

6140 228 86

U.O.V.S. BIBLIOTEK

01

University Free State



3430000989412

Universiteit Vrystaat

INTERNET RELATED COMMERCIAL CRIMES

by

Gerhardus Johannes Ebersöhn

LL.B. (UFS)

Submitted in accordance with the requirements for the
degree **Magister Legum**

in the **Faculty of Law,**

Department of Mercantile Law

of the **University of the Free State**

Supervisor:
Prof. J.J. Henning

Co-Supervisor:
Prof. T. Verschoor

BLOEMFONTEIN
30 November 2001

The Ten Commandments of Computer Ethics

by the *Computer Ethics Institute*:ⁱ

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that insure consideration and respect for your fellow humans."

Copied and printed in terms of section 12(1) of the *Copyright Act* 98 of 1978.

ⁱ A copy can be downloaded from www.cpsr.org/program/ethics/cei.html.

TABLE OF CONTENTS

CHAPTER ONE

INTRODUCTION

1. GENERAL INTRODUCTION	1
2. SCOPE AND PURPOSE OF THIS STUDY	2
3. DEMARCATION OF STUDY	3
4. EXPOSITION	4
5. REFERENCE SYSTEM USED	5

CHAPTER TWO

POSSIBILITIES WHICH THE INTERNET OFFERS

1. INTRODUCTION	6
2. ONLINE BANKING	6
3. ELECTRONIC COMMERCE	7
4. COMMUNICATION	8

CHAPTER THREE

RISKS THE INTERNET POSES	9
--------------------------	---

CHAPTER FOUR

MALICIOUS COMPUTER PROGRAMS

1. INTRODUCTION	13
2. EXAMPLES OF MALICIOUS COMPUTER PROGRAMS	13
2.1. Viruses	13
2.2. Worms	16
2.3. Trojan horses	17
2.4. Logic and time bombs	18
2.5. Virtual viruses	19
2.6. Bacteria	20

3. THE RISKS MALICIOUS PROGRAMS POSE	20
4. PREVENTING MALICIOUS PROGRAMS FROM ENTERING THE COMPUTER SYSTEM	21
4.1. Anti-virus software	22
4.2. Submitting suspected viruses to anti-virus software companies for inspection	23
4.3. Other anti-virus computer program protection	23

CHAPTER FIVE

MALICIOUS COMPUTER EXPERTS

1. INTRODUCTION	24
2. A FEW DEFINITIONS – HACKERS, CRACKERS, PHREAKERS, CYPHERPUNKS & SCRIPT KIDDIES	24
3. TECHNIQUES USED BY HACKERS	26
4. DAMAGE HACKERS CAN CAUSE	33
5. EXAMPLES OF REPORTED HACKING INSTANCES	37
5.1. South Africa	37
5.2. Worldwide	38
6. PREVENTING COMPUTER-RELATED CRIMES	40
6.1. Mere usernames and passwords insufficient	41
6.2. Firewalls	42
6.3. Public key encryption, symmetric encryption and digital certificates	43
6.4. Network intrusion-detection devices & software	45
6.5. Back-up copies	46
6.6. System administrator	46
6.7. Password policy	47
6.8. E-mail policy	48
6.9. Internet usage policy	49

CHAPTER SIX

CRIMINAL LIABILITY OF MALICIOUS COMPUTER PROGRAMMERS AND HACKERS

1. INTRODUCTION	50
2. LIABILITY IN TERMS OF DEDICATED LEGISLATION	50
2.1. Interception and Monitoring Prohibition Act	50
2.2. South African Police Service Act & Correctional Services Act	54
3. LIABILITY IN TERMS OF COMMON LAW AND OTHER NON-SPECIFIC STATUTORY PROVISIONS	56
3.1. Theft as common law offence	56
3.1.1. General principles	56
3.1.2. <i>Lucrum</i> as an element of theft	59
3.1.3. Theft of credit	77
3.1.4. Theft of electronic data/credit	78
3.1.4.1. Corporeal object	79
3.1.4.2. Intention to appropriate and <i>lucrum causa faciendi</i>	91
3.1.4.3. Appropriation	94
3.1.5. Theft of passwords and credit card information	98
3.1.6. Instructing and assisting hackers	101
3.1.7. <i>De minimis non curat lex</i>	102
3.1.8. Hacker making a mental copy or writing something down	102
3.1.9. Hacker found in possession of stolen electronic data, but owner of data unknown to prosecutor	104
3.2. Liability in terms of the General Law Amendment Act 50 of 1956	105
3.3. Receiving stolen property	107
3.3.1. The common law offence of receiving stolen property knowing that it is stolen	108
3.3.1.1. Stolen property	109
3.3.1.2. Receiving property	110
3.3.1.3. Knowing that it is stolen property	110
3.3.2. General Law Amendment Act 62 of 1955	116
3.3.2.1. Meaning of "goods"	117

3.3.2.2. Elements of offence in terms of section 37	126
3.3.2.3. Elements of offence in terms of section 36	127
3.4. Fraud as common law offence	129
3.4.1. General principles	129
3.4.2. Does hacking into computers constitute fraud?	135
3.4.2.1. Misrepresentation as an element of fraud	135
3.4.2.2. The element of prejudice	138
3.4.2.3. The element of "intent to defraud"	139
3.4.3. Must a system administrator be deceived?	140
3.4.4. Is the breaking or penetrating of security measures a requirement?	141
3.4.5. Does an unsuccessful attempt to hack constitute fraud or attempted fraud?	142
3.4.6. Does a denial-of-service attack constitute fraud?	148
3.4.7. Does a virus hoax constitute fraud or attempted fraud?	150
3.5. Theft by false pretences as common law offence	150
3.5.1. General principles	151
3.5.2. Relevance to hacking instances	153
3.6. Malicious injury to property as common law offence	155
3.6.1. General principles	156
3.6.2. Malicious injury to property over the Internet	160
3.6.2.1. Intent to injure the owner or the property of the owner	161
3.6.2.2. Damage	161
3.6.2.3. Property	162
3.6.3. Modification of digital content and malicious injury to property	166
3.6.4. Bacteria and malicious injury to property	167
3.6.5. Denial-of-service attacks and e-mail bomb attacks	167
3.6.6. Defacement of a web page by a hacker or computer program	168
3.6.7. Mental copying or writing down of confidential information	169
3.6.8. Attempt to commit malicious injury to property	170
3.6.8.1. Virus discovered prior to causing prejudice	171
3.6.8.2. Target computer not vulnerable to computer program	173
3.6.8.3. Defective malicious programs	174
3.7. The offences of housebreaking and trespassing	174

3.8. The offence of sabotage	174
3.9. <i>Crimen iniuria</i> – violation of privacy as a common law offence	175
3.9.1. General principles	175
3.9.1.1. Right to privacy and its infringement	176
3.9.1.2. Wrongfulness and seriousness	179
3.9.1.3. Intent	181
3.9.2. Hacking and <i>crimen iniuria</i>	182
3.9.3. Eavesdropping by means of the Internet and <i>crimen iniuria</i>	183
3.9.4. Obtaining information from a hacker	185
3.9.5. Disseminating unlawfully obtained private information	185
3.9.6. Attempted hacking and attempted <i>crimen iniuria</i>	186
3.9.7. Insertion of a computer program	186
3.10. Inchoate crimes	187
3.10.1. Accomplice	189
3.10.1.1. General principles	189
3.10.1.2. Making passwords, password sniffers and hackers' tools available	193
3.10.2. Incitement	196
3.10.2.1. General principles	196
3.10.2.2. Making passwords, password sniffers and hackers' tools available	199
3.10.2.3. Attempted incitement	204
4. CONCLUSION	205

CHAPTER SEVEN

COMPARATIVE LAW STUDY

1. INTRODUCTION	208
2. FOREIGN LEGISLATION	208
2.1. United States of America	208
2.1.1. Computer Fraud and Abuse Act	208
2.1.2. More federal computer crime legislation	220
2.1.3. Georgia Computer Systems Protection Act	220
2.1.4. Virginia Computer Crimes Act	226
2.2. Canada	228

2.3. United Kingdom - The Computer Misuse Act 1990	230
2.4. Singapore Computer Misuse Act	235
2.5. The Netherlands	236
2.6. EU Convention on Cybercrime	239

CHAPTER EIGHT

PROPOSALS FOR AMENDING SOUTH AFRICAN CRIMINAL LAW

1. ACTIVITIES TO BE CRIMINALISED	250
2. CURRENT DEVELOPMENTS	255
2.1. National Prosecuting Authority Amendment Bill	255
2.2. South African Law Commission: Discussion Paper 99	255
3. COMMENTS AND RECOMMENDATIONS	260

CHAPTER NINE

SUMMARY/OPSOMMING	262
--------------------------	-----

BIBLIOGRAPHY	265
--------------	-----

LIST OF REPORTS	278
-----------------	-----

TABLE OF CASES	279
----------------	-----

TABLE OF STATUTES AND DRAFT LEGISLATION	286
---	-----

KEY TERMS	287
-----------	-----

CHAPTER ONE

INTRODUCTION

1. GENERAL INTRODUCTION

The past 15 years has seen an exponential growth in computer technology as well as Internet usage. Nowadays the Internet can be used for multiple purposes such as research, conducting business, communicating with other Internet users and downloading games, video or music files. However, with this acceleration of the Internet and technology, computer-related crimes also emerged, posing a risk to economies and especially businesses with Internet connections. In fact, the world is witnessing a computer-related crime phenomenon.¹

Various computer-related risks have emerged in recent years, such as a) computer programmers writing and disseminating sinister programs such as worms and viruses that have the ability to delete, corrupt, modify or copy electronic files on any storage medium; b) computer experts penetrating ("hacking") computer systems by means of the Internet or interfering with the proper functioning of computer systems; and c) cyber-espionage where e.g. businessmen engage in espionage on their business competitors by using the Internet to eavesdrop on the latter's electronic communications or to locate confidential information stored on the latter's computer systems. Disgruntled employees have also engaged in espionage by e-mailing confidential information to third parties.

Criminals, therefore, use computers as well as the Internet as tools to commit commercial crimes.² The Internet allows them to commit crimes easier, faster and on a larger scale. Any computer, owned either by an individual, business, financial institution or government institution, is exposed to hackers and malicious computer programs. Furthermore, computers storing critical and sensitive business information are especially exposed to these cyber-criminals. Hackers and viruses are thus risks to the integrity of computer systems.³ Stated differently, they are information security

¹ eEurope 2001. According to a survey conducted in 2000 by the FBI, 90% of all US organisations questioned reported recent security breaches. This referred to virus and hacking instances. See Anonymous 2000(x):18.

² See Dyanti 2000.

³ See Atkins 1990:82.

risks.⁴ As one commentator observed: "Security threats increase as computers become more connected with one another and tools that automate attacks make hacking easier. Plus, as businesses become more dependent on e-commerce, there's more to lose."⁵

2. SCOPE AND PURPOSE OF THIS STUDY

The title of this dissertation is *Internet Related Commercial Crimes*. The study concerns the vexed question whether the vested legal principles of criminal law can successfully be applied to the online environment? Put differently, can hackers and creators of malicious computer programs be held liable, in terms of the South African criminal law, for deleting, copying, modifying and corrupting electronic files or interfering with the proper functioning of computers? Should it be found that these legal principles or some of them fail to provide adequate legal protection, the question then arises: how should the applicable legislation or common law be amended to provide adequate protection to victims of electronic commercial crimes.

The term "computer-related crimes" has many different connotations, but in this study it is used to denote two forms of unlawful conduct on the Internet: 1) "virus instances" that refer to introducing malicious computer programs causing prejudice to Internet and computer users and 2) "hacking instances" which, in turn, encompasses two aspects namely a) instances where a computer expert gains access to a computer without the computer owner's authorisation, irrespective of whether he causes prejudice or not and b) instances where computer experts interfere with the functioning of a computer, without gaining access to that particular computer.

All computer-related crimes have commercial consequences, as indicated in chapter three, in that it can result in loss of customers, reputation, goodwill, income, trust in the computer system as well as loss of electronic data. This, in turn, entails that the victim of such illegal conduct has to incur expenses to either regain reputation or goodwill or to recompile the lost electronic data. For these reasons the term "Internet related commercial crimes" is used as a synonym for "computer-related crimes".⁶

⁴ See Maritz 2000:11.

⁵ Anonymous 2000(za).

⁶ Some commentators use the term "Internet crime". Chen 1999 defines this term as follows: "Internet crime primarily involves the destruction, damage or theft through the operation of a data processing system. Internet crime can be divided into six major categories: 1. adding false entries or data into a

However, the purpose of this dissertation is not only to ascertain whether the law provides adequate protection against these Internet related risks, but also to indicate how businesses are protecting themselves against these risks. It is of paramount importance that lawyers take note of these prevention techniques in order to advise their clients how to protect themselves against these cyber-risks. Some of these prevention techniques are also important for the law in that they can provide either the plaintiff or the prosecution with sufficient evidence to institute proceedings against the particular cyber-abuser.

Concerning the issue of comparative study, the emphasis is mainly on the laws of the United States of America (USA) and the European Union (EU). These countries have vast experience in online criminal activities. Consequently we turn to these jurisdictions to draw guidance from their experiences. This is done with circumspection in that their legal principles differ to some extent from our own legal principles.

To summarise, this study addresses the following questions:

- a) Does a need exist in South Africa to promulgate legislation criminalising cybercrimes and, if so, what should legislation penalising these activities stipulate?
- b) How do foreign countries as well as foreign entities, such as the EU Parliament, address computer-related crimes?
- c) How can computer users protect their electronic assets from cyber-crimes?

3. DEMARCATIION OF STUDY

The purpose of this study is not to conduct an all-embracing study concerning the law as it applies to the Internet. In this study the following aspects are not dealt with:

- a) Jurisdiction and applicable law: it is presumed, for the purposes of this study, that a South African court enjoys jurisdiction over the proceedings and that the law of South Africa applies.
- b) Law of evidence: this study is not concerned with the issue whether particular evidence is admissible in a court of law.

computer system; 2. unauthorized use of computer systems; 3. modifying or damaging data stored on a computer system; 4. theft of money, financial documents, assets, and services through the agency of a computer, 5. theft of valuable computer software, data and information, and 6. damaging or destroying a computer system.”

- c) Procedural aspects: this study does not deal with issues such as the powers of investigating officers to search and seize computers and/or files stored on computers.
- d) Money laundering *via* the Internet.⁷

As mentioned above, this study determines whether criminals, namely hackers and the creators of sinister computer programs, who use their computers to engage in illegal criminal activities by means of the Internet can be held liable according to the South African law. Consequently we do not assess whether third parties, such directors, who fail to update their computer security systems, can be held liable when their companies suffer financial losses due to cyber-attacks.

Although it can be argued that certain types of handheld devices such as WAP⁸-enabled cell phones and palmtops can be regarded as computers, this study does not encompass such devices due to the fact that this technology is still in a development phase. Consequently, this study is limited to desktop and laptop computers connected to the Internet by means of a physical telecommunications line.

This study covers the law up to 10 November 2001.

4. EXPOSITION

This dissertation is divided into nine chapters. Chapter two briefly focuses on the various possibilities that the Internet offers. This is necessary because malicious computer users utilise these same possibilities to exploit Internet users. In chapter three the emphasis falls on the risks that the Internet poses. This chapter serves as a general introduction to computer-related crimes.

Chapter four focuses on the various types of malicious computer programs posing risks to Internet users and a few techniques employed to protect cyber-users against these programs.

⁷ It is estimated that it takes "about five minutes for criminals using the Internet, electronic banking and false plastic banking cards and accounts to filter \$100 000 of hot money into the system to legitimise the funds". See Payne 1998:35.

⁸ WAP, an acronym for "Wireless Application Protocol", "is a specification for a set of communication protocols to standardize the way that wireless devices, such as cellular telephones and radio transceivers, can be used for Internet access, including e-mail, the World Wide Web, newsgroups, and Internet Relay Chat". See http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci213337,00.html.

Chapter five turns to malicious computer users. The following aspects are emphasised: the techniques they use to either penetrate or interfere with computer systems, the risks these computer experts pose to the Internet community, as well as a few techniques employed to protect Internet-users against the dangers they pose. It should be noted here that both chapters four and five deal with technical aspects. The knowledge gained from the technical issues discussed in these chapters, such as the various forms of malicious computer programs in existence and the various techniques hackers use, for instance, to interfere with the operation of computer systems, is necessary to comprehend the criminal activities of these cyber-abusers as well as to criminalise their activities.

Chapter six addresses the question of law whether malicious computer users, including computer users who penetrate, or interfere with the operation of, computer systems and users who create devious computer programs, are guilty of any offences in terms of the South African criminal law.

Chapter seven turns to various foreign law systems to assess how they criminalise computer-related crimes. Chapter eight observes current developments in South Africa to criminalise hacking and virus instances. Specific reference is made to attempts by the South African Law Commission to address computer-related crimes. This chapter concludes with a few recommendations.

Chapter nine contains a summary of the research done in this study.

5. REFERENCE SYSTEM USED

In the writing this dissertation, the reference system of the *Journal for Judicial Science* ("Tydskrif vir Regswetenskap") is used. The term "Supreme Court of Appeal" is used throughout this study to refer to the highest court in South Africa. Although the name *Appellate Division of the Supreme Court* changed in 1997 to *Supreme Court of Appeal*, with the entering into force of the *Final Constitution of South Africa*, the latter name is used for uniformity and to avoid confusion between the various names. The same applies to the usage of the term "High Court": this also refers to the provincial divisions of the Supreme Court, as they were known prior to the commencement of the *Final Constitution*.

CHAPTER TWO

POSSIBILITIES WHICH THE INTERNET OFFERS

1. INTRODUCTION

The Internet⁹ (commonly referred to as either the *information superhighway*, *the Net* or *cyberspace*¹⁰), as an open network, can be used for various purposes such as online banking, e-commerce, communication and information dissemination and retrieval.

2. ONLINE BANKING

Internet banking (also known as *virtual banking*, *cyber banking*, *online banking* and *e-banking*) is a worldwide phenomenon¹¹ and virtually all South African banks offer Internet services. Virtually all banking transactions can today be executed by means of the Internet.¹² Foreign banks such as First-e, First Direct and Security First Network

⁹ The word Internet is derived from "The International Network". See Dutson 1997:495. For a description of how the Internet works, see *Brookfield Communications Inc v West Coast Entertainment Corp* 174 F.3d 1036 (9th Cir. 1999) and *Sporty's Farm v Sportman's Market* 202 F.3d 489 (2d Cir. 2000). A copy of these judgments can be downloaded, respectively, from www.ipwatchdog.com/brookfield-metatags.pdf and www.ipwatchdog.com/sportysfarm.html. In *Playboy Enterprises Inc v Webworld Inc et al* 968 F.Supp 1171 (N.D. Tex. 1997) the court explained the functioning of the Internet as follows: "The Internet ... consists of information transmitted from computer to computer via telephone lines. Internet Access Providers ('IAPs'), such as America Online and Netcom, enable computer users to access the Information Superhighway by providing the necessary electronic 'on-ramps.' Once a computer user has gained access to the Internet through an IAP, that user may 'visit' one of the many specific 'locations' on the Internet called 'websites.' Many thousands of commercial and non-commercial computer users operate websites to exchange information or to advertise goods and services to potential customers. To connect with a website, an Internet user, who has already gained access to the Internet through an IAP, simply types the website's Internet address on the user's keyboard." A copy of this judgement can be downloaded from www.louandy.com/CASES/PEI_v_Webbworld.html. For an explanation of the history of the Internet, see www.isoc.org/internet-history/.

¹⁰ Other names include "e-world", "the information society", "the global information infrastructure", "Third Industrial Revolution" and "the global phenomenon".

¹¹ Anonymous 2000(c):20-21.

¹² A few examples of online banking features offered are: a) cancellation or placing of stop orders using an electronic application form; b) viewing details of one's credit card accounts; c) downloading own transaction histories from the bank's mainframe onto one's PC over the Internet; d) changing personal details such as addresses, PIN numbers or phone numbers online; e) application for finance and finalising the credit transaction (e.g. personal loans, home loans) online; f) application for credit cards

Bank provide banking services only *via* the Internet.¹³ These banks are generally known as *cyberbanks* or *Internet banks*.

3. ELECTRONIC COMMERCE

Electronic-commerce (also known as *e-commerce*, *virtual commerce*, *e-business*, *cyber-business*, *cyber commerce* and *online trading*,) is the purchasing, selling and offering of goods and services by both consumers and businesses using the Internet as a medium either to conclude the transaction and/or to the deliver and obtain the performance.¹⁴

A few examples of e-commerce are: businesses using the Internet to disclose information about their services and products;¹⁵ the booking of airline tickets *via* the Internet;¹⁶ rendering of financial services over the Internet;¹⁷ online auctions executed by means of the Internet, such as BidorBuy.co.za;¹⁸ e-shopping; and the purchase of

and garage cards online; g) payment of third parties and h) balance inquiries. See www.btimes.co.za/98/0906/survey/survey04.htm; www.absa.co.za; Jury 2000:7; Braun 1997:56.

¹³ Hewitt 2000:20. See first-e.com; www.firstdirect.com; www.sfnb.com.

¹⁴ Van der Merwe 2000:xii; Ryrie 1999(a):44; McLeod 1999:109; Gordon 1998(b):76. The South African Department of Communications released the national *Green Paper on Electronic Commerce* in November 2000. A copy of this document can be downloaded from www.ecomm-debate.co.za/greenpaper/index.html. It defines e-commerce (at p 8) as: "The use of electronic networks to exchange information, products, services and payments for commercial and communication purposes between individuals (consumers) and businesses, between businesses themselves, between individuals themselves, within government or between the public and government and, last, between business and government." In this dissertation this document is referred to as the "Green Paper 2000". Lourens 1998 defines e-commerce (at p65-66) as "the combination of technologies that exchange data (e g electronic data interchange and the Internet), access data (e g shared databases and electronic bulletin boards) and automatically captured data (e g bar coding and magnetic/optical character recognition) in trading relations." At the *National Electronic Commerce Law Conference* held on the 20th-21st April 2001, e-commerce was defined to encompass "any form of business or administrative transaction or information exchange that is executed using any information and communications technology". See p 7 of the representation, which can be downloaded from www.ecomm-debate.co.za/docs/presentations/overview.pps.

¹⁵ Rutherford 2000:175.

¹⁶ See Ryrie 1999(a):44.

¹⁷ Meall 2000:56.

¹⁸ In the US the dominant online auction site is eBay.com. City Lodge Hotels also use a web site (bid2stay.co.za) where Internet users can bid for hotel rooms.

music over the Internet.¹⁹ Overseas, mobile e-commerce (also known as *m-commerce*) is the fastest growing market where mobile (i.e. wireless) electronic devices are used to purchase products *via* the Internet.

Virtually all South African businesses have web sites (also referred to as *web pages*, *web addresses*, *home pages* and *domain addresses*) where products can either be purchased or viewed by means of the Internet. The web sites of Woolworths and Edgars are good examples.²⁰

4. COMMUNICATION

The Internet, as a global public communication medium, is a conduit for the transfer and exchange of information.²¹ It follows that the Internet can be used for numerous communicational purposes, of which the following are a few examples:

- The sending and receiving of messages by means of electronic mail (e-mail).²² E-mail ensures enhanced customer communications and relationships.²³
- Bill presentment that enables people to receive and pay accounts electronically.²⁴
- Live viewing of share prices.
- Online education.
- Distribution of global news information.²⁵
- Videoconferencing.
- Broadcasting of radio shows by means of digital audio transmissions.²⁶
- Virtual exhibitions of paintings and sculptures in online museums.²⁷
- Research. For instance, most countries render their legislation available on the Internet for free.

¹⁹ The lawful sale of digital music over the Internet in 1999 was estimated to be \$1 million worldwide. Lawton 2000:15.

²⁰ See www.woolworths.co.za & www.edgars.co.za.

²¹ Webster 1998:2; Davies 1996:155.

²² Davidson 1998:48.

²³ In *Andersen Consulting LLP v UOP* 991 F.Supp. 1041 (N.D. ILL. 1998) the court remarked that "email is a necessary tool for almost any business today." A copy of this judgment can be downloaded from www.loundy.com/CASES/Andersen_v_UOP.html.

²⁴ Laing 1998:33.

²⁵ E.g. www.cnn.com.

²⁶ E.g. www.5fm.co.za.

²⁷ See e.g. www.hermitagemuseum.org.

CHAPTER THREE

RISKS THE INTERNET POSES

As indicated in chapter two, the Internet has opened up a host of opportunities for businesses, individuals and governments. This is evident from the statistics that there are approximately two million online users in South Africa.²⁸ It is estimated that worldwide there are between 200 and 300 million Internet users.²⁹ However, "with these opportunities come new challenges as far as network security is concerned."³⁰ The Internet poses the following risks to Internet users:

- a) HACKERS (malicious computer users) use the Internet to penetrate computer systems and either acquire, delete, corrupt or modify electronic content. They can also obtain passwords (used for gaining access to a particular computer or other computer systems) as well as confidential information and disseminate it to other Internet users. Hackers, generally speaking, also have the ability to render an entire hard drive inoperable. Hackers can further interfere with the proper functioning of web sites and can render a web site inaccessible in a matter of a few hours. Hackers can furthermore intercept e-mail communications "either for the purpose of simply reading it or to modify it for fraudulent purposes (such as changing the bank account on a request for transfer of funds)"³¹ or if it contains credit card details, it can be used for unauthorised purchases.³²
- b) VIRUSES (as an example of a malicious computer program) wreak havoc on the Internet. Whenever a computer user contracts a computer virus, by for instance opening an infected attachment to an e-mail message, the possibility exists that the virus can delete or corrupt all or some of the information stored on the user's hard drive or can interfere with the functioning of a computer system. Some devious computer programs have the ability to copy electronic information (such as passwords) and divulge it to other Internet users.

²⁸ Van Niekerk 2001; McLeod 2000(a):82; McLeod 2000(b):123; Franke 1999:21; McLeod 1999:109; *National Electronic Commerce Law Conference on the 20th-21st April 2001*:29. This means that South Africa is currently the 18th largest user of the Internet.

²⁹ Hurter 2000:201; *Primer on Electronic Commerce and Intellectual Property Issues 2000*:par 22; Anonymous 2000(zc); Bidoli 1999:99.

³⁰ Anonymous 1999(c):36.

³¹ Davidson 1998:48.

³² Davidson 1998:50.

It should further be kept in mind that employees can also penetrate the security measures of their employers' computer systems without authorisation and glean confidential information from such unlawful espionage.³³ Statistics indicate that over 70% of hacks occur internally, namely by employees who have access to the computer network and subsequently gain access to restricted information.³⁴

According to the *Ernst and Young 1998 2nd Annual Global Information Security Survey*, 8% of "South African respondents have had their network security compromised by unauthorised individuals."³⁵ This led to 75% of IT (information technology) managers lacking "confidence that their organisation is protected, and a further 58% were uncertain about their company's ability to withstand an external attack."³⁶

Consequently, computer networks containing confidential information are open to abuse, espionage and malicious sabotage.³⁷ It is a notorious fact that computer crimes can have devastating effects on any computer network:

- An attack on a network may cause loss of confidence in the network system, which, in turn, disrupts the whole production process.³⁸ A hacking or a virus instance can bring the economic, industrial or defence wheels of any nation to a halt.³⁹ For instance, in March 2001, Bibliofind, a subsidiary of Amazon.com, "was partially shut down after it was discovered that hackers had downloaded the names, addresses and credit card numbers of about 98 000 customers over a period of several months."⁴⁰
- Information stored on a computer system may become unreliable due to tampering

³³ Lloyd 1999:48.

³⁴ Anonymous 1999(c):36; Gordon 1998(a):67. Employees are the most successful *hackers* because they are "familiar with the network and knows where the critical data resides. The perpetrator can also take steps to thwart any back-up measures to rectify the hack ... Information spies can remain undetected throughout their term of employment - the company will never know that information such as accounts, sales targets, databases or research and development is being divulged to someone outside the organisation". Anonymous 1999(c):36. See also Beaver 2000:8.

³⁵ Anonymous 1998(b):60.

³⁶ Anonymous 1998(b):60.

³⁷ Anonymous 1998(b):60.

³⁸ Anonymous 1997:13.

³⁹ Goyal 1994:33.

⁴⁰ Anonymous 2001(o).

by hackers.⁴¹

- Confidential information such as sensitive price, tax or operational data may be obtained from the network system, which can give any competitor an unlawful advantage and/or can place any hacker in the position to extort the business.⁴²
- Where a consumer or an investor discovers that his confidential information, entrusted to the firm, was obtained or intercepted by hackers, probabilities are that he will not conduct business again with that particular firm or may hesitate to provide it with sensitive personal information such as his credit card details. Put differently, computer-related crimes can lead to loss of customers, business reputation, goodwill, income, competitive advantage and credibility.⁴³
- The repairing costs of a hacked network system or a system where a virus wreaked havoc are enormous.⁴⁴
- It inhibits e-commerce. The main reason why many Internet users, especially South Africans, have not yet made an electronic purchase *via* the Internet is due to the lack of confidence in the Internet.⁴⁵ The perception obtains that it is unsafe to furnish credit card details over the Internet.⁴⁶
- Where a business keeps its debtor-accounts only on computer, and such data is subsequently erased or corrupted, the business will be unable to collect the money owed to it by these debtors.⁴⁷

The Internet is also used for other criminal purposes:

(a) Some web sites disclose information about suspected police informants and the identity of officers working on covert operations.⁴⁸

(b) Some web sites are utilised by organised gangs as sources of information for the

⁴¹ Goyal 1994:37.

⁴² Goyal 1994:34.

⁴³ Van der Merwe 2000:170; Gordon 1999(a):125; Dowd & McHenry 1998:25; Goyal 1994:32.

⁴⁴ Anonymous 1999(c):36.

⁴⁵ www.internetnews.com; Gordon 1999(a):125; Anonymous 1999(f):43. Tim Ellis, general manager of SACA notes that: "[s]ecurity on the Internet remains the biggest single stumbling block to global electronic commerce." See www.btimes.co.za/98/0906/survey/survey03.htm.

⁴⁶ Anonymous 2001(n).

⁴⁷ See Atkins 1990:80.

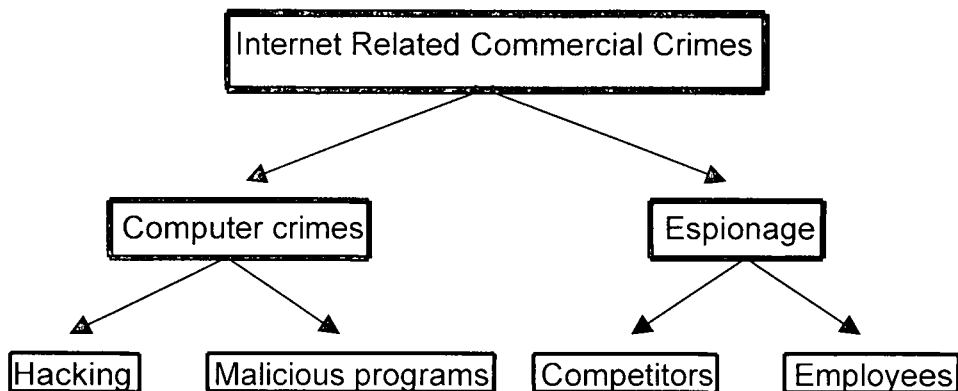
⁴⁸ Thompson 2000:36.

manufacturing of explosives, picking locks and creating false identities.⁴⁹

(c) Gangsters also use the Internet to arrange the sale of drugs and stolen vehicles, as well as to track their cocaine shipments.⁵⁰

(d) Some hackers have even used the Internet as a cyber-war medium.⁵¹

The risks examined in this dissertation can be illustrated as follows:



⁴⁹ Thompson 2000:36.

⁵⁰ See Thompson 2000:36.

⁵¹ Galvin 2001: As the war between the Israelis and Palestinians continued, both Israeli and Palestinian hackers defaced the other side's web sites, hacked web sites and/or interfered with the opponents' web sites. From the moment the World Trade Centre and Pentagon were attacked in September 2001, hackers (especially from the US) targeted Palestinian and Afghanistan web sites. See Lemos 2001.

CHAPTER FOUR

MALICIOUS COMPUTER PROGRAMS

1. INTRODUCTION

This chapter focuses on devastating computer programs that normally wreak havoc on computer systems. Some commentators define these computer programmes as a *specie of cyber-terrorism*.⁵² This chapter serves three purposes:

- a) To examine the various computer programs wreaking havoc on the Internet;
- b) To set out the threats they pose to the Internet community; and
- c) To look at a few techniques used to prevent these programs from causing prejudice to the online community.

2. EXAMPLES OF MALICIOUS COMPUTER PROGRAMS

The term “malicious computer programs” [also referred to as mischievous, sinister or nefarious computer programs] is used to denote programs that cause financial prejudice to the Internet community.

2.1. Viruses

A virus can be described as “a program that infects documents or systems by inserting or attaching a copy of itself [to an existing electronic file] or by rewriting files entirely. A virus operates without the knowledge or consent of the user. Therefore, when an infected file is opened, the embedded virus is also executed – often in the background.”⁵³

It is a fallacy to presume that all viruses have the ability to erase or corrupt electronic files. Some viruses, like the file infector virus⁵⁴ which effects executable files (“.EXE” or “.COM”), have this ability. However, the following two types of viruses serve different purposes:

⁵² Buys 2000:33.

⁵³ Anonymous 2000(p).

⁵⁴ File infector viruses “infect files containing applications such as spreadsheet programs or games.” Kephart *et al* 1999.

- a) System or boot-sector viruses, generally known as *boot disk viruses*, cause hard disks to be temporarily inaccessible;⁵⁵
- b) Macro viruses infect a victim's MS Word or Excell applications and typically insert words, phrases or letters.⁵⁶ Melamed, managing director of Fraudnet, remarks that-

"macro viruses ... have a potentially devastating effect on companies that rely on accurate figures. Macro viruses are those that are attached to documents that can run macro routines. A macro is a set of instructions recorded in a document. Virus writers use macro codes to trigger damage routines."⁵⁷

Once a micro virus infects a user's machine, "it can embed itself in all future documents created with the application ... every new document created in Word will carry a copy of the macro virus."⁵⁸ Therefore, macro-viruses modify electronic files and consequently affect the document's accuracy. They do not delete or corrupt electronic files.

Viruses are spread not only by moving disks between machines (for instance diskettes or CD-ROMs), but also *via* the Internet "by sending them as attachments to e-mail ... [or] by downloading infected programmes from other sites".⁵⁹ Today most viruses travel by means of the Internet.⁶⁰ It is a notorious fact that today we find viruses that spread by sending themselves as e-mail attachments to all the addresses listed in a computer user's e-mail application program.⁶¹ These viruses, in addition, pose the threat of overloading e-mail servers due to the volume of electronic mail sent automatically.⁶² A virus cannot, however, be activated by merely reading the plain text of an e-mail message; a computer user has to open the e-mail attachment, containing the virus. Furthermore, viruses are invariably attached to a host program. This is how they are distinguished from other malicious computer programs.⁶³ Examples of three recent viruses instances are:

⁵⁵ www.whatis.com/virus.htm; Jones 2000.

⁵⁶ Anonymous 2000(p).

⁵⁷ www.btimes.co.za/98/0906/survey/survey07.htm.

⁵⁸ Anonymous 2000(p).

⁵⁹ www.whatis.com/virus.htm. See Anonymous 1999(b):80.

⁶⁰ Buys 2000:33.

⁶¹ See Niccolai 2000:27; Buys 2000:33; Anonymous 2000(l):1; Anonymous 1999(b):80

⁶² Anonymous 2000(l).

⁶³ Anonymous 1999(b):78.

□ The Anna Kournikova virus.⁶⁴ This virus arrived in January 2001 as an e-mail message, with the subject line "Hi: Check This!" sent from someone the recipient knew. The plain text stated that the attachment contained a picture of a teenage tennis star, but in fact contained no such picture. Upon opening the attachment, a virus was released, which sent itself to everyone listed in the recipient's MS Outlook address book. Due to the vast number of e-mails automatically forwarded by this virus program some companies were forced to shut down their e-mail servers altogether.⁶⁵ Servers located in America, Europe and Australia were especially hard hit by this virus.⁶⁶ As can be seen the virus was not destructive in the sense of deleting or corrupting files, but in effect slowed down or brought e-mail servers to a stand still.

□ The ILOVEYOU virus (also known as the *Love bug virus*) in May 2000, sent via e-mail, deleted pictures, video and music files and installed a password-stealing programme.⁶⁷ Many South African Internet Service Providers (ISPs) were also caught off-guard by this virus.⁶⁸

□ In March 1999 the Melissa virus spread itself, as an e-mail attachment, to the first 50 people listed in an "infected" computer's e-mail address book.⁶⁹ Melissa could also send out sensitive documents to people, listed in address books, without the user's knowledge. Furthermore, the virus made infected e-mail attachments appear to come from someone the recipient knew.⁷⁰ The virus spread at such a pace that within hours e-mail servers were overwhelmed and forced to shut down.⁷¹ Due to the virus spreading so fast and its ability to send sensitive information to the wrong persons, many businesses were forced to shut down their e-mail servers, thus rendering them incapable of further communicating to others via e-mail.⁷²

From these examples it is evident that two of the most devastating viruses to date, have caused financial prejudice by forcing businesses to shut down their e-mail

⁶⁴ Anonymous 2001(f). When this dissertation was written, the creator of the Anna Kournikova virus was being prosecuted in the Netherlands. See Anonymous 2001(x).

⁶⁵ Baertlein 2001; Anonymous 2001(f).

⁶⁶ Baertlein 2001.

⁶⁷ Wolf 2000(b).

⁶⁸ Carroll 2000:1.

⁶⁹ See Van der Merwe 2000:165; Garber 1999:16.

⁷⁰ Garber 1999:16.

⁷¹ Garber 1999:17.

⁷² Garber 1999:17.

servers (consequently resulting in an inability to communicate by means of the Internet) and not by deleting or modifying electronic information.

2.2. Worms

A worm is "a type of virus ... that situates itself in a computer system in a place where it can do harm."⁷³ The difference between a virus and a worm is that the former has to be activated by the user. Until then, the virus is dormant on the computer.⁷⁴ Worms, on the other hand, need not be activated by the user; they are self-activating.⁷⁵ For example, by merely reading the plain text of an e-mail message, even though the attachment has not been opened, the worm can be activated. This is how the "Bubbleboy" worm functioned.⁷⁶ Worms are also far more powerful than viruses:

"When a worm gains access to a computer ... it launches a program which searches for other internet locations, infecting them if it can. At no time does the worm need user assistance ... in order to operate its programming."⁷⁷

However, not all worms are destructive in nature. In July 2001 a worm was released onto the Internet, called SirCam, with the "ability to suck data from the attacked machines and pipe it to its creators across the Internet."⁷⁸ The worm randomly picked a file from the victim's "My Documents" directory and e-mailed it (using its own e-mail engine) to Internet users listed in the victim's e-mail address program.⁷⁹

New generation worms can, like any virus, replicate themselves within machines and across networks.⁸⁰ When a worm sends copies of itself to other computers, it runs as a standalone program which does not attach to other files or programs.⁸¹ An example of a recent worm program is the ExploreZip worm that also spread *via* infected e-mail attachments, and deleted data contained in Microsoft Word, Excel and PowerPoint files.⁸² This worm functioned as follows:

⁷³ www.whatis.com/wormviru.htm.

⁷⁴ www.ifs.univie.ac.at/~c9225414/security/worm.html.

⁷⁵ Anonymous 2000(p):2.

⁷⁶ Anonymous 2000(d):48.

⁷⁷ www.ifs.univie.ac.at/c9225414/security/worm.html. See also Anonymous 2000(p):2.

⁷⁸ Gold 2001.

⁷⁹ Gold 2001.

⁸⁰ Anonymous 2000(p); Lawton 1999:15.

⁸¹ Garfinkel & Spafford 1997:8.

⁸² Lawton 1999:15.

"When someone sent e-mail to a user whose machine was infected, the worm automatically spawned a seemingly personal reply with an attachment named 'zipped_files.exe.' If the recipient opened the attachment, the worm installed itself on that person's machine. It then searched the hard drive and all drives linked to that computer via networks for Word, Excel, and PowerPoint files, and overwrote them with empty copies."⁸³

Even Microsoft was a victim of this malicious worm and suffered considerable damages. Reports of infected computers were received from 18 countries.⁸⁴

Enterprise networks are particularly vulnerable to worms "[s]ince worms are self-propagated, they can work their way through enterprise e-mail systems or shared network resources very quickly."⁸⁵ Because some worms e-mail themselves to every contact in a user's e-mail address list once activated, enterprises' e-mail systems are crippled by the sheer volume of e-mails generated.⁸⁶

2.3. Trojan horses

A Trojan horse can be defined as a "destructive computer program disguised as a game, a utility [for instance a screensaver], or an application. A Trojan horse does something devious to the computer system while appearing to do something useful."⁸⁷

A Trojan horse has to be activated (run/executed) by a computer user before it can do any damage.⁸⁸ However, it should be made clear that a Trojan horse will attach itself (like a virus) to another seemingly innocent program. Trojan horses differ from viruses in that the former do not necessarily replicate themselves.⁸⁹

A Trojan horse can either get "onto" a hard drive by downloading the file (merged with another computer program) from the Internet or by opening e-mail attachments containing the Trojan horse.⁹⁰ Trojan horses can do anything that the specific

⁸³ Lawton 1999:15.

⁸⁴ Lawton 1999:15.

⁸⁵ Anonymous 2000(q).

⁸⁶ Anonymous 2000(q).

⁸⁷ Anonymous 2000(p). See also www.stiller.com/aol4free.htm; Daniels 2000; <http://encarta.msn.com/index/conciseindex/6A/06A02000.htm?z=1&pg=2&br=1>.

⁸⁸ www.stiller.com/aol4free.htm.

⁸⁹ Anonymous 1999(b):81.

⁹⁰ Wing 2001.

computer user can do, for example -

“deleting files that the user can delete; transmitting to the intruder any files that the user can read; changing any files the user can modify; installing other programs with the privileges of the user, such as programs that provide unauthorized network access ... installing viruses; ... [install] other Trojan horses. If the user has administrative access to the operating system, the Trojan horse can do anything that an administrator can.”⁹¹

Many Trojans are used to steal passwords.⁹² They can even act as a tool for other to spy on users by recording keystrokes (such as credit card information) and transmitting them to a third party *via* the Internet.⁹³ In other words, they are used for electronic espionage.⁹⁴ Trojan horses are also used to discover private keys, used for public key encryption.⁹⁵

Trojan horses are furthermore used to create a backdoor on a computer system. The Trojan horse, when activated by the unsuspecting computer user, can install either a “Netbus” or a “Back Orifice” program which acts as a backdoor. This backdoor (link) allows the third party to have total control over the computer system.⁹⁶ This backdoor is used at a later stadium to allow the hacker easy and unnoticed access to the compromised system.⁹⁷ These Trojan horses are known as *Remote Access Trojans (RATs)*.⁹⁸

Finally, Trojan horses can be programmed to “self-destruct and leave no trace of themselves once achieving their goal.”⁹⁹

2.4. Logic and time bombs

These are programs that execute a command after being initialised a certain number of times (logic bombs), or on a certain date (time bombs).¹⁰⁰ Both programs can cause

⁹¹ www.eicar.com/trojan_horse.htm.

⁹² Chien 2000; Anonymous 2000(p). An example of a password sniffer is L0phtcrack. See Anonymous 2000(za).

⁹³ Wing 2001; Anonymous 2000(p); Goyal 1994:17.

⁹⁴ Daniels 2000.

⁹⁵ See chapter 5, par 6.3.

⁹⁶ Wing 2001; Mort 2000:2; www.geocities.com/TheTropics/Reef9201/vir/netb/NB-BO_txt.htm.

⁹⁷ Anonymous 2000(s); www.geocities.com/TheTropics/Reef9201/vir/netb/NB-BO_txt.htm.

⁹⁸ Wing 2001.

⁹⁹ Daniels 2000.

"the corruption of data or programs; or cessation of operations of the computer or network; or not allow some specific operations; or some similar act"¹⁰¹ or to release a virus onto the computer system.¹⁰²

The facts of *Corcoran v Sullivan*¹⁰³ illustrate how time bombs are used in practice. "A" was hired by a consulting firm to write computer programs that would enable the processing of data owned by the firm. His work was full of errors, and he became concerned that he would not be paid. So, in anticipatory revenge, he installed in one of the programs a software time bomb that was set to go off, deleting the programs from the firm's computer's memory, at a specified date and time if he activated the device by a harmless-appearing instruction. Deleting the program would also, as A knew and intended, delete any data that the firm had supplied to him for use in the programs as soon as someone entered new data into the computer. Eventually A instructed the firm to give the computer that innocent-appearing instruction. The firm did so, and unknowingly deleted the programs. As a result, the firm's data were lost forever when, still unaware of A's plot, the firm later inputted new data.

2.5. Virtual viruses

Virtual viruses (also known as *virus hoaxes*) entail e-mail messages warning people about viruses and security hazards.¹⁰⁴ Normally messages with subject lines such as "Fwd: Virus Warning!!!" request the recipient to send (forward) this important message warning to everybody he or she knows.¹⁰⁵ Such e-mail messages normally contain no virus. It is merely a hoax. However, the problem stems from the fact that ignorant computer users start sending these e-mail messages to everybody on their e-mail lists. This can cause network servers (of businesses as well as those of ISPs) to be overwhelmed with e-mail traffic and will either slow the computer system down in operational speed or force the system administrator to shut the e-mail server down or to disconnect the server from the Internet.¹⁰⁶

¹⁰⁰ Daniels 2000; Anonymous 1999(b):81.

¹⁰¹ Goyal 1994:20-21.

¹⁰² Daniels 2000.

¹⁰³ 112 F.3d 836 (7th Cir. 1997). A copy of this judgment can be downloaded from www.loundy.com/CASES/Corcoran_v_Sullivan.html.

¹⁰⁴ Anonymous 1999(b):81; Cobb 1999:34; <http://hoaxbusters.ciac.org>.

¹⁰⁵ Anonymous 1999(b):81; <http://hoaxbusters.ciac.org>.

¹⁰⁶ Anonymous 1999(b):81; <http://hoaxbusters.ciac.org>.

2.6. Bacteria

Daniels describes bacteria as “programs that replicate rapidly, usually exponentially, and consume system resources in doing so. It does not perform specific destructive functions, as worms do, so information is not in any particular danger.”¹⁰⁷ In other words, these computer programs do not delete or modify computer files; neither do they send (duplicate) themselves as e-mail attachments to other computer users. By merely replicating exponentially within one computer, it causes that particular computer to usurp all its available resources and this, in turn, causes the computer to slow down and virtually to cease operating.

3. THE RISKS MALICIOUS COMPUTER PROGRAMS POSE

As can be seen from the definitions of the various malicious computer programs examined above, they pose numerous risks to any computer user, whether he is a normal layman or a large multi-million dollar corporation.¹⁰⁸ Some of the risks that these sinister programs pose are:

- They can delete or corrupt critical files on one's hard disk, which can lead to financial losses of millions of Rands to a corporation. It follows that they pose the threat that confidential and/or valuable information can be lost.¹⁰⁹
- They can copy important files without the proprietor's authorisation and spread it to other persons who can, for instance, use such information to gain an unlawful advantage. They can, for instance, steal PINs and passwords as they are entered.¹¹⁰
- They can render a hard disk inaccessible or cause a computer to malfunction (crash) which may cause a loss of income to any business whilst endeavouring to retrieve the information.¹¹¹
- Whenever it infects a corporate network, it can cause havoc just by causing downtime while it is removed.¹¹²

¹⁰⁷ Jones 2000.

