENT OF THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT.....	47
3.6.1 Housebreaking.....	47
3.6.2 Trespassing Act.....	50
3.6.3 Malicious injury to property	51
3.6.4 Fraud	52
3.6.5 <i>Crimen Iniuria</i>	52
3.7 THE SOUTH AFRICAN ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT	54
3.7.1 The criminal action (conduct)	55
3.7.2 Unlawfulness.....	59
3.7.3 Culpability and criminal capacity.....	64
3.7.4 Related provisions.....	67
3.7.5 Sentence.....	68

3.8 FURTHER LEGISLATION IN SOUTH AFRICA IN RESPECT OF UNAUTHORISED ACCESS OFFENCES	69
--	----

CHAPTER 4

UNAUTHORISED MODIFICATION

4.1 INTRODUCTION.....	73
4.2 DANGEROUS OR ROGUE CODE	76
4.2.1 Viruses.....	77
4.2.2 Worms	79
4.2.3 Trojan Horse	80
4.2.4 Logic bombs	81
4.2.5 Bacterium	82
4.2.6 Crab	82
4.2.7 Hoaxes or virtual viruses	83
4.3 SHOULD UNAUTHORISED MODIFICATION BE CRIMINALISED?	83
4.4 COMPARATIVE LAW ANALYSIS IN RESPECT OF UNAUTHORISED MODIFICATION OFFENCES.....	84
4.4.1 United States of America.....	84
4.4.1.1 Federal statutes.....	84
4.4.1.2 State Laws.....	89
4.4.2 United Kingdom.....	91
4.4.3 Germany.....	95
4.4.4 Greece.....	96
4.4.5 Singapore.....	97
4.4.6 Philippines	98
4.4.7 Australia	99
4.4.8 Canada.....	100

4.5 INTERNATIONAL RESPONSES BY THE COUNCIL OF EUROPE.....	101
4.6 SOUTH AFRICAN OFFENCES BEFORE ENACTMENT OF THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT.....	103
4.6.1 Malicious injury to property	103
4.6.2 Housebreaking with the intent to commit an offence	108
4.6.3 Trespass Act.....	109
4.7 THE SOUTH AFRICAN ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT.....	109
4.7.1 The criminal action (conduct)	110
4.7.2 Unlawfulness	112
4.7.3 Culpability.....	113
4.7.4 Related provisions	115
4.7.5 Sentence.....	116
4.8 FURTHER SOUTH AFRICAN LEGISLATION IN RESPECT OF UNAUTHORISED MODIFICATION OFFENCES.....	117

CHAPTER 5

DENIAL OF SERVICE ATTACKS

5.1 INTRODUCTION.....	120
5.2 INTERNATIONAL RESPONSES.....	122
5.2.1 The United States of America and the United Kingdom	122
5.2.2 Canada	123
5.2.3 Council of Europe	123
5.3 SOUTH AFRICAN RESPONSES	124
5.3.1 South African Law Commission	124
5.3.2 The Electronic Communications and Transactions Act	125

CHAPTER 6

UNAUTHORISED INTERCEPTION

6.1 INTRODUCTION.....	128
6.2 INTERNATIONAL LEGISLATIVE RESPONSES.....	129
6.3 INTERNATIONAL RESPONSES BY THE COUNCIL OF EUROPE.....	130
6.4 SOUTH AFRICAN RESPONSES.....	131
6.4.1 The Interception and Monitoring Prohibition Act.....	131
6.4.2 The Interception and Monitoring Bill.....	132
6.4.3 The Regulation of Interception of Communications and Provision of Communication-Related Information Act.....	133
6.4.4 The Electronic Communications and Transactions Act.....	135

CHAPTER 7

DEVICES

7.1 INTRODUCTION.....	137
7.2 INTERNATIONAL RESPONSES	139
7.2.1 United States of America and the United Kingdom	139
7.2.2 Canada.....	141
7.2.3 The Convention on Cybercrime.....	142
7.3 SOUTH AFRICAN RESPONSES.....	143

CHAPTER 8

CYBER OBSCENITY

8.1 INTRODUCTION.....	148
8.2 CHILD PORNOGRAPHY	148

8.2.1 International responses to child pornography	148
8.3.2 South African responses.....	149

CHAPTER 9

EXTORTION

9.1 INTRODUCTION.....	155
9.2 INTERNATIONAL RESPONSES TO COMPUTER-RELATED EXTORTION.....	156
9.3 SOUTH AFRICAN RESPONSE TO COMPUTER-RELATED EXTORTION.....	157

CHAPTER 10

COMPUTER-RELATED FRAUD

10.1 INTRODUCTION.....	161
10.2 INTERNATIONAL EXAMPLES.....	162
10.2.1United States of America.....	162
10.2.2United kingdom.....	163
10.2.3Australia.....	164
10.3 INTERNATIONAL RESPONSES BY THE COUNCIL OF EUROPE.....	166
10.4 THE COMMON LAW CRIME OF FRAUD IN SOUTH AFRICA	168
10.4.1Introduction.....	168
10.4.2Misrepresentation.....	169
10.4.3Prejudice.....	173
10.4.4Unlawfulness and culpability.....	174
10.4.5Attempted fraud.....	174

10.5 SECTION 87(2) OF THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT.....	174
10.6 SPAMMING.....	177

CHAPTER 11

THEFT

11.1 INTRODUCTION.....	180
11.2 THEFT OF INFORMATION.....	181
11.2.1 International examples	181
11.2.2 The South African common law crime of theft with specific reference to theft of information.....	183
11.2.2.1 Introduction.....	183
11.2.2.2 Appropriation.....	185
11.2.2.3 A Certain kind of property.....	186
11.2.2.4 Intention to permanently deprive the owner of his property....	195
11.2.3 Comparison between theft, unauthorised use and copyright	197
11.3 IDENTITY THEFT	201
11.3.1 South African position regarding identity theft	201
11.3.2 International responses	202

CHAPTER 12

JURISDICTION

12.1 INTRODUCTION.....	204
12.2 INTERNATIONAL RESPONSE BY THE COUNCIL OF EUROPE.....	205
12.3 SOUTH AFRICAN POSITION.....	206

CHAPTER 13

INVESTIGATING CYBER CRIME

13.1 INTRODUCTION.....	210
13.2 ARREST.....	211
13.3 EXTRADITION.....	213
13.4 SEARCH AND SEIZURE.....	214
13.5 CYBER INSPECTORS.....	217

CHAPTER 14

PROVING CYBER CRIME

14.1 INTRODUCTION.....	222
14.2 DOCUMENTARY EVIDENCE, REAL EVIDENCE AND HEARSAY.....	224
14.2.1 International position.....	224
14.2.2 South African responses.....	225
14.3 ENCRYPTION.....	232
14.4 ELECTRONIC SIGNATURES.....	239

CHAPTER 15

PREVENTING CYBER CRIME

15.1 EDUCATION AND AWARENESS.....	245
15.2 INFORMATION TECHNOLOGY SECURITY.....	246
15.3 DETECTION, REPORTING AND THE JUSTICE SYSTEM....	246
15.4 INTERNATIONAL CO-OPERATION.....	247

CHAPTER 16**SIGNING OFF**

.....	249
BIBLIOGRAPHY	253
LIST OF ABBREVIATIONS	278
TABLE OF CASES	279
TABLE OF STATUTES	284
SUBJECT INDEX	288