¹⁰⁸ When this dissertation was written, there existed more than 50 000 malicious computer programs. See <http://www.symantec.com/avcenter/index.html>.

¹⁰⁹ Anonymous 2000(p); Bennette & Luber 1999:17; Anonymous 1999(d):38.

¹¹⁰ Asokan 1997:31.

¹¹¹ Buys 2000:33; Anonymous 2000(p); Nel 1990:6.

¹¹² www.btimes.co.za/98/0906/survey/survey07.htm.

- Where they infect a computer system, it may be difficult or impossible to re-establish trust in the specific computer system.¹¹³
- One of the risks that malicious programs pose by sending themselves as e-mail attachments to all the addresses listed in a user's e-mail application programs, is their ability to quickly spread and clog networks.¹¹⁴
- Seeing that some malicious computer programs can replicate themselves quickly, some companies will choose to shut down their e-mail servers until the network system has been cleaned and/or until anti-virus solutions have been found for the specific malicious program.¹¹⁵ This, in turn, disrupts a business' productivity.

Hence we may conclude that these programs, with the ability to spread over the Internet, can have a crippling effect on any business. For instance, in May 2000 the "Love bug" virus caused havoc on computers worldwide and caused an estimated \$15 billion's worth of damage.¹¹⁶

Finally, it should be mentioned that attacks by e-mail viruses in the UK rose by virtually 300 percent in 2000: an e-mail virus was spread in the UK once every three minutes. In October 2000, alone, roughly 30 000 virus incidents were reported in the UK.¹¹⁷

4. PREVENTING MALICIOUS PROGRAMS FROM ENTERING THE COMPUTER SYSTEM

It is of the utmost importance that the legal profession, and especially lawyers, take note of the various techniques employed as protection against risks posed by malicious computer programs, in that:

- a) Such knowledge will inevitably have to form part of their legal advice when they advise their clients on conducting business by means of the Internet.
- b) It can prevent financial prejudice associated with malicious computer programs.¹¹⁸ Such prejudice not only includes prejudice stemming from losing sensitive business information but also possible liability where third parties hold a lawyer's

¹¹³ www.eicar.com/trojan_horse.htm.

¹¹⁴ Niccolai 2000:27; Anonymous 2000(p).

¹¹⁵ See Anonymous 2000(q).

¹¹⁶ Buys 2000:3; Anonymous 2000(q).

¹¹⁷ Anonymous 2000(o); Anonymous 2000(u).

¹¹⁸ As one commentator put it: "The choice is yours: Do something about the problem now, or wait until it's too late." See Lewis 2001:75.

client liable for losses due to these computer-related crimes. One example is a virus that deletes all electronic information stored on a bank's computer system.

- c) Where lawyers fail to furnish adequate advice to their clients on how to protect themselves against these risks and the latter subsequently suffer financial losses due to such negligent advice, it is within the foreseeable future that these clients can and will hold their lawyers liable for negligent legal advice.

4.1. Anti-virus software

There are numerous anti-virus programs for sale on the open market such as "F-secure", "Norton's Anti Virus program", "McAfee's Anti-virus", "SOPHOS Anti-Virus", etc. which detect malicious computer programs and erase them from diskettes, hard drives as well as a computer's memory. Most of these anti-virus programs can even repair infected files.¹¹⁹ They can also scan downloaded files, incoming e-mail messages as well as their attachments.¹²⁰ It is imperative that all businesses keep their anti-virus software up-to-date by downloading the newest releases from their anti-virus software manufacturers' respective web sites.¹²¹ Virtually all anti-virus vendors provide such online services.¹²²

However, no business should place all its trust in its anti-virus software to protect its computer systems against malicious programs, because:

- a) Even though good anti-virus software exists, new malicious programs are able to spread quickly *via* the Internet, before any anti-virus company can produce software to eliminate the threat.¹²³ For this reason, anti-virus software will not help one's system if it is one of the first computers to be attacked by a new type of malicious computer program,¹²⁴ even if "some scanning programs today include heuristic search methods to detect viruses that are not even in their libraries but

¹¹⁹ Garber 1998:12.

¹²⁰ www.microsoft.com/privacy/safeinternet/security/best/antivirus.html.

¹²¹ www.microsoft.com/privacy/safeinternet/security/best/sending-email.html; Hoare 2000; Anonymous 1999(d):38.

¹²² After the Melissa virus had been reported, it took anti-virus vendors only 20 minutes to develop a pattern to recognise the virus and could subsequently provide a "cure" for businesses who had been infected by this virus. See Garber 1999:17.

¹²³ Nearly 90% of companies surveyed in 2001 "had been infected by worms or viruses despite having anti-virus software installed". See Anonymous 2001(y):73.

¹²⁴ Anonymous 1999(b):80.

display 'virus-like' behaviour".¹²⁵

- b) Some anti-virus programs are not able to remove all the threats from a computer, even if the anti-virus software is updated regularly.
- c) Some anti-virus software will cause a system to crash after the malicious program was removed or can even leave the computer inoperable.¹²⁶
- d) Some viruses, for instance stealth viruses, are designed in such a way that they hide from anti-virus software,¹²⁷ whilst other viruses, such as polymorphic viruses, change their appearance with each infection: "They are hard to detect as they use encryption to mask themselves as a method of prevention from being detected by anti-virus software ... Polymorphic viruses using a mutation engine can achieve up to 4 billion mutations".¹²⁸

4.2. Submitting suspected viruses to anti-virus software companies for inspection

Some anti-virus software companies, such as Symantec Security and Aladdin, render a service whereby any computer user (suspecting that he has received a file or an e-mail attachment infected by a malicious computer program) can submit the suspected file or e-mail attachment to them and they will check it for known viruses (etc), for free.¹²⁹

4.3. Other anti-malicious computer program protection

For the sake of convenience, further prevention techniques used to prevent sinister computer programs from entering a computer network are discussed in chapter five, paragraph six.

¹²⁵ Anonymous 1999(b):80.

¹²⁶ Marx 2000:25.

¹²⁷ www.cs.uct.ac.za/courses/CS400W/NIS/papers00/mnakene/classification.htm. See also Jones 2000. A stealth virus hides the modifications it makes to files or boot records. Consequently, the anti-virus program only sees the file in its original and uninfected form. Anonymous 2000(y). They conceal their presence by using compression; an infected program is compressed to the same length as the uninfected program.

¹²⁸ Jones 2000. See also Anonymous 2000(y).

¹²⁹ See www.symantec.com/avcenter/submit.html; www.esafe.com/home/csrt/vsubmit.asp.

CHAPTER FIVE

MALICIOUS COMPUTER EXPERTS

1. INTRODUCTION

This chapter focuses on computer experts who break into computer systems with malicious intentions. Judge Heath, head of the Heath Special Investigating Unit, stated in 1998 the following with regard to corruption in the South African Government, which applies with equal force to hackers:

“Humans are greedy by nature. They are prone to want more and more. In essence, humans are not satisfied with what they have and will seek until their needs and more have been satisfied or met. The temptation for abuse leads to exploitation of loopholes in the system or the hatching of ingenious plans to use the system to the benefit of the individual or group of individuals. The weaker the control measures or the implementation thereof within the system, the easier it is to exploit it without anyone being held accountable or responsible.”¹³⁰

The purpose of this chapter is threefold:

- (i) To observe the various techniques used by malicious computer experts to penetrate computer systems or to interfere with their functioning, in order to have a better understanding of the various risks they pose as well as the unlawful conduct they engage in;
- (ii) To assess the threats they pose to the Internet community; and
- (iii) To observe a few techniques employed as protection against the risks posed by sinister computer experts.

2. A FEW DEFINITIONS - HACKERS, CRACKERS, PHREAKERS, CYPHERPUNKS & SCRIPT KIDDIES

Hackers have been around since the 1960's.¹³¹ In the 1970's hackers began to hack the US Department of Defence's Advanced Research Projects named the ARPAnet, the precursor of the Internet.¹³²

¹³⁰ Anonymous 1998(a):2.

¹³¹ Le Page 1999:5.

¹³² Le Page 1999:5.

Some commentators distinguish between *hackers* (computer experts that gain access to a computer network for mere “glory”) and *crackers* (computer experts that gain access to a computer network with malicious intentions and subsequently cause damage to the network).¹³³ *Crackers* are also known as *criminal hackers*.¹³⁴ Their main goal is to destroy data.

The term *phreakers* connotes cyber-abusers who penetrate phone systems of companies and make illegal phone calls on these companies’ accounts, without paying for such calls. Thus the business phreaked (hacked) incurs financial expenses for phone calls made by these phreakers.

Cyberpunks endeavour to decrypt encrypted information, without authorisation from the dispatcher or the receiver.¹³⁵

The term *script kiddies*, in turn, refers to computer users who are not expert hackers; the tools they use are automated (many times merely downloaded from the Internet¹³⁶) and require little interaction: “they share a common strategy, randomly search for a specific weakness, then exploit that weakness.”¹³⁷ These *script kiddies* (also referred to as *black-hats*) are extremely dangerous, because they scan the entire Internet for specific weaknesses, amounting to a random selection of targets. Even where nobody knows of the existence of one’s company or web site, the *script kiddie* can locate this computer if it displays the specific weakness: “it is no longer a question of if, but when you will be probed.”¹³⁸ *Script kiddies* will attack any computer, irrespective of to whom it belongs or what type of information it stores.

For the purpose of this dissertation, the term *hacker*¹³⁹ is used to denote someone who uses his computer skills to either gain access to a computer system or to interfere with the operations or functioning of a computer system, without the necessary

¹³³ Van der Merwe 1999:228; Anonymous 1999(c):36.

¹³⁴ Anonymous 1999(c):36.

¹³⁵ Mort 2000:2.

¹³⁶ Script kiddies frequently use malicious program-making toolkits, available on the Internet. For instance, the Anna Kournikova virus (discussed in par 2.1 of chapter 4) was created by means of such a toolkit in 2001. See Anonymous 2001(x).

¹³⁷ Anonymous 2000(s).

¹³⁸ Anonymous 2000(s).

¹³⁹ The Afrikaans word for a hacker is a “kuberkraker” and a cyber café is a “kuberkafee”.

authorisation.¹⁴⁰ Nowadays, the term *hacker* is further divided into subcategories namely a) the *kiddie hacker* who penetrates a system to prove his capabilities to his friends; b) the *professional hacker* who designs sophisticated intrusion tools; c) the *technical hacker* who penetrates a system to prove how vulnerable a system is; d) the *political hacker* who specialises in defacing web sites; and lastly e) the *government hacker* who penetrates government and corporate web sites to locate information.¹⁴¹

3. TECHNIQUES USED BY HACKERS

Hackers (also known as *computer experts*, *cyber punks*, *super-highwaymen* and *digital burglars*) are notorious for hacking into computer systems. However, they pose numerous other risks to the Internet community such as interfering with the proper functioning of a company system or eavesdropping on electronic communications, without gaining access to the computer system. There are various techniques *hackers* use to interfere with the proper functioning of a computer system, to eavesdrop on electronic communications, to obtain confidential information or to defraud computer users. The following techniques do not constitute a *numerus clausus*.

Hackers use the technique of *spoofing* to defraud computer users and/or to gain access to confidential electronic communications. *Spoofing* can be defined as "a technique that is used to change the header information¹⁴² [normally of e-mail messages] to make it look as if the information from one source actually comes from another."¹⁴³ It can, therefore, be seen as a new form of impersonation. Two types of spoofing have been identified:

a) *DNS spoofing*. This causes either e-mail to be routed to non-authorized mail servers or users can be directed to wrong Internet sites. DNS spoofing occurs where the domain addresses of servers are replaced with forged data.¹⁴⁴ DNS spoofing may be used as a method to engage in electronic espionage. For instance all the e-mail that A sends to B are first routed to C and then forwarded to B, without A or B's knowledge. See diagram.

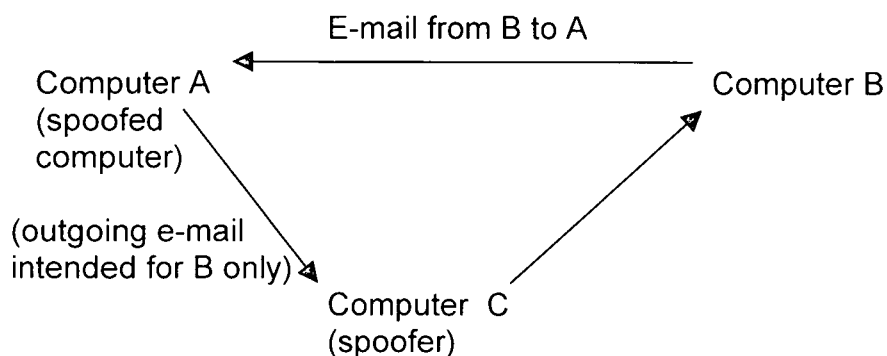
¹⁴⁰ It takes an average *hacker* 5 to 12 minutes to compromise a web site's security. See Hall 2000:23.

¹⁴¹ Anonymous 2000(z):58.

¹⁴² For instance jondoe@hackers.co.za or www.uovs.ac.za.

¹⁴³ Anonymous 1999(a):29; Oppliger 1998:43.

¹⁴⁴ www.menandmice.computer.infobase/mennmys/vefsidur/nsf/index/6.2.1.1.



Some *hackers* employ *DNS spoofing* to re-direct Internet traffic. For instance, A spoofs B's computer so that all Internet users who want to access B's web site are directed by B's own computer to A's web site.¹⁴⁵ For example, in *Yournetdating LLC v Mitchell et al*¹⁴⁶ A, a former employee of B, hacked into B's computer system and diverted Internet surfers, wishing to view B's web site, to his own web site.

Using this technique, *hackers* can "hijack" information "by establishing themselves as a trusted [internet] address."¹⁴⁷

b) Spoofing e-mail addresses. Some cyber-abusers send unsolicited bulk e-mail¹⁴⁸ (also known as *spam*) to unknown Internet users offering "services" or selling goods. For instance A sends his unsolicited e-mail messages to the subscribers of a particular Internet service provider (ISP) such as Mweb.com. Virtually all ISPs have computer software installed that filters through all incoming e-mail messages and prevents unwanted spam messages, from one source, from reaching their subscribers. To thwart these technical measures, A spoofs the header information¹⁴⁹ of his bulk e-mail messages to appear as if they come from various Internet sources.¹⁵⁰ Subsequently, the software allows the e-mail messages through.

¹⁴⁵ See e.g. www.sans.org/infosecFAQ/firewall/DNS_spoof.htm.

¹⁴⁶ 88 F.Supp.2d 870 (N.D. ILL. 2000). A copy of this judgment can be downloaded from www.loundy.com/CASES/YourNetDating_v_Mitchell.html.

¹⁴⁷ Anonymous 1999(a):29.

¹⁴⁸ Akin to junk mail.

¹⁴⁹ Stated differently, he forges his e-mail address.

¹⁵⁰ Software can be found on the Internet allowing the senders of junk e-mail messages to spoof the header information. In *America Online Inc v National Health Care Discount Inc* 121 F.Supp. 1255 (N.D. Iowa 2000) the court described one of these programs as follows: "one program substitutes a random arrangement of numbers and letters for the sender's name each time a message is transmitted. As a result, each message appears to originate from a different sender when, in fact, the messages are all

The facts of the following two cases illustrate e-mail spoofing. In *Parker et al v C.N. Enterprises et al*¹⁵¹ the plaintiffs were the owners of the web site "flowers.com". The defendants sent spam e-mail messages, simultaneously spoofing their e-mail addresses to appear as if "flowers.com" sent these messages.¹⁵² Another example is *Hotmail Corporation v Van\$ Money Pie Inc et al*.¹⁵³ In 1997 Hotmail (the applicant, an ISP) discovered that respondents were sending spam e-mails to thousands of Internet e-mail users, which were intentionally falsified in that they contained return addresses bearing Hotmail account return addresses including Hotmail's domain name, when in fact such messages did not originate from Hotmail or any Hotmail account. Respondents sent the spam by means of another ISP. As a result of the falsified return addresses, Hotmail was overwhelmed with hundreds of thousands of misdirected responses to respondents' spam messages, including complaints from Hotmail subscribers regarding the spam and "bounced back" e-mails which had been sent by respondents to non-existent or incorrect e-mail addresses. This overwhelming number of e-mails took up a substantial amount of Hotmail's computer space, threatened to delay and otherwise adversely affect Hotmail's subscribers in sending and receiving e-mail, further resulted in significant costs to Hotmail in terms of increased personnel necessary to sort and respond to the misdirected complaints, and damaged Hotmail's reputation and goodwill.¹⁵⁴

Sometimes *hackers* employ e-mail spoofing as a method to steal domain names.¹⁵⁵ It works as follows: a *hacker* forges the address of his e-mail message to make it appear as if the message is sent by company A, the proprietor of a particular web site. The *hacker* (appearing to be the system administrator of company A) requests the

coming from the same source." A copy of this judgment can be downloaded from www.law.asu.edu/HomePages/Karjala/cyberlaw/AOLv.NatHealthCare9-29-00.html.

¹⁵¹ (Tex. Travis County Dist. Ct. Nov. 10 1997). A copy of this judgment can be downloaded from www.loundy.com/CASES/Parker_v_CN_Enterprises.html.

¹⁵² Because many thousands of the Internet addresses, to which the spoofed e-mail messages were sent, were not valid addresses, thousands of copies of e-mail messages were returned to the plaintiffs' computers. This massive delivery of e-mail messages to the latter's computers caused substantial harm, including substantial service disruptions, lost access to communications, lost time, lost income and lost opportunities.

¹⁵³ 47 U.S.P.Q.2d 1020 (N.D. Cal. 1998). A copy of this judgment was obtained from Westlaw. A copy can also be downloaded from <http://eon.law.harvard.edu/h2o/property/alternatives/hotmail.html>.

¹⁵⁴ See para 8-10 of the judgment.

¹⁵⁵ Steward 2000.

registrar of the ISP to change the registered server information. Steward explains it further:

“Every domain name record includes the addresses of the primary and secondary computer servers for the Web site. When an Internet user types in a domain name, the Internet connects the user to the content located at the servers listed in the registration record. By changing the server address, a hacker effectively takes control of the domain name.”¹⁵⁶

In this way company A loses control over its domain name.¹⁵⁷ When company A discovers this, it will have to contact and inform its ISP of the situation. It will take the latter a few hours to correct this. Therefore, the *hacker* will definitely cause customers to lose confidence in the business.¹⁵⁸

Hackers use the following techniques to eavesdrop on or intercept electronic communications:

1) *Sniffing*: this is a technique that computer experts “use to determine what traffic is passing through a certain point.”¹⁵⁹ Some *hackers* use *password sniffers*¹⁶⁰ to monitor Internet or network traffic and to “sniff” passwords and usernames. *Hackers* install such *sniffers* on a particular web site and the program does the rest.¹⁶¹

2) *E-mail wiretapping*. This method works as follows: A sends an e-mail message to B with a proposal e.g. to buy or sell something. The e-mail message includes a few lines of invisible computer code. As B forwards this message to his co-executives, a copy is simultaneously forwarded to A without B’s knowledge.¹⁶² Therefore, this technique can be used to spy on business negotiations.

Hackers often use viruses and other malicious code to exploit weaknesses in network

¹⁵⁶ Steward 2000.

¹⁵⁷ Steward 2000.

¹⁵⁸ Steward 2000.

¹⁵⁹ Anonymous 1999(a):29.

¹⁶⁰ A “password sniffer” can be defined as a program that tries various combinations of letters in rapid sequence in the hope that one will be the authorised user’s password. See *US v Morris* 928 F.2d 504 (2nd Cir. 1991). A copy of this judgment can be downloaded from www.loundy.com/CASES/US_v_Morris2.html.

¹⁶¹ Oppliger 1998:43; Garfinkel & Spafford 1997:257.

¹⁶² Anonymous 2001(i); Beard 2001.

environments and computer software such as MS Outlook and MS Windows.¹⁶³ The following are two examples:

□ *Worm-assisted cracking*: the *hacker* infects any computer inside the target organisation with a worm “and then waits for the worm to spread. When the worm eventually find its way to the target computer, it will report this back to the attacker, who can now access the computer to steal and modify any data on it.”¹⁶⁴

□ The “salami” technique involves “the abstraction of small sums of money from large sums by rounding off figures to the nearest dollar or rand and then transferring the small amounts made up of cents to a special account opened for the purpose. This type of fraud may escape detection for a considerable period of time because of the negligible amount involved in each transaction.”¹⁶⁵

Hackers often interfere with the operations or functioning of computer systems. The following two techniques are frequently employed by *hackers* for this purpose:

A) *Denial-of-Service attacks* (also called *nuke*s¹⁶⁶). Planting explains it as follows: “The simplest form of attack is a flood of requests bombarding a computer, such as a Web server. The recipient computer responds and awaits the delivery of new information. But because the originating address of the message has been forged, the response will go to a non-existent computer which never responds. Flood the recipient computer with messages and it is paralysed in waiting for non-existent confirmations.”¹⁶⁷ In other words, a web site is bombarded/flooded with so much “false” requests, causing the system to be so busy, that legitimate users cannot access this particular web site; therefore rendering this web site inaccessible.¹⁶⁸ Normally *hackers* do not use their own computers for this purpose, but hack into other computers and instruct them to send large amounts of traffic to a web site.¹⁶⁹ For instance, eBay was bombarded with over 1 billion bits per second of bad traffic.¹⁷⁰

¹⁶³ Anonymous 2000(p).

¹⁶⁴ Delio 2000.

¹⁶⁵ Skeen 1984:262. See also Carstens & Trichardt 1987:123.

¹⁶⁶ Kehoe 2000.

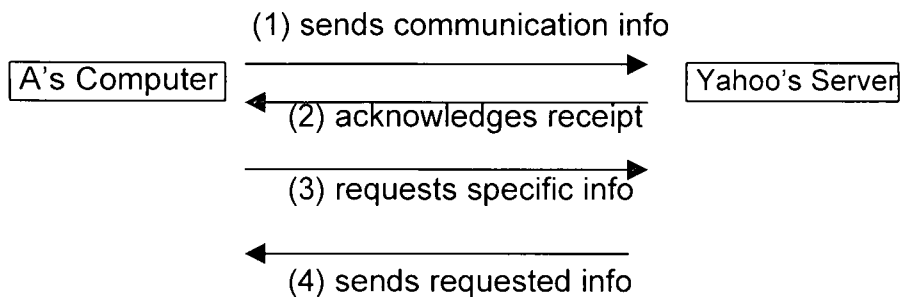
¹⁶⁷ Planting 2000(b):77.

¹⁶⁸ Anonymous 2000(e); Garfinkel & Spafford 1997:12.

¹⁶⁹ Anonymous 2000(e).

¹⁷⁰ Anonymous 2000(j). Even Microsoft’s web sites have been brought to a stand still by denial-of-service attacks: Anonymous 2001(h).

Denial-of-Service attacks (DoS attacks) may also be explained as follows: when A wants to access a specific web site, his computer sends “communication” information to the web site server indicating A’s Internet address. The latter replies by sending an acknowledgement “to indicate to the client that the server is ready for further communication.”¹⁷¹ When A’s computer receives this acknowledgement, it sends an acknowledgement (that it received the server’s acknowledgement) and simultaneously requests specific information to which the server replies, allowing A to see the web page or download a specific file.¹⁷² See diagram 1.



But when a *hacker* sends the “communication” information to the targeted server, he forges (*spoofs*) his own Internet address in such a way that it is an unreachable Internet address. Subsequently the recipient server (for instance Yahoo.com) sends an acknowledgement to a computer that does not exist (the responding server does not know that) and also does not respond. The result is that the responding server attempts again to contact the requesting computer. This continues for a few minutes, until the responding server gives up. What happens in the meantime is that the resources of the responding server are taken up when attempting to respond to the requesting computer.¹⁷³ The result is that when a *bona fide* computer user, attempts to request information from the server, the latter is so busy trying to reply to these non-existing computers (millions of fake visitors) that it simply cannot reply to the user’s request.¹⁷⁴ Normally, the message “time out” will be displayed.

A *Distributed Denial-of-Service attack* (DDoS attack) entails the instance where a

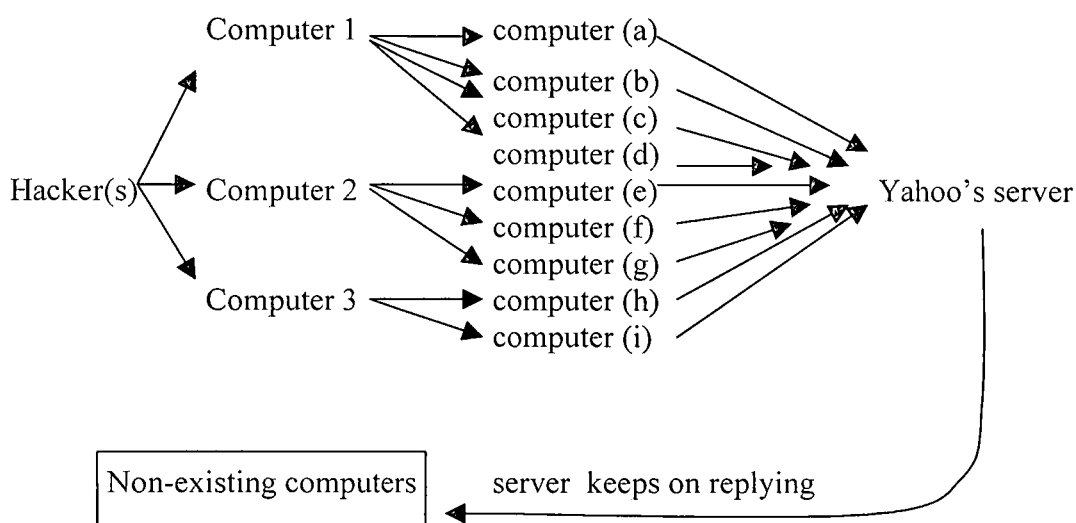
¹⁷¹ Shearman 2000.

¹⁷² Shearman 2000. This is known as the three-way handshake.

¹⁷³ Shearman 2000.

¹⁷⁴ Shearman 2000. If a DoS Attack is time correctly, just before the start of a big sporting event when the wagering activity is at its highest, such attack could deprive a big betting site of millions of rands worth of bets.

single user controls hundreds of compromised systems throughout the world, by installing programs on these computers *via* the Internet.¹⁷⁵ This is called a *mass intrusion phase*. These compromised systems, called *zombie* or *host computers*, are then remotely coordinated to execute denial-of-service attacks against a specific computer or computers.¹⁷⁶ Since multiple compromised systems are used, it is extremely difficult to defend against and identify the source of the attack.¹⁷⁷ Often, *script kiddie* methods are used to gain control over the *zombie* computers: "Vulnerable systems are randomly identified and then compromised to be used as DDoS launching pads. The more systems compromised, the more powerful the DDoS attack."¹⁷⁸ This can be illustrated as follows:



Some DDoS attacks take only about 15 minutes to bring down a particular web server, depending on the capacity of the server.¹⁷⁹

¹⁷⁵ Anonymous 2000(s); Dittrich 1999.

¹⁷⁶ Shearman 2000.

¹⁷⁷ Anonymous 2000(s); Dittrich 1999.

¹⁷⁸ Anonymous 2000(s). It should be added that DDoS attacks are normally more complex than described above: normally the computer hosts are instructed by the program installed by the *hacker* to penetrate other computers and finally all these computers attack the targeted server. Shearman 2000.

¹⁷⁹ Kehoe 2000. The software that enables *hackers* to launch DDoS is freely available on the Internet. One such program is "Stacheldraht". See Kehoe 2000. "Stacheldraht" means "barbed wire" in German. Kohoe explains it as follows: "It is used in a twophase assault. First, hackers use a computer virus to implant the software in dozens, perhaps hundreds, of computers linked to the internet without the permission of the computer owners. Once these software agents are in place, the hacker can command them, whenever he or she wants to, to launch a barrage of traffic at the target. Encrypted internet

B) *E-mail bombing* (also known as *mail-bombing*). Computer experts can utilise one of three techniques: either¹⁸⁰ -

- a) repeatedly send thousands of identical small e-mail messages to a particular e-mail address; or
- b) send a very large e-mail message (for instance a gigabyte-sized mail message) to a particular e-mail address; or
- c) request other Internet users to send e-mails to a particular e-mail address. In one instance, an Internet user (a journalist) received more than 2 000 e-mails.¹⁸¹

Normally computer experts employ mail bombs as a revenge mechanism,¹⁸² but often they use this technique to target famous individuals.¹⁸³ The consequence of an e-mail bomb attack is that the e-mail server is flooded (overwhelmed) with e-mail messages and consequently it becomes unavailable and unserviceable.¹⁸⁴ Thus "E-mail bombs have the power to shut down the communications capability of your system."¹⁸⁵ Furthermore, when e-mail bombs are sent to an Internet user with an ISP, all users of that particular ISP suffer.¹⁸⁶ Furthermore, *hackers* spoof their own e-mail addresses and normally make it appear as if the e-mail originated from someone else's e-mail address.

The risk e-mail bombing entails is that the only step a computer user can take, when he or she is the victim of an e-mail bombing act, is to disconnect from the Internet.¹⁸⁷ For Internet dependent businesses, this step is fatal.

4. DAMAGE HACKERS CAN CAUSE

The following are a few examples of the prejudice that *hackers* can cause:

addresses disguise the sources of the attack and, even if these are deciphered, the mastermind behind the attack may not be identified." Kehoe 2000.

¹⁸⁰ Anonymous 2001(l); Anonymous 2001(k).

¹⁸¹ Outing 1997.

¹⁸² Anonymous 2001(k).

¹⁸³ For instance, former president Clinton, Bill Gates and Al Gore have been victims of mail bombing. See Goldman 1996.

¹⁸⁴ Bass *et al* 1998; Outing 1997.

¹⁸⁵ Anonymous 2001(j). See also Goldman 1996.

¹⁸⁶ Anonymous 2001(k).

¹⁸⁷ Anonymous 2001(l).

⇒ They can destroy or corrupt information stored on any computer and they can also render a hard disk inaccessible.

⇒ They can manipulate information. An employee can hack into his employer's computer system to change details in the payroll system.¹⁸⁸ Such internal breaches can lead to serious financial losses.¹⁸⁹ *Hackers* can also change inventory prices on a web site.¹⁹⁰ Some *hackers* change the details of online stories published on newspapers' web sites. For instance, in 2000 a *hacker* modified an online report to read that "Bill gates, the co-founder of Microsoft, was arrested for breaking into Nasa computers".¹⁹¹ Other *hackers* have penetrated the computer servers of online casinos and corrupted the games so that players could not lose.¹⁹²

⇒ They often target famous web sites and deface them.¹⁹³

⇒ They engage in industrial espionage and for instance steal credit card information.¹⁹⁴ *Hackers* pose the threat that they can steal sensitive files, simply by copying them *without anyone knowing*.¹⁹⁵ Hence, is it abundantly clear that they constitute a serious problem for each and every country seeing that they can, without authorisation, enter computer networks unauthorised from anywhere in the world.¹⁹⁶ More than one million credit card numbers have been stolen thus far *via* the Internet. *Hackers* have specifically targeted computer systems associated with banking and e-commerce activities.¹⁹⁷

⇒ They use e-mail technology to obtain sensitive company information. Gordon explains: "Using the internet, they are able to introduce software that will find, for example, details of a company's financial standing. Once the information has been traced, it is bundled into an e-mail message and delivered electronically to whoever has ordered it. Data theft, by its nature, is difficult to trace."¹⁹⁸

¹⁸⁸ Anonymous 2000(t):1.

¹⁸⁹ Anonymous 2000(t):1.

¹⁹⁰ Gordon 1999(a):125.

¹⁹¹ Anonymous 2000(zb).

¹⁹² One online casino has alleged that it lost \$1.9 m as a result of such hacking.

¹⁹³ Anonymous 1999(c):36.

¹⁹⁴ Gordon 1998(a):67.

¹⁹⁵ Gordon 1999(b):92.

¹⁹⁶ Gordon 1999(a):125.

¹⁹⁷ Anonymous 2001(g).

¹⁹⁸ Gordon 1998(a):67.

⇒ They may also, after acquiring the company's security codes, broadcast it to the entire hacker pirate network or engage in cyber-extortion.¹⁹⁹ For instances, *Computing SA* reported that a music web site called CD Universe "was hacked by an extortionist who demanded \$100 000 to keep him from publishing 300 000 credit-card numbers stolen from CD Universe." When CD Universe refused to pay, the *hacker* published a handful of credit-card numbers on a web site before the FBI managed to shut it down.²⁰⁰ It is alleged that worldwide "cyber-extortion is on the increase, with hackers threatening to inject viruses and post confidential information, such as credit card numbers, on the Web."²⁰¹ Some *hackers* are even forming their own cyber-Mafia groups: the *hackers* will penetrate a computer system, steal proprietary information, then inform the victim of the theft of information and then offer protection against Internet security intrusions. Should the victim fail to obtain their services, the *hackers* threaten him that they will post the proprietary information (such as credit card information) and details about the compromise on the Internet.²⁰²

⇒ They can prejudice a company's business reputation. For instance, in the last quarter of the year 2000 the main computer system of Microsoft (the manufacturer of MS Windows) was penetrated and the *hacker* accessed Microsoft's source codes (used for programs such as Windows).²⁰³ Many consumers feared that the *hacker* altered the source code which he penetrated, even though Microsoft strenuously denies this.²⁰⁴ This hacking instance raised many questions "about the trustworthiness of future versions of applications such as Microsoft Word or Microsoft Internet Explorer."²⁰⁵

⇒ When some *hackers* detect an unknown weakness in a system, "they contract the supplier of the system and allow these suppliers two weeks in which to fix the problem.

¹⁹⁹ Anonymous 2001(g); Coetzer 1985:17. Some *hackers* have threatened businesses that they will expose alleged weaknesses in their computer systems if they fail to pay them to keep silent. DiSabatino 2000:13.

²⁰⁰ Hayes 2000:20.

²⁰¹ Bidoli 2000:76.

²⁰² Anonymous 2001(g).

²⁰³ Anonymous 2000(m). Microsoft first spotted the intruder on 14 October 2000 and kept track as he moved through the system until 25 October. See Heavens 2000. The Microsoft intrusion was detected when security employees noticed that passwords were sent remotely to an e-mail account in Russia. These passwords were used to transfer source codes. See Uhlig & Cave 2000.

²⁰⁴ Delio 2000; Anonymous 2000(m).

²⁰⁵ Delio 2000.

Thereafter, if the supplier hasn't made adequate progress to resolve the problem, they consider the system fair play game and publish the weakness on certain websites, making any company using the system vulnerable to attack."²⁰⁶

⇒ It is estimated that firms and governments in Europe have incurred R535 m expenses in phone bills, due to unauthorised phone calls by *phreakers*.²⁰⁷

However, some *hackers*, after penetrating a computer system, merely display a "calling" card in the form of a statement.²⁰⁸

Consequently, *hackers* pose a threat to any business dependent upon the Internet or electronic databases.²⁰⁹ For instance, in *US v Middleton*²¹⁰ the accused accessed the computer system of his former employee and changed all the administrative passwords. He also deleted software and internal databases. The result was that his former employer and his employees spent an entire weekend repairing the damage that he had caused to his employer's computers, including restoring access to the computer system, assigning new passwords, reloading the billing software, and recreating the deleted databases. They also spent many hours investigating the source and the extent of the damage. The former employer estimated that he spent 93 hours repairing the damage. Additionally, his former employer bought new software to replace software that the accused had deleted, and the company hired an outside consultant for technical support.

Some businesses are to such an extent reliant upon computers that "their income is solely provided by their ability to offer 24x7 service across the Internet."²¹¹ Furthermore, the integrity of the financial services sector is virtually dependent on the smooth functioning of computer systems.²¹² Similar considerations can be seen in the judgment of *R v Strickland and Woods* where the UK court stated that:

"There may be people out there who consider hacking to be harmless, but hacking is

²⁰⁶ Beaver 2000:8.

²⁰⁷ Anonymous 2001(d).

²⁰⁸ Beaver 2000:8.

²⁰⁹ Stanley 2000.

²¹⁰ 231 F.3d 1207 (9th Cir. 2000). A copy of this judgment can be downloaded from <http://laws.lp.findlaw.com/9th/9910518.html>.

²¹¹ Anonymous 2001(v):34.

²¹² Harris 2000. Many companies, such as VISA and Mastercard, rely heavily on the use and reliability of their electronic data, computer programs and computer applications.

not harmless. Computers now form a central role in our lives, containing personal details, financial details, confidential matters of companies and government departments and many business organisations. Some of these services, providing emergency services, depend on their computers to deliver those services. It is essential that the integrity of those systems should be protected and hacking puts that integrity into jeopardy."²¹³

5. EXAMPLES OF REPORTED HACKING INSTANCES

5.1. South Africa

Hackers are a paramount problem for South Africa.²¹⁴ According to a recent survey, *hackers* rate South Africa as the third easiest target country.²¹⁵ The following are instances of hacking that have occurred in South Africa:

- (i) In 1998 *hackers* broke into one of South Africa's ISP systems and stole client credit card details. Fortunately, it was immediately discovered.²¹⁶
- (ii) On 18 June 1998 two ISPs were hacked and the *hacker* obtained user names and password lists.²¹⁷
- (iii) In May 1999 a *hacker* crashed more than 600 Edgars stores for an entire day, causing losses in excess of R1 m.²¹⁸
- (iv) In 2000, NetActive (a South African ISP) experienced two DoS attacks.²¹⁹
- (v) In early 2000 the Johannesburg Stock Exchange's computer system was penetrated and its web site defaced.
- (vi) In 2000 a *hacker* penetrated Medinfo's²²⁰ (a South African medical news organisation) computer system and instructed its server to send spam e-mail to all its subscribers.²²¹

²¹³ This case was not available locally so Harris 2000 had to be relied upon.

²¹⁴ There is even a South African *hackers* group that publishes an underground newsletter called *Forbidden Knowledge*, containing instructions on hacking into web sites, etc. Beaver 2000:8.

²¹⁵ Anonymous 2000(r):3.

²¹⁶ www.btimes.co.za/98/0906/survey/survey03.htm.

²¹⁷ Furber 1998:1.

²¹⁸ Scala 2000:1.

²¹⁹ Planting 2000(b):77.

²²⁰ www.medinfo.co.za.

²²¹ Mkhwanazi 2000:1. The message sent to subscribers stated: "Would you like to subscribe to Medinfo."

- (vii) In 2000 a client of ABSA discovered that R13 000 had been withdrawn from her bank account, by means of the Internet.²²²
- (viii) In March 2001 the South African Police Service arrested a South African *hacker* for transferring money from a victim's account to various other accounts, by means of the Internet.²²³
- (ix) In April 2001 the South African Police Service arrested another *hacker* for transferring "money electronically from a number of international and South African financial institutions by hacking into their Internet databases."²²⁴
- (x) In June 2001 approximately 35 *hackers* penetrated the computer systems of the Western Cape Gambling and Racing Board and spoofed "e-mails purporting to come from the board to members of the public."²²⁵
- (xi) In September 2001, South African *hackers* added false newsreports to CNN's web site, implicating South Africa in the terrorist attack on the World Trade Center and Pentagon.²²⁶

5.2. Worldwide

In the US, computer attacks is "one of the fastest-growing areas of crime".²²⁷ This is illustrated by the fact that 76 000 passwords (used to gain access to university computers) were found on one *hacker's* personal computer. He earned \$300 to \$400 per week for publishing some of these passwords.²²⁸ In 1999 the FBI opened more than 1 100 computer intrusion cases.²²⁹

According to a newly published report, cyber-attacks cost the US \$266 million in 1999 – more than double their average annual losses for the previous three years.²³⁰ The FBI maintained in 1999 that an average security breach costs \$570 000 to repair: "90%

²²² Green 2000.

²²³ Anonymous 2001(p):7.

²²⁴ Anonymous 2001(q).

²²⁵ Steenkamp 2001:9.

²²⁶ Anonymous 2001(w).

²²⁷ Anonymous 2000(j).

²²⁸ Anonymous 2000(k).

²²⁹ Anonymous 2000(j).

²³⁰ Harrison 2000:13; Planting 2000(a):80. Camerer 1997:49 observes that: "[d]uring a two month period in 1995, an estimated \$300 million in untraceable computer transfers disappeared from US banks and securities firms."

of the money is spent on PR to fix a company's reputation."²³¹ In December 2000 the FBI issued a warning to all US Internet trading businesses that *hacker* activity designed to steal proprietary information was increasing.²³² Examples of reported hacking instances are:

- (i) DoS attacks have paralysed the web sites of Yahoo, Amazon, eBay, ZDnet, CNN and others.²³³ Some of the DoS attacks on Yahoo's and Amazon's web sites in February 2000, blocking access to these web sites, were caused by a 14 year old Canadian boy (calling himself Mafiaboy).²³⁴ eBay's share price fell 25% the day after its web site was taken down by a DoS attack. The firm had to spend \$100 000 in securing its site against further attacks.²³⁵
- (ii) On 4 April 2000 "[h]acker attacks wreaked havoc on 40 percent of Chinese web sites, and 44 percent of Chinese firms had their online information tampered with".²³⁶
- (iii) Even government web sites, such as the Japanese government's web site and the US White House's web site, have suffered from hacking attacks in 2000 and 2001, respectively.²³⁷ *Hackers* were even able to plant a virus on the US State Department's e-mail distribution system.²³⁸ In December 2000 a *hacker* broke into the computer network of Malaysia's parliament and erased all its information.²³⁹ Police web sites have also been attacked.²⁴⁰ During 1999, the US Defence Department's web site was hacked more than 22 000 times.²⁴¹
- (iv) Even NASA's computer system has been penetrated, more than once, by teenage

²³¹ Gordon 1999(a):125.

²³² Wolf 2000(a).

²³³ Planting 2000(b):77; Wolf 2000(a).

²³⁴ Anonymous 2000(e). The police arrested him in April 2000 and he was sentenced in September 2001 to a youth detention center for a period of eight months. See Anonymous 2000(f):1; Anonymous 2001(c).

²³⁵ Planting 2000(a):81.

²³⁶ Anonymous 2000(f).

²³⁷ Anonymous 2001(m); Anonymous 2000(f).

²³⁸ Anonymous 2000(g).

²³⁹ Anonymous 2000(n).

²⁴⁰ Anonymous 2000(h).

²⁴¹ Abreu 2000:17.

hackers in 2000.²⁴²

- (v) The Mafia in Italy has attempted in 2000 to commit online banking fraud by “cloning” an online bank and were preparing to move funds (264 billion lire) from one account to another.²⁴³
- (vi) In 2000 a *hacker* penetrated VISA’s computer system in London, stole credit card information from its electronic databank and subsequently demanded \$10 m.²⁴⁴ Another *hacker* penetrated the computer system of creditcard.com, an institution that processes credit transactions for online companies, and obtained the details of 55 000 credit cards. When creditcard.com refused to pay the ransom demanded (\$100 000) the *hacker* posted about 25 000 credit card details before the site containing the details were taken down by the FBI.
- (vii) In January 2001 *hackers* penetrated the database of the World Economic Forum in Switzerland and obtained sensitive information such as credit card numbers, passport information and cell phone numbers of 1400 participants at this forum.²⁴⁵
- (viii) In April 2001 a *hacker* was prosecuted in the US for obtaining access to 23 000 different credit card details and posting thousands of them on the Internet.²⁴⁶ VISA International is alleged to have suffered \$250 000 as a result of the credit card details illegally posted on *hacker* web sites.²⁴⁷

6. PREVENTING COMPUTER-RELATED CRIMES

Under this heading various methods used to protect electronic assets from cyber-risks are discussed. The reasons mentioned in paragraph four of the previous chapter, why jurists should take note of electronic techniques used to counter cyber-attacks, apply *mutatis mutandis* to prevention techniques used to counter the risks associated with

²⁴² Anonymous 2000(i); Anonymous 2000(k). Both a 16-year-old and a 20-year-old *hacker* have penetrated NASA’s computer systems.

²⁴³ Willan 2000:13.

²⁴⁴ Stanley 2000.

²⁴⁵ Thiel 2001:4.

²⁴⁶ Anonymous 2001(x).

²⁴⁷ Anonymous 2001(x). An example of such a web site is www.2600.com.

hacking instances.²⁴⁸ Furthermore, some of the prevention techniques briefly examined below may:

- a) Provide evidence of the attack as well as the attacker; and/or
- b) Indicate intention as well as malice on the part of the attacker.

As noted in the previous chapter,²⁴⁹ the prevention of malicious programs entering a computer system is further dealt with under this heading.

6.1. Mere usernames and passwords insufficient

The first technique used by businesses to protect the electronic contents of their computer systems is the usage of passwords and usernames which are assigned to each employee. Each employee's password and username is unique. A username identifies the person who wishes to access the web server and a password authenticates the person wishing to access the particular computer.²⁵⁰ As a log-in activity, they ensure that "an audit trail of who accessed your system and when" exists.²⁵¹

However, no business can solely rely on passwords and usernames as protection: "[t]he problem is that access controls such as one-time or user-name passwords are an extremely weak link in any security system."²⁵² One of the reasons for this statement is that usernames and passwords are vulnerable to *password sniffers*.²⁵³ In fact, some *password sniffer* programs have a database in excess of two million known passwords. Other *password sniffers* can search for a password by combining letters and numbers and can thus identify a password such as "brian928x".

²⁴⁸ The *Explanatory Report to the Convention on Cybercrime*, discussed in par 2.6 of chapter 7, states that "[t]echnical measures to protect computer systems need to be implemented concomitantly with legal measures to prevent and deter criminal behaviour." (At par 5).

²⁴⁹ Chapter 4, par 4.

²⁵⁰ Garfinkel & Spafford 1997:279. A password rendering access to a computer can be equated with a combination lock that grants access to a safe.

²⁵¹ Whipple 1999:10.

²⁵² www.btimes.co.za/98/0906/survey/survey03.htm.

²⁵³ Garfinkel & Spafford 1997:258.

6.2. Firewalls

A firewall can be defined as:

“a set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks. An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall *to prevent outsiders from accessing its own private data resources and for controlling what outside resources its own users have access to.*”²⁵⁴ (my italics)

Stated differently, a “firewall is a protective barrier ... that examines each piece of data coming in and out of a network and blocks suspicious activities. A firewall limits access to machines inside a network, deters casual probing for weaknesses, and alerts system administrators to patterns that might be attacks.”²⁵⁵ It therefore isolates internal networks (intranets) from the public Internet.²⁵⁶ A firewall can be a combination of hardware and software or software alone.²⁵⁷

It is imperative that businesses ensure that where employees access the corporate network from remote locations, their computers are also protected from *hackers* by means of firewalls, seeing that *hackers* may try to sniff the passwords (etc) from these computers in order to gain access to the network of the company.²⁵⁸ For instance, it is suspected that the *hacker* who penetrated Microsoft's computer system broke in *via* a computer being used by a remote employee.²⁵⁹

Firewalls protecting internal servers from unauthorised access by employees are also available.²⁶⁰ These are called *desktop (or personal) firewalls*.

²⁵⁴ www.whatis.com/firewall.htm. A firewall can also be described as a link between a computer network (an intranet) and the Internet. See Anonymous 2001(a). A proxy server is a computer program on a firewall that acts as a conduit between a computer on the intranet and the Internet. See Anonymous 2001(a). A proxy server is associated with or is part of a gateway server that separates the enterprise network from the outside network, whereas a firewall server protects the enterprise network from outside intrusion. http://whatis.techtarget.com/WhatIs_Definition_Page/0,4152,212840,00.html.

²⁵⁵ Fleishman 2001:117.

²⁵⁶ Voges 2001:36; Garfinkel & Spafford 1997:20-21.

²⁵⁷ Fleishman 2001:117. See also Voges 2001:36; Van der Merwe 2000:199. ZoneAlarm an example of a software-only firewall. A free copy of this firewall can be downloaded from www.zonelabs.com.

²⁵⁸ Harrison 2000:27.

²⁵⁹ Heavens 2000:11.

²⁶⁰ Andress 2000:12.

Ordinary firewalls are good at preventing unauthorised and unwanted access²⁶¹ but cannot, for example, stop viruses from entering the network.²⁶² In order to solve this problem, a *perimeter firewall* (a specific type of firewall) can be installed. It “can send all incoming messages to a virus server that will scan the message, strip any viruses out, and forward the message to the intended recipient. There is no user intervention, so employees’ privacy is not violated.”²⁶³ A perimeter firewall can also be installed to check for words that may be undesirable or suspicious, thereby aiding in combating industrial espionage.²⁶⁴ Firewalls are also used to prevent Trojan horses from transferring information from a corporate machine to a third machine outside the corporate network.²⁶⁵

However, firewalls are often attacked by *hackers* all over the world, trying to beat the security system in order to prove their own expertise.²⁶⁶

6.3. Public key encryption, symmetric encryption and digital certificates

Encryption means that the whole document is encoded.²⁶⁷ Put differently, the data transmissions are scrambled.²⁶⁸ *Symmetric encryption* (also known as *conventional cryptography*) uses the same “key” to encrypt and decrypt a message.²⁶⁹ *Public key encryption*, on the other hand, works on the basis of two “keys”: a public key and a private key that are generated simultaneously by the computer user’s encryption software. The “private key” “is either stored on his browser on his computer ... or it is stored on a cryptographic smart card”²⁷⁰ and a PIN number or a password protects the private key from unauthorised usage.²⁷¹ It can even be stored on a stiffer disk or a CD-ROM.²⁷² Therefore only the computer user possesses and has access to this private key. The computer user uses this key to encrypt all messages that he forwards to third

²⁶¹ Planting 2000(a):81; Chien 2000; Anonymous 1999(e):38.

²⁶² Anonymous 2000(a):27.

²⁶³ Anonymous 1999(c):36.

²⁶⁴ Anonymous 1999(c):36.

²⁶⁵ Chien 2000.

²⁶⁶ Van der Merwe 2000:199.

²⁶⁷ McNamara 1998:55.

²⁶⁸ Hedberg 1997:28.

²⁶⁹ Lesaoana 2000; Erdozain 1999:275; Dowd & McHenry 1998:25; Garfinkel & Spafford 1997:192.

²⁷⁰ Cristierson & Mostert 2000:28.

²⁷¹ Chadwick 1999:142; Garfinkel & Spafford 1997:110-111; Kuner 1996:186.

²⁷² Garfinkel & Spafford 1997:110.

parties and the latter employs the public key to decrypt these messages. Likewise, the computer user employs his private key to decrypt all messages that third parties have encrypted with the user's public key. Only the key that was *not* used to encrypt data can decrypt that data.²⁷³

In order to furnish the public key²⁷⁴ to someone else (the recipient), the computer user utilises a certification agency²⁷⁵ (as a trusted third party).²⁷⁶ The public key is made public along with a certificate binding an entity's identity to its public key.²⁷⁷ These digital certificates, also known as *Digital IDs* and *electronic credentials* are electronic credentials that establish the true identities of sites and site visitors.²⁷⁸ Of necessity, the computer user can also send a copy of his public key, as an attachment to an e-mail message, to the recipient.²⁷⁹ Other businesses choose to make their public keys available on their web pages.²⁸⁰

Encryption can also be used to secure, not only information transferred by means of e-mail (including both the e-mail message as well as attachments to the message), but also confidential or sensitive information stored on a hard drive, etc. The decryption keys can be provided to employees that require access to such information.

Note, however, that encryption software will make no system 100% *hacker-proof*. Many *hackers* will attempt to find errors in design, implementation or installation of the encryption software, instead of attempting to break the code of the encryption software. Furthermore, even though the connection between one's web browser and the web site server might be secure, the web server's data storage can still be compromised and unauthorised persons can in this way gain access to one's personal information such as credit card details.²⁸¹

²⁷³ Van der Merwe 2000:231.

²⁷⁴ An example of a public key can be viewed at www.cert.org/CERT_PGP.key.

²⁷⁵ An example of a certification authority is Verisign. See www.verisign.com.

²⁷⁶ Van der Merwe 1999:229; Erdozain 1999:275; ABA Guidelines 1996:13.

²⁷⁷ Asokan 1997:30.

²⁷⁸ Erdozain 1999:275.

²⁷⁹ Cobb 1998:54.

²⁸⁰ Garfinkel & Spafford 1997:214.

²⁸¹ Anonymous 2001(b).

6.4. Network intrusion-detection devices & software

Network intrusion-detection devices and software detect external as well as internal security breaches as they happen and immediately notify security personnel and network administrators.²⁸² These systems check user location and file activity for signs of attack.²⁸³ They also automatically react when an attack or suspicious activity, such as port scanning²⁸⁴ and successive login failures, is detected.²⁸⁵ Therefore an intrusion detective system functions like a burglar alarm alerting the system administrator of suspicious activities.²⁸⁶ It is alleged that such systems can even terminate a *hacker's* connection and examine what he did.²⁸⁷ Software such as RealSecure can record an entire session for later playback.²⁸⁸ Some companies aver that their intrusion detection systems can prevent denial-of-service attacks by identifying malicious attacks.²⁸⁹

There are various types of intrusion detection devices. Normal detection devices or software check for abnormal²⁹⁰ or suspicious behaviour.²⁹¹ Other detection software detects e.g. changes to the integrity of files. It will, for instance, inform system administrators whether any files were deleted, modified or added.²⁹² Therefore this software indicates attacks by external and internal *hackers* (employees) as well as detects password sniffers, Trojan horses, etc.²⁹³

From a legal point of view the following should be kept in mind: the prosecution will need to prove that the accused *hacker* penetrated a computer system and what he

²⁸² Anonymous 2000(v):26(4); Herringshaw 1997:6. Malicious Activity Detection (MAD) is an example of such intrusion detection devices. See Anonymous 2000(b):34.

²⁸³ Herringshaw 1997:6.

²⁸⁴ In *Moulton et al v VC3* (N.D. Ga 2000) the court explained port scanning as follows: "A port scan is a method of checking a computer to see what ports [communication channels] are open by trying to establish a connection to each and every port on the target computer. If used by a network administrator on his own network, the scan is a method of determining any possible security weaknesses. If used by an outsider, the scan indicates whether a particular port is used and can be probed for weakness." A copy of this judgment can be downloaded from <http://pub.bna.com/eclr/00434.htm>.

²⁸⁵ Dowd & McHenry 1998:27.

²⁸⁶ Beaver 2000:8.

²⁸⁷ Finn 1998:40; Herringshaw 1997:6.

²⁸⁸ Finn 1998:42.

²⁸⁹ Anonymous 2000(v):26(4).

²⁹⁰ Called Anomaly Detection Devices. See Dowd & McHenry 1998:27-28.

²⁹¹ Called Misuse Detection Devices. See Dowd & McHenry 1998:28.

²⁹² Anonymous 2000(w):24.

²⁹³ Anonymous 2000(w):24.

consequently did. Network intrusion detection software and devices can provide the necessary evidence for the prosecution to prosecute the *hacker* and even provide the necessary evidence to institute a civil action against the *hacker*.

6.5. Back-up copies

Businesses may consider it wise to make back-up copies, regularly, of their electronic files.²⁹⁴ Even though this does not prevent intrusion, it does offer protection where critical information is corrupted, deleted or altered by *hackers* or malicious programs. A business' hard drive or part of it can be backed up onto a removable medium such as a floppy disk, Zip disk, tape or CD-ROM.²⁹⁵ However, a business must ensure that the information backed up is virus free, otherwise malicious codes will be backed-up, rendering such information as dangerous and fragile as non-backed-up information and the business can re-infect itself by restoring files from the backed-up disks.

6.6. System administrator

It is of paramount importance for any firm to appoint a system administrator (also known as an *IT administrator*) that is in charge of the computer system, including network security. Where a firm is large and has many computers and computer users as well as valuable information stored on such computers, the firm might want to have an IT department where experts are responsible for the computer system. Normally a system administrator's duties are threefold:

- a) to ensure that the computers and computer system are functional;
- b) to update the anti-virus software whenever new releases become available on the Internet; and
- c) to monitor the computer system for suspicious activities such as attempted hacking instances and, where necessary, to terminate a specific connection.

It is also imperative to ensure that the system administrator is educated in

²⁹⁴ Jones 2000; Garfinkel & Spafford 1997:373. Lewis 2001 provides the following reasons (at 75) for backing-up hard drives: "Your hard disk will die eventually too. If not from mechanical failure or an operating system bug, it could be wiped out by a virus, fried by a lightning bolt, snatched by a burglar, forgotten on the train, or erased accidentally because you or some other computer genius leaned on the wrong button. It's a matter not of if, but when."

²⁹⁵ www.microsoft.com/privacy/safeinternet/security/best/backup.html.

"counterhacking". This refers to the techniques used to prevent hacking into a business' computer system. A representative of Ernst & Young indicated in 2000 that the main reason why systems get hacked is because system administrators fail to "keep up to date with discovered security problems and the 'patches' that come out to fix the problem."²⁹⁶

It is also very important that a business' system administrator should immediately inform the board of directors (or management) of any breaches in security that have occurred and whether any information was lost or corrupted. Furthermore, where a virus or hacking attack occurred, he should indicate to the board which steps he took to protect the business' electronic assets (data) from future cyber-attacks.

6.7. Password policy

All businesses should have a password policy incorporated into their employees' contracts of service. This policy may for instance provide the following:

1. Employees must choose passwords of at least eight characters. Such passwords are harder to crack than passwords of four or six characters.
2. When choosing passwords, employees are not allowed to use common words with which they can be identified, such as their names or the names of their family members. "These are the kinds of password features that thieves and hackers first try ... The more complicated the password, the better."²⁹⁷ Common words, such as love, God and sex should never be used as passwords.
3. Employees are not allowed to furnish their passwords to any other person, including another employee.²⁹⁸ Likewise, employees are not allowed to disclose their passwords to anyone, including their employers or the system administrators, by means of e-mail. *Hackers can forge (spoof) their e-mail address to make it appear as if the e-mail message came from an employee's employer or the system administrator.*²⁹⁹
4. Passwords must never be written down.
5. The system administrator should set the server so that it requests, for instance, an

²⁹⁶ Myers 2000:3.

²⁹⁷ www.microsoft.com/privacy/safeinternet/security/best/passwords.html.

²⁹⁸ Voges 2001:37; Atkins 1990:82.

²⁹⁹ Wing 2001.

employee to choose a new password at least every two months.³⁰⁰

6. Immediately when an employee retires or is dismissed his password must be cancelled.
7. After three failed attempts to log-on the user should be locked out. "This way, a hacker can try only twice and then has to wait for the user to log on and off. If the hacker tries the third time, the system administrator should start becoming suspicious."³⁰¹
8. Failure to comply with the above-mentioned provisions can lead to disciplinary measures and continuous failure to adhere to these rules as well as warnings may lead to dismissal.

One problem is where only the employee knows the password to his computer and he dies or disappears. The company will find it very difficult to access that specific computer in future. For this reason, employees might be compelled to disclose their passwords to the system administrator. The folder containing such passwords on the system administrator's computer must be encrypted and only two persons should have the decryption key: the system administrator and the managing director. Under no circumstances should a hard copy of these passwords exist.

6.8. E-mail Policy

All businesses should also have an e-mail policy, incorporated into their employees' contracts of employment. This can also be called an electronic communications policy. This policy should stipulate the following:

1. Employees must scan all files attached to an e-mail message for malicious programs, before opening the file, even if was sent by someone he or she knows.
2. All e-mail messages should be encrypted.³⁰²
3. Failure to comply with these provisions can lead to disciplinary measures and continuous failure to adhere to these rules as well as warnings may lead to dismissal.

The policy should also control the content of outgoing e-mail message. For instance, an employer may prohibit his employees from sending confidential information by means of e-mail messages. However, should the employer allow his employees or

³⁰⁰ Some commentators recommend once a month. See Atkins 1990:82.

³⁰¹ Anonymous 2000(r):3.

³⁰² Ryrie 1999(b):47.

specific employees to communicate confidential information by means of the Internet to other employees or other Internet users, the e-mail messages must be encrypted.³⁰³

6.9. Internet usage policy

This policy, also incorporated into the employees' contracts of service, should provide that -

1. Employees, when downloading files from the Internet, must first scan the files by means of their employers' anti-virus software.
2. If an employee suspects his office computer to be infected by a virus, he must inform the system administrator immediately.³⁰⁴
3. If an employee receives a virus warning which may be a hoax and which, in addition, may amount to a virtual virus, such warning may be forwarded only to the system administrator who can confirm whether or not the warning is genuine.³⁰⁵

³⁰³ Anonymous 1999(d):38. Programs such as MAILsweeper allows employers to define the e-mail usage policies for their businesses: in this policy the employer can state what is acceptable content in e-mails and e-mail attachments. The program will then check all e-mails leaving and entering the company server, validating them against the policy. Anonymous 2001(e):39. See www.netunlim.co.za.

³⁰⁴ www.sophos.co.za/virusinfo/articles/safehex.html.

³⁰⁵ www.sophos.co.za/virusinfo/articles/safehex.html.

CHAPTER SIX

CRIMINAL LIABILITY OF MALICIOUS COMPUTER PROGRAMMERS AND HACKERS

1. INTRODUCTION

The purpose of this chapter is to assess whether hacking and virus instances are adequately criminalised by the South African criminal law and specifically whether they constitute any of the following common law offences: theft, theft by false pretences, fraud, malicious injury to property, housebreaking or *crimen iniuria*. The question is also discussed whether individuals who receive electronic data, obtained by means of unlawful means, can be prosecuted for the offence of receiving stolen property knowing it to be stolen. It is further determined whether the selling and/or making available of illegally obtained passwords constitute any common law offence. This study also determines whether cyber-abusers can be prosecuted in terms of existing legislation.

2. LIABILITY IN TERMS OF DEDICATED LEGISLATION

Currently no legislation exists locally to prosecute *hackers* and virus writers in general. Hacking and virus instances can, however, be prosecuted in specific instances set out in the *Interception and Monitoring Prohibition Act of 1992*, the *South African Police Service Act of 1995* and the *Correctional Services Act of 1998*.

2.1. Interception and Monitoring Prohibition Act

The *Interception and Monitoring Prohibition Act*³⁰⁶ provides that:

“No person shall -

(a) intentionally and without the knowledge or permission of the dispatcher intercept a communication which has been or is being or is intended to be transmitted by telephone or in any other manner over a telecommunications line,³⁰⁷ or

³⁰⁶ Act 127/1992.

³⁰⁷ According to s 1, “telecommunications line” include “any apparatus, instrument, pole, mast, wire, pipe, pneumatic or other tube, thing or means which is or may be used for or in connection with the

(b) intentionally monitor any conversation or communication by means of a monitoring device so as to gather confidential information³⁰⁸ concerning any person, body or organisation."³⁰⁹ (own emphasis)

A monitoring device is defined to mean "any instrument, device or equipment which is used or can be used, whether by itself or in combination with any other instrument, device or equipment, to listen to or record any conversation or communication."³¹⁰ The Act is silent on the meaning of the word "conversation". The South African Law Commission (SALC) notes that the word "conversation" ensures that all types of conversations namely fax, e-mail, etc are included.³¹¹ The Act stipulates that the penalty for contravening the above-mentioned is a maximum fine of R40 000³¹² or a maximum period of imprisonment for two years.³¹³

The Act therefore prohibits the interception and monitoring of electronic communications. It follows that the Act attempts to protect the privacy of communications.³¹⁴ It is submitted that where a *hacker* intercepts electronic communications by means of his computer or by means of a computer program (such as a Trojan horse), he violates the above-mentioned provision.

sending, conveying, transmitting or receiving of signs, signals, sounds, communications or other information".

³⁰⁸ The question arose in *Protea Technology Ltd & Another v Wainer & Others* 1997 3 ALL SA 594 W as well as *S v Kidson* 1999 1 SACR 338 W what is meant by "confidential information" as used in the Act. In the former case the judge noted (at 603g-h) that confidential information "must surely mean such information as the communicator does not intend to disclose to any person other than the person to whom he is speaking and any other person to whom the disclosure of such information is necessarily or impliedly to be restricted." In the *Kidson* case the court enunciated (at 347g-h) that the term "confidential information" should be interpreted more narrowly and technically: "To [the] formulation [as provided by the *Protea Technology* judgment, *supra*] should ... be added that the information the communicator intended to restrict as confidential must be information upon which the law confers the attribute of confidentiality." In *S v Dube* 2000 1 SACR 53 N the court (at 76b-d) supported the line of reasoning enunciated in the *Kidson* case.

³⁰⁹ S 2(1).

³¹⁰ S 1.

³¹¹ www.law.wits.ac.za/salc/report/seclegsum.html.

³¹² S 1 of the *Adjustment of Fines Act* 101 of 1991 read with s 92(1)(b) of the *Magistrates' Act* 32 of 1944. GG 14498 issued on 31/12/1992 provides that each year is worth R20 000.

³¹³ S 8.

³¹⁴ In *S v Kidson* 1999 1 SACR 338 W the court maintained (at 344g-i) that the "Legislature's primary purpose seems to have been to protect confidential information from illicit eavesdropping ... that what is prohibited is the conduct of a third person acting in relation to a conversation between others."

The question that arises is whether a computer or a modum³¹⁵ can be regarded as a monitoring device, as defined by the Act, where a *hacker* uses his computer to monitor electronic communications. It is submitted that a computer or its modum may be regarded either as an instrument,³¹⁶ equipment³¹⁷ or a device³¹⁸ that can be used to intercept communications. Even though neither a computer nor a modum is primarily designed to monitor electronic communications, they can be used as instruments for this purpose.

Another question that has to be addressed is: where a *hacker* installs a computer program on A's computer, which monitors electronic communications, can it be stated the *hacker* employs a monitoring device? It is submitted that this question must be answered in the affirmative, for two reasons: a) a computer program can definitely be regarded as an instrument or a device in the hands of the *hacker* to monitor e-communications and secondly b) the *hacker* still uses his computer, in conjunction with the program, to monitor the communications. As found above, a computer falls within the definition of monitoring device.

³¹⁵ Modums are used to connect a computer to the Internet.

³¹⁶ The *Concise Oxford Dictionary* defines an "instrument" as "a tool or implement, esp. for delicate or scientific work". The *Short Oxford English Dictionary* defines "instrument" to mean "A thing with or through which something is done or effected: a means ... A tool, implement, weapon". *Webster's Third New Dictionary* defines "instrument" as "a means whereby something is achieved, performed or furthered". The Afrikaans text, which is signed by the State president, also uses the word "instrument", which is defined by the *Verklarende Woorde Boek van die Afrikaanse Taal* (HAT) to mean "Konkrete hulpmiddel met behulp waarvan die een of ander taak verrig word; apparaat werktuig". Bearing these definitions in mind, it can be argued that a computer may be regarded as an instrument or a tool that can be used, in conjunction with the necessary software, to monitor electronic communications.

³¹⁷ The *Oxford Advanced Learners Dictionary* defines equipment to mean "the things that are needed for a particular purpose or activity". See <http://www1.oup.co.uk/elt/oald/>. The *Concise Oxford Dictionary* defines "equipment" as the "necessary articles, clothing, etc for a purpose". *Webster's Third New Dictionary* defines "equipment" to mean "the implements (as machinery or tools) used in an operation or activity ... all the fixed assets other than land and building of a business enterprise". The Afrikaans text uses the word "toerusting". It is submitted that the courts will be willing to hold that a computer or its modum can be regarded as equipment used to monitor electronic communications.

³¹⁸ The *Concise Oxford Dictionary* defines a "device" as "a thing made or adapted for a particular purpose, esp. a mechanical contrivance". The Afrikaans text uses the word "toestel". The HAT defines "toestel" as "Werktuig, apparaat, meganiese hulpmiddel". Bearing these definitions in mind, it is submitted that a computer or its modum can be regarded as an apparatus or a thing adapted, in conjunction with the necessary software, to monitor electronic communications.

In 2001 the Department of Justice issued an *Interception and Monitoring Bill*.³¹⁹ The purpose of this bill is to repeal the *Interception and Monitoring Prohibition Act* and to regulate (for the purpose of this dissertation) the monitoring and interception of communications and messages. In this bill "communication" is defined to include "a conversation or a message, and any part of a conversation or message, whether (a) in the form of (i) speech, music or other sounds; (ii) data; (iii) text; (iv) visual images, whether or not animated; or (v) signals; or (b) in any other form or in any combination of forms".³²⁰ Therefore this definition clearly includes electronic communications by means of the Internet.

The prohibitions are identical to the prohibitions in the *Interception and Monitoring Prohibitions Act* and the definition for "monitoring device" remains the same.³²¹ However, the bill introduces certain exceptions to the above prohibitions namely that -

- a) Anyone is allowed to monitor any communication by means of a monitoring device where he is a party to that communication or where one of the parties to the communication has consented to such monitoring;
- b) Anyone who is a party to a communication is allowed to, in the course of the carrying on of any business and without the knowledge or permission of the other party to that communication,
 - (i) intercept the communication which has been or is being or is intended to be transmitted by telephone or in any other manner over a telecommunications system; or
 - (ii) monitor the communication by means of a monitoring device,

for the purpose of monitoring or keeping a record of any communications by means of which transactions are entered into in the course of that business or of any other communications relating to that business or taking place in the course of its being carried on.³²²

³¹⁹ Bill 50 of 2001. A copy of this draft bill can be downloaded from www.polity.org.za/govdocs/bills/2001/b50-01.pdf.

³²⁰ S 1.

³²¹ See ss 1 & 2(1) of the *Interception and Monitoring Bill*.

³²² S 2(2)-(3).

Accordingly, it remains unlawful for any *hacker* to intercept or to monitor electronic communications.

2.2. South African Police Service Act & Correctional Services Act

The *South African Police Service Act*³²³ provides for the criminalisation of unauthorised access to or modification of computer material stored on a computer belonging to the South African Police Service (SAPS). The Act provides for three offences, namely:

- 1) Any person who wilfully gains unauthorised access to any computer which belongs to or is under the control of the SAPS or to any program or data held in such a computer, or in a computer to which only certain or all members of the SAPS have restricted or unrestricted access in their capacity as members, commits an offence and is liable on conviction to a fine or to imprisonment for a period not exceeding two years.³²⁴ This clearly criminalises hacking instances: the mere gaining of unauthorised access is an offence.
- 2) Anyone who wilfully causes a computer which belongs to or is under the control of the SAPS or to which only certain or all members have restricted or unrestricted access in their capacity as members, to perform a function while such person is not authorised to cause such computer to perform such function, is guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding two years.³²⁵ This criminalises instances where a *hacker* copies, deletes or modifies electronic files stored on a computer as well as instances where a malicious computer program is used to copy, erase or modify such content.
- 3) Anyone who wilfully performs an act which causes an unauthorised modification³²⁶ of the "contents of any computer"³²⁷ which belongs to or is under the control of the SAPS or to which only certain or all members have restricted or unrestricted access

³²³ Act 68/1995.

³²⁴ S 71(2).

³²⁵ S 71(3).

³²⁶ The Act connotes that "modification" includes both a modification of a temporary or permanent nature. S 71(1).

³²⁷ "Contents of any computer" includes "the physical components of any computer as well as any program or data contained in the random access memory of a computer or stored by any computer on any storage medium, whether such storage medium is physically attached to the computer or not, where such storage medium belongs to or is under the control of the Service." S 71(1).

in their capacity as members -

“with the intention to either -

- (a) impair the operation of any computer or of any program in any computer or of the operating system of any computer or the reliability of data held in such computer; or
- (b) prevent or hinder access to any program or data held in any computer;”

commits an offence and is liable on conviction to a fine or to imprisonment for a period not exceeding five years.³²⁸ This criminalises hacking and virus instances that (1) cause the hard disk or information stored on it to be inaccessible or 2) modify, corrupt or delete information stored on the hard disk. It should be noted that the Act does not require the virus program to be programmed to attack the SAPS computer specifically but that it will suffice if the program was written with the intention to impair the operation of any computer. It is submitted that where a *hacker* gains access to a SAPS computer and changes the password, which allows access to that particular computer or particular data, the *hacker* can be found guilty of contravening this provision in that he modified the contents of the computer and he consequently prevented access to the data (or specific data) stored in that computer.

The Act provides that “access to a computer” includes “access by whatever means to any program or data contained in the random access memory of a computer or stored by any computer on any storage medium, whether such storage medium is physically attached to the computer or not, where such storage medium belongs to or is under the control of the SAPS.”³²⁹ Consequently, the Act encompasses hacking and virus instances by means of the Internet. Furthermore, “unauthorised access” includes instances where a member of the police force exceeds his authorisation.³³⁰

The provisions of section 128 of the *Correctional Services Act*³³¹ are virtually identical to the *South African Police Service Act*. The former deals with computers owned by or

³²⁸ S 71(4). Own emphasis.

³²⁹ S 71(1).

³³⁰ S 71(1). The Act provides that “unauthorised access” includes “access by a person who is authorised to use the computer but is not authorised to gain access to a certain program or to certain data held in such computer or is unauthorised, at the time when the access is gained, to gain access to such computer, program or data.”

³³¹ Act 111/1998.

under the control of the department of correctional services as well as computers to which correctional or custody officials have access.

3. LIABILITY IN TERMS OF COMMON LAW AND OTHER NON-SPECIFIC STATUTORY PROVISIONS

The next question to be addressed is whether hacking and virus instances in general can be accommodated in terms of existing common law and statutory crimes.

3.1. Theft as common law offence

Under this heading the requirements of theft are discussed and it is then determined whether someone can be found guilty of theft where he copies electronic content, including information and data or transfers electronic money either by means of hacking or by means of a computer program, such as a Trojan horse.

3.1.1. General principles

The definition of theft is the unlawful appropriation of someone else's movable corporeal property, with the intention permanently to deprive the owner of the benefits of his ownership rights.³³² A "specific" form of theft also exists comprising the theft of credit which entails the theft of incorporeal money.³³³ The four requisites for the offence of theft are appropriation, corporeal object, unlawfulness and *animus furandi*. They are each discussed in turn.

1) Appropriation ("*toe-eiening*") is also referred to as *contrectatio*.³³⁴ Some commentators define *contrectatio* as "conduct by means of which a person acquires effective control over property, and deprives the owner or other lawful possessor of his control."³³⁵ Appropriation in practice, therefore, means -

a) to appropriate the object for oneself. Put differently, to exercise or assume the rights/benefits of an owner in respect of the object – in other words, to gain control of the object and to deal with it as if one were the owner thereof; and

³³² Snyman 1999:483; LAWSA 1996:vol 6, par 294; Van der Merwe 1985:130.

³³³ Snyman 1999:489.

³³⁴ See Snyman 1999:490; LAWSA 1996:vol 6, par 296 & 297.

b) to deprive the owner of his property rights or benefits flowing from such ownership. Put differently, to deprive him of the enjoyment ("*genotsbevoegdheid*") of his property.³³⁶

The physical handling of property is no longer required.³³⁷ Nor is removal required for theft seeing that control can be exercised over an object without removing it.³³⁸ It should be borne in mind that theft does not affect the *dominium* (ownership), but only the owner's *possessio* (control) and usage of the object.³³⁹

2) The stolen object must normally be corporeal, except in the case where credit or money is stolen.³⁴⁰ Due to the requirement that the object stolen must be corporeal, commentators as well as local courts normally state that "ideas" and "board and lodging" cannot be stolen.³⁴¹

3) The appropriation must be unlawful.³⁴²

4) The appropriation must occur with *animus furandi*.³⁴³ *Animus furandi* entails an intention to appropriate ("*toe-eieningsopset*")³⁴⁴ and such an appropriation intention entails two facets:

³³⁵ LAWSA 1996: vol 6, par 296.

³³⁶ Snyman 1999:491-492; LAWSA 1996:vol 6, par 297; Loubser 1978:59; Snyman 1975:32 & 37. In *Premier Western Cape & Others v Parker & Mohammed & Others* 1999 1 ALL SA 176 C the court noted (at 187f-g) that the act of appropriation consists of two aspects: "the exclusion of the owner from his or her property and an exercise by the thief of the rights of an owner in respect of such property, the thief thus having taken the place of the owner."

³³⁷ Snyman 1999:490. See *S v Naryan* 1998 2 ALL SA 345 W:356g-h where the court maintained that actual possession is not necessary for *contrectatio*.

³³⁸ LAWSA 1996:vol 6, par 298; *R v Mlooi* 1925 AD 131:152.

³³⁹ *R v Oliver and Others* 1921 TPD 120:127. See Snyman 1999:492. In *R v Von Elling* 1945 AD 234 the Supreme Court of Appeal correctly noted (at 236-237) that "a fraudulent taking of a thing from its owner, or any other fraudulent dealing with it, cannot, as a general rule, deprive the owner of his legal right of ownership in the thing. It can, however, deprive him of the benefits of his ownership (such as use and possession), and so long as the thief remains in adverse possession or control of the stolen thing, he is continuously guilty of a *fraudulosa contrectatio* which deprives the owner of those benefits."

³⁴⁰ Snyman 1999:494; LAWSA 1996:vol 6, par 301. In Roman law as well as Roman-Dutch law the object of theft [*res*] had to be movable and corporeal. See Snyman 1999:488; *S v Mintoor* 1996 1 SACR 514 C:515B-C; Loubser 1978:49.

³⁴¹ Snyman 1999:494; LAWSA 1996:vol 6, par 301. With regard to the theft of ideas as well as the theft of board and lodging, see *R v Cheeseborough* 1948 3 SA 756 T and *R v Renaud* 1922 CPD 322, respectively.

³⁴² Snyman 1999:495.

³⁴³ According to Roman law *animus furandi* meant that something had to be taken with the intent to commit *furtum*. See Verloren van Themaat 1949:22.

- a) the intention to unlawfully appropriate the property. Put differently, intention to exercise or assume the rights or benefits of an owner in respect of the object;
- b) the intention to permanently deprive the owner of the full enjoyment or benefits (use and control) of his ownership.^{345 346}

An intention to prejudice the owner as such is not required by our law. The common law requires that the owner has to suffer prejudice due to the theft, in the sense of an infringement of his rights, but patrimonial prejudice is not required.³⁴⁷

³⁴⁴ *S v Luther en 'n Ander* 1962 3 SA 506 A:509H & 511C.

³⁴⁵ Burchell and Milton 2000:549; Snyman 1999:500; LAWSA 1996: vol 6, par 304, 305 & 306; De Wet & Swanepoel 1985:312; Loubser 1978:66; Snyman 1975:3. With regard to the intention to permanently deprive the owner of the enjoyment of his ownership rights, see *S v Mtshali* 1960 4 SA 252 N:254G; *R v Sibiya* 1955 4 SA 247 A:257B-C; *R v Smulian* 1928 TPD 762:764 & 765; *R v Oliver and Others* 1921 TPD 120:124. In *R v Laforte* 1922 CPD 487 the court put it as follows on p 497: "It seems to me that to constitute theft under our law there must be an intention to terminate and not merely suspend, the enjoyment by the owner of his rights or ownership." In *Premier Western Cape & Others v Parker & Mohammed & Others* 1999 1 ALL SA 176 C the court maintained (at 187g-h) that the intention to steal exists where a person "a) intentionally effects an appropriation, b) to deprive the owner permanently of the property, c) in the knowledge that the property is capable of being stolen and, d) that he or she is acting unlawfully in taking such property." See also *S v Boesak* 2000 1 SACR 633:659b-d. In *S v Heller* 1971 2 SA 29 A the Supreme Court of Appeal enunciated (at 45H-46) that "the intention to steal comprises (a) an intention 'to terminate the owner's enjoyment of his rights or, in other words, to deprive him of the whole benefit of his ownership', and (b) the absence of a belief that the owner had consented or would have consented to such a termination or deprivation." In *S v Boesak (supra)* the Supreme Court of Appeal maintained (at 659b-d) that "[t]he intent to steal (*animus furandi*) is present where a person (1) intentionally effects an appropriation (2) intending to deprive the owner permanently of his property or control over his property, (3) knowing that the property is capable of being stolen, and (4) knowing that he is acting unlawfully in taking it".

³⁴⁶ Snyman 1999 is of the opinion that local courts should rather work with the intention to appropriate than with the intention to deprive the owner permanently of his ownership rights in that the latter does not distinguish between theft and malicious injury to property. (At 499).

³⁴⁷ For instance, where A steals a motor vehicle and the police arrests him just as he is driving away with it, the owner does not suffer patrimonial prejudice. *Verloren van Themaat* 1949 maintains at 114: "Wel kan uit die verklarings van ons howe afgelei word dat nadeel in die vorm van inbreukmaking op iemand se regte 'n vereiste is." [my translation: It can be inferred from local judgments that prejudice in the form of an infringement of someone's rights is a requirement.] See also *Verloren van Themaat* 1949:115. The facts of *R v Carelse and Kay* 1920 CPD 471 were that A and B attempted to steal petrol by placing a can full of petrol amongst the empty cans. The plaintiff (owner of the petrol) discovered this and emptied the cans of petrol (that were put amongst the empty cans by A and B) and replaced it with water. B then (not knowing that the petrol had been replaced with water) poured the contents of the can into his car. The court found them guilty of theft. In *S v Vilakasi and Another* 1999 2 SACR 393 N the accused obtained possession and control of a truck, by means of force, and intended to use it as an

3.1.2. Lucrum as an element of theft

The question remains whether *lucrum faciendi gratia* (intent to gain a profit or benefit from theft) is still a requirement in our law. According to the *Corpus Juris Civilis*, Roman law posed *lucrum faciendi gratia* as an element of theft.³⁴⁸ This requirement

ambush, but distanced themselves from this plan later on and left the vehicle unattended. The question was whether the accused were guilty of robbery, but the *dictum* also applies to theft. The court stated (at 398c) that the "fact that the Dyna truck was never used in the roadblock and therefore not damaged or destroyed does not serve to absolve from them their criminal conduct. At best for them it may have a mitigating factor on sentence." According to Roman law, theft was required to be to the prejudice of the proprietor ("*reghebbende*"), which means that the proprietor's patrimonial rights ("*vermoënsregte*") had to be infringed. See Verloren van Themaat 1949:20.

³⁴⁸ See Loubser 1978:65; Verloren van Themaat 1949:23. D 47.2.1.3 reads (translated by Mommsen *et al* 1985): "Theft is a fraudulent interference with a thing with a view to gain, whether by the thing itself or by the use of possession of it. This natural law prescribes." D 47.55.1 reads (translated by Mommsen *et al* 1985): "When a person to whom something was lent for use himself lent it to a third party, the ruling was that he was guilty of theft. It adequately emerges from this that theft appears to have been committed if a person appropriate to his own profit the use of another's thing. One should not be disturbed by the seeming fact that he does nothing for personal profit; it is a form of gain to make large with another's property and thereby acquire a debtor who is under an obligation. Thus a person is liable for theft who removes a thing to give it to a third party." D 19.5.14.2 reads (translated by Mommsen *et al* 1985): "But again, if a man, intending to do harm and not to make a profit, tossed another's silver cup into the sea, Pomponius ... wrote that neither the action on theft nor that for wrongful harm lies; action must be brought *in factum*." D 47.2.43.4 reads (translated by Mommsen *et al* 1985): "A man who, for personal gain, takes away a thing belonging to another is guilty of theft, whether he knows the identity of the owner or not; for it in no way minimizes the fact of theft that the owner of the object is unknown." D 47.2.43.7 reads (translated by Mommsen *et al* 1985): "And if he picked up a thing, just lying there, which was not and which he did not think to be, abandoned, with the object not of personal profit but of returning it to its owner, he would not be guilty of theft." D 47.2.44.1 reads (translated by Mommsen *et al* 1985): "If I should give you, as being yours, a thing which you know to be mine, the better option is that you are guilty of theft, if you accept with a view to gain." D 47.2.45 reads (translated by Mommsen *et al* 1985): "it thus emerges that however the slave be taken away from his master, the action for theft nonetheless survives against the thief, and that is the rule we observe: the action lies not because he is now absent but because he ever was away to the thief's advantage [*benefit/beneficio*]." D 47.2.51 reads (translated by Mommsen *et al* 1985): "If the cattle should fall over a cliff, the action for damage wrongfully caused, on the analogy of that under the *lex Aquilia*, will be given." What is meant by this text is the following: If A drove B's cattle over a cliff with malicious intent, A is not guilty of theft. However, A is guilty of malicious injury to property. It is admitted that such conduct does not constitute theft in that A did not gain any benefit (*lucrum*) from the death of the cattle. D 47.2.66 reads (translated by Mommsen *et al* 1985): "One who appropriates another's thing with a view to his own gain is a thief, even if, changing his mind, he later returns it to the owner". D 47.7.8 reads (translated by Mommsen *et al* 1985): "Hence, if he cut the tree down and appropriate it for gain, he will further be liable for theft of the

also obtained in Roman-Dutch law.³⁴⁹ It would seem that the *lucri faciendi gratia* requirement was posed in order to distinguish theft from malicious injury to property.³⁵⁰

All commentators of modern books on South African criminal law are of the opinion that *lucri faciendi gratia* is no longer an element of theft.³⁵¹ However, it is contended that *lucri faciendi gratia* should be considered as a requirement of theft, in order to distinguish it from certain instances of malicious injury to property. Whenever a *hacker* or a virus merely deletes a file without making any reproductions, such conduct is not considered theft because the *hacker* or computer programmer did not gain any financial benefit. However, if *lucrum* is no longer required for theft, the mere erasure of electronic files may fall within the definition of theft.

wood". In the *Institutiones*, 2.1.16 (translated by Thomas 1975), it is stated that "Accordingly, if your geese or chickens, being disturbed by something, fly away, they are still held to be yours, wherever they may be: and anyone who detains such creatures with a view to gain [lucranda animo] is regarded as committing theft."

³⁴⁹ Voet in his *Commentarius Ad Pandectas* wrote at 47.2.1: "Furtum est contrectatio fraudulosa, lucri facienda gratia, vel ipsius rei, vel etiam usus eius possessionisve, quod iure naturali prohibitum est admittere." Likewise, Van der Linde wrote in his *Regtsgeleerd, Practicaal en Koopmans Handboek* at 2.6.2 that "Diefstal of dieverij is de ontvreemding van eenig roerend goed, buiten wetene en tegen den wil van de eigenaar, met oogmerk, om daar mede voor zig zelve, of voor anderen, eenig voordeel te doen." Moorman defines theft in his book *Verhandeling over de misdaden en der selver straffen* (1764) as follows at p 312: "De diefstal is niet anders dan een wegneming van een anders goed; met een quaed voornemen om sich daer mede te verriyken ondernomen". See also LAWSA vol 6:par 305 fn 1; Loubser 1978:65; Verloren van Themaat 1949:125.

³⁵⁰ Loubser 1978:65; Snyman 1973:288; Verloren van Themaat 1949:23, fn 161. See also D 47.2.51 in footnote 351.

³⁵¹ Snyman 1999 states at 498: "In Suid-Afrika is die *lucrum*-vereiste van die gemenerereg vroeg reeds oorboord gegooi, as gevolg van die invloed van die Engelse reg." [own translation: Under the influence of English law the common-law requirement of *lucrum* was abandoned at an early stage in the development of the crime in South Africa.] De Wet & Swanepoel 1985 remarks at 307: "Ons howe het nie konsekwent by die beginsels van ons gemene reg gehou nie, maar dikwels ons 'gemene reg' in die Engelse reg gaan soek ... So seer is die geval dat daar vandag op hierdie terrein omtrent geen reël is waaroor daar duidelikheid en eenstemmigheid bestaan nie. Die weselike kenmerk van *furtum*, nl die *lucri faciendi gratia* is byna verdring deur die 'intent to permanently deprive'." [own translation: Our courts failed to consistently adhere to the principles of our common law and often turned to English law to find our 'common law' ... The result is that with regard to this area of the law no clear and unanimous rule obtains. The essential characteristic of *furtum*, namely *lucri faciendi gratia* was ousted by the intent to deprive permanently.] In LAWSA 1996:vol 6 at par 305 the authors enunciate that "[t]he courts have, with one or two rare, early exceptions, never adopted this requirement, most probably because of the strong influence of English law, which does not recognise such a requirement." See also Loubser 1978:70.

Next a few South African judgments, dealing with the *lucrum* element, are scrutinized. It is contended that these judgments indicate that *lucrum* may still be required for theft.

A) Case law dealing with *lucri faciendi gratia*

1) In *R v Dier*³⁵² (1869) the court stated that *lucri causa* was an element of theft and it entailed "taking some supposed advantage". The court further remarked that "[i]n considering then, what is the definition of theft as punishable criminally by the Roman-Dutch Law, we may omit the words from 'vel' and we have it described by the words 'Furtum est contrectatio fraudulosa rei, lucri faciendi gratia.'³⁵³ The court posed the question of law as follows: "Was there, then in this case such a taking by the accused, *with a view to benefit himself or others*, as constitutes theft."³⁵⁴ (own emphasis)

Therefore, the judgment required an intention to benefit before conduct would constitute theft.

2) *James Walter Hill-Cathrine (Appellant) v The Clerk of the Peace for the County of Klip River (Respondent)*³⁵⁵ (1890): The facts were briefly that the accused took railway sleepers to secure a shaft's safety, where he was working, in order to prevent loss of life. He was subsequently charged with theft of the sleepers. The court simply stated that "[t]heft is the *fraudulosa contrectatio* of property *for gain* without the owner's consent"³⁵⁶ and consequently found the accused not guilty.

It is clear that the accused had no intent to benefit himself but to secure the mine and to safeguard the interests of his employer. He also had no intent to appropriate.

3) In *R v Pretorius*³⁵⁷ (1908) the accused was a partner. Instead of paying money which he received on behalf of the partnership over to the "partnership," he appropriated and converted the money to his own use. The court stated that: "But if it is clearly and positively shown that he was intending to deal with it fraudulently for *his own benefit*, and was *intending to appropriate it for himself*, contrary to the rights of his

³⁵² 1869 3 EDC 436. Unfortunately, this case was not available so Verloren van Themaat 1949:126 had to be relied upon.

³⁵³ 1869 3 EDC 436:437.

³⁵⁴ 1869 3 EDC 436:438.

³⁵⁵ 1890 NPD 69.

³⁵⁶ 1890 NPD 69:70. Own emphasis.

³⁵⁷ 1908 TPD 272.

partner, and contrary to his duty, then the Roman-Dutch law, in accordance with what seems to me ordinary common sense and justice, provides that he can be convicted of theft."³⁵⁸ (own emphasis)

4) *Maswana v R*³⁵⁹ (1909): the facts were briefly that A, a police officer, was used as a trap. After B committed theft, A was also charged with theft. The court stated:

"I am of the opinion that this appeal should be allowed for two reasons ... Secondly, by our law theft is defined as *contrectatio fraudulosa*, that is, a fraudulent handling of or dealing with the thing of another in such a way as to deprive the owner of his property. It is not necessary that the handling or dealing should be *lucris causa*. Both Matthaeus and Voet are very clear in their definition of theft. While they include the words *lucris causa* as an element in their definition, Van Leeuwen does not. It is plain there may be theft without the essential of *lucris causa* present. Such is the view of the law in South Africa, and there are English cases to the like effect ... I am therefore of the opinion that, though he acted *invito domino*, he did not deal with the calf *animo furandi*."³⁶⁰

The following comments are necessary to put the passage in perspective: (a) The English law has never posed *lucrum* as a requirement.³⁶¹ (b) The judge merely states that the criminal law of South Africa does not pose *lucrum* as a necessary requirement for theft, without referring to previous court cases. (c) The judge merely relied on Van Leeuwen's work, which did not pose *lucrum* as an element of theft, in deciding that *lucrum* was not an absolute requirement for theft. Voet, on the other hand, clearly required *lucris faciendi gratia* for conduct to constitute theft.³⁶² (d) The court maintained that there are instances of theft where *lucrum* is not essential, without providing an example. (e) It is clear from the facts that A did not act *animo furandi* and thus also did not act *lucris faciendi gratia*. (f) Some commentators are of the opinion that the above-mentioned *dictum* is merely *obiter* in that the court held that the accused had no *animus furandi* and thus it was unnecessary for the court to discuss *lucris faciendi gratia*.³⁶³ (g) Verloren van Themaat observes that the court merely replaced the *lucris faciendi gratia* requisite with the "intention to deprive the owner"³⁶⁴ which, may be

³⁵⁸ 1908 TPD 272:273.

³⁵⁹ 1909 EDC 253.

³⁶⁰ 1909 EDC 253:255.

³⁶¹ LAWSA 1996:vol 6, par 305.

³⁶² See footnote 356.

³⁶³ Verloren van Themaat 1949:126.

³⁶⁴ Verloren van Themaat 1949:126.

added, was a requirement according to English law and not South African or Roman-Dutch Law. (h) Lastly, the authors of LAWSA are of the opinion that local courts did not pose *lucrum* as a requirement after the 1900's due to the influence of the English law.³⁶⁵

5) In *Moodley v R*³⁶⁶ (1914) the court observed that conduct will constitute theft where "the thing is wrongfully and fraudulently dealt with, as it was here, *for the purpose of gain*."³⁶⁷ (own emphasis)

6) *R v Siboya* (1919):³⁶⁸ The facts were briefly that the accused found a strayed horse between his horses. He took the horse to a blacksmith and instructed the latter to castrate the horse and to put a private mark on its ear. The accused also stated in his evidence that he intended to keep the horse as his own if the owner did not turn up to claim it. The accused's defence argued that the facts did not disclose theft in that both *fraudulosa contrectatio* and *lucris causa*, as elements of theft, were absent. The court stated that:

"Dealing with the second reason first, that there must be a taking *lucris causa*, there is no doubt a great deal of authority to show that in the Roman-Dutch law this was considered to be an essential element in the constitution of theft. We find this to be supported by the definition of theft in the passage ... (*Dig. 47.2.1.3*). But when we look at the *Institutes* we find that Justinian, copying this definition, omits the words '*lucris causa*.'³⁶⁹ Van Leeuwen, in his *Commentaries*, Vol. 2, Book 4, follows the definition given by Justinian, and also omits the words '*lucris causa*'.³⁷⁰ On the other hand the great majority of authorities say that '*lucris causa*' is an essential element in the crime of theft. But in South Africa we have not strictly adhered to the Roman-Dutch definition; we have given a somewhat wider definition to the term 'theft,' and have generally adopted that laid down in the Transkeian Code, which has also been taken over in Tredgold's *Criminal Law*. Theft is defined in our modern law as the fraudulent taking, or

³⁶⁵ LAWSA 1996:vol 6, par 305.

³⁶⁶ 1914 NPD 514.

³⁶⁷ 1914 NPD 514:519.

³⁶⁸ 1919 EDL 41.

³⁶⁹ The *Institutes* defines theft as follows at 4.1.1. "Furtum est contrectatio rei fraudulosa vel ipsius rei vel etiam usus eius possessionisve: quod lege naturali prohibitum est admittre." Translated it means that "theft is the fraudulent dealing with a thing whether the thing itself, the use or possession of which one is barred from countenancing by natural law." See Thomas 1975:258.

³⁷⁰ Van Leeuwen in his book *Het Roomsche Hollandsche Recht* (1780) states at 4.38.1. "Diefte is een heymelyke en bedriegelyke handeling en houding van eens anders goed."

dealing with, or converting to the use of another, the property of some other person. Let us take the case of a trader who is travelling from one district to another, and who maliciously drives an ox along the road. He does not inspan the animal or use it in any way, but just drives it along. When he gets the ox to a different district, say on the border of the Kalahari, he maliciously turns the animal adrift, knowing full well that the probability is the owner will not be able to recover his property. In such a case, although it cannot be said that it was done *lucris causa*, the trader has acted in a wrongful and fraudulent manner with the property of another, there is a *contrectatio fraudulosa*, and he would be guilty of theft ... When we come to the facts in the present case, however, it appears that the accused did take the horse *lucris causa* because he stated that he intended to keep it as his own if the owner did not come forward. This statement is material as showing the accused's intention and state of mind."³⁷¹

A few comments are necessary: (a) the court correctly refers to the *Institutiones* where *lucris faciendi gratia* is not posed as an element of theft. However, in 2.1.16 it is stated that: "Accordingly, if your geese or chickens, being disturbed by something, fly away, they are still held to be yours, wherever they may be: and anyone who detains such creatures with a view to gain [*lucrandi animo*] is regarded as committing theft."³⁷² (own emphasis). Therefore, even though the *Institutiones* does not pose *animus lucrum faciendi* as a requirement for theft in 4.1.1, it would appear that this last quoted passage poses such mentality as a requirement for theft. (b) The court failed to bear in mind that most Roman-Dutch authorities³⁷³ (except Van Leeuwen)³⁷⁴ required *lucrum* as an element. (c) The court failed to mention South African judgments where local courts gave recognition to this element. (d) With regard to the court's example of theft without *lucris faciendi gratia*, we may observe that in D 19.5.14.2 it is stated that where a person throws another's silver cup into the sea, for the purpose of injuring him, and not *lucris faciendi gratia*, his conduct does not constitute theft. (e) In this case the accused was charged in terms of the *Native Territories Penal Code* (Act 24 of 1886) which stipulated that theft is "the act of fraudulently and without colour of right

³⁷¹ 1919 EDL 41:43-44.

³⁷² Translated by Thomas 1975.

³⁷³ See Moorman 3.2.2; Huber *Heedendaegse Rechtgeleertheit* 3.5.1 & 2.3.5; Matthaëus *De Criminibus* 47.1.2.

³⁷⁴ See *R v Laforte* 1922 CPD 487:487. Van Leeuwen states in *Het Roomsche Hollandsche Recht*, at 4.38.1, that "Diefte is een heymlijke en bedriegelijke handeling en houding van eens anders goed" and in his *Censura Forensis* he observes at 1.5.29.1 that "Furtum est quaelibet fraudulosa contrectatio rei alienae vel usus vel possessionis." But as observed by the court in *R v Laforte* 1922 CPD 487 at 490 he fails to explain why he does not include the element *lucris causa*.

converting to the use of any person anything or the use of anything capable of being stolen, with the intent to deprive the owner thereof or to deprive any person having any special property or interest therein of such property or interest.” (f) Verloren van Themaat correctly states that the above mentioned *dictum* is merely *obiter*, as can be seen from the last quoted sentences.³⁷⁵ (g) This was an Eastern Division judgment as was the case in *Maswana v R* (*supra*). It follows that the court was bound by the judgment in *Maswana v R*. The court failed to take note of the latter judgment.

7) In *R v Oliver and Others*³⁷⁶ (1921) the facts were that the accused took the complainant’s car with the intention to use it for a joyride and to leave it at a place that would suit them. However, before they had gone very far, the complainant jumped onto his car and brought it to a standstill. The court stated that “[t]he definition of *Van Quisdorp* is superior to that of *Van der Linden* and may be accepted as a definition of theft according to our modern conceptions.”³⁷⁷ (own emphasis). The definition which the court referred to is the following:

“At the present day theft consists in the taking away of a movable thing (*ablatio rei mobilis*) with evil intent (*boshafftes*), where such a taking away is without the knowledge and wish of the person who is the owner of the thing and with the intention to derive some benefit therefrom.”³⁷⁸ (own underlining)

8) *R v Laforte*³⁷⁹ (1922). Until 1922, only the two above mentioned judgments had ruled that *lucri faciendi gratia* was not an element of theft.³⁸⁰ The facts in *Laforte* were briefly that A, a worker of B, removed B’s car and drove away. The accused’s defence argued that A did not have the intention to permanently deprive the owner of his *possessio*. The court stated the following:

“To sum up, the great mass of Roman-Dutch authorities require *lucri causa*, but are prepared to take a somewhat wide view of the meaning of the term ... Many modern commentators on Roman law reject the necessity for *lucri causa*, and it is not required according to the law of Scotland. Such cases as there are in our courts go to show that *lucri causa* is not a necessary element in theft, and this doctrine has been adopted by the Legislature in the Native Territories Penal Code. In these circumstances it seems to

³⁷⁵ Verloren van Themaat 1949:127.

³⁷⁶ 1921 TPD 120.

³⁷⁷ 1921 TPD 120:124.

³⁷⁸ 1921 TPD 120:123-124.

³⁷⁹ 1922 CPD 487.

³⁸⁰ *R v Laforte* 1922 CPD 487:487.

me right to hold that the element of *lucri causa* is not required in theft under our law, and this view is in accordance with modern jurisprudential ideas and with the public interest ... But even if I were of the opinion that *lucri causa* is a necessary ingredient in theft, I should hold that in the present case the taking was *lucri faciendi causa*.³⁸¹

A few observations: (a) Again, this *dictum* is merely *obiter* as can be seen from the last quoted sentence.³⁸² (b) This was the first Cape Division judgment ruling that *lucrum* was not a requirement for the offence of theft. (c) It should be borne in mind that the *Native Territories Penal Code* was based upon the British *Larceny Act*. (d) Note however that section 183 of the *Native Territories Penal Code* (Act 24 of 1886) provided that “[e]veryone commits theft who, having received any money ... on terms requiring him to account for or part the same or the proceeds thereof to any other person, though not requiring him to deliver over in *specie* the identical money, fraudulently converts to his own use”. (own underlining)

9) In *R v Davies*³⁸³ (1928) the Supreme Court of Appeal maintained that conduct will constitute theft “if the prejudice is actual and consists in the deprivation of another of his ownership in property capable of being stolen, and further if the accused *converts that property to his own use*”.³⁸⁴ (own emphasis)

Some observations: (a) Although the court was dealing here with theft by false pretences, the court stated the above to indicate the difference between fraud and theft by false pretences. Therefore we may conclude that the quoted *dictum* also applies to “normal” theft.

10) In *R v Buffel Dikgat*³⁸⁵ (1928) the accused, an employee of the complainant, killed two of the complainant’s sheep with no motive of gaining any benefit from such killings. The court remarked that “[i]t will thus be seen that there is not a vestige of evidence going to show that the accused took the sheep or converted them *to his own use*, which is an essential element in the crime of theft.”³⁸⁶ (own emphasis). Accordingly, the court stated that the evidence did not disclose the offence theft, but instead the

³⁸¹ 1922 CPD 487:493. See also p 499: “To constitute theft it is not necessary that the taking should be *lucri faciendi gratia*.”

³⁸² See *Verloren van Themaat* 1949:128.

³⁸³ 1928 AD 165.

³⁸⁴ 1928 AD 165:170.

³⁸⁵ 1928 GWL 11.

³⁸⁶ 1928 GWL 11:11.

offence malicious injury to property.³⁸⁷

11) In *R v Weiss*³⁸⁸ (1932) the accused was employed by the plaintiff to receive money on her behalf. Instead of handing the money over to her, he deposited it into his own banking account, which was overdrawn. The Supreme Court of Appeal made the following observation: "The presumption of fact is strong that there was a *conversion to his own use*. I am not prepared to go to the length of saying that, in no case where trust money has been paid by a person into an overdrawn banking account, can he give evidence that will discharge *the presumption that he intended to convert the money paid in to his own use* and deprive the owner of his property in it. But, if the accused fails satisfactorily to displace the presumption, the Court is entitled to draw the inference that the crime has been proved."³⁸⁹ (own emphasis). The court found him guilty of theft.

It is abundantly clear that the court was of the opinion that the intention to use the stolen property for own gain (*animus lucri faciendi*) is part of the intent to steal (*animus furandi*).

12) In *R v Maruba*³⁹⁰ (1942) the accused, an employee of the complainant, battered a sheep to its death and left it there. The accused never informed the court why he had done this. The court quoted the definition of theft from Gardiner and Lansdown³⁹¹ and stated: " 'Theft is committed when a person, fraudulently and without claim of right made in good faith, takes or converts to his use anything capable of being stolen with intent to deprive the owner thereof of his ownership, or any person having any special property or interest therein of such property or interest.' Although in this definition two elements of the Roman and Roman-Dutch Law of theft – *furtum usus* and *lucris gratia* – are jettisoned, it can for all practical purposes be considered as setting out the correct position."³⁹² (own emphasis). The court further remarked that:

"Applying this definition to the facts of the present case, I find it difficult to discover sufficient evidence justifying the interference that the accused fraudulently took or

³⁸⁷ 1928 GWL 11:12.

³⁸⁸ 1932 AD 41.

³⁸⁹ 1932 AD 41:42-43.

³⁹⁰ 1941 OPD 51.

³⁹¹ 1939:1350.

³⁹² 1942 OPD 51:53.

converted the sheep to his own use.”³⁹³ (own emphasis)

The court held that the accused was not guilty of theft and considered whether he was guilty of malicious injury to property.³⁹⁴ The court maintained that the accused had “destroyed the sheep wrongfully, unlawfully and maliciously and [thus] he is guilty of” malicious injury to property.³⁹⁵

Some comments: (a) The court found the accused not guilty of theft in that he did not appropriate the sheep for his own benefit. This seems to indicate that the court regarded *lucri faciendi gratia* as an element of theft.³⁹⁶ This is corroborated by the court’s remarks concerning the definition of theft provided by Gardiner and Lansdown. This boils down, it is submitted, to the fact that the accused lacked a theftuous intent in that he did not take the dead sheep for his own gain. (b) The court emphasised appropriation as taking something from the owner. Therefore, even though the accused obviously had the intention to deprive the owner of the benefits of his ownership when he killed the animal, the court still found him not guilty of theft.³⁹⁷

13) In *R v Rautenbach*³⁹⁸ (1943) the facts were that the plaintiff offered a reward to anyone who managed to bring the culprits, stealing his sheep, to book. The accused (an employee) slaughtered one of the plaintiff’s sheep, planted the carcass in the stable of another employee, secured the latter’s arrest and claimed the reward from his employer. The court stated that there had been an unlawful and fraudulent taking of another’s property by the accused.³⁹⁹ The court continued to state that:

“In the present case the accused may have been animated by spite, excessive and unscrupulous zeal, a suspicion that Sebi was indeed a thief and a determination to see justice done even on fabricated evidence or, in the last resort, a desire to win the prize. In the last instance only would the deed be one performed *lucri faciendi gratia*, but not in the sense contemplated by the law since there is a break in the chain of causation between the thing taken and the consequent advantage secured for the taker or for another. In any event he sacrificed his employer’s animal in the interests of the owner. Whichever of these conceivable motives actually prompted the act renders it

³⁹³ 1942 OPD 51:53.

³⁹⁴ 1942 OPD 51:54.

³⁹⁵ 1942 OPD 51:55.

³⁹⁶ Verloren van Themaat 1949:129.

³⁹⁷ Verloren van Themaat 1949:129.

³⁹⁸ 1943 OPD 60.

³⁹⁹ 1943 OPD 60:60.

reprehensible and even criminal, but does not support the concept of theft. 'In truth,' says Ulpian, D. 47.2.39. 'a person who takes away or conceals the female slave of another to have her as his light of love is not guilty of theft; for the deed itself is not decisive; intention (*causa faciendi*) is the test. In his case lust motivated the taking, not furtive intent.'⁴⁰⁰ (own underlining)

Some observations have to be made: (a) the court clearly confirmed *lucrum* as an element of theft.⁴⁰¹ (b) The facts clearly constitute malicious injury to property, but the question remains whether the accused's conduct amounts to theft: (i) the accused definitely had the intent to benefit himself by killing the animal so as to receive a reward for the arrest of someone else and (ii) the accused also acted *animus furandi* in that he had the intent to deprive the owner of the benefits of his ownership rights (*possessio*) permanently. However, (iii) he did not appropriate the property for himself. Accordingly, it is submitted that the accused's conduct did not constitute theft.

14) In *R v Bazi*⁴⁰² (1943) the facts were that the accused bought two tyres from A. A few days later he acquired the knowledge that the tyres were stolen property and that the police were investigating the matter. He removed the tyres from his car, took it to a native woman and asked her to keep it for him. The court stated that "the crime of theft is committed when all the elements coincide i.e. the *fraudulosa contrectation* with ... the *animus lucri faciendi* and the interference with the rights of the *dominus*."⁴⁰³ This was an Eastern Division judgment where the court clearly did not regard itself bound by the previous Eastern Division judgments.

15) In *R v Harlow*⁴⁰⁴ (1955) the facts were that a director took his company's money and used it to obtain goods, that were in short supply, for the benefit of the company. The court stated that "[h]e appropriated the tobacco and/or the proceeds and the question is to what use did he appropriate the tobacco or the proceeds. If his explanation may reasonably be true, he certainly did not appropriate the proceeds to his own use ... *he used these monies – not for himself – but for the benefit of the company*, though he did so without the approval of the Board."⁴⁰⁵ (own emphasis). In a separate judgment Roper J stated that "[a]cts may be done without the consent or

⁴⁰⁰ 1943 OPD 60:61.

⁴⁰¹ Verloren van Themaat 1949:130.

⁴⁰² 1943 EDL 222.

⁴⁰³ 1943 EDL 222:224-225.

⁴⁰⁴ 1955 3 SA 259 C.

⁴⁰⁵ 1955 3 SA 259 C:262E-G.

against the wish of the owner which will not amount to theft if the motive is not to steal the property in question."⁴⁰⁶

A few remarks: (a) It is apparent from this judgment that the court did not consider the accused to be guilty of theft in that he did not use the money for his own benefit and thus *lucri faciendi gratia* was absent. It is submitted that the judgment is correct in that the accused's patrimony was not increased by his conduct; put otherwise: there was no self-enrichment.⁴⁰⁷ (b) Furthermore, the accused had no intention to benefit from his acts.

16) In *R v Kinsela*⁴⁰⁸ (1961) the facts before the Cape High Court were briefly that an officer of the South African Defence force decided to improve the conditions of the camp. He obtained possession of a number of articles belonging to the Defence Force (Government) and without the authorisation of the owner and with knowledge that no authorisation would be given for their sale (for the purposes intended by him), nevertheless sold these articles to third persons in order to raise money for improving the camp. The court accepted that the accused's motive was to raise money for the improvement of the camp and, in the *bona fide* view of the appellant, to the benefit of the owner.⁴⁰⁹ The accused averred that his conduct did not constitute theft in that "he intended to use the proceeds, not for himself, but for what he conceived to be the benefit of the owner."⁴¹⁰ In other words, he lacked *lucri faciendi gratia*.

The court stated that the accused's defence referred to his motive. In *R v Sibiya*⁴¹¹ the Supreme Court of Appeal had maintained that the prosecution was only required to prove that "the thing [was] taken without belief that the owner (where it is the owner whose rights have been invaded) had consented or would have consented to the taking but also that the taker should have intended to terminate the owner's enjoyment of his rights, or, in other words, to deprive him of the whole benefit of his ownership."⁴¹² The court (in *Kinsela*-case) stated that *lucri causa* was not a requirement of theft.⁴¹³

⁴⁰⁶ 1955 3 SA 259 C:264G.

⁴⁰⁷ De Wet en Swanepoel 1985 correctly submits (at 316) that the facts do not constitute theft in that the accused "hom niks toegeëien het nie." [own translation: had not appropriated anything for himself.]

⁴⁰⁸ 1961 3 SA 519 C.

⁴⁰⁹ 1961 3 SA 519 C:524A-D

⁴¹⁰ 1961 3 SA 519 C:525A.

⁴¹¹ 1955 4 SA 247 A.

⁴¹² 1955 4 SA 247 A:257.

⁴¹³ 1961 3 SA 519 C:526C-D.

The court maintained that:

"The 'mental state requisite to constitute theft' does not require that the taker should have the idea of benefiting himself. If he intended to use the property for the benefit of a charitable organisation, his conduct would still be theft. Does the full knowledge that the owner does not and will not consent to being deprived of his ownership make the conduct of the taker any the less theftuous because he intends to apply the proceeds to a purpose which he considers to be of benefit to the owner but of which the owner would not, to his knowledge, approve. In my opinion, the answer is in the negative. The property is deliberately taken out of the ownership of the owner with the intention of depriving him of the ownership. That the taker nourishes a determination to apply the proceeds derived from the sale to what he conceives to be the benefit of the owner makes no difference. In the circumstances of the instant case it seems to me that it is possible to hold that the property was taken and 'converted' to the taker's uses. For once he knew that the purpose to which he proposed to devote the proceeds of the sales would not be acceptable to the owner he was using the property for his own ends."⁴¹⁴

The court also rejected the *Harlow* judgment in that, according to the court, the latter judgment confused motive with the requirement that the accused must have the intent to deprive the company of its ownership.⁴¹⁵ The court stated that the accused's motive is irrelevant.⁴¹⁶ The court found the accused guilty of theft.

Some observations: (a) This case clearly rejects the *lucri faciendi gratia* requirement. (b) The court's ruling is inherently contradictory: the court enunciates that *lucrum* is not a requirement of theft, yet the court stated in its own example (*supra*) "he was using the property for his own ends." (c) It is submitted that the case was erroneously decided in that the facts did not disclose theft: (i) the accused had neither appropriated the property of his employer nor the money from selling such property and (ii) the accused had no intention to enrich himself by means of his conduct. (d) The court failed to do a thorough study of local judgments dealing with the *lucri faciendi gratia*. (e) It is incorrect to state that the accused deprived the owner of his ownership: a thief does not become the owner; he mere deprives the owner of the benefit of his ownership rights. (f) Local courts have interpreted the *lucri* element to entail an

⁴¹⁴ 1961 3 SA 519 C:526E-H.

⁴¹⁵ 1961 3 SA 519 C:527B-E.

⁴¹⁶ 1961 3 SA 519 C:527E-F.

intention to benefit oneself or a third party.⁴¹⁷ Therefore, where A steals money, or property, and gives it to a charitable organisation, his conduct constitutes theft in that he had the intent to benefit a third party, namely the organisation.

17) In *S v Ndhlela*⁴¹⁸ (1964) the court confirmed the *Kinsela* judgment by remarking that:

"This quite clearly, if I may say so with respect, fully justified the learned Judge in coming to the conclusion that, however laudable the accused's motives might have been, he acted at a time when he had full knowledge that he neither had authority nor would obtain authority if he asked for it, and that therefore he could not claim to have acted under any sort of colour of right in disposing of his employer's property."⁴¹⁹

18) In *S v Dreyer*⁴²⁰ (1967) the appellant forged certain documents to ensure that civilians exercising certain "police duties" were paid for the services they rendered to the police. The appellant did this, not to benefit himself, but "to provide staff to carry out essential duties at a remuneration".⁴²¹ The court warned against confusing intent with motive: "Assuming that the appellant's motives were to benefit the authorities and not himself, his intention was nonetheless to cause these persons to receive payments to which they were not entitled; or, to put it another way, to cause payments to be made to the prejudice of the payer, which would not have been made but for his deliberate false pretence ... Whatever the appellant's ulterior intent or motive may have been, therefore, I am satisfied that his immediate intent was fraudulent".⁴²² The court found the accused guilty of theft.

It is submitted that the accused should rather have been prosecuted for, and convicted of, fraud. This case can be distinguished from the *Kinsela* case in that in the latter case the accused used the money for the benefit of his employer (the owner) whereas in this case the accused defrauded the government in order to remunerate "employees". Therefore the accused had the necessary intent to benefit third parties by his fraudulent conduct and it follows that *lucri gratia faciendi* was present.

⁴¹⁷ See *R v Dier (supra)*; *S v Nel (infra)*.

⁴¹⁸ 1964 4 SA 703 N.

⁴¹⁹ 1964 4 SA 703 N:705H-706A.

⁴²⁰ 1967 4 SA 614 E.

⁴²¹ 1967 4 SA 614 E:619C-D.

⁴²² 1967 4 SA 614 E:619F-G & 620A-B.

19) In *S v Nel*⁴²³ (1970) the accused found a tame rabbit underneath a car. The accused (an animal lover) played with it and took it home with him. He could not care for it, so he gave it to A. The owner of the rabbit subsequently accused him of theft. The court stated:

"The magistrate, however, did not in my judgment give sufficient weight to the vital element in the crime of theft, namely, *animus furandi*. The onus rested upon the State to prove beyond reasonable doubt not merely the taking of the animal, but a taking with the intention of depriving the owner of his property therein ... There is first of all the appellant's own evidence, which was to the effect that he did not have the intent required to support the crime of theft. His attitude was that he would have been only too happy to give the animal back to its owner, but he said that he had no idea where the owner might be and he didn't have the time nor was he willing to make extensive enquiries ... He, therefore, according to his own evidence, decided to take the rabbit, not because he wanted it, but in order to protect it ... But what is more important than what he said was what he did, because the actions of the appellant were such that quite clearly he had *neither the intention nor the desire to keep the animal for himself* ... It is I think abundantly clear that the appellant at no stage acted in relation to the rabbit with a *desire to acquire it for himself or to benefit himself, or with a desire to benefit anyone else*. His motive was to find it a home ... Here the distinguishing feature is that the appellant did not want the rabbit for himself, and although he acted unwisely and foolishly, in such a manner that the owner might well have lost her ownership, that, on the record read as a whole, was not his intention. If there is any doubt in that regard, the appellant is entitled to the benefit of that doubt, and in my judgment the conviction cannot stand."⁴²⁴ (own emphasis)

It is clear from this judgment that the court squashed the conviction because the accused had no intention to benefit himself or anybody else, but merely protected and cared for the rabbit.

20) As an example of a recent court case dealing with theft we may take notice of *S v Visagie*⁴²⁵ (1991). The facts were that the accused was an estate agent. Without authorisation from her employer or from her customers, she took the money they deposited with her (intended for the account of her employer) and deposited it in her own account, converting a debit balance (i.e. she owed the bank money) into a credit

⁴²³ 1970 4 SA 440 T.

⁴²⁴ 1970 4 SA 440 T:441E-443D.

⁴²⁵ 1991 1 SA 177 A.

balance. When the specific properties had to be transferred, she credited from her own account the purchasers' accounts with the full deposit plus interest. Therefore nobody suffered any financial harm or prejudice due to her conduct. The Supreme Court of Appeal accepted for the purpose of the judgment that the accused throughout intended to pay the deposited amounts, plus interest, to the purchasers.⁴²⁶ The court noted that the accused had appropriated the cheques for herself: "In die onderhawige geval het die appellant 'n toe-eieningshandeling verrig deur, teenstrydig met haar verpligting om die kopers se tjeks in Terra Trust te stort, die tjeks in haar eie persoonlike rekening te deponeer."⁴²⁷ The court maintained that she was guilty of the theft of the particular cheques:

"Storting deur die appellant in haar persoonlike bankrekening van die tjeks wat vir Terra Trust se trustrekening bestem was, kom op 'n doelbewuste toe-eiening van die tjeks deur die appellant neer wel wetende dat dit ongeoorloof was. Sy kon dus aan die diefstal van die tjeks as sodanig skuldig bevind gewees het."⁴²⁸

With regard to the question whether she was guilty of the theft of the proceeds of the cheques (she was in fact charged with theft of the proceeds of the cheques and not of theft of the cheques as such) the court stated that:

"Toe die appellant die tjeks in haar bankrekening gestort het, het sy die opbrengs van die tjeks bewustelik vir haarself toegeëien en dit aangewend, waar haar rekening oortrokke was, *vir die betaling van haar skuldeiser (Volkskas Bank), en tot die mate dat daar 'n kredietsaldo was, vir haar eie gebruik.* Haar optrede in dié verband kom, volgens die beslissings van hierdie Hof waarna verwys is, op diefstal neer van die geld wat die tjeks verteenwoordig het."⁴²⁹ (own emphasis)

⁴²⁶ 1991 1 SA 177 A:181G-H & 183C-D.

⁴²⁷ 1991 1 SA 177 A:181I-J. [own translation: In the case under consideration the appellant appropriated the checks, contrary to her obligation to pay the cheques into Terra Trust, by depositing the checks into her own personal account.]

⁴²⁸ 1991 1 SA 177 A:183G-H. [own translation: Depositing the cheques destined for the trust account of Terra Trust by the appellant into her personal bank account, constitutes an intentional appropriation of the cheques by the appellant, knowing that it was unlawful. Consequently she could have been found guilty of the theft of these cheques.]

⁴²⁹ 1991 1 SA 177 A:183I-184A. [own translation: When the appellant deposited the cheques into her bank account, she appropriated the proceeds of the cheques for herself and used it, when her account was in debt, for the payment of her creditor (Volkskas Bank), and as far as a credit balance existed, for her own use. Her conduct, according to the judgments which this Court was referred to, constitutes theft of the money that the cheques represent.]

The court subsequently found her guilty of theft. Some observations need to be made: (a) the court nowhere referred to *lucri faciend gratia*. However, it is clear that from the last passage quoted that the court referred to the "gain" which the accused procured by depositing the money in her account and not directly into her employer's account. (b) Therefore it is my submission that courts do not generally refer (or for that fact require explicitly) that the alleged thief must have an intention to gain any benefit or profit from his or her unlawful conduct. Generally speaking, when the thief has *animus furandi*, he also intends to procure some advantage either for himself or a third party by committing the offence. It is only when a court entertains doubt whether the accused's conduct constitutes theft that the court will specifically refer to *lucri faciendi gratia* as a requirement. It may even be contended that *lucri causa* is included in *animus furandi* and that it was only when the courts were uncertain whether such an intent was present (when the accused committed the theft) that the courts looked at the intention of the accused, as evidenced by the objective facts as well as the accused's submissions. (c) The court only mentioned "toe-eiening" and "toe-eieningsopset" without ever referring to the intention to deprive the purchasers of their property.

21) In *S v Nedzamba*⁴³⁰ (1993) the accused stole two cheques and thereafter made out one cheque to cash and presented it to the bank in order to withdraw R960 from the complainant's account. The question arose whether the defence of *de minimis non curat lex* was available because the two cheques, as such, were of little value. The court indicated that where someone scribbles something on a blank cheque leaf in order to remember something, and later on destroys the piece of paper, the rule applies; but not in the present case where the stolen cheques were used to defraud the bank.⁴³¹ The court went on to state that "[w]here in the first example above, the cheque was obviously *not taken for purposes of gain*, that was clearly the purpose in the present matter."⁴³² It is, therefore, clear that this court posed *lucrum* as an element of theft.

B) Conclusion

Therefore, it is concluded that authority exists to submit that the law requires the following for conduct to constitute theft: the alleged thief must have appropriated the

⁴³⁰ 1993 1 SACR 673 V.

⁴³¹ 1993 1 SACR 673 V:676h-j.

⁴³² 1993 1 SACR 673 V:676j. Own emphasis.

object with a view to benefit or some gain. The term *lucrum* should be understood as follows: self-enrichment or increasing your patrimony (“*vergroting van vermoë*”) or gaining an advantage for yourself or someone else.⁴³³ Verloren van Themaat maintains quite convincingly that -

“die vereiste van *lucri faciendi gratia* [is] noodsaaklik om tussen diefstal en opsetlike saakbeskadiging te onderskei. Die vereiste van ‘intent to deprive the owner’ is hiervoor nie bevredigend nie want in baie gevalle van opsetlike saakbeskadiging (b.v. deur 'n skaap of bees dood te maak) bestaan daar wel 'n ‘intent to deprive the owner of the benefits of his ownership’. Ons regsgevoel sê ons egter dat sodanige doodmaak van 'n skaap of bees nie diefstal is nie tensy die oogmerk om voordeel daaruit te verkry aanwesig is.”⁴³⁴

⁴³³ Verloren van Themaat 1949 defines *lucrum* as follows: “Die opset om wins te behaal, as die tipiese kenmerk, wat diefstal van ander misdade onderskei, is net soos in die Romeinse reg deur ons skrywers ruim opgeneem. Dit was nie nodig dat die opset van die dader op direkte en oombliklike behaal van wins gerig was nie. Die dief wat 'n saak steel om dit as geskenk weg te gee, was nog skuldig, omdat hy moontlik wins kon kry uit die dankbaarheid van die ontvanger. Daarenteen is 'n *contractatio teneinde* 'n ander te benadeel sonder dat die dader self 'n voordeel daaruit kry of uit brooddronkenheid of dardelheid, of om iemand daardeur te beledig of in sy eer aan te tas, geen diefstal nie. Ons insiens toon Rautenbauch se saak aan wat die vereiste behoort te omvat, nl. die opset om *direkte* voordeel vir die dief self of iemand anders uit die hantering van die saak te behaal. Hierdie voordeel hoef nie noodsaaklikerwys op die vermoë betrekking te hê nie maar die voordeel moet direk wees ... Maar om die saak weg te neem bloot om iemand te hoon of te benadeel of uit brooddronkenheid of dardelheid is geen diefstal nie omdat die opset om voordeel te behaal ontbreek ... Want vereis word 'n *direkte* band tussen die hanteer van die saak en die voordeel wat verkry moet word. Waarskynlik was die bedoeling met die woorde ‘*lucri faciendi gratia vel ipsius rei vel usus ejus possessionisve*’ juis om die vereiste aan te dui dat die oogmerk moet wees om *direk* voordeel te behaal uit die *hanteer* van die *saak*.” (At 131-132). [own translation: The intent to profit, as a typical characteristic, which distinguished theft from other offences, was also interpreted generously by our writers, as in Roman law. It was not required that the intent of the perpetrator should have been aimed at gaining a direct and instant benefit. The thief who stole property to give it away as a gift, was still guilty, in that he could possibly gain a profit from the gratitude of the receiver. Contrary, the *contractatio* to prejudice another without the perpetrator benefiting from such conduct or as a result of intoxication or to offend someone by means of such conduct or to infringe his honour, did not constitute theft. The Rautenbauch case indicates what the requirement should encompass, namely the intent to obtain a direct benefit for the thief or someone else by handling the property. The benefit does not necessarily have to relate to patrimony, but the benefit must be direct ... However to remove the property to merely spite or prejudice someone or as a result of intoxication does not constitute theft in that the intent to profit is lacking ... because a direct link is required between handling the property and the benefit obtained therefrom. Probably the intention with the words ‘*lucri faciendi gratia vel ipsius rei vel usus ejus possessionisve*’ was to indicate that the aim must be to obtain a direct benefit from handling the property.]

⁴³⁴ Verloren van Themaat 1949:128. See also p 130. [own translation: the requirement of *lucri faciendi gratia* is necessary to distinguish theft from malicious injury to property. The requirement of ‘intent to

Many commentators quote the following *dictum* of the Supreme Court of Appeal in *R v Von Elling*⁴³⁵ in support of the contention that *lucrum* is not a requirement of theft: "Nor is it a defence that Von Elling apparently had no personal financial interest in the car."⁴³⁶ The court was not dealing with theft but with receiving stolen property knowing it to have been stolen.

3.1.3. Theft of Credit

Whenever one deposits money at a bank, the bank becomes the owner thereof, and one merely retains a personal right against the bank for the money deposited. In other words, a debtor-creditor relationship comes into existence.⁴³⁷

For this reason, the Supreme Court of Appeal in *S v Kotze*⁴³⁸ remarked that, when an employee (or agent) withdraws money from his employer's (principal's) bank account and subsequently uses that money for his own unauthorised private purpose, it amounts to a diminishing of the employer's/principal's personal rights, and this would further amount to the -

"erkenning van diefstal van onliggaamlike sake ... 'n gevolgtrekking wat teenstrydig sou wees met die mening van feitlik al ons ou skrywers."⁴³⁹

However the Supreme Court of Appeal further stated that:

"Sonder om die oortuigingskrag van hierdie benadering enigsins te onderskat, moet die werklikhede van die posisie ... egter ook nie oor die hoof gesien word nie. Inderdaad verloor die Bank geen geld deur die beskuldigde se oneerlike optrede nie ... In teenstelling, word die prinsipaal wel deur die beskuldigde se optrede skade berokken want, sodra die gewraakte tjeks teen die prinsipaal se rekening gedebiteer word, word die waarde van die *prinsipaal se regte teen die Bank* deur die bedrag van die betrokke

deprive the owner' is not satisfactory because in many instances of malicious injury to property (e.g. by killing a sheep or an ox) an 'intent to deprive the owner of the benefits of his ownership' is present. Our legal sense tells us that such killing of a sheep or an ox does not constitute theft unless there's an aim to profit.]

⁴³⁵ 1945 AD 234.

⁴³⁶ 1945 AD 234:251.

⁴³⁷ *S v Kotze* 1965 1 SA 118 A:124H; *S v Kearney* 1964 2 SA 495 A:502-503.

⁴³⁸ 1965 1 SA 118 A.

⁴³⁹ 1965 1 SA 118 A:125D-E. [own translation: recognition of the theft of incorporeal property ... a conclusion that would be contrary to the views of virtually all our old authorities.]

tjek verminder of, in die geval van 'n oortrokke rekening, word die prinsipaal se skuld aan die Bank deur daardie bedrag vergroot. In hierdie sin is die prinsipaal, *al is hy nie eienaar van die geld in sy bankrekening nie, inderdaad 'n persoon met 'n 'special property or interest'* daarin binne die betekenis van daardie woorde in Gardiner and Lansdown, 6de uitg. band 2 bl. 1562, se omskrywing van diefstal, wat deur WATERMEYER, H.R., in R v Von Elling, 1945 AD 234 op bl. 236, as 'the ordinary accepted definition of the crime of theft' beskryf is.⁴⁴⁰ (own emphasis)

However, the court dealt with the case as follows: the employee had control over his employer's bank account and this relationship between employee and employer amounted to a trust/fiduciary relationship.⁴⁴¹ Whenever the person holding money in trust misuses it he is guilty of theft.⁴⁴²

It thus appears that the court viewed the theft of personal rights (under given circumstances) as constituting theft. Some commentators are of the opinion that the court tacitly confirmed that intangible property, such as personal rights, could be stolen.⁴⁴³ It further seems that the court called these personal rights "special property or interest".

3.1.4. Theft of electronic data/credit

Keeping in mind the general principles as well as the principles regarding the theft of money as enunciated above, the question whether the theft of electronic information (data) and electronic money is possible in terms of the South African criminal law is now discussed. This study deals with three elements of theft, namely corporeal object, intent to appropriate (which includes the intent to permanently deprive the owner of the

⁴⁴⁰ 1965 1 SA 118 A:125E-H. [own translation: Without in anyway underestimating the persuasiveness of this approach, the reality of the position must ... not be overseen. The Bank does not lose any money by means of the accused's dishonest conduct ... Contrary, the principal is prejudice by the accused's conduct in that, as soon as the cheques in question are debited against the principal's account, the value of the principal's rights against the bank are diminished by the amount of the cheques in question, or in the case of an overdraft account, the principal's debt to the Bank is increased by such amount. Therefore the principal, even though he is not the owner of the money in his own bank account, is after all a person with a 'special property or interest' within the definition of theft as stated in Gardiner and Lansdown's, 6th ed. vol 2 p. 1562, which is described by WATERMEYER, C.J., in R v Von Elling, 1945 AD 234 on p. 236, as 'the ordinary accepted definition of the crime of theft'.]

⁴⁴¹ 1965 1 SA 118 A:123G & 126C-D.

⁴⁴² 1965 1 SA 118 A:126D-E & 127F-H.

⁴⁴³ Coetzee 1970:374.

enjoyment of his ownership rights as well as the intent to exercise such rights) and appropriation, separately. Furthermore, the effect that *lucri faciendi gratia*, as an element of theft, has on computer-related crimes is also observed.

3.1.4.1. Corporeal object

The first question that needs to be addressed is whether the unlawful appropriation of electronic information, data or credit constitutes theft, seeing that it is an intangible asset.⁴⁴⁴

Some courts have been reluctant to extend the common law crime of theft to incorporeal objects. For instance, in *S v Mintoor*⁴⁴⁵ the accused was found guilty in a magistrate's court of the theft of 901 electricity units.⁴⁴⁶ The accused was not charged with contravening the *Electricity Act*.⁴⁴⁷ The case went on review to the High Court and the question arose whether electricity could be the object of theft? The court stated that the legislature made it an offence to use electricity without authorisation, by enacting the *Electricity Act*. Furthermore, the court maintained that:

"Dit is dus onnodig om die gemenereg op die onderhawige punt uit te brei. In die algemeen gesproke, is dit in elk geval juridies ongesond om die trefwydte van ons strafreg deur Hofbeslissings te vergroot. Die uitbouing van strafregtelike sanksies is 'n taak wat normaalweg aan die Wetgewer oorgelaat word om te verrig indien en insoverre hy dit nodig ag."⁴⁴⁸

The court set the judgment aside. From reading the court case, it seems that in the end the court found the accused not guilty because electricity was not a corporeal

⁴⁴⁴ See Van der Merwe 2000:133.

⁴⁴⁵ 1996 1 SACR 514 C.

⁴⁴⁶ Unfortunately, the judgment does not inform the reader of what the accused did, but it can be presumed that he (at least) used electricity without paying for it.

⁴⁴⁷ Act 41 of 1987.

⁴⁴⁸ 1996 1 SACR 514 C:517A-B. [own translation: It is, therefore, unnecessary to extend the common law with regard to this issue. Generally speaking, it is judicially undesirable to extend the parameters of our criminal law by means of judicial judgments. The extension of criminal sanctions is normally left to the discretion of the Legislature.] See also *S v Augustine* 1986 3 SA 294 C where the court remarked (at 302I-J) that "[t]here are always people to be found who invite and favour 'extensions' by the Court of the existing principles of the common law to encompass situations which they feel 'should' be encompassed, even if they have not hitherto been so encompassed. I do not think the Courts should respond too readily to such invitations. Fundamental innovations of this kind are for the Legislature (if so advised) and not the Courts."

object. See p 517D-E where the court stated that “[m]et water en gas, wat in die besit van iemand is, het ek nie 'n probleem nie, omdat dit as stoflike sake beskou kan word. Anders as elektrisiteit, bestaan water en gas immers as spesifieke sake”⁴⁴⁹ as well as p 517F where the court remarked that: “is dit duidelik dat [elektrisiteit] nie as stoflike of liggaamlike sake beskryf kan word nie.”⁴⁵⁰

Foreign courts also support a similar line of reasoning as the court in *S v Mintoor*. In the Canadian case *R v Stewart*⁴⁵¹ the court held that information was not property for the purposes of criminal law.⁴⁵²

On the other hand, some local courts have been willing to give effect to the economic reality and extended the crime of theft to incorporeal objects. In *S v Harper*⁴⁵³ an interesting scenario arose: the accused (a director of a company) transferred A's shares in company Z to B, without A's authorisation. The accused was subsequently charged with theft of A's shares.⁴⁵⁴ It must be remembered that shares constitute incorporeal movable property.⁴⁵⁵ The court stated that “the question [is] whether incorporeals can in law be the subject of theft.”⁴⁵⁶ The court remarked the following:

“[D]espite what is said in *Kotze's* case at 125D-E, the Appellate Division did, with respect, in effect decide that a conviction of theft of an incorporeal is, in the case of a credit balance, permissible in our law. In principle there seems no reason why it should not be.”⁴⁵⁷

Furthermore, the court stated that where someone wrote something to his advantage on the credit side in another's book, it amounted to credit being stolen.⁴⁵⁸ The court continued to state that “once the Courts have moved away from the requirement of a physical handling, then the reason for saying that there can be no theft of an

⁴⁴⁹ [own translation: With water and gas, in the possession of someone, I have no problem, in that it can be regarded as corporeal property. Unlike electricity, gas and water exist as specific property]

⁴⁵⁰ [own translation: it is clear that electricity cannot be described as corporeal or tangible property.]

⁴⁵¹ 1988 1 SCR 963; 1988 50 DLR (4th) 1 SCC.

⁴⁵² Unfortunately this case was not available locally so Hammond 1988:527 *et seq* had to be relied upon.

⁴⁵³ 1981 2 SA 638 D.

⁴⁵⁴ 1981 2 SA 638 D:664G.

⁴⁵⁵ 1981 2 SA 638 D:664G.

⁴⁵⁶ 1981 2 SA 638 D:664G-H.

⁴⁵⁷ 1981 2 SA 638 D:666E. Snyman 1999 is also of the opinion that in such instances an incorporeal thing is stolen. (At 494).

⁴⁵⁸ 1981 2 SA 638 D:666G-H.

incorporeal in any circumstances would seem to have fallen away. In fact this is clearly recognised by the decision of the Appellate Division in *S v Graham*⁴⁵⁹.

The court found the accused guilty of theft in that he “assumed [A’s] rights in respect of the shares in the first place and excluded him from benefits of those rights in the second place. He therefore appropriated the shares to himself or for the benefit of himself and his company”⁴⁶⁰.

From the above it becomes evident that the courts have explicitly recognised the appropriation of personal rights⁴⁶¹ as constituting theft. In view of this court case, it may be inferred that when a *hacker* penetrates the security system of a bank or a creditor and causes an electronic entry to be made in the credit side of the bank’s or creditor’s electronic accounting system, he is guilty of theft. This line of thinking is accentuated by the following judgments.

In *R v Sibiya*⁴⁶² (1955) the Supreme Court of Appeal stated that:

“Nowadays in cases of theft we are apt to look at the economic effect of the act by which a person fraudulently converts value to his own use rather than be hypnotised by the concrete mechanics by means of which the crime is committed.”⁴⁶³

The facts in *S v Graham*⁴⁶⁴ (1975) concerned a double payment by mistake. The second payment was made by cheque and the accused knew that the second payment was not due to him. The trial judge convicted the accused of the theft of R37 000. The question of law was whether this conviction was correct or whether it should have been the theft of a cheque of R37 000.⁴⁶⁵ The Supreme Court of Appeal put it as follows:

“The first question is whether the proceeds of the cheque, not being money in the corporeal sense, can be the subject of a charge of theft. It may well be that, strictly according to Roman-Dutch law, only corporeal things were capable of being stolen ... *However, the Roman-Dutch law is a living system, adaptable to modern conditions ... And so it has evolved that this Court has come to regard money as being capable of*

⁴⁵⁹ 1981 2 SA 638 D:666H.

⁴⁶⁰ 1981 2 SA 638 D:667C.

⁴⁶¹ Shares merely give a shareholder a personal right.

⁴⁶² 1955 4 SA 247 A.

⁴⁶³ 1955 4 SA 247 A:261.

⁴⁶⁴ 1975 3 SA 569 A.

⁴⁶⁵ 1975 3 SA 569 A:576D-E.

being stolen even where it is not corporeal cash but is represented by a credit entry in books of account ... In the result, I hold that it was competent for the trial Judge to convict the appellant of the theft of R37 153,88."⁴⁶⁶ (emphasis added)

In *S v Kimmich*⁴⁶⁷ the accused, as director of company A, concluded a contract with company B to the effect that when the former ceded its claims against its debtors to the latter, the former was under an obligation to (whenever it should receive payment from the debtors, whose debts were ceded to company B) to pay all the cash and/or hand over the cheques to the cessionary. Subsequently some of the debtors furnished cheques to the accused and, in breach of the above-mentioned agreement, he paid the cheques into the bank accounts of his company without transferring the money to the cessionary. The question of law was whether the depositing of, and therefore the appropriation of, the incorporeal proceeds of the corporeal cheques into company A's accounts constituted theft.⁴⁶⁸

It can be argued that, in effect, the accused stole the complainant's personal rights ("*vorderingsregte*"), as embodied in the cheques furnished by the debtors to the accused, which the complainant enjoyed against the debtors, whose debts were ceded to it by company A. The court maintained that:

"All rights flowing from the cheques as corporeal movables and as negotiable instruments were as between the company and MIC intended to accrue to the latter. The company, by not having handed the cheques over to MIC and by having paid them into its own bank accounts, arrogated [appropriated] to itself the rights that adhered thereto and not only appropriated them as corporeal objects but also the proceeds thereof by having utilised the same to defray its financial obligations."⁴⁶⁹

The court concluded by stating that:

"To the extent that it is permissible in cases of theft to have regard to the economic effect, rather than the concrete mechanisms by which the crime is committed ... the company's said conduct resulted therein that it obtained a benefit of R103 893,97 which should, and would have, accrued to MIC had it not paid the cheques in question into its own bank accounts."⁴⁷⁰

⁴⁶⁶ 1975 3 SA 569 A:576E-577C.

⁴⁶⁷ 1996 2 SACR 200 C.

⁴⁶⁸ 1996 2 SACR 200 C:210C-E.

⁴⁶⁹ 1996 2 SACR 200 C:209I-210A.

⁴⁷⁰ 1996 2 SACR 200 C:210A-C.

And

"Although in terms of the Roman-Dutch law only corporeal things are capable of being stolen ... our Courts have expanded the concept of theft, in respect of money other than physical notes and coins, and have held that a conviction of theft of an incorporeal in the form (a) a diminution of a credit balance in a complainant's bank account ... and (b) the appropriation of the proceeds of a cheque ... is competent in our law. Our Courts furthermore do not appear to have had any difficulty in holding that other incorporeals, such as shares, in contra-distinction to share certificates, are capable of being stolen ... The company, by having appropriated the cheques in question and having paid them into its bank accounts, excluded [the complainant] from the economic benefit of amounts corresponding with the face value thereof. The following decided cases appear to support the proposition that the exclusion of a complainant from the economic benefit could form the subject-matter of a charge of theft: (a) *S v Visagie* ... and (b) *S v Harper and Another*".⁴⁷¹

Keeping the above-mentioned judgments in mind, it may safely be stated that when a *hacker* penetrates a bank's computer network system and transfers credit from A's account to his own account or to someone else's account he is guilty of theft. This is supported by Dreyer who submits that "[w]here the amount which is being stolen is transmitted to a fictitious account, thus creating a credit balance which the criminal can draw at a later stage, it is submitted that the criminal could be charged with theft on the authority of *S v Graham*."⁴⁷² Snyman describes money in the form of credit entries as "economic assets".⁴⁷³

Likewise, it is submitted that where a *hacker* programs a computer program to create false entries in the electronic accounting books of a firm or a bank, such conduct also constitutes theft in that the computer program may be seen as an instrument in the hands of its creator.

Next the following questions, dealing with hacking instances, need to be addressed:

- (1) When a *hacker* penetrates a firm's computer system, copies sensitive files and exits the system, does he appropriate and simultaneously deprive the owner of incorporeal property?
- (2) When a *hacker* penetrates a firm's computer system and deletes the files, is he

⁴⁷¹ 1996 2 SACR 200 C:210E-J.

⁴⁷² Dreyer 1983:537.

⁴⁷³ Snyman 1999:507.

guilty of theft?

Possible answers to both questions:

The courts in *S v Kotze*, *Harper* and *Graham* have explicitly relaxed the requirement that the object of theft must be corporeal in instances where money is involved. The courts did this in recognition of the commercial reality that money was not invariably represented by physical objects, but also by incorporeal objects such as electronic cash/credit and even mere entries in accounting books. It is submitted that the South African courts will, when faced with this problem, recognise the need for a further exception to the general rule that the object must be corporeal in instances where electronic data is involved. Van der Merwe is also a proponent of the idea that incorporeal objects should be recognised as an object capable of being stolen.⁴⁷⁴

Snyman indicates, quite convincingly, that where someone is accused of *furtum possessionis* (A removed his own property from B, where the latter enjoyed a right of retention), it is not really the corporeal thing that is stolen, but B is deprived of his right of retention.⁴⁷⁵

Information stored on a hard disk can constitute immaterial property and thus the legal object of an immaterial property right. The following immaterial property rights are recognised by the South African intellectual property law: copyright, right to a trader's distinctive marks (trade and service marks); right to trade secrets and confidential information;⁴⁷⁶ and the right to goodwill. Accordingly, the following legal objects have been recognised as immaterial (intellectual) property: trade names and trade marks,⁴⁷⁷ goodwill ("*werfkrag*"),⁴⁷⁸ trade secrets and confidential information,⁴⁷⁹ and content

⁴⁷⁴ Van der Merwe 1985:139: "Diefstal van incorporales is 'n werklikheid in ons strafreg en vervul 'n nuttige rol." [own translation: Theft of incorporales is a reality in our criminal law and serves a useful purpose.]

⁴⁷⁵ Snyman 1999:494.

⁴⁷⁶ Van Heerden & Neethling 1995:108-110.

⁴⁷⁷ Van Heerden & Neethling 1995:93-94.

⁴⁷⁸ Van Heerden & Neethling 1995:94; *Weber-Stephen products Co v Alrite Engineering (Pty) Ltd & Others* 1990 2 SA 718 T:744J. It should be kept in mind that goodwill (as immaterial property) is an example of incorporeal property which cannot be stolen but only diminished by an unlawful act. This of course poses no problem in that not all corporeal property can be stolen.

⁴⁷⁹ Van Heerden & Neethling 1995:224. See also *Harchris Heat Treatment (Pty) Ltd v ISCOR* 1983 1 SA 548 T:555E-F; Knobel 1990:492.

which qualifies for copyright protection.^{480 481}

It should be born in mind that immaterial property is incorporeal property according to the law.⁴⁸² Therefore, where content stored on a hard disk is the subject of copyright protection, according to the South African *Copyright Act*,⁴⁸³ such content accordingly constitutes incorporeal property. Furthermore, South African law has recognised both trade secrets and confidential information as legal objects of an immaterial property right to trade secrets and confidential information. Therefore, where a *hacker* copies either copyright protected content or confidential information (which is protected by the law as confidential information and/or trade secrets), he in effect steals the computer user's immaterial (incorporeal) property.

However, it is possible that particular electronic content, stored on a hard drive, does not either constitute the victim's confidential information or form the subject of copyright protection. The question of law thus arises whether such content can constitute a legal object (incorporeal property) in respect of which the computer user enjoys a subjective right.

Commentators generally maintain that the law only confers legal protection upon a personal interest as a legal object, whenever such interest complies with two requirements: "first, the interest must be of value – that is, relatively scarce – to the person concerned; and secondly, it must have such a measure of distinctiveness, definiteness and independence that it is possible to use it, enjoy it and (where possible) dispose of it."⁴⁸⁴ Labuschagne indicates convincingly that economic value should not be set as a requirement for the recognition of legal objects in that some

⁴⁸⁰ Domanski 1993 correctly submits (at 127) that copyright, patents, designs and trade marks are forms of statutory immaterial property.

⁴⁸¹ In *Tie Rack plc v Tie Rack Stores (Pty) Ltd & Another* 1989 4 SA 427 T the court maintained that trade marks concerned the "law of incorporeal property" (at 430B-C) and the court approved (at 443F-G) a passage stating that a business' right to goodwill constituted an "intangible right to property".

⁴⁸² Domanski 1993:138 shares this view by stating that immaterial property constitutes incorporeal property. He states that "[t]he incorporeal property of the undertaking (such as literary and artistic works, inventions, designs, trade marks, trade secrets and 'werfkrag') is protected by an array of statutory and common-law immaterial-property rights."

⁴⁸³ Act 98/1978.

⁴⁸⁴ Van Heerden & Neethling 1995:80. See also Geldenhuys 1993:90, 91 & 95. Geldenhuys is of the same opinion and maintains that the object must be of personal value and that it must serve his personal needs. See Geldenhuys 1993:90. He adds a third requirement at p 93 namely that the

existing legal objects, such as personality property ("*persoonliheidsgoed*"), has no economic value.⁴⁸⁵

The question whether electronic data stored on a computer can form the legal object of a subjective right bears on another question namely what does immaterial property rights such as copyright, patent rights, right to confidential information, etc protect? Put differently, what is the legal object of these rights?

Immaterial property can be explained as follows: say for instance A has copyright on a specific page he wrote. The subjective right is an immaterial "copyright". The page itself is the physical object; the corporeal property. The incorporeal property is the idea or information embodied in the page. However, the words, subject to copyright protection, do not constitute the incorporeal property but the idea, expressed by the words on this particular page. Therefore incorporeal property is the embodiment ("*vergestalting*") of an idea.

This is substantiated by Joubert's statement that "[d]ie basis van enige immateriele regsgoed is 'n idee wat die resultaat is van 'n geesteskepping."⁴⁸⁶ He uses the following examples to illustrate his point of view:⁴⁸⁷

- Patent law protects the idea for trading processes or products where it is novel and unique. This idea is only protected where the patent was registered;
- Model law protects the idea for a container. This idea is protected where the model was registered in terms of the relevant legislation;
- The law of trade marks protects the idea for a specific trade mark. This idea is protected where the trade mark was registered in terms of the relevant legislation or where such mark has become a well-known trade mark; and
- The law of plant breeders' rights protects the idea for the creation of a new plant variety.

Therefore, ideas *per se* are not protected and hence cannot be stolen. Only when the

allotment of the object to a legal subject must be able to serve a constituent community function ("die toedeling van 'n entiteit aan 'n regsobject [moet] 'n gemeenskapsordende funksie kan vervul").

⁴⁸⁵ Labuschagne 1990:561.

⁴⁸⁶ Joubert 1985:35. [own translation: the basis of any immaterial property is an idea which is the result of a mental creation.] Geldenhuys 1993 correctly submits that immaterial property rights, such as copyright, patent rights and the right to trade secrets, are subjective rights on a "specific class" of information / ideas / thoughts ("'n subjektiewe reg op 'n bepaalde kategorie inligting"). See p 98-109

⁴⁸⁷ Joubert 1985:35.

idea is expressed does it constitute incorporeal property. Not all expressions, however, of an idea are automatically protected. The expression of an idea will only be protected when such expression complies either with the relevant legislation or the common law in the case of confidential information and trade secrets. Therefore, it is further submitted that when information/ideas are expressed (embodied) as digital information⁴⁸⁸ ought such expression to be protected by law as incorporeal property. It is no longer merely an idea but an idea embodied/expressed as digital data and stored on someone's hard drive. Put differently, the hard drive is the corporeal property and the subject of ownership rights and the digital data expressing the information, thus an embodiment of the idea, is the incorporeal property. The information is therefore the subject of an immaterial property right and thus constitutes incorporeal property.⁴⁸⁹ It is submitted that the law should not only protect digital data that embodies/expresses confidential information. Keeping in mind an individual's right to privacy in terms of the common law⁴⁹⁰ as well as his constitutional right to privacy, as enshrined in section 14 of the *Constitution*,⁴⁹¹ all digital information stored on his hard drive should be protected by the law.⁴⁹² A similar view is supported by Copeling:

"[i]n the field of immaterial property law it is well accepted that the intellectual product of man's mind is, in the legal sense, just as much 'property' as is the tangible product of

⁴⁸⁸ It can even be called a digital idea.

⁴⁸⁹ Joubert 1958 defines immaterial property (at 133) as "onstoflike produkte van die menslike gees en werkdadighede." [own translation: intangible products of the human mind and creations.] Van Heerden & Neethling 1995 correctly maintain (at 80) that when the law recognises an interest as a legal object, the person concerned acquires a subjective right to the legal object.

⁴⁹⁰ See par 3.9.1.1 of this chapter.

⁴⁹¹ Act 108/1996. S 14 provides that "[e]veryone has the right to privacy, which includes the right not to have (a) their person or home searched; (b) their property searched; (c) their possessions seized; or (d) the privacy of their communications infringed." (own emphasis).

⁴⁹² Geldenhuys 1993 maintains (at 97) that the law may recognise new categories of information as legal objects: "Te aanvang moet daarop gewys word dat die kategorieë [inligting] wat as regsobjekte beskou kan word, geen *numerus clausus* daarstel nie, net soos wat daar geen *numerus clausus* van regsobjekte bestaan nie. Benewens hierdie kategorieë wat reeds erkenning as regsobjekte geniet, kan ander kategorieë inligting in die toekoms ook deur die objektiewe reg erken word". [own translation: At the outset it must be pointed out that the categories [of information] that may be regarded as legal objects constitute no *numerus clausus*, just as there is no *numerus clausus* of legal objects. In addition to the categories that are already recognised as legal objects, other categories of information may in future also be recognised by the objective law.]

his physical skills."⁴⁹³

However, some commentators such as Joubert, are of the opinion that information cannot be incorporeal property in that "so 'n beskouing ... 'n monopolie oor die aanwending van die inligting aan die reghebbende sal verleen."⁴⁹⁴ In *Dun & Bradstreet (Pty) Ltd v SA Merchants Combined Credit Bureau (Cape) (Pty) Ltd*⁴⁹⁵ the plaintiff averred that the "confidential information imparted in 'Credit Records' ... is incorporeal property at common law and that the plaintiff is entitled to be protected against the unlawful use of this property by defendant."⁴⁹⁶ The court maintained that:

"In my view, this claim is unfounded. I do not think that, except in a somewhat loose sense, such information, as distinct from the contractual rights, can be regarded as property at common law; nor do I believe that the plaintiff can found a cause of action upon an alleged invasion of its rights of 'property' in such information".⁴⁹⁷

Yet the court was willing to protect such information as confidential information. It follows that the court was in fact willing to protect such information as immaterial property (a legal object).

South African as well as foreign courts have protected incorporeal property (not constituting incorporeal money/credit):

1) In the United States of America, the court in *International News Service v The Associated Press*⁴⁹⁸ regarded news articles in a newspaper as *quasi* property (between rival newspapers).

2) In *R v Milne & Erleigh*⁴⁹⁹ one of the accused granted, without authorisation, 40 000 shares to himself, without paying for it. The Supreme Court of Appeal found him guilty of the theft of the shares, but stated that it was "unnecessary to express any opinion

⁴⁹³ Copeling 1968:188. Copeling correctly maintains (at 189) that the subject of copyright protection constitutes incorporeal property, by stating that: "It is the productions themselves which, being the object of this proprietary right, constitute, in the legal sense of the word, 'property', albeit immaterial property."

⁴⁹⁴ Joubert 1985:37. [own translation: such a view ... would provide a monopoly to the proprietor over the usage of such information.]

⁴⁹⁵ 1968 1 SA 209 C.

⁴⁹⁶ 1968 1 SA 209 C:215H-216A.

⁴⁹⁷ 1968 1 SA 209 C:216A.

⁴⁹⁸ 248 US 215 (1918). A copy of this judgment can be downloaded from www.law.uconn.edu/homes/swilf/ip/cases/ins.html.

⁴⁹⁹ 1951 1 SA 791 A.

upon the validity of the argument that incorporeals cannot be the subject of theft.⁵⁰⁰

3) In *S v Willcocks*⁵⁰¹ the accused allegedly furnished a computer print-out containing strategic marketing information to his employer's competitor, without the former's consent. He raised the defence that the information (contained in the document) could not be stolen in that incorporeals were not capable of being stolen. The regional magistrate's court held that the information contained in the print-out was capable of being stolen and was convicted of theft.⁵⁰²

Furthermore, it should also be borne in mind that South African courts have maintained that a member's interest in a close corporation constitutes movable incorporeal property.⁵⁰³

It should, in passing, be stated that local courts have, under given circumstances, regarded subjective rights as incorporeal property. The following courts have maintained that subjective rights constitute incorporeal property:

□ in *Du Plessis & Others v De Klerk & Another*⁵⁰⁴ the court observed that a "right of action is a form of incorporeal property."⁵⁰⁵

□ in *MV Snow Delta Serva Ship Ltd v Discount Tonnage Ltd*⁵⁰⁶ the Supreme Court of Appeal maintained that:

"Rights in relation to the (contractual) performance (*obligatio*) of another have since time immemorial been classified as incorporeal. The obligation of the debtor is not property; it is the right (often referred to as the 'action') of the creditor. Obligations can therefore not be attached because they do not form part of the patrimony of the creditor, whereas rights can be attached and do form an asset in the estate of the

⁵⁰⁰ 1951 1 SA 791 A:826A-B.

⁵⁰¹ Regional magistrate court case, no 41/273/83 (Durban).

⁵⁰² This case was not available so Van der Merwe 1987:38-39 had to be relied upon.

⁵⁰³ See *Badenhorst v Balju, Pretoria Sentraal, & Andere* 1998 4 SA SA 132 T:138G-H: "'n Ledebelang in 'n beslote korporasie is 'n onliggaamlike roerende saak ..." [own translation: a member's interest in a close corporation is incorporeal movable property.] The court also maintained (at 139E-F) that the right to such incorporeal property was evidenced by the certificate of member's interest issued in terms of s 31 of the *Close Corporations Act* 69 of 1984 and where such document could not be found, the founding statement represented and proved this incorporeal right.

⁵⁰⁴ 1996 3 SA 850 CC.

⁵⁰⁵ 1996 3 SA 850 CC:866B.

⁵⁰⁶ 2000 4 SA 746 SCA.

creditor.”⁵⁰⁷

□ In *Dun & Bradstreet (Pty) Ltd v SA Merchants Combined Credit Bureau (Cape) (Pty) Ltd*⁵⁰⁸ the court stated that personal rights (“*vorderingsregte*”) flowing from a contract constitutes incorporeal property.⁵⁰⁹

□ In *Hewlett v Minister of Finance & Another*⁵¹⁰ the court also maintained that personal rights constitute incorporeal property. The court merely focused on the other side of the issue by stating that debts (obligations) constitute “property”. The court maintained that:

“As a money debt due by the State to the applicant this was in the ordinary sense of that term ‘property’. As was said by POLLOCK CB in *Queensbury Industrial Society Ltd v William Pickles and Others* (1865) LR 1 Exch 1 at 4 - 5: ‘... “property” is not a term of art, but a common English word, which must be taken in an ordinary sense, and any ordinary person would certainly think it strange, if he were told that a debt due to him was not part of his property.’ It was put even more widely by PEPYS MR in *Jones v Skinner* (1835) 5 LJ Ch 87 at 90: ‘It is well known that the word property is the most comprehensive of all the terms which can be used, in as much as it is indicative and descriptive of every possible interest which the party can have.’”⁵¹¹

Therefore where a *hacker* or a virus copies digital content, stored on A’s hard drive, he appropriates A’s immaterial property rights, which, according to the above judgments, constitute incorporeal property and accordingly such conduct may constitute theft.

In conclusion it is submitted that electronic credit can be the object of theft. It is further submitted that digital content stored on hard drives can be the object of theft.

⁵⁰⁷ 2000 4 SA 746 SCA:753E

⁵⁰⁸ 1968 1 SA 209 C.

⁵⁰⁹ The court stated (at 215G-H): “Moreover, incorporeal property, such as a personal right flowing from contract, also enjoys a measure of protection in that a delictual remedy is available to a party to a contract who complains that a third party has intentionally and without lawful justification invaded his enjoyment of such property by inducing the other party to the contract to commit a breach thereof ... In the present case, however, the plaintiff is not claiming that the defendant has invaded the contractual rights which it enjoys as against its subscribers and thereby disturbed its *rights of property* therein.” (own emphasis).

⁵¹⁰ 1982 1 SA 490 ZSC.

⁵¹¹ 1982 1 SA 490 ZSC:494D

3.1.4.2. Intention to appropriate and *lucrum causa faciendi*

Another element of the offence of theft that needs to be examined is the element that the alleged thief is required to have the intention to appropriate the stolen thing which (as stated above) entails the intention to permanently deprive the victim (owner) of the benefits of his ownership rights as well as the intention to exercise/assume such benefits or rights.

With regard to the postulated question whether a *hacker* that appropriates electronic credit, can be found guilty of theft, it is submitted that when someone electronically transfers credit from A's account to his own account, he has the necessary intention to deprive the owner permanently of his personal rights against the bank and simultaneously to assume ownership rights or the benefits flowing from such rights.

When a *hacker* merely makes a false electronic entry in the accounts of the bank to his own advantage, without moving money from someone else's account to his own, he also commits theft in that he has the intention to deprive the bank of its own money and to assume ownership rights over the money credited to his own account.

Likewise, where a *hacker* uses a computer program to do the above-mentioned acts, he has the necessary intent to deprive the bank or a specific person of its or his "money", or the rights thereto, and to gain control over such electronically stolen credit.

With regard to the postulated example of a *hacker* who penetrates a firm's computer system and deletes the files, it is submitted that where a *hacker* deletes or corrupts information stored on a hard drive or on another electronic medium, he has the necessary intention to permanently deprive the owner of the enjoyment of his ownership rights. Legally speaking, this cannot be distinguished from tearing up pages containing confidential information. As noted above, the fact that such information is electronically stored, should not pose a problem. It should also be kept in mind that the proprietor of confidential information (which the law recognises as protectable confidential information), enjoys an immaterial property right over such information. Likewise, where such information as embodied in the page complies with the requirements of the *Copyright Act*, the proprietor also enjoys an immaterial property right namely copyright. As submitted above, the digital data stored on a computer should also form the legal object of an immaterial property right. Therefore, the *hacker* deprives A of his subjective rights.

We may further argue that the *hacker* had the intention to exercise ownership rights in regard to the information in that one of an owner's "powers" is to delete or to destroy such electronic content.

Where a sinister computer program is designed to cause these results, *dolus indeterminatus* is present in that the computer programmer foresaw that his program, which he intentionally launched onto the Internet with the purpose to delete or corrupt information, could cause such damage. Therefore, it may be argued that he had *dolus indeterminatus* to deprive anybody, who contracted the virus, of their subjective rights over the electronic information. It may further be contended that the computer programmer had *dolus indeterminatus* to exercise control (as one of the benefits of ownership rights) over the information of which he gained control, by deleting/erasing the electronic content.

In both instances where either the *hacker* or the malicious computer program deletes or corrupts the electronic content, the *hacker* or the computer programmer has the intention to permanently deprive the owner of the electronic content of the file.

However, the law requires that the thief must have the intention to enrich himself (or someone else) by means of his act. This requirement is lacking and thus it is submitted that the mere deletion or corruption of electronic files (content) does not constitute theft. However, as will be indicated later on, such conduct constitutes malicious injury to property. Where a competitor deletes or corrupts files in order to cause the proprietor of the information (e.g. his rival) financial losses, it can be argued that *lucri faciendi gratia* is present in that the conduct entails some gain/advantage for him.

With regard to the postulated scenario where a *hacker* penetrates a firm's computer system and merely copies electronic content, without deleting such content, the question arises whether the mere unlawful copying of information, without deleting such information, constitutes the necessary intention to deprive the owner permanently of his electronic content or the enjoyment of such digital content as well as the intention to assume ownership rights over such electronic content? Stated differently, does electronic espionage constitute theft?

The *hacker* clearly has the intention to exercise ownership rights over the electronic copy that he made and it should be kept in mind that the electronic copy is identical to

the original electronic file.⁵¹² It can further be argued that the *hacker* has the intention to temporarily deprive the proprietor of his control of electronic content in that when the *hacker* made the electronic copy the proprietor temporarily lost control over the digital file: the proprietor could not prevent the *hacker* copying the electronic content. It is submitted that our courts should give effect to the economic reality and stipulate that the intention to temporarily deprive the owner of the benefits of his ownership rights (control) by making an electronic copy and the intention to exercise control over the electronic copy suffices for the purposes of theft.^{513 514}

It can furthermore be argued that the *hacker* has the intention (either *dolus directus* or *dolus eventualis*) to appropriate the file's electronic content and to exclude the proprietor from (some of) the benefits of his file's electronic content: where the *hacker* copied electronic confidential information such information will no longer be recognised by the law as "confidential information" and thus the proprietor will in effect be deprived of an immaterial property right. In other instances where a proprietor enjoys another immaterial property right to the electronic content (for instance copyright or a possible right to his digital content) the *hacker* has the intention to diminish the proprietor's subjective right by making unlawful copies.

The same reasoning applies where a computer programmer instructs a computer program to merely copy electronic content: he has the intention to exercise/assume the benefits which the owner enjoys over the electronic content and he also has the intention to temporarily deprive the owner of control over the electronic content and to deprive the owner of the benefits which he enjoys in regard to such content. Where electronic content is copied, both the *hacker* or the computer programmer has the intention to benefit from his own conduct.

⁵¹² In fact, the copy cannot be distinguished from the original file.

⁵¹³ In *S v Mtshali* 1960 4 SA 252 N the court maintained (at 254G-H) that "[t]ermination of an owner's enjoyment of rights connotes a reasonable measure of permanency. An intention to suspend temporarily such enjoyment ... excludes a conviction for theft. Each case must turn on its own facts. The question of permanency may often be one of degree, in relation to such matters as the durability of the thing taken and the contemplated period of retention."

⁵¹⁴ The following word of caution by the US 9th Circuit Court of Appeal in *Brookfield Communications Inc v West Coast Entertainment Corp* 174 F.3d 1036 (9th Cir 1999) is worth noting: "We must be acutely aware of excessive rigidity when applying the law in the Internet context; emerging technologies require a flexible approach." (At par 13).

Finally, it should be emphasised that in *S v Visagie*⁵¹⁵ the Supreme Court of Appeal merely referred to appropriation and intent to appropriate, without referring to an intent to deprive the owner of the benefits of his ownership. When we apply this *dictum* to the postulated scenarios it may be concluded that where a *hacker* copies electronic data or a computer programmer instructs a computer program to copy electronic content he has the intention to appropriate the benefits of the electronic content. Of necessity, *lucri causa faciendi* is also present.

3.1.4.3. Appropriation

The question that needs to be answered is whether appropriation of electronic credit and/or information constitutes theft?

With regard to the postulated scenario of a *hacker* who transfers electronic credit or creates false electronic accounts, it may be stated that whenever a *hacker* transfers credit (electronic "money") from A's account to his own, A is deprived of his personal rights against the bank and the *hacker* gains control over such rights. Where a *hacker* merely makes a false electronic entry in the bank's financial statements, he deprives the bank of its funds and simultaneously gains control of such funds.

Where a *hacker* penetrates a firm's computer system and merely deletes or corrupts electronic files (content) he deprives the owner of his immaterial property rights (specifically the right of control over the content) and simultaneously exercises such rights (*possessio*) by destroying the information.⁵¹⁶ However, as noted above, this

⁵¹⁵ 1991 1 SA 177 A.

⁵¹⁶ Snyman 1999 makes the following observation: "Daar is een feitesituasie waar die toepassing van die toe-eieningsopsetvereiste tot verskil van mening kan lei. Dit is die geval waar X Y se saak vernietig voordat daar nog sprake van enige benutting van die saak deur X kon gewees het. Een van die bevoegdhede van 'n eienaar is om sy eie saak te vernietig, en as X Y se saak vernietig, kan betoog word dat X deur sy handeling hom die bevoegdhede van 'n eienaar oor die saak aangematig het en hom derhalwe die saak toegeëien het. Sodoende word handeling wat in werklikheid saakbeskadiging is, as diefstal gestraf. Na my mening moet 'n mens aanvaar dat die grens tussen saakbeskadiging en diefstal nie in alle opsigte waterdig is nie, en dat by hierdie gevalle van die vernietiging van 'n saak, daar 'n beperkte gebied is waar die twee misdade mekaar oorvleuel. Om te besluit of X in so 'n geval van diefstal of saakbeskadiging aangekla moet word, moet 'n mens maar van geval tot geval oordeel of dit die toe-eienings- dan wel die vernietigingsaspek van die gebeure is wat die meeste op die voorgrond is." (At 501). [own translation: There is one type of situation where an application of the requirement of intention to appropriate may result in a conclusion in respect of which there may be differences of opinion. This is where X destroys Y's property before there can be any question of its utilisation by X.

does not constitute theft in that the *hacker* lacks the intention to gain benefit from his own conduct and furthermore he gained no benefit from his actions.⁵¹⁷ He simply did not convert the content to his own use.

With regard to the scenario where a *hacker* penetrates a firm's computer system and merely copies an electronic file's content, the following may be stated: some commentators harbour doubts whether copying a file, without deleting it, amounts to *contrectatio*.⁵¹⁸ It should be borne in mind that the theft of electronic content cannot be equated to the theft of money in that where money is stolen, it leads to economic loss; in the instance where sensitive information, stored on a floppy or a hard drive, is copied, the duplication may lead to the diminishing of the information's economic value to the owner, but the owner still possesses the information.⁵¹⁹

It is clear that the *hacker* gains control over the electronic file to such an extent that he is able to make an electronic copy. He may acquire knowledge of the trade secret/confidential information and he obtains an electronic copy of the content. He thus obtains *possessio* over an electronic copy. Moreover, he acquires the benefits or rights stemming from the electronic content. It can further be argued that the owner loses *possessio* over his confidential information (trade secrets): such information will no longer be confidential information and thus the owner loses control over his trade secret. In other instances, the proprietor loses temporary control over the digital content when the *hacker* copies it. Moreover, the owner of the electronic content may

One of the rights of an owner is to destroy his own property, and if X destroys Y's property, it may be argued that in so doing X has assumed the rights of an owner in respect of the property and has therefore appropriated it. In this way acts which in reality amount to injury to property are punished as theft. It is submitted that the borderline between theft and injury to property is not watertight in all respects, and that in cases such as these where property is destroyed, there is a limited field in which these two crimes overlap. It is submitted that in order to decide whether in such a case X should be charged with theft or injury to property, one has to decide whether it is the appropriation or the destruction aspect of X's conduct that is most evident.]

⁵¹⁷ In *R v Hedley* 1930 CPD 113 the court maintained (at 114) that "[t]heft is committed when a person fraudulently and without claim of right made in good faith, takes or converts to his own use anything capable of being stolen with intent to deprive the owner thereof of [the benefits and enjoyment of] his ownership or any person having any special property or interest therein of such property or interest." (own emphasis). See also *R v Gush* 1934 AD 260 where the Supreme Court of Appeal noted (at 261) that "theft or fraud is committed as soon as he acts in such a way as to convert the money to his own use." (own emphasis).

⁵¹⁸ Skeen 1984:264.

⁵¹⁹ Skeen 1984:264-265.

lose the economic benefit that he derives from the electronic content. As the court in *S v Kimmish*⁵²⁰ stated:

“The company by having appropriated the cheques in question and having paid them into its bank accounts excluded MIC from the *economic benefit* of amounts corresponding with the face-value thereof.”⁵²¹ (own emphasis)

It is submitted that the courts should not require “permanent deprivation of the information” where an electronic duplication is made; temporary loss of control of the electronic file ought to suffice even where it is only the duration of time that it takes to click a mouse button. Should the South African courts fail to adhere to this proposal and require permanent loss of control, a clear *lacuna* will exist in the South African criminal law.⁵²² However, seeing that some courts have stated that the “Roman-Dutch law is a living system, adaptable to modern conditions”⁵²³ it is submitted that local courts will not only recognise electronic content as a possible object of theft, but will also hold that mere temporary loss of control over electronic files constitutes theft.⁵²⁴

⁵²⁰ (*supra*). Also reported at 1996 2 ALL SA 403 C.

⁵²¹ 1996 2 ALL SA 403 C:413e & 414b.

⁵²² The English legislature discovered that its own criminal law was inadequate and provided in the *Theft Act* 60 of 1968 that “property capable of being stolen includes “money and all property, real and personal, including things in action and other intangible property.”

⁵²³ *S v Graham (supra)*.

⁵²⁴ South African courts have maintained that where trust money is concerned the ordinary principles governing theft do not apply *strictu sensu*. In *S v Botha* 1970 1 SA 688 T the court observed (at 695D) that: “Dit is waar dat diefstal van geld wat vir besteding volgens opdrag ontvang is, beskou word as 'n besondere soort diefstal waarby die beginsels wat gewone diefstal beheers, nie altyd te pas kom nie”. [own translation: It is true that the theft of money, received for the purpose of spending, is seen as a unique type of theft where the principles that govern normal theft do not always apply.] See also *S v Verwey* 1968 4 SA 682 A where the Supreme Court of Appeal maintained (at 687B-D) that: “By oorweging van hierdie geval is dit nodig om in gedagte te hou dat diefstal van geld wat vir besteding volgens opdrag ontvang is, sy beslag gekry het as 'n besondere soort diefstal waarby die beginsels wat gewone diefstal beheers, nie altyd te pas kom nie. So is dit bv. vir 'n skuldigbevinding ten aansien van 'n bepaalde klaer se geld nie nodig nie dat die klaer eienaar van die geld was of dieselfde soort reg daarop gehad het wat by ander goed vereis word, of dat die identiteit van die bedrag nie reeds deur *confusio* verlore geraak het, toe die onregmatige aanwending daarvan plaasgevind het.” [own translation: When considering this case it is necessary to keep in mind that theft of money received for spending purpose, according to a mandate, originated as a unique type of theft where the principles that govern normal theft do not always apply. For instance, where the case concerns the theft of money it is not necessary that the complainant must be the owner of the money or that he enjoys the same right as required for other property, or that the identity of the amount should not have been lost due to *confusio*, when the

It should further be borne in mind that many courts have merely stated that the requirements for theft are that the thief unlawfully "takes or converts to his use anything capable of being stolen, with the intent to deprive the owner thereof of his ownership".⁵²⁵ Surely it can be argued that the *hacker* procures a copy of the electronic file, constituting immaterial (incorporeal) property, capable of being stolen. In *S v Ncube en 'n Ander*⁵²⁶ the court held that the removal of property from the owner's possession was not important; only the fact that the accused obtained control of the property.⁵²⁷ This point of view was also confirmed in *S v M*⁵²⁸ that -

unlawful spending occurred.] In fact, in *S v Kotze* 1965 1 SA 118 A the Supreme Court of Appeal maintained (at 123E) that in these instances an extenuation of the normal principles have occurred.

⁵²⁵ For instance in *R v Von Elling* 1945 AD 234 the court stated (at 236) that the ordinary definition of theft is: "Theft is committed when a person fraudulently and without claim of right made in good faith takes or converts to his use anything capable of being stolen with intent to deprive the owner thereof of his ownership, or any person having any special property or interest therein of such property or interest." See also *S v Kotze* 1965 1 SA 188 A:125; *R v Sibiya* 1955 4 SA 247 A:250-251; *R v Harlow* 1955 3 SA 259 T:263. In *Premier Western Cape & Others v Parker & Mohammed & Others* 1999 1 ALL SA 176 C the court, although dealing with civil issues, defined theft (at 186j-187a) as follows: "Theft consists in an unlawful *contractatio* with intent to steal a thing capable of being stolen."

⁵²⁶ 1998 1 SACR 174 T.

⁵²⁷ The accused were arrested by the police while they were lifting a box from the back of an open delivery vehicle, with the intention to steal it. The police's intervention prevented them from actually removing the box from the vehicle. The question of law of was whether the accused had committed theft or attempted theft. The court maintained (at 176c-e) that: "Ek is van mening dat die beskuldiges, toe hulle die doos opgelig het, fisiese beheer daarvoor gehad het. Die feit dat die doos nog weggedra moet word van die bakkie om die diefstal 'n volslae sukses te maak is myns insiens nie belangrik nie. Die man wat 'n artikel in 'n winkel op sy persoon versteek met die doel om uit die winkel te loop sonder om te betaal en dit dus te steel pleeg diefstal al word hy deur die sekuriteitsbeamptes van die winkel dopgehou en onmiddellik op toegeslaan. Die feit dat hy onsuksesvol is meen nie dat hy alleen gepoog het om te steel nie. Die vraag is nie sukses in die sin van heeltemal wegkom nie; die vraag is of die beskuldigde beheer oor die artikel verkry het en uitgeoefen het." [own translation: I am of the opinion that the accused, when they lifted the box, had physical control thereof. The fact that the box still had to be carried away from the truck in order to make the theft successful is irrelevant. Where an individual conceals an article on his person in a shop, with the intent to walk out of the shop without paying for it and to steal it, he commits theft even though he is watched by the shop's security officers and they immediately apprehend him. The fact that he is unsuccessful does not mean that he only attempted to steal. The question is not whether the accused successfully got away; the question is whether the accused obtained and exercised control over the property in question.] See also *S v Tekane en 'n Ander* 1998 1 SACR 291 O where the court maintained (at 292e-f) that "[d]ie soort van diefstal (of poging daartoe) hier tersaaklik, is die mees alledaagse verskyningsvorm van diefstal, naamlik die onttrekking van 'n saak aan die beheer van 'n ander met die bedoeling om jou die saak toe te eien." [own translation: The type of theft (or attempted theft) that we are dealing with here is the most common form

“dit is nie soveel die beheer van die eienaar waarop gelet moet word nie as die beheer wat die beskuldigde onregmatiglik vir homself toe-eien afgesien daarvan of hy die goedere verwyder het ... Van die wyse waarop die beskuldigde met die goedere handel word sy bedoeling afgelei en die bedoeling moet daarop neerkom dat hy die eienaar (indien die eienaar die klaer is) permanent van sy voordeel van sy eienaarskap ontnem het.”⁵²⁹

It is abundantly clear that where a *hacker* copies the content of an electronic file, he obtains control over the content to such an extent that he is able to make a copy and subsequently obtains control over the electronic copy. Therefore, he appropriates for himself a power that the owner enjoys.⁵³⁰

3.1.5. Theft of passwords and credit card information

The next question that arises is whether digital passwords can be the subject of theft. To answer this question, it must be assessed whether passwords constitute legal objects capable of being stolen. As mentioned above, South African commentators pose two requirements for the recognition of new legal objects namely a) that it must be of value to the person concerned and b) “it must have such a measure of distinctiveness, definiteness and independence that it is possible to use it, enjoy it and

of theft namely the removal of property from control of another with the intent to appropriate the property.]

⁵²⁸ 1982 2 SA 309 O.

⁵²⁹ 1982 2 SA 309 O:312D-E. [own translation: it is not so much the control of the owner which should be looked at but the control that the accused unlawfully appropriated for himself irrespective whether he removed the property ... The accused's intent is inferred from the manner in which he deals with the property and such intent must indicate that he wants to deprive the owner (if the complainant is the owner) permanently of the benefits from his ownership.]

⁵³⁰ In *S v Van den berg* 1979 3 SA 1027 NK the court maintained (at 1035F-G) that “[w]at wel ter sake en belangrik is, is dat hy homself 'n bevoegdheid aangematig het wat 'n eienaar toekom.” [own translation: what is important is that he appropriated for himself a power which the owner enjoys.] Loubser 1978 maintains: “Thus a person may commit theft by unlawfully assuming rights over another's property while already having lawful control over it, e.g. where he is holding it on behalf of another for a particular purpose and the essence of his act of theft is then not the gaining or exercising of control, but the unlawful assumption of rights over the object whereby the owner or rightful holder is excluded from the benefits of those rights, i.e. conduct that can accurately be described as an appropriation of the object.” (At 59).

(where possible) dispose of it.”⁵³¹

Neethling, for instance, observes that the law protects trade secrets because they represent a legally protectable economic interest (“*regtensbeskermwaardige, ekonomiese belang*”) for the entrepreneur.⁵³² Likewise, Joubert states that the -

“[o]bjek van 'n subjektiewe reg is 'n regsgoed wat ekonomiese waarde vir die reghebbende verteenwoordig, wat dus uit sy relatiewe skaarsheid sy betekenis as regsgoed verkry. Wat dienooreenkomstig regsobjek kan wees, hang dus grotendeels af van die ontwikkeling van die kultuur. So was vir die Romeine 'n kunswerk of 'n uitvinding nog nie regsgoed nie; outeursreg en patentreg is 'n ontwikkeling eers van die afgelope eeue.”⁵³³

On this same basis it may be contended that a password represents a legal economic interest that is protectable according to the law: it is unique to each computer user and it provides access to digital content that may include 1) personal letters, 2) confidential information and/or trade secrets, 3) copyright protected material or 4) electronic credit.

It is therefore submitted that passwords constitute protectable legal objects that should be recognised by our courts as the objects of an immaterial property right. Furthermore, digital passwords may constitute confidential information, which is recognised as immaterial property.⁵³⁴

⁵³¹ Van Heerden & Neethling 1995:80.

⁵³² Neethling 1983:24.

⁵³³ Joubert 1958:112. [own translation: object of a subjective right is a legal object that represents an economic value for the lawful owner thereof, and which derives its value, as legal object, from its relative scarceness. Therefore cultural developments determine what can be a legal object or not. For instance, the Romans did not recognise either an artwork or an invention as a legal object; copyright as well as patent rights are developments of the previous century.]

⁵³⁴ Generally speaking, our courts pose the following requirements before information qualifies as protectable “confidential information” for the purposes of the law of unlawful competition: a) the information must be kept secret, b) labour and skill must have been spent to obtain or compile the information and c) gaining access to such information will provide a competitor with an advantage (in the sense of he is saved a great deal of labour and money by filching the plaintiff’s know-how) and/or the proprietor of the information will suffer prejudice when someone else obtains this particular information.

However, other types of information are also protected as confidential information such as discussions at meetings of board of directors (*Janit & Another v Motor Industry Fund Administrators (Pty) Ltd & Another* 1995 4 SA 293 A:303F; *Motor Industry Fund Administrators (Pty) Ltd & Another v Janit & Another* 1994 3 SA 56 W:61B) and internal business facts/affairs (*Financial Mail (Pty) Ltd & Others v Sage Holdings Ltd & Another* 1993 2 SA 451 A:465D-E; *SA Historical Mint (Pty) Ltd v Sutcliffe &*

Moreover, it is submitted that credit card information, which refers to the credit card's account number as well as the PIN number associated with that account, constitutes a legal protectable object or interest. Identical considerations to those stated above with

Another 1983 2 SA 84 C:89H & 91A). It appears from the following judgments that South African courts have a wide perception of what constitutes confidential information.

In *Coolair Ventilator Co (SA) (Pty) Ltd v Liebenberg & Another* 1967 1 SA 686 W the court maintained (690B-C) that: "What would constitute information of a confidential nature would depend on the circumstances of each case, and in this regard the potential or actual usefulness of the information to a rival would be an important consideration in determining whether it was confidential or not." In *Meter Systems Holdings Ltd v Venter & Another* 1993 1 SA 409 W the court observed (at 428A-C) that: "In principle, there can be no limit to the number of potential categories of information which may qualify for protection as 'confidential' under our law, either in delict (by way of a legal duty arising from the application of the principles of Aquilian liability to situations in which a fiduciary relationship not based on contract is recognised), or in contract (by way of a contractual term implied by law where the contract is one that creates a fiduciary relationship)." In *Van Castricum v Theunissen & Another* 1993 2 SA 726 T the court approved (at 731I-732C) the following four principles to ascertain whether information constitutes confidential information or a trade secret worthy of protection, namely a) the owner of the information must believe that its release would be injurious to him or of advantage to his rivals or others, b) the owner must believe that the information is confidential or secret; i.e. not already in the public domain, c) the owner's belief under (a) and (b) must be reasonable, and d) the information must be judged in the light of the usage and practices of the particular industry or trade concerned.

In *Gordon Lloyd Page & Associates v Rivera & Another* 2001 1 SA 88 SCA the Supreme Court of Appeal noted (at 95E-F) that "the mere fact that knowledge or information is useful or of value does not make it legally worthy of protection. Something more is required, for instance the information must have the necessary quality of confidentiality. The plaintiff must also have at least a *quasi*-proprietary or legal interest ('regsbelang') in the information." The same way of thinking is enunciated by Joubert 1985 by stipulating (at 42) the following requirements for confidential information: a) the information must not be known to the defendant and the public and b) the plaintiff must treat the information as confidential.

The question arises whether passwords constitute confidential information? It is submitted that passwords do constitute "information" in that such knowledge is used to gain access to other documents. Furthermore, passwords are of necessity of a confidential nature; they are valuable to any business in that it provides its employees access to other confidential information and it protects its economic and digital assets from third parties; the disclosure of such knowledge could be destructive to any business in that it can (and will) render access to the computer to any unauthorised third party; and finally all computer users utilising passwords to protect their computers' contents have a *quasi*-proprietary or legal interest in the password and its secrecy. In *Easyfind International (SA) (Pty) Ltd v Instaplan Holdings & Another* 1983 3 917 W the court stated (at 927C) that: "To my mind the simple practical guide in cases of appropriation of confidential documents or ideas is the commandment 'Thou shalt not steal'." Passwords, at the very least, constitute confidential ideas and should therefore, according to this judgment, be protected from theft.

stated above with regard to passwords apply to credit card information. Such information may also constitute confidential information.

3.1.6. Instructing and assisting hackers

The following should be kept in mind at all times: where a competitor, for instance, instructs a *hacker* to penetrate a computer system to “steal” confidential information or passwords and the former subsequently purchases it from the *hacker*, both the *hacker* as well as the competitor are guilty of theft.⁵³⁵ the *hacker* is the perpetrator and the competitor (instructor) is an accomplice. In *R v Karolia*⁵³⁶ the court maintained that where an accused instructs another to steal certain property and the former then receives such stolen property, he is guilty of theft:

“It is sufficient for me to say that in my opinion if certain acts amount strictly to the commission of theft by the accused, then such acts cannot at the same time constitute ‘receiving’. In the present instance the accused on the facts found by the magistrate could have been found guilty of theft. He did in fact steal the goods by using the delivery boy to get them for him.”⁵³⁷

Furthermore where A assists a *hacker* in disposing of the stolen electronic content, A also commits theft (as an accessory after the fact).⁵³⁸ In *R v Von Elling*⁵³⁹ the Supreme Court of Appeal maintained that “it is also clear that any person who receives stolen property from a thief knowing it to be stolen, and handles it, is necessarily guilty of *fraudulosa contrectatio* and he will have the intention to deprive the owner of the benefits of his ownership.”⁵⁴⁰ The court further maintained that:

“Such assistance, given after the taking, if it involves handling or dealing with the stolen property, may amount to a *fraudulosa contrectatio* by the assistant. If there be such a *fraudulosa contrectatio* by the assistant or if he assists the principal thief in his *fraudulosa contrectatio*, and if his act be accompanied by the necessary intention to

⁵³⁵ See De Wet & Swanepoel 1985:345.

⁵³⁶ 1956 3 SA 569 T.

⁵³⁷ 1956 3 SA 569 T:571H-572A. See also *R v Correia* 1958 1 533 A:535H: “On these facts the appellant had been *socius criminis* with the thief who did the actual stealing and was himself guilty of theft.”

⁵³⁸ See *S v Naryan* 1998 2 ALL SA 345 W:356g.

⁵³⁹ 1945 AD 234.

⁵⁴⁰ 1945 AD 234:239.

deprive the true owner of the benefits of his ownership, then the assistant is guilty of theft."⁵⁴¹

3.1.7. De minimis non curat lex

The question arises whether a *hacker* can raise the defence *de minimis non curat lex* where the file that he copied was of little value to its owner. In *S v Nedzamba*⁵⁴² the court maintained:

"In view of the above authorities it can therefore be concluded that in deciding whether the *de minimis* rule should be applied to a case of theft of an article of little value not only the value of the article but also the purpose of the thief in stealing it, the effect the deed has on the interests of the community and all the circumstances under which the deed was committed should be taken into consideration."⁵⁴³

Therefore it may be concluded that a *hacker* cannot raise this defence in that hacking is against the interests of justice and the community, which cannot be condoned. Furthermore, the court must also take the surrounding circumstances into account such as a) why did the *hacker* copy that specific file and b) what did he do with it afterwards: "It is also evidence from which the effect of the deed on the interests of the community becomes relevant ... it will adversely affect the interests of the community if the *de minimis* rule is applied".⁵⁴⁴

3.1.8. Hacker making a mental copy or writing something down

The question that needs to be addressed is whether a *hacker* who gains access to a computer system, sees a password or confidential information and subsequently either memorises the information or writes it down on a piece of paper, without making an electronic copy of such information, commits theft?

In paragraphs 3.1.4 and 3.1.5 above it was concluded that when a *hacker* electronically copies incorporeal property (digital content) he is guilty of theft in that he appropriates information (an identical copy of the digital content) and he assumes or acquires or exercises the benefits as well as the rights that the proprietor of the

⁵⁴¹ 1945 AD 234:239.

⁵⁴² 1993 1 SACR 673 V.

⁵⁴³ 1993 1 SACR 673 V:676f-g.

⁵⁴⁴ 1993 1 SACR 673 V:676g-677a.

information enjoys in regard to such content. Furthermore, he deprives the owner of the benefits and rights of his digital content, especially where such content constitutes confidential information or trade secrets: it is not longer confidential. It was also concluded that he acquires control over digital content/information (the identical copy) as well as the rights accompanying such content and simultaneously deprives the owner temporarily of control over the content, when he makes an electronic copy.

It is submitted that whenever a *hacker* makes a mental copy or writes the information down such conduct constitutes theft. The reasons are the following: As noted in paragraph 3.1.4.1 above, our courts have maintained that when A makes a false entry into B's accounting book, he commits theft. It is clear that A does not gain physical control of the incorporeal property or the accompanying subjective rights and neither does B lose physical control. A appropriates and B loses a subjective right as well as incorporeal property. Therefore the law does not require that the thief has to obtain a physical object or an electronic copy. It follows that where a *hacker* makes a mental copy of confidential information or sees the confidential information on his computer screen and scribbles it down on a piece of paper he appropriates incorporeal property (namely the confidential information) as well as the benefits accompanying the property and the proprietor "loses" the benefits and enjoyment of his confidential information⁵⁴⁵ and he temporarily "loses control" over his incorporeal property when the *hacker* memorises the information or writes it down.

As numerous South African courts have stated (see paragraph 3.1.4.1 above), one must look at the economic effect of the culprit's act and should not be hypnotised by the mechanisms by means of which theft can be committed.⁵⁴⁶ It is submitted that our courts will maintain that where confidential information is stolen, by either making a mental copy or writing it down, the proprietor is deprived of the economic benefits of his incorporeal property and the *hacker* simultaneously gains the benefits the owner enjoys over such information.

Similar considerations apply to the memorising or writing down of passwords: the proprietor is deprived of the rights and benefits (control) he enjoys in regard to such incorporeal property/information – it protects the contents stored on his computer from third parties' prying eyes – and the *hacker* gains control over a copy of this password and appropriates the benefits the owner enjoys: the *hacker* can also access the

⁵⁴⁵ The law does not recognise the information any longer as confidential.

computer or provide third parties with the necessary information to access that particular computer.

Therefore, merely the mechanism used in copying the electronic content differs. Instead of using a computer to copy the password, he uses his brain.

3.1.9. Hacker found in possession of stolen electronic data, but owner of data unknown to prosecutor

Local courts have maintained that an accused can be found guilty of theft where he found a bag full of new clothes and appropriated it to himself, even if neither he, nor the state, knows to whom the property belongs.⁵⁴⁷ However, it is incumbent upon the state to prove that

- a) the property was stolen⁵⁴⁸ and
- b) that the accused stole the property.⁵⁴⁹

“The onus of proving his guilt continues to rest throughout on the State, but the absence of an explanation by the accused, in circumstances when one would reasonably expect one if his possession were innocent, may well be taken into consideration in determining whether or not the State has discharged the onus

⁵⁴⁶ For instance, *R v Sibiya (supra)*.

⁵⁴⁷ In *S v Abrahams en 'n Ander* 1998 1 SACR 314 K the court noted (at 316f-g) that “[d]aar is geen rede waarom diefstal nie gepleeg kan word met betrekking tot optelgoed nie. Die rede hiervoor is dat hoewel daar onder sulke omstandighede nie gesê kan word dat die goedere aan 'n ander se beheer onttrek is nie, dit insgelyks nie aan die toe-eienaar toevertrou is nie, en deur sy toeëieningshandeling ontnem hy die eienaar van sy genot en beheer van die saak.” [own translation: there is no reason why theft cannot be committed with regard to findings. The reason being that even though it cannot be stated that the property was removed from someone else’s control, it was not handed over to the appropriator, and by means of his act of appropriation he deprived the owner of his enjoyment and control over the property in question.] See also *S v Kariko & Another* 1998 2 SACR 531 NmHC:535f; *S v Daniels* 1970 3 SA 96 E:96E-G; *R v Kwessa* 1947 1 SA 428 C:429I-430A; *Petersen v R* 1909 TS 263:264. In *S v Siswana* 1968 4 SA 251 E the court maintained (at 252B-C) that “[i]t is perfectly permissible for the State to charge an accused person of stealing an article from someone to the prosecutor unknown, if such be the case, but in such cases the Court should always be very circumspect in its consideration of the evidence to ensure that the State has proved each element of the offence beyond a reasonable doubt.” The prosecution is assisted by s 84(2) of the *Criminal Procedure Act* 51 of 1977 which stipulates that “[w]here any of the particulars referred to in subsection (1) are unknown to the prosecutor it shall be sufficient to state that fact in the charge.”

⁵⁴⁸ *S v Kariko & Another* 1998 2 SACR 531 NmHC:535h.

⁵⁴⁹ *S v Siswana* 1968 4 SA 251 E:252H; *Petersen v R* 1909 TS 263:264.

resting on it ... however such an explanation [as to how the accused came into possession of the alleged stolen property] can only be required of an accused person after the State has succeeded in proving that a theft had been committed, when it was committed, and that the accused was in possession of the stolen property shortly after the theft. It is true that the State is entitled to rely on all the evidence before the court in its attempt to show that the offence had been committed, and that the conduct of an accused in giving no explanation or in giving a false explanation are facts which can be taken into consideration in determining whether or not a theft has been proved but the weight to be attached to these facts must depend to a large extent on the strength of the other circumstantial evidence pointing to the commission of the offence."⁵⁵⁰

Therefore only where the state prove that the property was stolen, does an onus rest on the accused's shoulders to explain how he came into possession of the said property.⁵⁵¹ The court can also find the accused guilty of receiving stolen property knowing that it was stolen.⁵⁵²

c) or that the accused knew that the property was stolen and he participated in the commission of the offence by e.g. selling or disposing of such property.⁵⁵³ It should be kept in mind that theft is a continuous offence and that it makes no difference that the accused was not involved in the original *contrectatio*.⁵⁵⁴

Therefore where the police, after raiding and/or searching a *hacker's* computer system, finds electronic data (or passwords) that clearly does not belong to the *hacker*, the state can prosecute him for theft even though it is unable to prove the identity of the owner of the electronic property.

3.2. Liability in terms of the General Law Amendment Act 50 of 1956

The consequence of *R v Sibiya*⁵⁵⁵ is that the mere use of something, without the authorisation of the owner or the person in control thereof, does not constitute an offence. According to our common law such conduct constituted the offence of *furtum*

⁵⁵⁰ *S v Siswana* 1968 4 SA 251 E:252H-253H.

⁵⁵¹ *S v Siswana* 1968 4 SA 251 E:254B-C.

⁵⁵² *Petersen v R* 1909 TS 263:264.

⁵⁵³ *S v Cassiem* 2001 1 SACR 489 SCA:493d-g.

⁵⁵⁴ *S v Cassiem* 2001 1 SACR 489 SCA:493f.

⁵⁵⁵ 1955 4 SA 247 A.

usus.⁵⁵⁶ In 1956 the *General Law Amendment Act*⁵⁵⁷ was promulgated which provides that anyone who -

“without a bona fide claim of right and without the consent of the owner or the person having the control thereof, removes any property from the control of the owner or such person with intent to use it for his own purposes without the consent of the owner or any other person competent to give such consent, whether or not he intends throughout to return the property to the owner or person from whose control he removes it, shall, unless it is proved that such person, at the time of the removal, had reasonable grounds for believing that the owner or such other person would have consented to such use if he had known about it, be guilty of an offence”.⁵⁵⁸ (own underlining)

Furthermore, the Act stipulates that an accused charged with theft may be found guilty of this offence, where it appears that the accused is guilty of this offence, rather than theft.⁵⁵⁹

An essential element of the offence is that the property in question had to be *removed from the control of the owner*.⁵⁶⁰ It can be argued that a *hacker* procuring control over an electronic file by copying or modifying such file, causes the proprietor to lose control (even for only a few seconds) over the electronic file. It is to be doubted whether a court will be willing to rule that the *hacker* removed the electronic file from the owner's control by mere copying or reading the electronic file.⁵⁶¹

A further element of the offence is that the *hacker* must have had the intent to use the electronic file. It follows that whenever a *hacker* merely deletes a digital file, without copying it, such conduct does not fall within the ambit of this offence in that, even though the electronic file was removed (deleted) from the hard drive, the intent to use the file was absent: the *hacker* only had the intent to erase the file. Of necessity then,

⁵⁵⁶ Skeen 1984:266.

⁵⁵⁷ Act 50/1956.

⁵⁵⁸ S 1(1).

⁵⁵⁹ S 1(2).

⁵⁶⁰ This section penalises the unlawful removal of an object and not the usage thereof. See Snyman 1999:517; *S v Schwartz* 1980 4 SA 588 T:592A-B: “Die misdryf word gepleeg by die verwydering uit beheer, met ander woorde, by besitverkryging, en waar toestemming vir 'n sekere doel verkry word, maar later vir 'n ander doel aangewend word, word die artikel nie oortree nie”. [own translation: The crime is committed when the property is removed from control, in other words, by means of obtaining possession, and where consent is obtained for a specific purpose, but later on the object is used for another purpose, the section is not contravened.]

⁵⁶¹ Skeen 1984:266.

the sole instance that is covered by this Act is when a *hacker* makes an electronic copy and thereafter deletes the file.

However, in *S v Rheeder*⁵⁶² the Supreme Court of Appeal gave the following interpretation to the word "control":

"Dit vereis volkome beheer, dws *liggaamlike* besit met gepaadgaande geoorloofde seggenskap oor die voertuig ingeslote ... die reg of vergunning om dit te kan gebruik of te kan laat gebruik, hetsy vir 'n bepaalde doel of na goeddunke. Waar iemand anders as die eienaar dus 'n artikel in sy *liggaamlike* besit het, is die aard van die artikel en die omstandighede rakende sodanige besit loutsbepalend of daar beheer oor die artikel is soos in art 1(1) beoog."⁵⁶³ (own emphasis)

As noticed, the Supreme Court of Appeal mentioned "liggaamlike besit" (physical possession) twice. However, it should be kept in mind that the court was not dealing with the question whether incorporeal property could form the subject of this offence. However, seeing that the Act (as explained) only applies to the instance where a *hacker* copies, as well as deletes, the electronic content and such instance is covered by the offence of theft, it is unnecessary to come to a final conclusion whether someone can only be prosecuted in terms of this section where he unlawfully removed corporeal property.

3.3. Receiving stolen property

Under this heading there are two offences relevant to cybercrimes, namely a) receiving stolen property knowing it to be stolen and b) receiving stolen property and having no reasonable cause to believe that the seller was the lawful owner of such property. These offences are relevant in two ways for the purposes of this dissertation:

a) Where a *hacker* electronically copies digital content (data or passwords) and then sells or gives that content to A, the question of law is whether A is guilty of

⁵⁶² 2001 1 SA 348 SCA.

⁵⁶³ 2001 1 SA 348 SCA:358F-G. [own translation: It requires complete control, that is physical possession accompanied by lawful authority over the motor vehicle ... the right or permission to use it or to allow it to be used, either for a specific purpose or at own discretion. Where someone else, other than the owner, has an object in his physical possession, the nature of the object as well as the circumstances surrounding such possession are decisive whether the control as contemplated in section 1(1) is present.]

receiving stolen property knowing it to be stolen.

- b) Where a *hacker* electronically copies digital content (data or passwords) and displays or puts such content on a web page, the question of law arises whether the owner of the web page (the person in control of the web page) is guilty of receiving stolen property knowing it to be stolen.

3.3.1. The common law offence of receiving stolen property knowing that it is stolen

This offence is committed when A receives stolen property into his possession unlawfully and knowing that it is stolen property.⁵⁶⁴ A can be charged with theft⁵⁶⁵ or with the offence of *receiving stolen property knowing that it is stolen*, but mostly the accused is charged with the latter offence.⁵⁶⁶ The elements of this offence are:⁵⁶⁷ (a) the property must be stolen,⁵⁶⁸ (b) unlawfulness, (c) receiving the property, and (d) the accused must appreciate the fact, when he receives the property, that such property is stolen.

Next, each element of this offence, except unlawfulness, is discussed.

⁵⁶⁴ Snyman 1999:523; LAWSA 1996: vol 6, par 317; Hunt-Milton 1990:731

⁵⁶⁵ See *Ex Parte Minister of Justice: in Re R v Maserow & Another* 1943 AD 164:170.

⁵⁶⁶ Snyman 1999:524. Our courts' attitude is that the offence "receiving stolen property knowing that it is stolen" is merely a *specie* of the crime of theft. See Snyman 1999:525; De Wet & Swanepoel 1985:358; *S v Bolus & Another* 1966 4 575 A:580A; *R v Bhardu* 1945 AD 813:825. In *R v Joffe* 1925 TPD 86 the court noted (at 86) that "[i]n essence, the crime of receiving stolen property knowing it to be stolen is in law the crime of theft. The receiver intends to further the theft, and he makes himself *particeps criminis*; if it were not a distinct crime in itself, in principle I see no reason why such a person should not be charged in our law as a principle in the commission of the offence of theft." In *R v Correia* 1958 1 533 A Reynolds AJA, in his minority judgment, noted (at 544A) that "in law every receiver is a thief ... With knowledge that the goods were stolen, he appropriates the goods of another for himself and thus commits theft and receiving." It should invariably be kept in mind that the offence of receiving stolen property knowing it to be stolen is a substantive offence. See *S v Bolus & Another* 1966 4 575 A:580A; *R v Arbee* 1956 4 SA 438 A:441F.

⁵⁶⁷ See Snyman 1999:524-525; Hunt-Milton 1990:731; De Wet & Swanepoel 1985:359-360. *Animus furandi* is not an element of this offence and consequently the law does not require an intent to deprive the owner permanently of the benefits of his ownership. See Hunt-Milton 1990:738

⁵⁶⁸ Property obtained by means of *theft by false pretences* suffices. See *R v Vilakazi* 1959 4 SA 700 N:701H-702B; LAWSA 1996:vol 6, par 319.

3.3.1.1. Stolen property

Snyman submits that only movable property in commerce can be the subject of this offence, in that, according to him, only movable property in commerce can be unlawfully appropriated.⁵⁶⁹ Seeing that the courts have relaxed the requirement that only corporeal "property" can be stolen,⁵⁷⁰ it is submitted that incorporeal property can also form the subject-matter of the offence of *receiving stolen property knowing that it is stolen* (hereafter referred to as "receiving").

Where the receiver of the digital data is charged with the offence of receiving the prosecution must prove that the *hacker* stole such content. The prosecution cannot simply submit a court record of the *hacker's* conviction for theft of such content. The court in *R v Lee*⁵⁷¹ noted:

"Now a judgment *in personam*, whether given in civil or in criminal proceedings, though it is evidence of the fact that the judgment was given, is not evidence, against persons who are not parties to the proceedings, of the truth or correctness of the judgment ... The general rule being as I have stated, it would appear that a conviction for theft is no proof, against a person subsequently charged with receiving the goods from the thief, that the goods were in fact stolen property ... In my view, on these authorities, it is clear that upon a charge against a receiver the Crown does not discharge the onus of proving that the property in issue was stolen by mere proof of the conviction of the thief. It is not, however, necessary in every case against a receiver to lead formal evidence of the theft. The circumstances in which the accused person has received the goods may of themselves be sufficient proof that they had been stolen, and further, may prove that he knew this when he received them".⁵⁷²

A mere statement by the *hacker*, where the receiver is prosecuted in a subsequent case, that he was convicted of theft will not suffice.⁵⁷³ Therefore it is advised that both the *hacker* and the receiver be prosecuted in the same case.⁵⁷⁴ Otherwise, the

⁵⁶⁹ Snyman 1999:524. See also LAWSA 1996:vol 6, par 319.

⁵⁷⁰ See par 3.1.4.1 of this chapter.

⁵⁷¹ 1952 2 SA 67 T.

⁵⁷² 1952 2 SA 67 T:69D-71B. See also *R v Markins Motors (Pty) Ltd & Another* 1959 3 SA 508 A:510G.

⁵⁷³ *R v Lee* 1952 2 SA 67 T:71C.

⁵⁷⁴ S 155(2) of the *Criminal Procedure Act* 51 of 1977 provides that "(1) Any number of participants in the same offence may be tried together and any number of accessories after the same fact may be tried together or any number of participants in the same offence and any number of accessories after that fact may be tried together, and each such participant and each such accessory may be charged at such

prosecution will have to prove that the *hacker* committed theft by copying the electronic data without authorisation.

3.3.1.2. Receiving property

Receiving property consists of two elements. The first element is that the accused must have taken the property into his possession.⁵⁷⁵ In *R v Van der Bank*⁵⁷⁶ the court stated that “[i]t is not necessary for a receiving of goods that they should be placed in the hands of the receiver. It is sufficient if they are put under his control and he agrees to assume control.”⁵⁷⁷ This was confirmed in *R v Saffy & Bennett*⁵⁷⁸ where the Supreme Court of Appeal noted that “such possession may either be actual or constructive; but it must be such as to give him some measure of control.”⁵⁷⁹ The second element entails that the receiver must have the intention to exercise or acquire control over the property.⁵⁸⁰

It follows that the receiver may gain control over the copied electronic data e.g. by -

- a) opening an e-mail attachment sent by the *hacker* and copying the content to his computer or any storage medium; or
- b) obtaining a floppy, containing the digital content, from the *hacker*.

3.3.1.3. Knowing that it is stolen property

The accused must be aware of the fact, when he receives the property, that it constitutes stolen property.⁵⁸¹ If the accused innocently receives (takes possession of) the property but subsequently discovers that it is stolen and either keeps or uses the

trial with the relevant substantive offence alleged against him. (2) A receiver of property obtained by means of an offence shall for purposes of this section be deemed to be a participant in the offence in question.”

⁵⁷⁵ *Snyman* 1999:525; *Hunt-Milton* 1990:732.

⁵⁷⁶ 1941 TPD 307.

⁵⁷⁷ 1941 TPD 307:309.

⁵⁷⁸ 1944 AD 391.

⁵⁷⁹ 1944 AD 391:420.

⁵⁸⁰ *LAWSA* 1996:vol 6, par 320; *Hunt-Milton* 1990:732-735.

⁵⁸¹ *R v Sipendu* 1932 EDL 312 the court maintained (at 319) that “[t]his knowledge must exist at the very instant of the receiving, that is, at the time the receiver takes possession of the property from the thief.” See also *LAWSA* 1996: vol 6, par 321.

property or sells it to someone else or hides it (in order to secure for himself the continued possession of the stolen articles), he is guilty of theft and not receiving stolen property.⁵⁸² Local courts have maintained that in such instances there was a "fresh *contrectatio* with the knowledge that the goods were stolen"⁵⁸³ coupled with the intention to deprive the owner of his property rights or possession. It follows that such conduct constitutes a new and independent (original) theft.^{584 585}

Knowledge as such is not set as requirement for this offence. Where the accused believes that the property is stolen, he will also be guilty of receiving. In *R v Sipendu*⁵⁸⁶ the court stated that "it is not necessary to prove that the receiver had such direct knowledge as would flow from witnessing of the theft, and that ... 'it is sufficient if the circumstances accompanying the transaction were such as to make the prisoner believe the goods to have been stolen.' In other words, if the facts at the trial are such as to justify a conclusion ... that the accused must have believed the goods to have been stolen at the time he received them."⁵⁸⁷ Finally the court remarked that:

"I also agree that such proof of guilty knowledge on the part of the accused may be indicated by the circumstances of the receipt, the class of person from whom the article was obtained, the paid price, the time and place of the transaction, the character of the property and the manner it was subsequently dealt with."⁵⁸⁸

The authors of LAWSA add to this list the fact that the accused gave false explanations.⁵⁸⁹

Therefore, the court will take various factors into consideration to determine whether

⁵⁸² *R v Naidoo* 1949 4 SA 858 A:862D-E; *R v Saffy & Bennett* 1944 AD 391; *R v Bazi* 1943 EDL 222:225; *R v Attia* 1937 TPD 102:106; *R v Sipendu* 1932 EDL 312:319; LAWSA 1996:vol 6, par 318 & 321; Hunt-Milton 1990:737.

⁵⁸³ *R v Bazi* 1943 EDL 222:223.

⁵⁸⁴ In *R v Bazi* 1943 EDL 222 the court noted (at 225) that "the theft commenced at the time when the accused manifested his intention by the *contrectatio* ... and with a view of retaining them in conflict with the rights of the owner." In *R v Attia* 1937 TPD 102 the court maintained (at 106) that "he would be guilty of a fresh and independent theft, in respect of which he may be charged."

⁵⁸⁵ The accused can be found guilty of theft, even where he was charged with receiving stolen property. S 265 of the *Criminal Procedure Act* provides that "[i]f the evidence on a charge of receiving stolen property knowing it to have been stolen does not prove that offence, but (a) the offence of theft ... the accused may be found guilty of the offence so proved."

⁵⁸⁶ 1932 EDL 312.

⁵⁸⁷ 1932 EDL 312:319.

⁵⁸⁸ 1932 EDL 312:319.

the accused had the necessary guilty knowledge (belief), namely the age of the person selling the digital content; the circumstances of the sale; the price he asks for it; the nature of the electronic content and the manner the accused (purchaser) subsequently dealt with it. It is submitted that where A proposes to sell passwords to B (which will allow him access to another computer) the courts will invariably rule that B knew that the passwords were stolen property.

Where the accused did not know that the property was stolen, nor did he believe that it was stolen, but suspected that such property was stolen and deliberately refrained from making enquiries, he is also guilty of receiving. In *R v Patz*⁵⁹⁰ the Supreme Court of Appeal noted that where an accused's "abstention from enquiry was dictated by a belief or conviction that the goods were stolen" his mental state amounted to guilty knowledge.⁵⁹¹ But, the court continued, a mere suspicion that goods were stolen, not amounting to a conviction or belief, was not knowledge.⁵⁹² The court further maintained that "the customary and proper way of judging a man's state of mind is to compare it with what one thinks one's own state of mind would be in the circumstances in which such man was placed."⁵⁹³

In *R v Markins Motors (Pty) Ltd & Another*⁵⁹⁴ the Supreme Court of Appeal further elaborated upon this issue:

"[T]he factor of wilfully refraining from making enquiries, if the reason for refraining is to avoid the confirmation of one's suspicions which one fears might well result, is a most important addition to the initial suspicion. Where such refraining is present as an additional factor it will generally justify the conclusion that what one might otherwise hold to be no more than suspicion is really a state of mind properly describable as conviction or belief."⁵⁹⁵

In *S v Ushewokunze*⁵⁹⁶ the court expounded upon the issue by stating that -

"if it is proved that the accused must have known that there was a *real possibility* of the

⁵⁸⁹ LAWSA 1996:vol 6, par 321.

⁵⁹⁰ 1946 AD 845.

⁵⁹¹ 1946 AD 845:858.

⁵⁹² 1946 AD 845:857.

⁵⁹³ 1946 AD 845:859.

⁵⁹⁴ 1959 3 SA 508 A.

⁵⁹⁵ 1959 3 SA 508 A:516G-H.

⁵⁹⁶ 1971 2 SA 362 RAD.

goods having been stolen and he *deliberately refrained* from enquiring whether the goods were stolen or not in case his fears were confirmed, that is certainly enough evidence on which to convict."⁵⁹⁷ (own emphasis)

It follows that where A suspects that the digital data is stolen, but receives it careless of whether his suspicions are correct, he is also guilty of receiving. Put differently, *dolus eventualis* suffices for this offence.⁵⁹⁸

In *S v Ushewokunze*⁵⁹⁹ the person who sold certain property (medical drugs) to the accused had little knowledge of the property he was handling. The court found that this must have raised serious suspicions and convicted the accused of the offence of receiving. Therefore where a person (the *hacker*) attempts to sell confidential information to A, but it is clear to A that the former has little or no knowledge about this information, the court will maintain that this must have raised serious suspicions that the information were stolen property.

Furthermore, in *R v Joffe*⁶⁰⁰ the court stated that the "very appearance of the boy [who sold the stolen property to the accused] should make the purchaser of such an article from him suspicious."⁶⁰¹ Therefore where a young *hacker* (say, between the ages of 18 and 23) sells confidential business information to X, X is guilty of receiving in that he must have suspected such incorporeal property to be stolen and either deliberately refrained from making enquiries as to how the *hacker* acquired such information or carelessly proceeded to purchase such property.⁶⁰² Section 240(3) of the *Criminal Procedure Act*⁶⁰³ must be borne in mind. It provides that -

⁵⁹⁷ 1971 2 SA 362 RAD:363C-D.

⁵⁹⁸ Snyman 1999:525; Hunt-Milton 1990:737. In *S v Ushewokunze* 1971 2 SA 362 RAD the court held (at 364B-C) that "if the State shows that an accused, when he received the stolen goods, must have foreseen the real possibility that the goods had been stolen and did not care whether the goods had been stolen or not, that is sufficient to prove guilty knowledge. It is not necessary to go further and decide why the accused did not make enquiries as to the ownership of the goods. If the facts show that he recklessly received the goods not caring whether or not they were stolen the crime is proved, provided, of course, he did not receive them for some lawful purpose, such as returning them to their owner or handing them over to the police."

⁵⁹⁹ *Supra*.

⁶⁰⁰ 1925 TPD 86.

⁶⁰¹ 1925 TPD 86:88.

⁶⁰² For instance in *R v Lee* 1952 2 SA 67 T the court noted (at 71E): "The tape is not the sort of property which a fifteen-year-old native boy would normally have in his possession ... Furthermore the boy gave the accused an explanation of his possession of the two tins which was clearly false".

⁶⁰³ Act 51/1977.

"Where the accused is proved to have received the property which is the subject of the charge, from a person under the age of eighteen years, he shall be presumed to have known at the time when he received such property that it was stolen property, unless it is proved

- (a) that the accused was at that time under the age of twenty-one years; or
- (b) that the accused had good cause, other than the mere statement of the person from whom he received such property, to believe, and that he did believe, that such person had the right to dispose of such property." (own emphasis)

Therefore, where someone purchases any digital information or data from A, a *hacker* under the age of 18, the law presumes that the former knew that the content ("property") was stolen unless he can prove that good reasons existed for him to believe that A was permitted to dispose of such content.

Furthermore, section 240 provides that the prosecution is allowed to submit evidence to the effect that the accused was, within the period of twelve months immediately preceding the date on which he first appeared in a magistrate's court in respect of a charge of receiving stolen property knowing that it was stolen, found in possession of other stolen property. A court of law may take this into consideration for the purpose deciding whether the accused knew that the property, which forms the subject of the present charge, was stolen property.⁶⁰⁴ Section 241 is also available to the prosecution. It provides that -

"evidence may at any stage of the proceedings be given that the accused was, within the five years immediately preceding the date on which he first appeared in a magistrate's court in respect of such charge, convicted of an offence involving fraud or dishonesty, and such evidence may be taken into consideration for the purpose of proving that the accused knew that the property found in his possession was stolen property."

Therefore, in conclusion, it may be stated that where A hacks into B's computer and copies electronic content (such as information or passwords) and subsequently sells this to C, the latter knowing or suspecting or believing that such digital content is stolen property, C is guilty of receiving stolen property knowing that it is stolen.

The final question remaining is whether the owner of a web site, where the *hacker* posted the passwords or digital information for display, is guilty of receiving stolen

property knowing it to be stolen. It has already been submitted that such digital content can form the subject of this offence. It is further submitted that the owner of the web site (X) receives the stolen property in that he gains control over the property. When information is uploaded to a web site, a copy of the file is copied onto the server's hard drive and consequently X gains control over the digital content in that it is located on his computer and he can remove it at will. Normally where web site owners allow other Internet surfers to post information or files, the latter can only copy such information onto the web site owner's hard drive but cannot delete (remove) the information thereafter. Therefore the web site owner has full control over the "property". One of the remaining questions is whether X knew that the information or passwords posted on his site constituted stolen property when it was posted onto his web site? This question is preceded by another question namely whether he knew that he was receiving property? Two scenarios can arise:

- a) Where the web site owner (or an employee such as his system administrator) actively monitors the web site and material or content posted on the web site – this will be a question of fact.
- b) Where the web site owner (or an employee) either does not monitor the content or seldomly monitors it.

In the case of (a), it can be argued that both elements of receiving stolen property into possession are complied with as soon as he acquires the knowledge (either himself or by means of an employee) that content has been posted on his web site. With regard to the question whether he knew, suspected or believed that the property was stolen, it is submitted that whenever passwords are posted on this web site, the owner of the site must immediately suspect that it is stolen property. Stated differently, suspect that such passwords were illegally obtained. Whether other information posted on this web site will raise similar suspicions will depend upon the particular information. As noted above, *dolus eventualis* is sufficient: therefore if the state can prove that the web site owner foresaw the possibility that such information/data might be stolen, but acted recklessly, the court will hold that he had the necessary knowledge and may therefore find him guilty of receiving.

In the case of (b), the prosecution will find it very difficult to prove (if not impossible) that the web site owner was aware of the fact that the particular content was located or

⁶⁰⁴ S 240(1) & (2).

posted on his web site, unless the web site owner drew attention to the particular content.

Two final aspects must be dealt with. In *R v Von Elling*⁶⁰⁵ the Supreme Court of Appeal noted that it is not a requisite that the accused controls the property for his own gain or profit.⁶⁰⁶ Therefore it is no defence for the web site owner to allege that he gained no profit from receiving control over the digital content. In passing it should be stated that web site owners do profit from such illegal content posted on their web sites in that such content draws Internet surfers to their web pages and this, in turn, can lead to other profit making scenarios, for instance by offering products for sale on the web site or requesting and obtaining donations, etc.

Finally, some courts have enunciated that it is not necessary for the receiver or acceptor of the goods to have knowledge of what the exact content of these goods is.⁶⁰⁷ In appropriate circumstances the "doctrine of recent notice" applies which stipulates that where the accused is found in possession of recently stolen property and he fails to provide an explanation which might reasonably be true, the "court may infer from the facts ... that he received the goods knowing them to be stolen."⁶⁰⁸

3.3.2. General Law Amendment Act 62 of 1955

In the previous paragraph it was concluded that receivers of stolen digital content, knowing or suspecting or believing that such content is stolen, are guilty of the common law offence of receiving stolen property knowing that it is stolen. The next question to be addressed is whether these receivers are also guilty of certain statutory

⁶⁰⁵ 1945 AD 234.

⁶⁰⁶ 1945 AD 234:251. It would appear that some courts have tacitly enumerated that the accused must have received the property for his own gain or profit. See *Ex Parte Minister of Justice: in Re R v Maserow & Another* 1943 AD 164 where the Supreme Court of Appeal noted (at 170) that receiving was the acquiring of "stolen property from the thief not for the purpose of assisting the thief but for his own profit or gain." In *R v Nkwana* 1953 2 SA 190 T the court envisaged a broader element by stating (at 191H-192A) that "'n [b]ewering dat 'n persoon wederregtelik gesteelde goed met kennis dat dit gesteel is ontvang het, hou onomwonde die bewering in dat hy 'n 'ontvanger' is *of vir sy eie voordeel of vir die voordeel van iemand anders as die ware eienaar.*" (own emphasis). [own translation: An allegation that a person unlawfully received stolen property with the knowledge that it is stolen, necessarily includes an allegation that he is a 'receiver' either for his own benefit or for the benefit of someone else than the true owner.]

⁶⁰⁷ *R v Van der Bank* 1941 TPD 307:310.

⁶⁰⁸ Hunt-Milton 1990:740.

provisions in the *General Law Amendment Act*,⁶⁰⁹ specifically sections 36 and 37. Section 37(1), as amended,⁶¹⁰ provides that:

“(a) Any person who in any manner, otherwise than at a public sale, acquires or receives into his or her possession from any other person stolen goods, other than stock or produce as defined in section one of the Stock Theft Act, 1959, without having reasonable cause for believing at the time of such acquisition or receipt that such goods are the property of the person from whom he or she receives them or that such person has been duly authorized by the owner thereof to deal with or to dispose of them, shall be guilty of an offence ...

(b) In the absence of evidence to the contrary which raises a reasonable doubt, proof of such possession shall be sufficient evidence of the absence of reasonable cause.”
(my underlining)

This provision is relevant to computer-related crimes in the following instance: A hacks into B's computer and steals confidential information. A subsequently sells this information to C. Where C cannot prove that reasonable grounds existed, when he received the data, upon which he relied that A was the lawful owner of such information or was authorised to sell such information, C can be prosecuted in terms of section 37(1).

Section 36 provides that:

“Any person who is found in possession of any goods, other than stock or produce as defined in section one of the Stock Theft Act, 1959 (Act 57 of 1959), in regard to which there is reasonable suspicion that they have been stolen and is unable to give a satisfactory account of such possession, shall be guilty of an offence”. (my underlining)

This offence is relevant to cybercrimes: Where the South African police raids or confiscates a *hacker's* computer system and finds confidential data or passwords on this system, which clearly does not belong to him and he is unable to furnish a satisfactory account of his possession, the state can prosecute him for being in possession of such digital property (content).

3.3.2.1. Meaning of “goods”

Before examining the elements of sections 36 and 37, the meaning of the word

⁶⁰⁹ Act 62/1955.

⁶¹⁰ By s 2 of the *Judicial Matters Amendment Act* 62 of 2000, which entered into force on 23/3/2001.

“goods” must first be determined in order to ascertain whether the same meaning can be attached to “goods” as to “property”. Stated differently, it must be determined whether “goods” include electronic content.

In *R v Monyane en 'n Ander*,⁶¹¹ which concerned the question whether money was “goods” for the purpose of section 36, the court noted that -

“[d]ie woord [goedere] het nie 'n tegniese betekenis nie en soos blyk uit die Afrikaanse Woordeboek het dit 'n wye en onbepaalde betekenis. Die eintlike betekenis van die woord hang dus in elke geval af van die besondere sin en verband waarin dit gebruik word. Waar die woord soos in die onderhawige geval in 'n statuut gebruik word ontleen dit sy eintlike betekenis aan die verband waarin dit gebruik word, dit wil sê beide die onmiddellike verband van die artikel waarin die woord voorkom en die algemene verband van die statuut met inagneming van die verklaarde bedoeling van die statuut en die ooglopende euwel wat dit beoog is om te bestry.”⁶¹²

The preamble of the *General Law Amendment Act* states that the purpose of this Act is to amend the law relating “to the possession and acquisition of stolen property”.⁶¹³ (own underlining)

Furthermore, the court observed that:

“Goed sluit dus in goed wat uit hulle aard regtens gesteel kan word. Geld word gewoonweg onder sulke goed ingesluit. Voordat die betekenis van die woord ‘goed’ ondersoek word aan die hand van die verband en die sin waarin dit in die gemelde arts. 36 en 37 gebruik word, is dit miskien raadsaam om vir 'n oomblik te let op die aard van geld wat in omloop is. Waar geld gesteel word, word normalerwys gelet op hoeveelheid en nie die besondere munt of banknote wat gesteel word nie. Daar kan natuurlik gevalle wees waar op die spesifieke munt of banknote gelet word, waar dit byvoorbeeld in 'n besondere vorm of wyse bewaar is en so teruggevind word of waar dit gemerk is. Anders as in die geval van gesteelde goed in die engere sin van die woord wat nie geld insluit nie, kan gesteelde geld nie van 'n derde persoon wat dit *bona fide* verkry het, teruggevorder word nie. Sodra dit met sy geld vermeng is, is die identiteit daarvan

⁶¹¹ 1960 3 SA 20 T.

⁶¹² 1960 3 SA 20 T:22D-E. [own translation: The word goods does not have a technical meaning and as appears from the Afrikaans' dictionary it has a wide and indeterminate meaning. The actual meaning of the word therefore depends in each case upon the context in which it is used. Where the word is used in a statute, as in the present instance, it derives its actual meaning from the context wherein it is used, that is the immediate context in which the word appears and the general context of the act, taking the postulated object of the act as well as the mischief which it is aimed to expunge into consideration.]

verloor ... Indien die aard van geld, wat in omloop is, in gedagte gehou word, kon dit nie die bedoeling van die wetgewer gewees het om gangbare geld by die betekenis van goed, soos die woord gebruik word in art. 37, in te sluit nie. Die teendeel sou 'n onhoudbare toestand skep en 'n ondraaglike verantwoordelikheid op verkopers van goedere en handelsbanke plaas en die omloop van geld ernstig strem."⁶¹⁴ (own emphasis)

The court went on to state that:

"Mynsinsiens het *die wetgewer goed beoog wat gesteel kan word en uitkenbaar is*. Dit mag in sekere gevalle wel geld insluit waar dit nie as gangbare geld of geld in omloop beskou kan word nie en in *specie* uitkenbaar is."⁶¹⁵ (own emphasis)

This case was followed in *S v Boshoff*⁶¹⁶ where the question of law was whether the word "goods" in terms of section 36 covered or included unidentified currency in the form of banknotes.⁶¹⁷ The court confirmed that the word "goed" (in die Afrikaans text) "is not a technical term but that it has a wide and indeterminate content ... and may, in this regard, be equated to the word 'goods' which is used in the English version. It is equally clear that the word 'goods' can in appropriate circumstances, comprehend or include certain varieties of currency."⁶¹⁸ The court took notice of the maxim "*in poenis strictissime verborum significatio accipienda est*"⁶¹⁹ and continued to state that:

⁶¹³ See 1960 3 SA 20 T:22F.

⁶¹⁴ 1960 3 SA 20 T:23A-D. [own translation: Goods therefore include goods that can legally be stolen due to their nature. These goods normally include money. Prior to investigating the meaning of the words 'goods' by means of the context wherein it is used in sections 36 and 37, it is wise to observe the nature of money in circulation. Where money is stolen, the emphasis is normally on the quantity and not the particular notes or coins stolen. Of course, there can be instances where the emphasis is on the particular notes or coins, for instance where it was marked or where it was encumbered in a specific manner or way and thus found. Contrary to the theft of stolen goods, as understood in the strict meaning of the word that does not include money, money cannot be reclaimed from a third party that received it *bona fide*. As soon as it mixes with his own money, it loses its identity ... If the nature of money, in circulation, is kept in mind, it could not have been the intention of the legislature to include money in circulation within the meaning of the word goods, as used in section 37. The opposite would entail an untenable position and would impose an unbearable responsibility upon sellers of goods as well as mercantile banks and would further severely restrain the circulation of money.]

⁶¹⁵ 1960 3 SA 20 T:23D-E. [own translation: Of necessity then, the legislature contemplated goods that can be stolen and which are identifiable. Under given circumstances it may include money where it is not regarded as money in circulation and which is identifiable in *specie*.]

⁶¹⁶ 1962 3 SA 175 N.

⁶¹⁷ 1962 3 SA 175 N:176F-G.

⁶¹⁸ 1962 3 SA 175 N:176H.

⁶¹⁹ Freely translated: "a penal provision must be strictly interpreted".

"In particular, since the words 'any goods' are at least ambiguous, attention must be paid to a series of Full Bench decisions in various Provinces to the specific effect that 'if there is a reasonable interpretation which will avoid the penalty in any particular case, the Court should adopt that construction' ... Thus, unless there is a *compelling necessity* - arising from the discernible 'mischief' and object of sec. 36 - to hold that 'any goods' there includes money or currency, it should be decided that it does not. This would enable the accused to avoid attracting the penalty in this particular case. In my view there is no such compelling necessity. With respect, the reasons given in *Monyane's* case, *supra*, appeal to me as showing that the contrary is true and that there are sound practical reasons why unidentifiable money should not be held to be included in the term 'any goods'. In addition it must be remembered that ... such provisions 'should be very discreetly administered, otherwise these sections may very easily become instruments of oppression in the hands of over-zealous policemen' ... Thus in my judgment there is no compelling necessity to hold that the Legislature intended *unidentified* current money to be included within the prohibition contained in sec. 36."⁶²⁰ (own emphasis)

Therefore, the effect of the *Monyane* and *Boshoff* judgments is that money in general circulation is not included within the meaning of the word "goods", as used in sections 36 and 37.⁶²¹ In *S v Mohapie*⁶²² the question of law was whether the word "goods" encompassed foreign currency such as a 100 dollar note. The court confirmed the *Monyane* judgment to the effect that "money which is identifiable or which consists of currency which is not in normal circulation, is goods within the meaning of sec. 36 of the Act."⁶²³ The court continued:

"In the present case there was a 100 dollar note, which is not normally in current circulation in South Africa, and the note was, as I have said, identifiable in the sense that it formed part of the list of [stolen] notes which was in the possession of Mr. Elliot or of Thos. Cook & Son. The evidence that such a list existed would, of course, always be admissible in order to establish identification of the particular note in question. I am,

⁶²⁰ 1962 3 SA 175 N:177D-178B. The court confirmed (at 178A-B) the reasons expressed by the *Monyane* court for holding that section 36 and 37 did not include unidentifiable money: "In my view such criticism is not justified since it would indeed be extremely difficult for such persons to discharge the onus placed upon the possessor of stolen goods in terms of sec. 37 which was passed simultaneously with, and in the same enactment as, sec. 36."

⁶²¹ See *S v Mohapie* 1969 4 SA 446 C:447C-D.

⁶²² 1969 4 SA 446 C.

⁶²³ 1969 4 SA 446 C:447F.

therefore, of the view that this note represented 'goods' within the meaning of that word in sec. 36 of the said Act."⁶²⁴

In *S v Ganyu*,⁶²⁵ a Zimbabwean judgment, the court, also dealing with the question whether money was included in the term "goods," observed:

"Assuming the word 'goods' is wide enough to include money, could it possibly have been the intention of the Legislature that sec. 14 (2) [of the Zimbabwean Miscellaneous Offences Act, Chap 68; the counterpart of section 37] would not apply to the acquisition or receipt of currency proved to have been stolen? The answer, I believe, is very clearly in the negative ... The common law offences of theft and receiving will usually prove inadequate where the State is not in a position to prove the identity of the owner of the goods and where this is the situation the statutory provisions are invoked. Bearing in mind the purpose of the legislation, there is no possible reason why sec. 14 should be construed to relate to some goods only and not to all goods, to some money but not all money. To the extent to which the section is held not to apply to certain goods, the legislation becomes *pro tanto* ineffective. Since the section is clearly intended to deal with theft generally, in my view the word 'goods' must of necessity be given a wide and unrestricted meaning so as to embrace goods generally and not only some goods. Once it is decided that so construed the word includes money, there is no justifiable reason for including some types of money and excluding others. To do so would not only partially defeat the purpose of the legislation, but would also involve reading into the section words which are not there and cannot properly be implied ... I have some difficulty in any event in understanding the sense in which the word 'identifiable' is used in these cases. It cannot possibly mean that the money must be identified as being stolen money, because if that is established there is no room at all for the application of sec. 14 (1). If it means something else, what is the restricted meaning and, even more importantly, what is the purpose of the restriction?"⁶²⁶

Turning to other legislation, the court in *Padyachi v R*⁶²⁷ was of the opinion that the word "goods" in section C(2) of the regulations contained in *Government Notice 161 of 1917* (precursor of the *Customs Act*) included gold coins. The court observed that:

"I think it may be conceded that in many cases, perhaps in the ordinary case, the word 'goods' is not to be taken to comprehend current coin of the realm, although in its general sense, it is wide enough to do so. But, as has been pointed out ... 'Even where

⁶²⁴ 1969 4 SA 446 C:447F-G.

⁶²⁵ 1977 4 SA 810 RAD.

⁶²⁶ 1977 4 SA 810 RAD:812G-813C.

⁶²⁷ 1919 NPD 145.

the usual meaning of the language falls short of the whole object of the legislature, a *more extended meaning may be attributed to it*, if fairly susceptible of it. If there are circumstances in the Act showing that *words are used in a larger sense than their ordinary meaning*, that sense must be given to them.' That 'goods' is fairly susceptible of the wider meaning which will include money I think is clear ... And I can see no reason for holding that in the form of money it is not covered by the expression 'goods' for the purposes of the Act. Even therefore if it be conceded that in its ordinary meaning the word 'goods' will not include money I see no reason why the more extended meaning of which it is susceptible should not be attributed to it here because I think that the circumstances of the Act *show that the word is used in its larger sense*."⁶²⁸ (own emphasis)

The court (although a different judge) further made the following remark:

"There are few nouns in the English language which are not capable of both a restricted and an extended meaning. In construing a statute it is the duty of the Court so to construe it as to *suppress the mischief and advance the remedy*. The word 'goods,' like many other words, is capable of either a restricted or an extended meaning."⁶²⁹

Bearing the above-mentioned court cases in mind, it can safely be stated that a) digital content (such as confidential data as well as passwords) are "property" (within the broad meaning of the word) capable of being stolen; b) digital data and passwords are clearly identifiable objects and cannot be equated with normal currency. Certain electronic photographs, for instance Playboy photographs, are also identifiable objects; c) some courts, although not South African courts, have been willing to give a wide interpretation to the word "goods" in view of the purpose that sections 36 and 37 serve and d) by giving "goods" an interpretation which includes digital content ("property") a court will advance the remedy provided by the legislature.

The next step is to undertake a study in terms of the law of statutory interpretation. The dictionary meanings of the words "goedere" and "goods", the mischief at which these sections are aimed as well as relevant common law presumptions need, therefore, to be examined.

One of the meanings which the *Oxford Advanced Learners Dictionary*⁶³⁰ ascribes to "goods" is "possessions that can be moved: stolen goods". It also defines "property" as

⁶²⁸ 1919 NPD 145:147-148.

⁶²⁹ 1919 NPD 145:149.

⁶³⁰ <http://www1.oup.co.uk/elt/oald/>.

"a thing or things that are owned by [somebody]; a possession or possessions". *Webster's Third New International Dictionary* defines "goods" as "tangible movable personal property having intrinsic value usu[ally] excluding money and other choices in action but sometimes including all personal property and occas[ionally] including vessels and even industrial crops or emblements, buildings". One of the meanings which *The Shorter Oxford English Dictionary* attaches to the word "goods" is "property." The "*Verklarende Woordeboek van die Afrikaanse Taal*" defines "goed"⁶³¹ as "Versamelnaam vir besittings; ... Handelware ... geweeftde goedere".⁶³² It also defines "goed" as "Wat aan 'n persoon of liggaam behoort; besitting".⁶³³ Therefore, dictionaries ascribe more or less the same meaning to "goods" as to "property".

The mischief that the provisions of the *General Law Amendment Act* seek to eradicate is fourfold:

- a) It is very difficult, under given circumstances, for the state to prove that the accused, when he received the property, knew that such property was stolen.⁶³⁴ In terms of section 37, the onus is placed on the accused to show that he had reasonable grounds to believe that such property was not stolen property, when he received it and in terms of section 36 the onus is placed on the accused to give a satisfactory account of being in possession of the property, suspected to be stolen.⁶³⁵
- b) These sections can be invoked where the state cannot prove to whom the stolen property belongs.⁶³⁶ This is, of course, a very useful remedy where the state searches a *hacker's* hard drive and finds confidential files concerning other companies or passwords rendering access to other computers. It is not incumbent upon the state to prove to whom such digital content belongs.

⁶³¹ [own translation: goods.]

⁶³² [own translation: Collective name for possessions ... commercial products ... woven goods.]

⁶³³ [own translation: that which belongs to a person or body; possession.]

⁶³⁴ The purpose of section 37 is "to cover, inter alia, cases where the accused receives stolen property direct from the thief but the Crown is unable to prove knowledge of the theft." *R v Vilakazi* 1959 4 SA 700 N:701G. See also Snyman 1999:526 & 532; Hunt-Milton 1990:741.

⁶³⁵ In the Assembly one of the ministers (but not the Minister of Justice) noted that "[t]his clause [section 37] is evidently aimed at the activities of receivers of stolen property." (At p 6912 of the *Hansard*, 2 June 1955).

⁶³⁶ In *S v Ganyu* 1977 4 SA 810 RAD the court noted (at 813A) that the underlying reason for section 37 is "to cope with the situation in which there is no evidence to identify the owner of the goods reasonably suspected of having been stolen." See Snyman 1999:526.

c) Section 36 penalises (*inter alia*) persons selling stolen property (goods).⁶³⁷

d) To combat theft.⁶³⁸

When interpreting sections 36 and 37 the following common law presumptions are relevant:

(i) *The legislature does not intend to alter the existing law more than is necessary*

Firstly, this presumption means that a statutory provision must be interpreted within its context: "This is achieved by reading the words in the light of their immediate linguistic context as well as their wider legal and jurisprudential context."⁶³⁹ Devenish puts the effect of this presumption as follows:

"The presumption therefore results in a restrictive interpretation in favour of the existing general system of law, common and statutory ... Therefore, statutes should, as far as possible, be construed 'in conformity with the common law rather than against it' ... However, if it is categorically clear from both the language and the import of the statute that it is designed to alter the common law, 'then full effect must be given to this object.' Alteration to the common law by a statute 'must either expressly say that it is the intention of the legislature to alter the common law, or the inference ... must be such that we can come to no other conclusion.' Our courts require clear and unequivocal language to effect a change to the common law."⁶⁴⁰

(ii) *The extension, restriction, or modification of language may be necessary to give effect to the intention or purpose or design of the legislation.*

⁶³⁷ See the debate in the Senate: p 4498-4499 of the Afrikaans text. The English text was not available.

⁶³⁸ Snyman 1999:528. In the Senate, the Minister of Justice stated the following concerning the proposed sections 36 and 37: "Dan word daar bepalinge gemaak in verband met diefstal. Ons vind dat daar deesdae geweldig baie gasteel word, diefstalle van sake soos koperdraad van telefoondrade, motorradio's en talle sulke dinge word voortdurend gasteel en die persoon wat dit gaan steel dit orals verkoop." At p 4498, 16 June 1955. [own translation: Also included are provisions concerning theft. We find that currently a lot of theft occurs, theft of property such as copper cables of telephone cables, motor radios and numerous such things are continuously stolen and the person who steals it, selling it everywhere.]

⁶³⁹ Devenish 1992:289. At p 290 he maintains that "statute law must be interpreted against the background of an evolving and dynamic common law."

⁶⁴⁰ Devenish 1992:159-161. See also *Johannesburg Municipality v Cohen's Trustee* 1909 TS 811 where the court stated (at 823) that "[i]t is a sound rule to construe a statute in conformity with the common law rather than against it, except where and so far as the statute is plainly intended to alter the course of the common law."

This is not a presumption, but a principle of common law and Devenish explains it as follows: "The extension, restriction, or modification of the ordinary meaning of words may be necessary to give expression to the meaning of the legislation and to establish the legal meaning of words using the context of the legislation."⁶⁴¹

In this regard it may be stated that the common law offence, as background to sections 36 and 37, is the offence of receiving stolen property knowing it to be stolen. Furthermore, the aim of these provisions was not to change the common law offence, but to supplement it in order to assist the state in prosecuting individuals in possession of stolen property where it is unable to prove that these individuals had reasonable grounds to presume that it was not stolen property. Therefore it can be argued that the word "goods" must be construed widely to include property in general, which, in turn, will include both corporeal as well as incorporeal property. The possible counter-arguments to this submission may be threefold:

- a) When the legislature promulgated sections 36 and 37, theft of digital data/content was unknown.
- b) To bring digital content within the meaning of the word "goods" is far-fetched.⁶⁴²
- c) Sections 36 and 37 are penal provisions and therefore "goods" must be given a strict interpretation.⁶⁴³

The argument to the first statement is that one should refrain from emphasising what was and was not known to the legislature, when the Act was promulgated. Since the *Interim Constitution*⁶⁴⁴ came into operation in 1994, South African courts, especially the Constitutional Court, have followed a contextual approach to the interpretation of statutes, focusing on the aim and purpose of the statute, rather than on the "intention of the legislature". The former is much more objectively determinable than the latter. Therefore, as stated numerous times, the mischief that these provisions endeavour to encompass must be looked at and from this perspective, their purpose and aim must be determined.

⁶⁴¹ Devenish 1992:289.

⁶⁴² In *Union Share Agency & Investment Ltd v Spain* 1944 AD 74 the Supreme Court of Appeal maintained (at 77) that "[t]he words 'for goods sold and delivered' [as stated in the Prescription Act] are in common use and are well understood. They would ordinarily not include a sale of shares ... as the language of this section is perfectly clear and cannot be extended to a sale of shares."

⁶⁴³ Snyman 1999:528; Hunt-Milton 1990:662.

⁶⁴⁴ Act 200/1993.

With regard to the second statement, it is submitted that the courts have already interpreted the word "goods" wider than its narrow meaning, by holding that it includes foreign currency that can be identified and that it includes any "goed wat uit hulle aard regens gesteel kan word".⁶⁴⁵ Therefore South African courts might be willing, when the issue arises, to include digital property within the meaning of the word "goods" as stated in sections 36 and 37, provided that no specific cybercrime statutory legislation exists, criminalising such illegal transgressions.

However, the third counter argument indicated above cannot be side-stepped that easily. These sections remain penal provisions that must be strictly interpreted.

To summarise: many South African courts have maintained that the word "goods" does not have a technical meaning and that it should be given a wide interpretation in order to refer to property than can be stolen; the aim and purpose of these provisions are to supplement the common law with regard to the possession and acquisition of stolen property; previous judgments, dealing with the question whether unidentifiable currency falls within the ambit of these provisions, have no bearing on the issue whether incorporeal property can be included within the meaning of "goods"; various courts have indicated that the word "goods" must be given an extended meaning to eradicate the mischief at which these provisions are aimed; one South African court, however, refused to include shares within the meaning of "goods"; and finally these sections are penal provisions. Keeping the above in mind, it is submitted that South African courts may be willing to extend the meaning of "goods" to include incorporeal data. However, this issue remains uncertain. For this reason, the requirements of sections 36 and 37 are briefly discussed.

3.3.2.2. Elements of the offence in terms of section 37

The prosecution must prove that a) the accused received into his possession b) stolen property.⁶⁴⁶ The possession element, in turn, entails two requirements namely physical control and *detentio* (the accused knew that he had control of the property in question).⁶⁴⁷ Where the prosecution succeeds in proving these factors, the accused

⁶⁴⁵ See *R v Monyane en 'n Ander (Supra)*.

⁶⁴⁶ In *R v Vilakazi* 1959 4 SA 700 N the court maintained (at 701H-702B) that section 37 also applies to *theft by false pretences*: "Any goods fall into the category of stolen goods irrespective of the manner in which they were stolen."

⁶⁴⁷ *Manamela & Another v S* 1999 4 ALL SA 161 W:166g-h; *S v Moller* 1990 3 SA 876 A:887F-G.

bears the onus to prove on a balance of probabilities that he had (at the moment when he received the property⁶⁴⁸) reasonable cause (grounds) to believe that the person from whom he received possession was the owner or authorised seller of the property.⁶⁴⁹ Possession of stolen property establishes a rebuttable presumption that there were no reasonable grounds to believe that the person from whom the accused obtained the property was the owner or authorised dealer of such property.⁶⁵⁰

3.3.2.3. Elements of the offence in terms of section 36⁶⁵¹

The elements of this offence are that a) the accused was found in possession of goods;⁶⁵² b) a reasonable suspicion existed, when the accused was found in control of the property, that such property was stolen and c) the accused is not able to give a satisfactory explanation of the possession.⁶⁵³ The onus is on the state to prove that such reasonable suspicion existed as well as that the accused is unable to give a satisfactory explanation.⁶⁵⁴

Element (b) entails that the police officer who found the accused in possession of the property must at that specific time⁶⁵⁵ have suspected that it was stolen and he must be able to prove that reasonable (objective) grounds existed for his suspicion. He must prove that the reasonable person would also have held such a belief.⁶⁵⁶ Snyman

⁶⁴⁸ *S v Mkhize* 1980 4 SA 37 N:39A.

⁶⁴⁹ See Snyman 1999:532; LAWSA 1996:vol 6, par 445; Hunt-Milton 1990:742-743. In *S v Mkhize* 1980 4 SA 37 N the court noted (at 38C) that s 37 "does not require him to investigate the matter fully if the circumstances in which he receives the goods would satisfy a reasonable man on a balance of probabilities that the goods in question were the property of the person from whom he received them. If he establishes that, he is entitled to an acquittal."

⁶⁵⁰ S 37(1)(b).

⁶⁵¹ Two courts, namely *S v Du Toit* 1995 2 SACR 651 K and *Osman v Attorney-General of Transvaal* 1998 1 SACR 28 T, have maintained that s 36 is justified in terms of the *Constitution*.

⁶⁵² In *S v Wilson* 1962 2 SA 619 A the Supreme Court of Appeal held (at 623E-F) that an accused would still be in possession of the goods even if he was temporarily absent from the premises where it was stored or kept. See also *S v Mangquku* 1971 2 SA 365 E:368A-B.

⁶⁵³ *S v Du Preez* 1998 2 SACR 133 K:136i-137a; *S v Langa & Others* 1998 1 SACR 21 T:25h-j; Snyman 1999:527; LAWSA 1996:vol 6, par 445; Hunt-Milton 1990:661.

⁶⁵⁴ *S v Du Preez* 1998 2 SACR 133 K:137b; *S v Khumalo* 1964 1 SA 498 N:505E.

⁶⁵⁵ *S v Du Preez* 1998 2 SACR 133 K:136i-j; *R v Ismail & Another* 1958 1 SA 206 A:213A.

⁶⁵⁶ Snyman 1999:529; Hunt-Milton 1990:664-665. However, in *S v Zuma* 1992 2 SACR 488 N the court was of the opinion (at 490-491) that any court may, under the appropriate circumstances and where the finder failed to mention that he suspected such property to be stolen and to show his reasonable grounds for such belief, infer both such suspicion and grounds from the known facts. In *S v Khumalo*

indicates the following factors that will determine whether such suspicion was reasonable:

“[D]ie aard en hoeveelheid van die goed wat gevind is, die plek waar dit gevind is, die nuutheid van die goed, die finansiële vermoëns en status van X, en die reaksie van X toe die goed by hom gevind is.”⁶⁵⁷

Element (c) entails that the accused is not able to give a satisfactory explanation, either when the property was found in his possession or at the trial.⁶⁵⁸ His explanation will be satisfactory where a) it is reasonably possible and b) he indicates that he believed that his possession was *bona fide* and innocent.⁶⁵⁹

1964 1 SA 498 N the court maintained (at 499F-500D) that “[t]he suspicion that the goods are stolen goods must be formed, in the mind of some person, substantially contemporaneously with a finding of the accused in possession of them ... This subjective suspicion must be based upon grounds actually existing at the time of its formation ... It follows that the factual basis which would make any suspicion which is actually formed a reasonable one must also exist at the material time: a suspicion cannot be held to be reasonable if it is founded on non-existent facts ... a suspicion cannot be a reasonable suspicion if it is based upon a *non sequitur*, no more than a belief can be a reasonable belief if it is so based ... A suspicion originally based on insufficient grounds can become a reasonable suspicion as a result of something the accused says or does at the time when he is found in possession of the goods.” Furthermore, the court noted (at 505H-506A) that “[t]he reasonableness or otherwise of the suspicion must be judged upon the basis of the facts known to the person who entertains the suspicion at the time when he forms it, with, however, this qualification, that he may form the suspicion, perhaps not reasonably, but be confirmed in it by the facts he ascertains thereafter; those facts are to be taken into consideration in judging of the reasonableness of the suspicion, provided the person accused was still in possession. For practical purposes this means that when a policeman has found a person in possession of goods in circumstances which arouse a suspicion in his mind, and thereupon questions that person (as in the present case) whilst he is still in possession of the goods, and as a consequence is confirmed in his suspicions, all the information he obtains is to be taken into consideration in judging the question of reasonableness. One judges the reasonableness of his state of mind in the light of all the information he has before him.” In *S v Mohapie* 1969 4 SA 446 C the court maintained (at 448E-F) that “at the time of the trial the court must be satisfied that the suspicion as such is reasonable upon all the facts.”

⁶⁵⁷ *Snyman* 1999:530. [own translation: the nature and quantity of the goods, the place where they were found, whether they were still new, X’s status and financial standing, and X’s reaction when the goods were found in his possession.]

⁶⁵⁸ *Snyman* 1999:530; *LAWSA* 1996:vol 6, par 445; *Hunt-Milton* 1990:667. In *S v Khumalo* 1964 1 SA 498 N the court noted (at 500H) that “[i]f the accused gives no satisfactory account at the time he is found in possession of the goods but gives a satisfactory account at the trial, he will be entitled to an acquittal.”

⁶⁵⁹ *Snyman* 1999:530; *LAWSA* 1996:vol 6, par 445; *Hunt-Milton* 1990:667.

3.4. Fraud as a common law offence

Next, the question is addressed whether virus and hacking instances constitute fraud, according to the South African common law.

3.4.1. General elements

Fraud can be defined as the unlawful and intentional misrepresentation that causes actual prejudice, or is potentially prejudicial, to another.⁶⁶⁰ Therefore the elements of this offence are: (a) misrepresentation concerning an existing fact;⁶⁶¹ (b) actual or potential prejudice/harm;⁶⁶² (c) unlawfulness;⁶⁶³ and (d) intention.⁶⁶⁴

With regard to causation, the general opinion seems to be that because prejudice is so widely interpreted (potential prejudice will suffice), the causation requisite serves no purpose anymore.⁶⁶⁵ It is no longer required that deception has to be successful. The sole requirement is that the deception must be of such a nature that it is potentially prejudicial⁶⁶⁶ and therefore the court will hold that the accused committed fraud where there was actual prejudice which was not proven to be induced by the misrepresentation, provided the misrepresentation was potentially prejudicial.⁶⁶⁷

The intention element refers to two aspects: a) the accused must firstly know or

⁶⁶⁰ Snyman 1999:534; LAWSA 1999:par 322. In *R v Henkes* 1941 AD 143 the Supreme court of Appeal maintained (at 161) that the prosecutor must prove the following: "a perversion of the truth by the accused, that such perversion was wilful, that the accused made it with intent to defraud, and that the misrepresentation caused prejudice or was calculated to cause prejudice." See also *S v Isaacs* 1968 2 SA 187 D:191C.

⁶⁶¹ See *S v Isaacs* 1968 2 SA 187 D:191C-D.

⁶⁶² See Snyman 1999:538; LAWSA 1996:vol 6, par 328.

⁶⁶³ The court in *S v Campbell* 1991 1 SACR 503 Nm noted (at 506e-f) that: " 'Because a fraudulent misrepresentation is *ex hypothesi* unlawful, the element of unlawfulness is of scarcely any practical importance in fraud. ... Even if the party to whom the misrepresentation is made ... knew it had been false, it is no defence."

⁶⁶⁴ Snyman 1999:534; LAWSA 1996:vol 6, par 323.

⁶⁶⁵ Snyman 1999:541; LAWSA 1996:vol 6, par 323. For a contrary view see *S v Isaacs* 1968 2 SA 187 D, where the court stated (at 192A) that "[t]here must be a causal connection between the misrepresentation and the prejudice, whether the prejudice be actual or potential."

⁶⁶⁶ *R v Kruse* 1946 AD 524:533-534; Snyman 1999:541; LAWSA 1996:vol 6, par 328-330.

⁶⁶⁷ *R v Kruse* 1946 AD 524:533-534; LAWSA 1996:vol 6, par 330.

suspect that his (tacit or implied) representation/statement⁶⁶⁸ is false and b) the accused must intent to defraud the complainant. The "intent to defraud" entails that a mere intention to deceive someone does not suffice; an intention to cause someone prejudice is required. Generally speaking, this means that A must induce B to embark on a course of action prejudicial to himself as a result of the misrepresentation.⁶⁶⁹ Therefore the intent to defraud includes an intent to prejudice.⁶⁷⁰ In *R v De Vos*⁶⁷¹ the court approved the following explanation of "intent to defraud": "with intent to deceive in such a manner as to expose any person to loss or risk of loss."⁶⁷² It should also be kept in mind that the accused's motive is irrelevant and no intention to acquire some advantage is required.⁶⁷³

Next, it must be ascertained what prejudice entails. All South African courts have maintained that the prejudice element does not necessarily refer to financial or proprietary damages.⁶⁷⁴ Our courts have interpreted "prejudice" very widely and consequently it includes a vast spectrum of prejudice facets ("*benadelingsfasette*"). South African courts have indicated that the following constitutes potential prejudice:

- 1) Where the accused's conduct constitutes a risk of prosecution for the complainant or that the latter may lose his license (for instance to sell liquor).⁶⁷⁵

⁶⁶⁸ In *Standard Bank of South Africa v Coetsee* 1981 1 SA 1131 A the Supreme Court of Appeal maintained (at 1135F-G) that objectively "there must be clarity concerning 'the exact content' of the [implied or tacit] representation."

⁶⁶⁹ *Snyman* 1999:542; *LAWSA* 1996:vol 6, par 323 & 331; *R v Jones and More* 1926 AD 350:352: "there must be a wilful pervasion of the truth made with intent to defraud, and to the prejudice of another."

⁶⁷⁰ *LAWSA* 1996:vol 6, par 330.

⁶⁷¹ 1898 EDC 145.

⁶⁷² 1898 EDC 145:150.

⁶⁷³ *S v Shepard* 1967 4 SA 170 W:179D; *S v Van Biljon* 1965 3 SA 314 T:318; *LAWSA* 1996:vol 6, par 331.

⁶⁷⁴ *S v Myeza* 1985 4 SA 30 T:32C; *S v Kruger & Another* 1961 4 SA 816 A:828B; *R v Dhlamini* 1943 TPD 20:23; *LAWSA* 1996:vol 6, par 323 & 329.

⁶⁷⁵ See *R v De Vos* 1898 EDC 145:149 & 150. In *R v Seabe* 1927 AD 28 the facts were that the accused (a black person) pretended on several occasions that a European woman signed an order for a bottle of spirits. Black persons were not allowed to purchase spirits for themselves. The Supreme Court of Appeal noted (at 33) that potential prejudice was present in that there was a risk that the complainant who sold the spirits to him, on the basis of such misrepresentation, could be prosecuted for contravening the law. The risk also existed that the complainant could have his liquor license revoked due to such sale. The court further stated (at 33-34): "It has been said that Seabe had no *mens rea*; no intention to defraud anyone. He merely wanted to get the liquor. That, however, is no answer. If he intended to obtain liquor by false pretences ... and by doing so he prejudiced the person who supplied him with the liquor, then he is guilty of [fraud]".

- 2) Where the accused's conduct constitutes a risk of dishonour or loss of reputation to the complainant.⁶⁷⁶ In *R v Dlamini*⁶⁷⁷ the court maintained that a court must take "the widest view ... of what prejudice means. It includes impairment of reputation or personal dignity ... and we have assumed that the term is wide enough to cover any substantial inconvenience which the perpetration of the forgery may cause ... The question is not what the forger obtains, but what the effect, or the potential effect, is upon some person other than the forger."⁶⁷⁸ Various other courts, including the Supreme Court of Appeal, have also stated that "potential prejudice to one's honour or to one's reputation" is sufficient.⁶⁷⁹ Some courts have even stated that "a man's good name and reputation are more of value to him than his purse".⁶⁸⁰
- 3) Where the accused's conduct constitutes a risk that the state may e.g. lose control over petrol consumption and/or liquor consumption and/or drivers of motor vehicles and/or foreign exchange.⁶⁸¹ In *R v Heyne & Others*⁶⁸² the Supreme Court of Appeal concluded:

"False representations, calculated to weaken that control by deceiving the police, are also calculated to harm the State really and not only theoretically. The requirement of prejudice is thus satisfied by the risk of harm to the State".⁶⁸³

The same line of argument can be seen in *R v Thabeta & Another*.⁶⁸⁴ The first accused wrote a teacher's examination on behalf of the second accused. The court observed that "[t]here was ... a possibility of prejudice to the Departmental examiners in having passed an entrant who was not fit to pass in the written examination."⁶⁸⁵ This also bears a resemblance of the risk to control individuals

⁶⁷⁶ Some of our common law authorities, such as Carpzovius, consider that dishonour or loss of reputation may alter mere deceit into criminal fraud. See *R v Seabe* 1927 AD 28:33.

⁶⁷⁷ 1943 TPD 20.

⁶⁷⁸ 1943 TPD 20:23.

⁶⁷⁹ *R v Macatlane* 1929 TPD 708:712. See also *S v Ressel* 1968 4 224 A:232F-G; *R v Heyne & Others* 1956 3 SA 604 A:624H; *R v Jolosa* 1903 TPD 694:698.

⁶⁸⁰ *R v Jolosa* 1903 TPD 694:698.

⁶⁸¹ *R v Heyne & Others* 1956 3 SA 604 A. See the authorities quoted on p 623. See also *S v African Bank of South Africa Ltd & Others* 1990 2 SACR 585 W:647e-f; *R v Jass* 1965 3 SA 248 E:250F-G; *R v Thebeta* 1948 3 SA 218 T:222; Snyman 1999:540; LAWSA 1996:vol 6, par 329.

⁶⁸² 1956 3 SA 604 A.

⁶⁸³ 1956 3 SA 604 A:625A.

⁶⁸⁴ 1948 3 SA 218 T.

⁶⁸⁵ 1948 3 SA 218 T:222.

who are allowed to teach pupils at schools.

4) Where the accused's conduct infringed third parties' rights. The following court cases illustrate this aspect:

A) In *S v Myeza*⁶⁸⁶ the court noted that:

"Die nadeel hoef nie noodwendig die persoon teenoor wie die wanvoorstelling gemaak is te tref nie ... [nadeel] sluit ook in die risiko van nadeel vir die Staat, plaaslike gemeenskappe, publiek *en derde persone in die uitoefening van hulle regte en die nakoming van hulle verpligtinge.*"⁶⁸⁷ (own emphasis)

B) In *R v Jones & Others*⁶⁸⁸ the Supreme Court of Appeal maintained that prejudice "include any invasion of his civil rights."⁶⁸⁹

5) Where the accused's conduct affected the complainant's state of mind. In *S v Harper & Another*⁶⁹⁰ the court maintained that "[i]f the misrepresentation is likely to lull the investor into a false sense of security about the investment he has already made then, in my view, it involves the risk of harm ... These representations were potentially prejudicial because, quite apart from any other consideration, they would affect the state of mind of each investor when that investor was considering ... whether or not to renew his investment or ... whether or not to give notice withdrawing the investment."⁶⁹¹ (own emphasis)

6) Where the accused's conduct affects the general public.⁶⁹² In *R v Frankfort Motors (Pty) Ltd & Others*⁶⁹³ the facts were that the first accused was a company controlling a petrol station. The directors procured by means of false documents more petrol from the main sellers of petrol (such as BP and Shell) than they were allowed to by law. The court held that the accused's conduct prejudiced the state,

⁶⁸⁶ 1985 4 SA 30 T.

⁶⁸⁷ 1985 4 SA 30 T:32C. [own translation: The prejudice does not necessarily have to effect the individual towards whom the misrepresentation was made ... prejudice also includes a risk of prejudice for the State, local communities, the public and third parties in the exercise of their rights and the fulfilment of their obligations.]

⁶⁸⁸ 1926 AD 350.

⁶⁸⁹ 1926 AD 350:352.

⁶⁹⁰ 1981 2 SA 638 D.

⁶⁹¹ 1981 2 SA 638 D:655D-H.

⁶⁹² The authors of LAWSA 1996:vol 6, par 323 remark that "fraud ... can also be regarded as a crime against the interests of the community in general."

⁶⁹³ 1946 TPD 255.

the main sellers of petrol, other petrol stations as well as the general public:

"Gevolglik is die vervalsing van 'n dokument met die bedrieglike oogmerk om aan 'n bepaalde herverkoper 'n groter voorraad te besorg as wat hom regtens toekom staatsgevaarlik: dit is skadelik teenoor die staat en dwarsboom sy noodregulasies; dit skaad ander herverkopers omdat dit die voorraad, wat aan almal eweredig beskikbaar gestel kan word, verminder; in dieselfde wyse skaad dit die burgery. Dit skaad die skatkis, omdat dit met sig meebring die verkoop van petrol sonder koepons; ter verkryging waarvan 'n fooi betaalbaar sou gewees het. Denkbaar stel dit ook die groothandelaars bloot aan vervolging indien die Kroon, ondanks die uiters lakse maatreëls van die petrolkontroleur, besluit om te vervolg."⁶⁹⁴

Therefore it may be stated that potential prejudice includes a) a risk of loss of control; b) a risk of invasion of the complainant's civil rights; c) a risk of loss of reputation; d) a risk of prosecution for the complainant; e) lulling the complainant into a false sense of security which can lead to his prejudice; f) a risks that state's control over something valuable might be weaken; and g) affecting other "rights" which really cannot be classified as subjective rights such as affecting the general public's and petrol stations' "right to obtain petrol". In *R v Jolosa*⁶⁹⁵ the court stated (although by means of a minority judgment):

"In my opinion, and that is the ground of the decision in the case of *Queen v. de Vos*, it is not necessary to prove prejudice to the person's pocket or property, but it is enough to prove that the act done is calculated to prejudice his rights ... the widest meaning should be given to these words, 'to the prejudice of another.'⁶⁹⁶

Courts have indeed understood prejudice in a very wide sense. In *R v De Beer*⁶⁹⁷ the facts were that the accused borrowed money from his employer, the Railway Administration. The latter loaned the money to him on certain conditions, which the accused failed to adhere to. The accused thereafter forged certain documents, which

⁶⁹⁴ 1946 TPD 255:266. [own translation: It follows that the counterfeiting of a document with the fraudulent intent to provide a particular reseller with more stock than he is allowed to receive constitutes a threat to the state: it constitutes prejudice towards the state and thwarts its emergency regulations; it prejudices other resellers because it reduces the stock that should be made equally available. It prejudices the treasury, because it results in petrol being sold with coupons, for which a fee would have been payable. Conceivably, it also exposes the main retailers to prosecution if the Crown resolves to prosecute, irrespective of the extreme lax measures of the petrol controller.]

⁶⁹⁵ 1903 TPD 694.

⁶⁹⁶ 1903 TPD 694:700.

⁶⁹⁷ 1940 OPD 268.

he presented to his employer, indicating that he adhered to the said conditions. The court stated the following with regard to the question whether the state proved prejudice:

"The Railway Administration had certain legal rights against him. It is unnecessary to consider exactly what the Administration's right was. It may have been a right to claim specific performance, that is, an order that he pay the debts the payment of which was a condition of the loan. It may have been a claim for an interdict, that is, restraining him from spending any more of the money unless he paid these debts. It is possible that there may have been some form of *condictio*; that the Administration would be entitled to claim a refund from him of the amounts which he had not paid and which he should have paid out of the £116. I am satisfied that there was a legal right in the Administration. The result of the conduct of appellant in falsifying these documents was that the Administration was kept unaware of its rights. The position was that the Administration in fact at that stage had this right the appellant, by the representation involved in these false documents, induced the Administration to believe that it had not this right; and consequently it did not pursue its right which otherwise it might have done. It appears to me that it was not only a false representation, but a representation which caused such prejudice as is necessary to establish a charge of forgery."⁶⁹⁸ (own emphasis)

The law does not require potential prejudice to be probable, but merely requires a risk of prejudice to the complainant or a third party.⁶⁹⁹ It should also be kept in mind that many South African courts have maintained that the potential prejudice (the risk of prejudice) must not be too remote or fanciful.⁷⁰⁰ However, in some cases the courts were willing to regard a very small risk of prejudice as sufficient potential prejudice. For

⁶⁹⁸ 1940 OPD 268:270.

⁶⁹⁹ In *R v Seabe* 1927 AD 28 the Supreme Court of Appeal noted (at 32) that "[i]t seems to me that it is too narrow a view of potential prejudice to say that the risk must be reasonably certain or probable. It seems to me that where there is some risk, though perhaps slight, the element of prejudice necessary to support the *crimen falsi* exists." In *R v Heyne & Others* 1956 3 SA 604 A the Supreme Court of Appeal stated (at 622A-623A) that a risk of harm must exist; not a probability. See also *S v Harper & Another* 1981 2 SA 638 D:654H.

⁷⁰⁰ *R v Seabe* 1927 AD 28:34. In *R v Heyne & Others* 1956 3 SA 604 A the Supreme Court of Appeal remarked (at 622F) that "it seems correct to say that the false statement must be such as to involve some risk of harm, which need not be financial or proprietary, but must not be too remote or fanciful, to some person, not necessarily the person to whom it is addressed." In *R v Kruse* 1946 AD 524:533-534 the Supreme Court of Appeal maintained that "[t]he test is whether the misrepresentation is such that a reasonable person might ... in the ordinary course of events, be deceived."

instance, in *R v Macatlane*⁷⁰¹ the court maintained that where the complainant furnished the accused with a specific certificate, based on forged documents handed to him by the accused, his (the complainant's) superiors may remove him from office if they discover that he recommended people such as the accused for a certificate.⁷⁰²

Finally, in *S v Kruger & Another*⁷⁰³ the Supreme Court of Appeal noted that prejudice or potential prejudice must be determined as at the time when the representation was made.⁷⁰⁴

3.4.2. Does hacking into computers constitute fraud?

Having examined the general principles of the offence of fraud, the question must be addressed whether gaining access to a computer system, or part of a computer system, without the necessary authorisation constitutes fraud.

3.4.2.1. Misrepresentation as an element of fraud

Think of the following hacking instances:

- (i) A *hacker* penetrates a bank's security system and transfers money from A's account to his own or he merely credits his own (fictitious) account; or
- (ii) A *hacker* penetrates a firm's computer network and either looks around or after finding sensitive information, copies such information and/or deletes it.

In the UK computer criminals cannot be convicted of fraud in terms of the 1968 *Theft Act* in that the courts held that a computer cannot be deceived.⁷⁰⁵ In Australia, the Supreme Court of South Australia ruled in *Kennison v Daire*⁷⁰⁶ that a machine (*in casu* an ATM) could be misled.⁷⁰⁷ However, the court still found the accused guilty of larceny (theft).

⁷⁰¹ 1929 TPD 708.

⁷⁰² 1929 TPD 708:713.

⁷⁰³ 1961 4 SA 816 A.

⁷⁰⁴ 1961 4 SA 816 A:828 & 832.

⁷⁰⁵ Carr *et al* 1994:153.

⁷⁰⁶ 1985 38 SASR 404.

⁷⁰⁷ 1985 38 SASR 404:406.

In *S v Myeza*⁷⁰⁸ (South Africa) the accused was found guilty of fraud because he placed a counterfeit coin in a parking meter. The court remarked that:

“Op die gestelde feite wil 'n persoon sy voertuig in die afgebakende ruimte, ongesteurd en met 'n skyn van wettigheid, vir 'n besondere termyn parkeer. Om dit reg te kry aktiveer hy die parkeermeter opsetlik met die genoemde voorwerp om die skyn te verwek dat hy reëlmatig 'n muntstuk in die parkeermeter gevoer het en dus betaal het vir die termyn wat sy voertuig geparkeer word. Deur sy gedrag bewerkstellig hy dus 'n verdraaiing van die waarheid, 'n wanvoorstelling wat dit onmoontlik maak om, vir die termyn wat die voertuig oënskynlik wettig geparkeer staan, die bepalings van die Munisipaliteit Johannesburg Parkeerterreinverordeninge toe te pas en af te dwing. Persone wat belas is met die toepassing van die verordeninge kan verkeerdelik onder die indruk gebring word dat die voertuig in terme van die bepalings van die verordeninge geparkeer word ... So 'n persoon is gevolglik skuldig aan die misdaad van bedrog.”^{709 710}

In other words, the court maintained that the accused made a misrepresentation to the traffic officers that he was adhering to the law, whilst the opposite was true.⁷¹¹ Therefore the question of whether the accused *misled the parking meter* never arose. The parking meters were mere instruments to ensure that the prescribed amount of money was paid by drivers parking their cars in the designated zones.⁷¹² Therefore where a counterfeit coin or other object is inserted into the parking meter, the traffic officer makes an erroneous conclusion that the particular driver paid the prescribed amount of money. It follows that the traffic officer is misled.⁷¹³

⁷⁰⁸ 1985 4 SA 30 T.

⁷⁰⁹ 1985 4 SA 30 T:32D-G. [own translation: On the basis of the stated facts a person seeks to park his vehicle in a designated area for a particular period of time, undisturbed and with a façade of lawfulness. In order to achieve this he intentionally activates the parking meter with the mentioned object to cause a façade that he lawfully inserted a coin into the parking meter and therefore paid for the period of time that he parked his car. By means of his conduct he causes a perversion of the truth, a misrepresentation that makes it impossible, for the period of time that his vehicle is parked there with ostensible authority, to enforce the provisions of the Johannesburg Municipality Parking area bylaws. Those individuals who are responsible for the enforcement of the bylaws can be deceived to think that the vehicle in question is parked according to the provisions of the bylaws ... It follows that this individual is guilty of fraud.]

⁷¹⁰ The charge-sheet stated that the accused made a misrepresentation to the local traffic department or local municipality. (At 33B-D).

⁷¹¹ Botha 1986:73.

⁷¹² Botha 1986:74.

⁷¹³ Botha 1986:74.

Consequently an answer to the questions posed above may be attempted: Where a *hacker* breaks the username and password protection (or for that matter, any security measure utilised by an institution), he makes a misrepresentation to the system administrator (of the institution) or anyone in control of that particular computer that he is an authorised user of the computer.⁷¹⁴ Hence, the element of deception is present. Two court cases can also be cited as authority for this particular view:

a) In *S v Mbokazi*⁷¹⁵ the accused was an employee of the complainant, a bank. He withdrew funds from A's account without the latter's consent and appropriated it to his own use, employing the bank's computer. He was charged with fraud in that he made a misrepresentation to the complainant that he was authorised to withdraw the money from A's account. The court made the following observation:

"Misrepresentations may however take a variety of forms. They may be made by entries in books or records ... or by conduct or even by silence when there is a duty to speak ... I think that as such an employee, the accused impliedly represented to the bank, whenever he effected a withdrawal of money from a customer's account, that the customer had duly authorised the transaction; that the necessary steps had been taken for the due withdrawal of the money standing to the credit of the account. Furthermore the accused, in order to effect the transaction, made certain entries on the computer. Those entries carried with them the implied representation that it was the customer who had withdrawn the money or at least that the customer had authorised him to operate the computer in order to effect the withdrawal of the money."⁷¹⁶

Therefore it can be stated that when a *hacker* transfers money from A's account to his

⁷¹⁴ On the basis of *S v Myeza (supra)* Carstens and Trichardt 1987 argue (at 132) that "the element of misrepresentation with regard to the crime of fraud, in cases of computer crimes by means of the ATM, lies therein that the perpetrator unlawfully and fraudulently represents to the bank by means of his actions channelled through the ATM, that he has sufficient funds, or made sufficient deposits or transfers enabling him to withdraw money. The perpetrator is thus misrepresenting results on his account, results produced by means of the ATM and herein lies the misrepresentation to the bank, inducing the bank to believe that the results were lawfully produced by means of information channelled through the ATM and that he (the perpetrator) is now entitled to withdraw money. It is further submitted that, just as the element of misrepresentation in this case was not considered to be a misrepresentation made to a parking meter, the same argument is valid in the case where money is fraudulently withdrawn, transferred or deposited by means of an ATM, that the misrepresentation is made to the bank and not to the computer." Cooke & Fryer 1998 also submit (at 4) that *hackers* appear to be authorised users seeing that they normally break passwords and match login names.

⁷¹⁵ 1998 2 ALL SA 78 N.

⁷¹⁶ 1998 2 ALL SA 78 N:86f-87d.

account or to someone else's account, he can be charged with fraud (in that he makes a misrepresentation to the bank's system administrator with the intent to defraud the bank) or with theft (in that he stole A's "money" or more correctly stated: he diminished A's personal rights against the bank).

b) In *S v Van der Berg*⁷¹⁷ the accused, an employee of the complainant (a bank) transferred money from A's account to B's account (her ex-husband's) by means of the bank's computer terminal, without the necessary authorisation. The accused was subsequently charged with fraud. The court made the following observation:

"[I]t would appear to be that she unlawfully credited a particular account in Santam Bank with an amount of R800 when the account was not entitled to such a credit. This was, in my view, a misrepresentation to the bank, and the fact that the misrepresentation was introduced into the computer system electronically differs not one whit from the clerk who, with the intention to deceive, makes a false entry with a pen into a ledger account. The account has been falsely credited and in this instance the computer system was the means by which such an entry was made and consequently it is a misrepresentation ... Once the account has been credited with R800, the crime has been completed. The actions of the accused had long gone past the preparation stage and it is irrelevant that no one drew money from the bank or took some other similar step."⁷¹⁸

3.4.2.2. The element of prejudice

As noted earlier, the courts have indicated that a mere *risk*, and not a probability, of harm is required for fraud.⁷¹⁹ Bearing in mind the different types of conduct which constitutes potential prejudice, as indicated in paragraph 3.4.1 of this chapter, it may be stated that whenever a *hacker* successfully penetrates a computer system by either "breaking" the security measures or using someone else's username and password, without the necessary permission, his conduct constitutes at least potential prejudice in that -

- a) he infringed the computer user's civil rights and more specifically his right to privacy; and
- b) the computer user loses control over who has access to his computer system.

⁷¹⁷ 1991 1 SACR 104 T.

⁷¹⁸ 1991 1 SACR 104 T:106b-f.

⁷¹⁹ *S v Kruger and Another* 1961 3 SA 816 A:828-829. In other words, to constitute potential prejudice.

Where the *hacker* copies, modifies or deletes digital files, his conduct constitutes actual prejudice in that -

- (i) he infringes the computer user's copyright rights or right to confidential information and possibly his right to digital information. Put differently, he infringes the user's immaterial property rights;
- (ii) he infringes the computer user's common law as well as constitutional right to privacy;
- (iii) the computer user loses control (even if only for a few seconds) over the digital content stored on his hard drive;
- (iv) should third parties learn that the computer user's system was penetrated, such conduct might lead to a loss of *fama* and/or goodwill.

3.4.2.3. The element of "intent to defraud"

As noted earlier, the accused (the *hacker*) must have the intent not only to deceive the computer user, but also to prejudice him. It is submitted that since the mere intrusion of a computer constitutes potential prejudice to the computer user (as indicated in paragraph 3.4.2.2), and seeing that the accused is aware that by means of his unlawful conduct he is infringing upon the computer user's civil rights (the right to privacy, the right of control over the digital content stored on his hard drive, the right of controlling access to such digital content and possibly his right to immaterial property) he has the necessary intent to prejudice.

The authors of LAWSA observe that "South African practice seems to be only one step away from regarding any misrepresentation with the intention to defraud as fraud."⁷²⁰

An example of another type of fraud by means of the Internet is found in the case of *Hotmail Corporation v Van\$ Money Pie Inc et al.*⁷²¹ The defendants sent spam (unsolicited commercial e-mail) to the e-mail accounts of other Hotmail subscribers. The defendants altered (*spoofed*) the return addresses of their e-mails to falsely indicate that it was sent from a Hotmail account, rather than from its true source. The plaintiff (Hotmail) applied for an interdict prohibiting the defendants from sending spam

⁷²⁰ LAWSA 1996:vol 6, par 323.

⁷²¹ 47 USPQ 2D (BNA) 1020 (N.D. Cal. 1998). A copy of this judgment was obtained from Westlaw. A copy can also be downloaded from <http://eon.law.harvard.edu/h2o/property/alternatives/hotmail.html>.

and indicating that it came from Hotmail. Each and every e-mail sent by a Hotmail user displayed the Hotmail trade mark.⁷²² The court held that the defendant's conduct constituted fraud, stating that -

"defendants fraudulently obtained a number of Hotmail accounts, promising to abide by the Terms of Service without any intention of doing so and suppressing the fact that such accounts were created for the purpose of facilitating a spamming operation, and that defendants' fraud and misrepresentation caused Hotmail to allow defendants to create and use Hotmail's accounts to Hotmail's injury. In addition, the evidence supports a finding that defendants' falsification of e-mails to make it appear that such messages and the responses thereto were authorized to be transmitted via Hotmail's computers and stored on Hotmail's computer system - when defendants knew that sending spam was unauthorized by Hotmail - constitutes fraud and misrepresentation, and that Hotmail relied on such misrepresentations to allow the e-mails to be transmitted over Hotmail's services and to take up storage space on Hotmail's computers, to Hotmail's injury."⁷²³

Address spoofing can also be prosecuted under South African criminal law as fraud. In the US such conduct is now known and prosecuted as "*Internet forgery*".⁷²⁴

3.4.3. Must a system administrator be deceived?

In the previous paragraphs it was stated that the *hacker* misrepresents to the system administrator that he is an authorised user of the system. The question under this heading is: Who does the *hacker* deceive, if there is no system administrator, for instance, where a *hacker* penetrates the security system of a normal (home) computer?

It is submitted that under such circumstances the *hacker* misrepresents to the computer owner (or any person in control of the computer at that particular moment) that he is either the "operating system" of the user's computer, when he views, copies, modifies or deletes files or that he has authorised access to that particular computer such as the user's ISP. Even if this submission is incorrect, the prosecution is assisted by section 103 of the *Criminal Procedure Act*⁷²⁵ which reads as follows:

⁷²² 47 USPQ 2D (BNA) 1020 (N.D. Cal. 1998):1021, par 1.

⁷²³ 47 USPQ 2D (BNA) 1020 (N.D. Cal. 1998):1025, par 37.

⁷²⁴ See Bearzi 2000:1.

⁷²⁵ Act 51/1977.

"In any charge in which it is necessary to allege that the accused performed an act with an intent to defraud, it shall be sufficient to allege and to prove that the accused performed the act with intent to defraud without alleging and proving that it was the intention of the accused to defraud any particular person, and such a charge need not mention the owner of any property involved or set forth the details of any deceit." (own underlining)

It is, therefore, not required to stipulate or prove that the *hacker* intended to defraud a particular person. Furthermore, the prosecution is not obliged to stipulate who the owner of the computer system is.

3.4.4. Is the breaking or penetrating of security measures a requirement?

When fraud was discussed in the context of making misrepresentations to the system administrator or a person in control of the computer, the example used was where the *hacker* penetrated the computer's security measures or used someone else's password and username. Another question to be addressed is: Whenever a particular computer system does not have security measures utilising passwords and/or usernames (such as firewalls, etc) does the *hacker* still make a misrepresentation that he is an authorised user or that he has authorised access. Many home computers, connected to the Internet, have no security measures installed to either protect the computer from hacking and/or virus instances.

As noted above, in *S v Mbokazi*⁷²⁶ an employee withdrew funds by means of a computer. The court maintained that the accused (as an employee) *impliedly* represented to the bank (his employer) that the client had duly authorised the transaction.

The fact that the computer in question lacks security measures providing protection against *hackers* should make no difference: the *hacker* still makes the misrepresentation that he enjoys the authorisation of the computer owner to use the computer. Whenever a *hacker* gains access to a computer and either merely observes the content (by clicking on files and documents) or deletes or copies such files, he uses the computer.

⁷²⁶ 1998 2 ALL SA 78 N.

3.4.5. Does an unsuccessful attempt to hack constitute fraud or attempted fraud?

The question in this context is: when a *hacker* attempts to hack into another person's computer but fails to succeed, does he commit fraud or attempted fraud?

The basic principles of fraud have already been stated in paragraph 3.4.1 of this chapter. The elements are: unlawfulness, misrepresentation, intent and prejudice or potential prejudice. In paragraph 3.4.2.1 it was concluded that a *hacker* makes a misrepresentation that he is an authorised user of the computer system, or that he has authorised access to that particular computer, and that such conduct is unlawful. Therefore, only two elements of fraud namely intent and (potential) prejudice still need to be addressed.

With regard to intent, it was observed that the mere intent to mislead the complainant does not suffice; the law requires an intent to defraud the complainant. Stated differently, an intent to cause prejudice to the complainant is required. South African courts have also noted that for conduct to constitute fraud, it is not required that the complainant should have believed the accused (the *hacker*).⁷²⁷ The question of law that arises is: whenever a *hacker* attempts to penetrate a computer system but fails, is an intent to defraud the complainant present?

With regard to the element of prejudice, it was noted that local courts do not require actual prejudice, but maintain that potential prejudice suffices for a conviction of fraud. A risk, calculated upon all the surrounding circumstances, to cause prejudice suffices.⁷²⁸ It was also noted that the law attaches a very comprehensive meaning to the concept "potential prejudice," such as a risk of loss of reputation and control as well as an infringement of the complainant's civil rights. It was furthermore stated that such prejudice must not be too remote.

It is submitted that where a *hacker* attempts to penetrate a computer system, he poses the following risks:

- a) A risk that the owner may lose control over his computer, if the *hacker* (for instance) renders the owner's hard drive inaccessible or inoperable.
- b) A risk that the owner may lose control, temporarily or permanently, over his digital files, if the *hacker* deletes, modifies, copies or views them.

⁷²⁷ See e.g. *S v Swarts en 'n Ander* 1961 4 SA 589 OK:591D-E.

- c) A risk of infringing the owner's immaterial property rights (such as copyright, right to confidential information; right to goodwill and right to trade without unlawful interference), should the *hacker* succeed in penetrating the security system.
- d) A substantial risk of infringing the owner's common law as well as constitutional right to privacy.⁷²⁹
- e) A risk of loss of reputation should third parties such as clients or potential clients discover or learn that a *hacker* penetrated the business' computer system. There is also the risk of negative media publicity.⁷³⁰
- f) A risk of loss of credibility in the computer system: Employees may be reluctant to store confidential information on the hard drive for fear that the *hacker* may have installed an undetectable Trojan horse that will forward to its creator sensitive business information as well as inform him of the passwords that render access to the computer system.⁷³¹

It is submitted, therefore, that the element of potential prejudice is present: a risk of prejudice, as indicated above, existed when the misrepresentation was made.⁷³² It is further submitted that such "potential prejudice" is not too remote in that some local courts were willing to recognise a risk of loss of reputation where the complainant was defrauded by the accused.⁷³³

It is also contended that there is authority for the submission that an unsuccessful hacking attempt constitutes potential prejudice. Snyman gives the following example of fraud:

"Veronderstel X verseker alle items wat aan hom behoort by 'n sekere versekeringsmaatskappy teen diefstal. Daarna eis hy 'n bedrag geld van die versekeringsmaatskappy op grond daarvan dat sekere artikels wat aan hom behoort, gesteel is ... Veronderstel egter dat, nadat X sy eis ingedien het, die versekeringsmaatskappy uitvind dat die tersaaklike items nie gesteel is nie en dat X se eis dus op 'n valse bewering gegrond is. Die maatskappy weier gevolglik om die bedrag geëis aan hom uit te betaal. Kan X nietemin nog aan bedrog skuldig bevind word? Die

⁷²⁸ See *R v Heyne & Others* 1956 3 SA 604 A:622F; *R v Seabe* 1927 AD 28:34.

⁷²⁹ See par 3.9.1.1 of this chapter.

⁷³⁰ See chapter 3 as well as par 4 of chapter 5.

⁷³¹ See chapter 3 as well as par 4 of chapter 5.

⁷³² See *S v Campbell* 1991 1 SACR 503 Nm:508h-l; *S v Kruger & Another* 1961 4 SA 816 A:828A; *R v Deale* 1960 3 SA 846 T:848A-B.

⁷³³ See par 3.4.1.1. of this chapter.

antwoord op hierdie vraag is bevestigend, omdat, alhoewel die maatskappy geen daadwerklike nadeel gely het nie, X se wanvoorstelling *potensiële* nadeel ingehou het.”⁷³⁴

This argument is supported by South African judgments. In *Moolchund v R*⁷³⁵ the accused fraudulently claimed compensation from the government. The government, however, discovered this and refused to pay. The court found the accused guilty of fraud, stating that potential prejudice was present.⁷³⁶ The court further remarked that:

“It would be monstrous, we think, if because a person’s wicked machinations have been defeated, or unsuccessful, on account of the intervention of some third person, or the occurrence of some event beyond his control, or because his misrepresentations were not believed or were not acted upon, that he should escape the penalty of law.”⁷³⁷

738

Further authority for Snyman’s submission is *R v Seabe*⁷³⁹ where the Supreme Court of Appeal remarked: “A person who can barely write and has no idea of spelling presents to a bank a cheque which purports to be drawn by an educated client of the bank. The forgery is so gross that no bank clerk would be deceived. The forger in his ignorance of banking business thought he would get the money. Can we say that because it was probable or reasonably certain that the bank would not cash the cheque there was no potential prejudice to the bank? It has never been suggested to my knowledge that in such a case there is no *crimen falsi*. It seems to me therefore that where there is some risk, though perhaps slight, the element of prejudice necessary to support the *crimen falsi* exists.”⁷⁴⁰

⁷³⁴ Snyman 1999:538. [own translation: Assume that X insures all the items he owns at an insurance company against theft. Thereafter he claims compensation from the insurance company on the basis that certain items, which he owns, had been stolen ... Assume further that after X has submitted the claim, the insurance company discovers that the said items are not stolen and therefore that X’s claim is based on a false statement. As a result the company refuses to pay the amount claimed by the accused. Is X still guilty of fraud? The answer is in the affirmative, because, although the company suffered no actual prejudice, X’s misrepresentation contains potential prejudice.]

⁷³⁵ 1902 33 NLR 76.

⁷³⁶ 1902 33 NLR 76:81.

⁷³⁷ 1902 33 NLR 76:81.

⁷³⁸ It should be borne in mind that until 1956 many South African courts did not recognise the offence of attempted fraud.

⁷³⁹ 1927 AD 28.

⁷⁴⁰ 1927 AD 28:32.

Likewise, in *R v Butler*⁷⁴¹ the accused handed a forged cheque, knowing that the cheque was forged, to his bank with the intent to cash it. The bank refused to cash the cheque. The court found the accused guilty of fraud, stating that “[a]ccused had forged the signature to the cheque, he issued the cheque knowing that it was not a good and available cheque, and did so with the fraudulent intention of obtaining money thereon to the prejudice of the bank. He therefore committed the crime of fraud.”⁷⁴² The court in *R v Jolosa*⁷⁴³ was of the same opinion: “It would be indeed monstrous that if a man forged a cheque and presented it at the bank, and the bank did not cash it, he should not be guilty of the crime of falsity because no one had been injured ... The act would be one calculated and intended to prejudice a third person”.⁷⁴⁴

Other judgments also support this line of thinking.⁷⁴⁵ In *R v Dyonta & Another*⁷⁴⁶ the Supreme Court of Appeal observed that “[i]f the representation is one which in the

⁷⁴¹ 1947 2 SA 935 C.

⁷⁴² 1947 2 SA 935 C:937.

⁷⁴³ 1903 TS 694.

⁷⁴⁴ 1903 TS 694:698.

⁷⁴⁵ In *R v Armstrong* 1917 TPD 145 the accused, a police officer, handed a false complaint to the complainant with the intention of scaring him. The latter did not believe the accused. The court found the accused guilty of fraud and stated (at 150): “The only reasonable inference seems to me that the accused intended to intimidate [the complainant] from doing his duty and that clearly amounts to such a serious direct or potential prejudice as comes within the limits of the ordinary definition of falsity”. In *R v Yenson* 1933 TPD 510 the court pointed out (at 513) that “[i]t may well be that the mere fact that a false representation has not succeeded in producing the benefit aimed at by the accused does not make it any less the crime of fraud.” In *R v Nay* 1934 TPD 52 the accused attempted to obtain £12 from the complainant by misrepresenting to the latter that he had done work on his car. The court maintained (at 54) that “[u]nder the circumstances it would appear that ... the Crown might have charged the [accused] with fraud in that he had falsely represented that he had done work on the car with the intention of extracting £12 10s from the complainant. That would have been fraud, whether he succeeded in obtaining the extracting £12 10s or not ... as soon as the false representation was made by the [accused] that work worth £12 10s had been done, and £12 10s was demanded, the [accused], knowing well that his representation that the work had been done was false, had committed the crime of fraud, assuming once more that potential prejudice was proved.” In *R v Dyonta & Another* 1935 AD 52 the accused attempted to sell pieces of glass imitations to the complainant, alleging to him that it was real diamonds. The complainant disbelieved them and informed the police, whereupon the accused were arrested. The court maintained that the accused were guilty of fraud: “The law looks at the matter from the point of view of the deceiver. If he intended to deceive, it is immaterial whether the person to be deceived is actually deceived or whether his prejudice is only potential.” (At 57). In *R v Kruse* 1946 AD 524 the Supreme Court of Appeal noted (at 534) that “even if the evidence had not proved that the giving of the cheque influenced [the complainant] to part with his rings, and if the evidence had been consistent with the view that other factors might have induced [the complainant] to give the accused the rings, the accused would nevertheless have been properly convicted of the crime of fraud, because the

ordinary course is capable of deceiving a person, and thus enabling the accused to achieve his object, the fact that the person to whom the misrepresentation is made has knowledge or a special state of mind which effectively protects him from all danger or prejudice does not entitle the accused to say that the false representation was not calculated to prejudice."⁷⁴⁷

On a similar basis it may be contended that where the representation is one which in the ordinary course is capable of circumventing computer security measures or capable of penetrating a computer system, and thus enabling the accused to achieve his object, the fact that the person to whom the misrepresentation is made has knowledge or special software or equipment which effectively protects him from all danger or prejudice does not entitle the accused to say that the false representation was not calculated to prejudice.

With regard to the *intent to defraud*, numerous courts have stated that the "words 'intent to defraud' must be taken, not in the ordinary narrow sense, but in a wide sense."⁷⁴⁸ It can be argued that the *hacker* intended the computer user to be deceived, by assuming that the *hacker* was an authorised user or that he had authorised access to the computer system, and that his (the computer user's) action should be affected by the deception.⁷⁴⁹

It is submitted that where the *hacker* attempts to penetrate the computer system, he has the intention to prejudice seeing that he knows and/or foresees that if he succeeds he will infringe the computer user's right to privacy and depending on the *hacker's* intention, he further knows and/or foresees that if he copies, modifies or deletes digital files, he will cause prejudice to the computer user, for instance by exposing the computer user to negative media publicity, should the latter discover this. The courts

giving of the cheque was a false representation; he gave it with the fraudulent intention of deceiving [the complainant] and thereby obtaining possession of the rings, and the false representation was one which was likely, in the ordinary course, to influence a shopkeeper in the circumstances in which it was made and thus to cause prejudice."

⁷⁴⁶ 1935 AD 52.

⁷⁴⁷ 1935 AD 52:57.

⁷⁴⁸ *R v De Vos* 1898 EDC 145:150. In *R v Jones & Others* 1926 AD 350 the Supreme Court of Appeal also noted (at 352-353) that prejudice must not be construed narrowly.

⁷⁴⁹ See *R v Heyne & Others* 1956 3 SA 604 A where the Supreme Court of Appeal stated (at 625B-C): "It is clear that those who were responsible for the wilfully false entries and deliberate omissions from the books intended that the inspecting members of the police should be deceived and that their action should be affected by the deception."

(including the Supreme Court of Appeal) have noted that -

"if a misrepresentation which is capable of deceiving is made wilfully and the person making it intends to deceive the person to whom it is made, that is sufficient to prove the intention to defraud where the misrepresentation is one which causes actual prejudice or is calculated to prejudice."⁷⁵⁰

Therefore, it is submitted that an unsuccessful hacking attempt constitutes fraud.

Even if it were to be argued that an intentional but unsuccessful hacking attempt does not constitute fraud, it is submitted that the accused is guilty of attempted fraud.⁷⁵¹ De Wet & Swanepoel submit that "[a]s die man wat optree met die opset om 'n ander deur misleiding te beweeg om tot sy nadeel te handel nie daarin slaag nie, maak hy hom skuldig aan poging tot bedrog."⁷⁵² This submission is also supported by local judgments. In *S v Isaacs*⁷⁵³ the court expressed the contrary view as to those held by the courts in *R v Jolosa*⁷⁵⁴ and *Moolchund v R*.⁷⁵⁵ The court, in *S v Isaacs*, noted that "it seems questionable to me to say that an unsuccessful fraudulent misrepresentation, because it deserves punishment, should be regarded as fraud, for, logically, as with other common law crimes, it might well be said that such conduct constitutes an attempt to commit the crime, and that the offender will not go free, for an attempt to commit a crime is punishable at common law".⁷⁵⁶ In *S v Ostilly & Others (1)*⁷⁵⁷ the court stated that "in principle there can be no distinction between such a case, where the consummation of the crime is frustrated [because the false representation did not reach the representee] ... and the instant case, where the absence of proof of potential prejudice is fatal to a fraud conviction. In both instances the overt act and intention are the same end".⁷⁵⁸

Therefore, it is submitted that the following instances constitute attempted fraud: a)

⁷⁵⁰ *R v Henkes* 1943 AD 143:161. See also *S v Isaacs* 1968 2 SA 187 D:191D-E.

⁷⁵¹ The offence of attempted fraud was recognised by the Supreme Court of Appeal in *R v Heyne & Others* 1956 3 SA 604 A:622D-E.

⁷⁵² De Wet & Swanepoel 1985:404. [own translation: Where A acts with the intent to induce B to act, as a result of the misrepresentation, to his prejudice, but fails to succeed, he is guilty of attempted fraud.]

⁷⁵³ 1968 2 SA 187 D.

⁷⁵⁴ *Supra*.

⁷⁵⁵ *Supra*.

⁷⁵⁶ 1968 2 SA 187 D:189D-E.

⁷⁵⁷ 1977 4 SA 699 D.

⁷⁵⁸ 1977 4 SA 699 D:714H.

where a *hacker* (who made up his mind to hack into the computer system) fails to gain access to the system, after he did everything he could to penetrate the targeted computer's security system and b) where his conduct constitutes at least the commencement of the consummation of the offence.⁷⁵⁹

3.4.6. Does a denial-of-service attack constitute fraud?

The question is whether a denial-of-service attack⁷⁶⁰ constitutes fraud? Three elements of fraud namely misrepresentation, prejudice and intent to prejudice are relevant to this discussion.

It is submitted that where A launches a denial-of-service attack upon B's computer server, A misrepresents (by *spoofing*⁷⁶¹ the replying address) that he honestly wants to make a connection with B's computer in order for their computers to communicate. A also misrepresents that the address which his computer furnishes to B's computer is his (A's) actual Internet address.

Furthermore, a denial-of-service attack normally results in a computer server being rendered inaccessible or inoperable, which, in turn, results in loss of income, communication, business reputation, etc. Where A fails to launch a denial-of-service attack successfully, his conduct entails potential prejudice. Finally, it is submitted that A has the intent to prejudice in that it is his intention to bring A's computer server down; stated differently, to render it inaccessible or inoperable. Therefore, it is submitted that where a *hacker* launches a denial-of-service attack attack on A's computer system, he is guilty of the offence of fraud.

⁷⁵⁹ See par 3.6.8 of this chapter for a discussion of the principles pertaining to an attempt to commit a crime. The authors of LAWSA state that where a deliberate fraud was made but no prejudice (actual or potential) resulted, such conduct constitutes attempted fraud. See LAWSA 1996:vol 6, par 332. Likewise, Hunt-Milton 1990 aver that the following two instances, *inter alia*, constitute attempted fraud: a) "Where the misrepresentation is communicated, but it causes no actual prejudice, and because it is so patently ridiculous it is not such as could reasonably harm anyone and there is therefore no potential prejudice either" and b) "Where for some other reason the misrepresentation, though communicated, contains a risk of prejudice which is 'too remote or fanciful'." (At 778). From these authorities it may be concluded that where a *hacker* attempts to penetrate A's computer system, but, in effect, there is no possibility of successfully penetrating the computer's security measures, such conduct constitutes attempted fraud.

⁷⁶⁰ Discussed in par 3 of the previous chapter.

⁷⁶¹ In other words, forging. See par 3 of the previous chapter.

Where A penetrates B's computer and uses it as part of a distributed denial-of-service attack on X's computer, A's conduct constitutes a risk of prosecution for B in that it may appear to the investigating authorities that B launched a denial-of-service attack on X.

For the sake of interest, where A penetrates many computers in order to launch a distributed denial-of-service attack on X, his conduct can be prosecuted as one offence, namely fraud. In *R v Heyne & Others*⁷⁶² the Supreme Court of Appeal stated: "Those considerations require that in a proper case a planned course of fraudulent conduct may be charged as a single crime of fraud, even if it might also be possible to analyse it into a series of separate frauds."⁷⁶³ The court also noted:

"In the case of other crimes when there is a series of acts done in pursuance of one criminal design the law recognises the practical necessity of allowing the Crown, with due regard to what is fair to the accused, to charge the series as a criminal course of conduct, that is, as a single crime ... The correct view, it seems to me, is that if the Crown relies upon a course of conduct, with such advantages from its point of view as there may be, the course of conduct must be regarded as one continuing crime, provable in various ways, including the proof of individual criminal acts making up the course of conduct."⁷⁶⁴

With regard to the instance where *hackers* conspire to launch a denial-of-service attack upon a particular web site, the following *dictum* of the court in the *Heyne*-case is relevant. The Supreme Court of Appeal held that all persons who acted in concert to make a systematic series of false representations could be charged upon a fraudulent course of conduct.⁷⁶⁵ The court continued to state that:

"Where the participations of several collaborators have not covered precisely the same period, particulars may be necessary to inform them of the extent of their alleged participation, but the Crown would not be precluded from charging them together on a course of conduct basis. In each case it is necessary to decide whether there has been prejudice to the accused".⁷⁶⁶

⁷⁶² 1956 3 SA 604 A.

⁷⁶³ 1956 3 SA 604 A:616H.

⁷⁶⁴ 1956 3 SA 604 A:626G & 628B-C.

⁷⁶⁵ 1956 3 SA 604 A:617A.

⁷⁶⁶ 1956 3 SA 604 A:617A-B

3.4.7. Does a virus hoax constitute fraud or attempted fraud?

As explained earlier,⁷⁶⁷ a virus hoax entails instances where A sends B an e-mail message stating that a new virus was discovered and that the latter must forward this message to everyone he knows. These false warnings pose the risk that too many Internet users might commence e-mailing each other resulting in e-mail servers (either those of employers or Internet Service Providers) being overwhelmed with e-mail messages and consequently either forces system administrators to shut down these servers or causes these servers to crash before system administrators can do anything.

Without repeating the general principles enunciated in the previous paragraphs, it is submitted that such conduct constitutes fraud in that:

- a) A makes a misrepresentation – the e-mail message is a pervasion of the truth;
- b) A has the necessary intention: *dolus indeterminatus* is present in that he intentionally sends these false warnings and does not care whose computers will be rendered inoperable. Snyman describes *dolus indeterminatus* as follows: this form of intent is present where someone does not direct his act against a particular person but at anybody who may be affected by his act; the identity of his victims are of no importance to him.⁷⁶⁸
- c) His conduct is unlawful: the convictions of the community clearly stipulate that these acts are reprehensible in that they can cause financial loss to any Internet connected business, especially businesses that are Internet or e-mail dependent.
- d) Where A is prosecuted before his false warnings had any negative effect on the Internet community, potential prejudice is present in that the virus hoax has the potential to cause financial loss as well as the potential that third parties have to expend time and labour to repair the system. Where A is prosecuted after his hoax has already caused financial losses and inconvenience, prejudice is present.

3.5. Theft by false pretences as common law offence

Under this heading the general elements of the offence of theft by false pretences are first discussed. Thereafter it is assessed whether a *hacker* can be found guilty of this

⁷⁶⁷ See par 2.5 of chapter 4.

⁷⁶⁸ Snyman 1999:198.

offence where he penetrates a computer's security system and steals (copies) digital content.

Even though theft by false pretences is merely a *specie* of the offence of theft and therefore should have been discussed directly after theft, it was decided to discuss theft by false pretences after fraud because the former includes elements of both theft as well as fraud. This prevents repetition.

3.5.1. General principles

Theft by false pretences is committed whenever a person unlawfully and intentionally obtains another's movable property (things *in commercio*) "with the consent of the person from whom he obtains it, such consent being given as a result of an intentional misrepresentation by the person committing the crime, and appropriates it."^{769 770}

⁷⁶⁹ Snyman 1999:547; LAWSA 1996:vol 6, par 338; Hunt & Milton 1990:799. No South African court has ever given a definition of this crime. See LAWSA 1996:vol 6, par 338, fn 1. In *R v Coertzen* 1929 SWA 20 the court maintained (at 20-21) that "[i]n a case of theft by false pretences it must be proved that the handling or *contractatio* of the goods by the accused came about or was caused as a direct result of the false pretences. It must therefore be alleged and proved that the false representations preceded the *fraudulosa contractatio* in which the theft culminated." Where the state charges someone with theft by false pretences, it must allege that the accused knew that his representations were false. See *S v Salemane* 1967 3 SA 691 O:692H.

⁷⁷⁰ Some commentators harbour doubt whether such an offence should be recognised in South Africa, seeing that such conduct can be prosecuted as either theft or fraud. See Burchell & Milton 2000:553; Snyman 1999:549; LAWSA 1996:vol 6, par 339; De Wet en Swanepoel 1985:416-417; Verloren van Themaat 1949:176. At p 417 De Wet states that: "Pleeg die man diefstal moet hy van diefstal aangekla word, en pleeg hy bedrog moet hy van bedrog aangekla word. Of mens met die een dan wel die ander te doen het, hang daarvan af of die slagoffer deur die misleiding beweeg is om die *saak aan die verdagte in eiendom oor te dra* of nie. Het hy die *saak in eiendom oorgedra*, kan daar van diefstal geen sprake wees nie, maar wel van bedrog. Is die *saak nie in eiendom oorgedra nie*, selfs al is besit of beheer daarvan deur misleiding verkry, is diefstal wel moontlik. Tussen die twee moontlikhede bestaan daar nie ruimte vir 'n misdad wat nog diefstal nog bedrog is, maar tog ook albei is nie." (own emphasis) [own translation: If someone commits theft then he should be prosecuted for theft, and if he commits fraud then he should be prosecuted for fraud. Whether conduct constitutes fraud or theft, depends upon the question whether the victim was moved by means of misrepresentation to transfer the property in ownership to the accused. If the owner transferred the property in ownership, then theft was not committed but fraud. If the property was not transferred in ownership, even if possession or control was obtained by means of misrepresentation, then theft is possible. Between these two possibilities there exists no room for a crime that is neither theft nor fraud, yet both.] In *S v Stevenson* 1976 1 SA 636 T the court maintained, when dealing with the offence of *theft by false pretences* that "we believe there is no need for it." (at 637H). In *R v Mofokeng* 1939 OPD 116 the court noted (at 118) that "[d]iefstal deur

All the elements necessary to constitute the offence of theft must also be present for the offence of *theft by false pretences* as well as the element that A handed over property as a result of B's fraudulent misrepresentation (or B obtained it as a result of his misrepresentation).⁷⁷¹ This last requirement can be subdivided into three aspects: a) a misrepresentation; b) A must know that his representation is false and that B will act upon such misrepresentation (put differently, he must intent to defraud) and c) a causal link between the misrepresentation and the handing over of the property (or permitting the handing over) must exist.⁷⁷² *Theft by false pretences* also requires that the prejudice suffered must be actual and patrimonial in nature.⁷⁷³

All instances of *theft by false pretences* constitute both the offences fraud and theft.⁷⁷⁴ For this reason Snyman correctly submits that where *theft by false pretences* occurs, two offences are committed: firstly fraud and then theft⁷⁷⁵ – the thief obtains by his

middel van valse voorwendsels is as 'n juridiese figuur in ons regstelsel wanstaltig." [own translation: Theft by false pretences is juridicially unsound.] Snyman 1999:549 submits that the accused should be charged with "ordinary" theft and a specific allegation should be included in the charge sheet to the effect that X obtained the property as a result of false pretences. See also Hunt & Milton 1990:803; LAWSA 1996:vol 6, par 341; *R v Coovaida* 1957 3 SA 611 N:612H-613H. In *R v Hyland* 1924 TPD 336 the court remarked the following (at 336-337): "It has been the practice in the Cape, and frequently here, to charge offences of this character as theft by false pretences, but it has certainly been the practice in this Court for quite a considerable time to charge purely theft, and undoubtedly that is a good charge in law. If you take a man's money or property without his consent, and appropriate it to your own use, that is really theft. Where he does not really consent, but you merely procure his apparent consent by fraud, there is no consent in law, and on that principle it has been held safe to charge the crime purely as theft." However, local courts have stated that such an allegation is not an absolute necessity. *S v Salemane* 1967 3 SA 691 O:692H. See also p 692E-F where the court noted that "die klem [word] op diefstal as die dieftige toeëiening van vreemde besittings gelê, [ongeag] watter metode of metodes die dief ook al vir sy doeleindes aanwend solank hy dit aanwend met die opset om te steel." [own translation: in the case of theft the emphasis is on the theftuous appropriation of someone else's things, irrespective of the method or methods employed by the thief for this purpose provided that it was done with the intent to steel.] However, *theft by false pretences* was recently confirmed by the Supreme Court of Appeal in *De Wet v Santam Bpk* 1996 1 SA 926 A. This was a civil case concerning an insurance claim, but the court maintained that the conduct, which formed the subject-matter of the case, constituted *theft by false pretences*. (at 637A). *Theft by false pretences* was also expressly confirmed in *Ex Parte Minister of Justice: In Re R v Gesa; R v De Jongh* 1959 1 SA 235 A:239C-240E.

⁷⁷¹ Burchell & Milton 2000:553; Snyman 1999:549; LAWSA 1996:vol 6, par 340.

⁷⁷² Snyman 1999:549; LAWSA 1996:vol 6, par 340; Hunt & Milton 1990:800.

⁷⁷³ Snyman 1999:548; LAWSA 1996:vol 6, par 339.

⁷⁷⁴ *R v Davies* 1928 AD 165:170; Snyman 1999:548; LAWSA 1996:vol 6, par 339.

⁷⁷⁵ See also Hunt & Milton 1990:799; Verloren van Themaat 1949:175; LAWSA 1996:vol 6, par 339.

misrepresentation property from the owner.⁷⁷⁶ However, many courts have held that *theft by false pretences* is merely a *specie* of the offence of theft.⁷⁷⁷ Therefore where an accused is charged with theft and the evidence shows *theft by false pretences*, the court will still find the accused guilty of theft.⁷⁷⁸ For the purpose of this dissertation it is, therefore, accepted that theft, fraud and theft by false pretences are recognised crimes in South African law.

3.5.2. Relevance to hacking instances

Theft by false pretences is appropriate to hacking instances where the *hacker* obtains/appropriates digital content by means of fraud. As explained above,⁷⁷⁹ the *hacker* misrepresents to the system administrator (or person in control of the computer) that he is an authorised user of the computer system. It was further concluded that digital content constitutes incorporeal property capable of being stolen.⁷⁸⁰ The *hacker* thus commits theft as well as fraud, but cannot be found guilty of both offences in that the same facts constitute these two offences.⁷⁸¹

For the purposes of this dissertation, two specific issues relating to *theft by false pretences* need to be examined. Firstly, some commentators maintain that this offence can only be committed against movable corporeal property. As support for this contention they list *R v Renaud* and *R v Coertzen*. In *R v Renaud*⁷⁸² the accused was charged with the crime of theft in that he pretended to the complainant that both he and his wife were employed at a specific store in Cape Town and that on this basis the complainant was induced to give them free board and lodging. The court maintained that "[i]t cannot be said that he actually stole any particular thing, and upon that ground, and on that ground alone, I think the conviction should be

⁷⁷⁶ Snyman 1999:548. See also LAWSA 1996:vol 6, par 338.

⁷⁷⁷ *S v Salemane* 1967 3 SA 691 O:692G; *R v Vilakazi* 1959 4 SA 700 N:701H; *R v Teichert* 1958 3 SA 747 N:753E-F; *R v Manuel* 1953 4 SA 523 A:524H; *R v Medziso* 1950 4 SA 282 R:283B. See also LAWSA 1996:vol 6, par 338.

⁷⁷⁸ *R v Teichert* 1958 3 SA 747 N:753H. However, the prosecution must ensure that the accused is not prejudiced. The charge-sheet must indicate that the state alleges that the accused obtained the property by means of false pretences.

⁷⁷⁹ See par 3.4.2.1 of this chapter.

⁷⁸⁰ See par 3.1.4.1 of this chapter.

⁷⁸¹ See Snyman 1999:549.

⁷⁸² 1922 CPD 322.

squashed.”⁷⁸³

It must immediately be noted that obtaining board and lodging by means of fraud cannot be equated with being granted access to a computer system and copying digital content. As noted above, in the latter instance he procures the former’s confidential information and/or immaterial property.

In *R v Coertzen*⁷⁸⁴ the accused was charged with *theft by false pretences* in that he received from the landlord the use of beds and meals on the understanding that he would pay for it upon departure, which turned out to be a false misrepresentation. The court noted that:

“A further defect in the charge is that strictly there can be no *fraudulosa contrectatio* of a benefit conferred or services rendered. When the false pretence results, not in the handing over of property, but in granting some service or conferring some benefit, such as the use of rooms or beds, the offence is not theft [or theft by false pretences] but fraud.”⁷⁸⁵

Therefore, when A logs onto an Internet Service Provider’s (ISP’s) service, pretending to be an authorised (paying) user, so as to gain access to the Internet, such conduct does not constitute *theft by false pretences*, but fraud. Gaining access to a computer without authorisation and copying electronic content cannot be equated with services such as the use of beds or board and lodging. It follows that *theft by false pretences* should also be available where *hackers* copy digital content stored on a storage medium.

Secondly, the question arises whether the property must be physically handed over to the culprit. Where *hackers* penetrate a computer system and copy electronic content, the latter is not handed over to them; they are merely allowed to copy the information seeing that they misrepresent that they are authorised users of the computer system or that they have authorised access to these computers.

Some authorities are of the opinion that it is not necessary for the owner to physically deliver the property (object) to the thief; the “victim might well be induced simply to remain inactive while the thief assumed control.”⁷⁸⁶ This contention is supported by the

⁷⁸³ 1922 CPD 322:322-323.

⁷⁸⁴ 1929 SWA 20.

⁷⁸⁵ 1929 SWA 20:21.

⁷⁸⁶ Hunt & Milton 1990:801.

court's *dictum* in *R v Coovadia*⁷⁸⁷ concerning the difference between theft and theft by false pretences as follows: "[in the case of theft by false pretences] a complainant voluntarily gives up possession of property because of what the thief has pretended to him whereas in theft *simpliciter* property is taken from him without his consent."⁷⁸⁸ The court also stated that where the accused "actually obtained control of the complainant's goods by making false misrepresentations" such conduct constituted *theft by false pretences*.⁷⁸⁹ It is clear that where a *hacker* penetrates a computer system, by making a tacit or an express misrepresentation that he is an authorised user of the computer system or that he has authorised access to it, the owner of the computer system allows him to copy the files. Stated differently, the *hacker* obtains control over the complainant's electronic content by means of his false misrepresentations.

In conclusion it may be stated that it is possible for the state to prosecute a *hacker* for *theft by false pretences*, where he copied (stole) digital content after he had gained access to the computer system, without authorisation, thus deceiving the system administrator into thinking that he was an authorised user.

3.6. Malicious injury to property as common law offence

Under this heading the elements of the offence of malicious injury to property are briefly set out and, in addition, it will be determined whether hacking and virus instances deleting, modifying or corrupting electronic files or rendering a hard drive (permanently or temporarily) inaccessible/inoperable constitute malicious injury to property.

The South African Law Commission is of the opinion that gaining access to a computer without authorisation and modifying information stored on that computer does not constitute malicious injury to property in that, according to them, the law requires the damaged property to be corporeal.⁷⁹⁰ They further state that it is uncertain how the concept of "damage", in relation to computer data and software applications, will be

⁷⁸⁷ 1957 3 SA 611 N.

⁷⁸⁸ 1957 3 SA 611 N:612F.

⁷⁸⁹ 1957 3 SA 611 N:612H.

⁷⁹⁰ SALC's Discussion Paper 99:6. See par 2.2 of chapter 8.

interpreted by our courts.⁷⁹¹ Some South African commentators are of the same opinion.⁷⁹²

3.6.1. General principles

The traditional definition of malicious injury to property is the unlawful and intentional damaging of property belonging to another.⁷⁹³ Local courts created a specific exception to this definition, namely that A can be found guilty of malicious injury to property where he sets fire to his own insured property in order to claim its value from the insurance company.⁷⁹⁴ This aspect shall be dealt with below.

Five elements have to be present in order for conduct to constitute this offence namely damage, unlawfulness, causation, intention and property.⁷⁹⁵ These elements are now discussed separately:

a) Damage. Seeing that in the case of computer-related crimes no physical property is damaged, it has to be determined whether the law recognises other forms of "harm" or prejudice as sufficient "damage" for the offence of malicious injury to property. In *R v Bowden*⁷⁹⁶ the accused painted two statues. The court, dealing with the question whether such conduct constitutes damage to property, noted that:

"Dit is egter wenslik dat daar êrens 'n lyn getrek moet word in verband met die beskadiging van 'n saak. Word 'n saak permanent geskend dan is daar beskadiging as die saak van enige waarde is vir die eienaar. Word 'n saak geskend maar op so 'n manier dat dit herstel kan word en die herstelling lewer koste of moeite vir die eienaar dan is daar ook beskadiging. As die saak self geen waarde het nie of die skade wat berokken word is onbenullig behoort die beskadiging nie as 'n misdad te

⁷⁹¹ SALC's Discussion Paper 99:7.

⁷⁹² Van der Merwe 2000:193; LAWSA 1996:vol 6, par 343.

⁷⁹³ Burchell & Milton 2000:593; Snyman 1999:550; LAWSA 1996:vol 6, par 342. In *R v Mashanga* 1924 AD 11 the Supreme Court of Appeal maintained (at 12) that "[a]ll that is necessary in our law to the constitution of the crime is an intentional wrongful injury to the property of another."

⁷⁹⁴ Snyman 1999:551

⁷⁹⁵ See *Thompson & Strydom* 1964 1 PH H4 N:13; *R v Witbooi Motaung* 1954 2 PH H 116 O; *R v Maruba* 1942 OPD 51:55; *R v Malamu Nkatlapan* 1918 TPD 424:428. In *R v Ncetendaba and Another* 1952 2 SA 647 SR:651B the court identified four elements of the crime: a) wrongfulness, b) property c) damaged, killed or destroyed and d) intent to injure the owner or the property of a person.

⁷⁹⁶ 1957 3 SA 148 T.

geld nie.”⁷⁹⁷

Therefore, Snyman correctly notes that “[d]aar sal gewoonlik aangeneem word dat daar beskadiging is as daar op so 'n manier met die saak gepeuter is dat dit die eienaar geld, arbeid of moeite kos om dit weer te herstel tot sy oorspronklike vorm.”⁷⁹⁸ For this reason, Burchell and Milton maintains that letting out the air of A's tyres will constitute malicious injury to property in that such conduct interfered with A's use of the property, albeit temporarily.⁷⁹⁹ Finally, De Wet en Swanepoel observe that “[a]an vernietiging moet mens gelyk stel die wegdoen van 'n saak op so 'n wyse dat dit vir alle praktiese doeleindes nie teruggevind kan word nie.”⁸⁰⁰ Hunt attaches the following meaning to “damage”:

“Subject then to the *de minimis* principle, there is damage where X meddles with the property in such a way that it is destroyed or lost or permanently damaged, or damaged with the result that it reasonably requires repair, whether this costs the owner money or labour, or in such a way that its use is permanently or temporarily interfered with”.⁸⁰¹ (own underlining)

- b) Unlawfulness. A's conduct in causing damage to B's property must be unlawful according to the *boni mores*. The damage caused must not be too trivial.
- c) Causation.⁸⁰² There must be a causal connection between the damage and the conduct.
- d) Intention. Malice is not required by our courts, even though the offence is known as “malicious injury to property”.⁸⁰³ Mere inten (“*opset*”) is required⁸⁰⁴ and thus *dolus*

⁷⁹⁷ 1957 3 SA 148 T:150F-H. [own translation: It is desirable that a limit should be drawn with regard to the damaging of property. Where the property is of any value to its owner and it is permanently damaged then it follows that the property is damaged. Where the property is damaged in such a way that it can be repaired and such repair entails the incurring of expenses or labour for the owner it follows that such conduct constitutes damage to property. Where the property has no value or the damage inflicted is trivial such damage ought not to constitute an offence.]

⁷⁹⁸ Snyman 1999:552. [own translation: it will usually be assumed that there is damage if the property has been tampered with in such a way that it would cost the owner money or at least some measure of effort or labour to restore it to its original form.] See also LAWSA 1996:vol 6, par 344.

⁷⁹⁹ Burchell & Milton 2000:595.

⁸⁰⁰ De Wet & Swanepoel 1985:288. [own translation: to destruction must be equated the instance where an object is thrown away in such a way that it cannot, for all practical reasons, be retrieved.]

⁸⁰¹ Hunt 1967:144.

⁸⁰² Hunt-Milton 1990:822.

eventualis as well as *dolus indirectus* will suffice: "die beskadiging van die eiendom [hoef] nie X se hoofdoel ... te wees nie: dit is voldoende dat hy die moontlikheid voorsien dat skade mag voortvloei uit sy handeling, maar nietemin voortgaan met sy dade."⁸⁰⁵ It is submitted that *dolus indeterminatus* also suffices for the purpose of this offence: "X hoef nie die opset te hê om die een of ander bepaalde persoon te benadeel nie. In baie gevalle van saakbeskadiging weet X trouens nie eers wie die eienaar is nie."⁸⁰⁶

South African courts have invariably required an intention to injure (either the owner or property of the owner) as an essential element of the offence of malicious injury to property.⁸⁰⁷ In *R v Maruba*⁸⁰⁸ the court noted that "it is not necessary for the Crown to establish the existence of a specific intention to injure the owner: when proof is provided that an accused injured the property of a person, it will be presumed that he intended to injure the owner."⁸⁰⁹

⁸⁰³ *S v Mnyandu* 1973 4 SA 603 N:605H. See also Burchell & Milton 2000:596; Snyman 1999:553; LAWSA 1996:vol 6, par 346; Hunt-Milton 1990:820; De Wet & Swanepoel 1985:289.

⁸⁰⁴ *R v Mashanga* 1924 AD 11:12.

⁸⁰⁵ Snyman 1999:553 [own translation: damaging the property need not be X's principle aim: it is sufficient if he foresees the possibility that the damage may be caused and nevertheless proceeds with his actions.] See also Burchell & Milton 2000:596; LAWSA 1996:vol 6, par 346; Hunt-Milton 1990:826. As the court in *R v Ncuba* 1968 2 SA 18 R put it (at 19D): "the Crown has to prove affirmatively that the accused must ... have known of the risk." See also *S v Kgware and Another* 1977 2 SA 454 O:455E-F; *R v Ncetendaba and Another* 1952 2 SA 647 SR:651H. In *R v Shelembe* 1955 4 SA 410 N the court noted (at 411E-F): "It may be that his main purpose was to escape, and that the breaking of the door was merely a means to that end. But it seems to me that that cannot help him, for, at its best for him, he intended to apply to the door the violence which he did apply to it, and, even assuming in his favour that he did not intend all the damage which resulted, an intention to do some damage is inescapable, as I think is also the imputation to him of an indifference as to how much damage he actually caused." I.e. *dolus indirectus* suffices.

⁸⁰⁶ Snyman 1999:553 [own translation: X need not intend to harm any particular person. In many instances of malicious injury to property the owner of the property is unknown to X.] See also LAWSA 1996:vol 6, par 346.

⁸⁰⁷ See *S v Mnyandu* 1973 4 SA 603 N:606A; *R v Nkomozombanzo* 1959 1 SA 746 SR:764G; *R v Shelembe* 1955 4 410 N:411D-E; *R v Ncetendaba and Another* 1952 2 SA 647 SR:652B; *R v Maritz* 1944 EDL 101:103; *Kohrs v R* 1940 NPD 11:14; *R v Malamu Nkatlapan* 1918 TPD 424:425 & 426; *R v Gordon* 1916 CPD 69:70; *R v Laubscher and Others* 1913 CPD 123:126; *Bruyns v R* 1901 NLR 75:78; *R v Kumana* 1900 EDC 167:168.

⁸⁰⁸ 1942 OPD 51.

⁸⁰⁹ 1942 OPD 51:55. In *R v Mashanga* 1924 AD 11 the Supreme Court of Appeal stated (at p12): "The accused being angry with the animals, intended to injure the property of his master and he must therefore be presumed to have intended to injure his master." Hunt-Milton 1990:824 put it as follows: "If

e) Property. All South African commentators maintain that the object of this offence must be corporeal.⁸¹⁰ The following observations have to be made: a) it needs to be kept in mind that the *offence* of malicious injury to property did not exist in our common law and that it was created by the Cape Provincial courts.⁸¹¹ b) There exists an exception to the general definition stated above namely that where someone else has a substantial interest in A's property (such as an insurance company) and A destroys it in order to claim money from the insurance company, such conduct not only constitutes fraud but also malicious injury to property.⁸¹² Therefore it seems that "property" includes not only the physical property but also rights that other people have in such property. This submission is confirmed by the following judgments:

⇒ In *R v Mavros*⁸¹³ the applicant set his own store on fire with the intent to defraud the insurance company of the money for which he had insured the said store. The accused was charged and found guilty of arson. It should be borne in mind that arson is a *specie* of the offence of malicious injury to property. The Supreme Court of Appeal maintained that arson is committed by "a man who sets fire to his own house wrongfully, maliciously and with the intent to injure or defraud another person."⁸¹⁴

⇒ In *Kohrs v R*⁸¹⁵ the accused set four huts on fire. The court stated that "the term 'property' seems to me capable of covering physical objects *as well as rights of all kinds in and to physical objects*, as well as any goods which may reasonably be

he intentionally harms property, intention to injure its owner is present". In *R v Malamu Nkatlapan* 1918 TPD 424 the court maintained (at 428) that "it is not necessary to show that the accused knew the owner. If a man injures property which he knows is not his own, he must be taken to know he is injuring the person in respect of that property."

⁸¹⁰ Burchell & Milton 2000:595; Snyman 1999:551; LAWSA 1996:vol 6, par 343; Hunt-Milton 1990:821; De Wet & Swanepoel 1985:289.

⁸¹¹ Burchell & Milton 2000:593; Snyman 1999:550-551; LAWSA 1996:vol 6, par 342; De Wet & Swanepoel 1985:286-287. In *R v Reikert* 1874 Buch 142 the Attorney-General stated (at 143) that "Since 1837, indictments had been laid and convictions obtained in this Colony for the crime of malicious injury to property." See also *S v Solomon* 1973 4 SA 644 K:647H; *R v Maruba* 1942 OPD 51:54-55. *Damnatio iniuria datum* existed in Roman and Roman-Dutch law as a private delict. See De Wet & Swanepoel 1985:286.

⁸¹² See *R v Mavros* 1921 AD 19 below.

⁸¹³ 1921 AD 19.

⁸¹⁴ 1921 AD 19:23.

⁸¹⁵ 1940 NPD 11.

believed to be in that structure.”⁸¹⁶ (own emphasis)

⇒ In *S v Mtetwa*⁸¹⁷ the accused killed two cattle belonging to the complainant. The court noted that “in regard to the crime of malicious injury to property it is not necessary that the complainant should be the full and unencumbered owner of the property injured. What is required is that the intentional and unlawful act be an *injury to the rights of another person in and to that property*. Just as a person may be guilty of theft of property of which he is owner (e.g. of pledged property belonging to him) so too he may be guilty of malicious injury to property of which he is, in law, the owner but in which other persons have rights.”⁸¹⁸ (own emphasis)

⇒ In *S v Mnyandu*⁸¹⁹ the court maintained that “ ‘Malice’ beteken nie wrok of kwaadgesindheid teenoor die eienaar van die beskadigde eiendom of iemand wat ‘n *wesenlike belang* daarin het nie”.⁸²⁰ (own emphasis)

Consequently, in the light of these judgments, it is submitted that the South African courts have expanded the term “property” to include “substantial interests” as well as “rights in such property”, for the purposes of malicious injury to property.^{821 822}

3.6.2. Malicious injury to property over the Internet

The question now to be assessed is whether the offence of malicious injury to property can be committed with regard to electronic data/content. The following two examples of computer-related abuses serve as points of departure:

- a) A hacks in to B’s computer and deletes a file or files, corrupts such data or causes a hard drive to be inaccessible by formatting it;
- b) A releases a virus onto the Internet that does the above-mentioned. A knew that

⁸¹⁶ 1940 NPD 11:14-15.

⁸¹⁷ 1963 3 SA 445 N.

⁸¹⁸ 1963 3 SA 445 N:449D-F.

⁸¹⁹ 1973 4 SA 603 N.

⁸²⁰ 1973 4 SA 603 N:605H-606A. [own translation: Malice does not contemplate a grudge or unfriendliness towards the owner of the damaged property or someone that has a substantial interest therein.]

⁸²¹ In *S v Mnyandu* 1973 4 SA 603 N the court maintained (at 606A) that malicious injury to property “is dus die wederregtelike en opsetlike beskadiging van ‘n saak van iemand anders of waarin ‘n ander ‘n *wesenlike belang* het.” [own translation: is the unlawful and intentional damaging of property that belongs to someone else or in which a third party has a substantial interest.]

the virus had such capabilities.

As in the case of fraud and theft such conduct is clearly against the *boni mores* and thus unlawful. Furthermore, it is assumed that the state can prove that the *hacker/virus* caused such damage. Accordingly, only three elements need to be examined namely, intent to injure the owner or the property of the owner, damage, and property.

3.6.2.1. Intent to injure the owner or the property of the owner

It is clear that where a *hacker* intentionally deletes files on a computer he has the intent to injure the owner in that such data will be lost (forever, if the proprietor does not have any back-ups of the information). The same line of reasoning applies where a *hacker* intentionally causes files to be corrupted as well as where he formats a hard drive or causes such hard drive to be permanently inaccessible. By formatting a hard drive, the *hacker* intends to delete all the files saved on the hard disk. Where a *hacker* renders a hard drive temporarily inaccessible/inoperable, he has the intent to injure the owner of the computer in that it will take the latter time as well as labour to repair the computer. Where the computer owner uses third parties (such as computer experts) to repair the computer or operating system of the computer or to recover the electronic content or some of the content, he suffers financial prejudice. The owner is also "damaged" in his usage of the computer system.

Where a virus released onto the Internet causes such damage, the virus writer definitely had *dolus indeterminatus* in that he released such a dangerous computer program onto the Internet and did not care whose computers would be rendered inoperable or whose data would be deleted/corrupted.

3.6.2.2. Damage

Where a *hacker* or a virus program deletes a file (or even a part of a file) such conduct constitutes damage in that it will take the owner considerable time to recompile the information contained in the original document. The question that arises is what happens where the proprietor made back-up copies. It is submitted that normally the information contained in back-ups will, at least, be a few hours or days old and thus

⁸²² However, note must be taken of *R v Malamu Nkatlapan* 1918 TPD 424 where the court maintained (at 428) that one cannot commit this offence with regard to one's own property.

new information is lost. Where up-to-date back-up copies exist, it is submitted that an electronic file (incorporeal property) was still damaged (destroyed) and it will be of no avail for the accused to say that the victim did not suffer losses in that he possessed up-to-date back-up copies.

Furthermore, it is submitted that where a *hacker* or a virus causes a hard drive to be inaccessible, the *hacker* not only "harms" the electronic data previously stored on the disk, but also damages the disk in that it will take the complainant considerable time to reload all the computer programs onto the disk in order for the computer to function properly.

Finally, in all these instances the *hacker* substantially interferes with the usage of the property, namely either the electronic file or the hard disk. He either renders the specific data or the entire computer unusable.

3.6.2.3. Property

As indicated above, the question arises whether the property damaged must be corporeal in nature. There are three possible arguments in favour of the view that incorporeal data/content will suffice for his particular requirement:

- i) As indicated above, the courts have repeatedly referred to the rights or interests that people have in corporeal objects. For instance, where A insured his car and then intentionally damaged or destroyed his car in order to defraud the insurance company in giving him the insured value, he infringes their rights/substantial interests that they have in regard to the specific car.

In the case of computer-related crimes, the corporeal object is the hard drive. It is submitted that where a *hacker* or a malicious computer program deletes files or corrupts them, he or the program "destroys" the owner's rights/interests that he has in connection with such hard drive. As mentioned earlier, the owner has an immaterial property right with respect to the electronic content (files) stored on his hard drive. Therefore, although the deletion of the files does not physically damage the hard drive, such deletion does in fact infringe (actually destroys) the owner's immaterial property rights. In *R v Malamu Nkatlapaan*⁸²³ the court stated that the

⁸²³ 1918 TPD 424.

accused must injure the owner in his property.⁸²⁴

Of course, where the *hacker* or a malicious program causes the entire hard drive to be formatted or renders it inaccessible, such conduct damages the hard drive as indicate above and therefore physical property is damaged in such instances.

- ii) The second argument is that the offence of malicious injury to property should develop in an identical way as the offence of theft did. According to Roman law, as well as Roman-Dutch and early South African law, only physical objects (property) could form the subject of theft. New questions of law arose namely whether money in the form of credit as well as shares, as incorporeal property, could form the object of theft. The courts extended the meaning of "property" to include not only corporeal property but also incorporeal property. In fact, it will be remembered that the courts stated that a mere false entry in an accounting book's credit side constitutes theft.

The same line of reasoning can be followed in the case of malicious injury to property: the meaning of the word "property" should be extended to include incorporeal property embodied in electronic files: By deleting or corrupting data the *hacker* destroys the electronic content, constituting incorporeal property, and this amounts to what can be called "constructive malicious injury to property". It will be up to the courts to decide what type of information/content can form the object of "constructive malicious injury to property". Hunt-Milton correctly point out that the "property" damaged need not be of commercial value and likewise need not be diminished in commercial value. Put differently, the conduct need not result in financial loss.⁸²⁵

- iii) A third possible argument which was upheld by the UK Court of Appeal in *R v Whiteley*⁸²⁶) is that where information/data stored on a hard drive is deleted or corrupted, tangible property is damaged:

"What the Act [Criminal Damage Act of 1971] requires to be proved is that tangible property has been damaged, not necessarily that the damage itself should be tangible. There can be no doubt that the magnetic particles upon the metal discs were a part of the discs and if the appellant was proved to have intentionally and

⁸²⁴ 1918 TPD 424:427.

⁸²⁵ Hunt-Milton 1990:824.

⁸²⁶ 1991 93 Cr App R 25. A copy of this judgment can be downloaded from www.austlii.edu.au/au/other/crime/Whiteley.html.

without lawful excuse altered the particles in such a way as to cause an impairment of the value or usefulness of the disc to the owner, there would be damage within the meaning of section 1. The fact that the alteration could only be perceived by operating the computer did not make the alterations any the less real, or the damage, if the alteration amounted to damage, any the less within the ambit of the Act ... Any alteration to the physical nature of the property concerned may amount to damage within the meaning of the section. Whether it does so or not will depend upon the effect that the alteration has had upon the legitimate operator (who for convenience may be referred to as the owner). If the hacker's actions do not go beyond, for example, mere tinkering with an otherwise 'empty' disc, no damage would be established. Where, on the other hand, the interference with the disc amounts to an impairment of the value or usefulness of the disc to the owner, then the necessary damage is established."

The same court confirmed the *dicta* of Justice Auld in *Morphitis v Salmon*⁸²⁷ where he maintained that "damage should be interpreted so as to include not only permanent or temporary physical harm, but also permanent or temporary, impairment of value or usefulness."⁸²⁸

This line of reasoning is also followed in the USA. The facts of *American Guarantee & Liability Insurance v Ingram Micro Inc*⁸²⁹ (2000) were the following: American Guarantee (applicant) insured the computers of Ingram Micro (respondent) in terms of its "Primary-All-Risk Policy". This policy insured all respondent's "[r]eal, and personal property, business income and operations in the world" against "[a]ll risks of direct physical loss or damage from any cause, howsoever or wheresoever occurring, including general average, salvage charges or other charges, expenses and freight". As a result of a power outage, respondent's computer systems were rendered inoperable. Specifically, the main frame computers lost all of the programming information that had been stored in their "random access memory". Respondent's employees had to reload the lost programming information, which took about one and a half hours. However, it took these employees a further six and a half hours to restore the computers, and their connections to other computers around the world, to their normal functioning. It follows that respondent could only conduct business as normal after eight hours.

⁸²⁷ 1990 Crim LR 48.

⁸²⁸ Unfortunately this case was not locally available, so Akdeniz 1996 had to be relied upon.

⁸²⁹ (D.Ariz 2000). A copy of this judgment can be downloaded from www.2001law.com/article_445.htm.

Applicant refused to pay the claimed insurance, averring that respondent's computers were not physically damaged "because their capability to perform their intended functions remained intact. The power outage did not adversely affect the equipment's inherent capability to accept and process data and configuration settings when they were subsequently reentered into the computer system." Respondent argued that "physical damage" must be interpreted more generously to include "loss of use and functionality". The court sided with the plaintiff and held:

"At a time when computer technology dominates our professional as well as personal lives, the Court must side with Ingram's broader definition of 'physical damage.' The Court finds that 'physical damage' is not restricted to the physical destruction or harm of computer circuitry but includes loss of access, loss of use, and loss of functionality ... Lawmakers around the country have determined that when a computer's data is unavailable, there is damage; when a computer's services are interrupted, there is damage; and when a computer's software or network is altered, there is damage. Restricting the Policy's language to that proposed by American would be archaic In this case, Ingram does allege property damage - that as a result of the power outage, Ingram's computer system and world-wide computer network physically lost the programming information and custom configurations necessary for them to function. Ingram's mainframes were 'physically damaged' for one and one half hours. It wasn't until Ingram employees manually reloaded the lost programming information that the mainframes were 'repaired.' [The computer] was 'physically damaged' for eight hours. Ingram employees 'repaired' [the computers] by physically bypassing a malfunctioning matrix switch. Until this restorative work was conducted, Ingram's mainframes and [computers] were inoperable."

In *Retail Systems Inc v CAN Insurance Cos*⁸³⁰ (1991) the facts were that the appellant lost A's computer tape, containing valuable information. Respondent insured the appellant against damage claims resulting from "Personal Injury or Property Damage to which this insurance applies." The policy continued to define property damage as "physical injury or destruction of tangible property." The respondent contended that only the loss of the computer tape was covered by the insurance policy and not the data stored on the tape. The question of law was

⁸³⁰ 469 N.W. 2d 735 (Minn. App 1991). A copy of this judgment was obtained from Westlaw.

whether the computer tape and the data stored on it were tangible property under the insurance policy.⁸³¹ The court answered this question in the affirmative by noting that -

“[t]he data on the tape was of permanent value and was integrated completely with the physical property of the tape. Like a motion picture, where the information and the celluloid medium are integrated, so too were the tape and data integrated at the moment the tape was lost.”⁸³²

Therefore, it is submitted that where a *hacker* or the creator of a malicious computer program causes information to be deleted or corrupted or causes a hard drive to be inaccessible, such conduct justifies a conviction of the offence of malicious injury to property.

3.6.3. Modification of digital content and malicious injury to property

It is submitted that where a *hacker* modifies the electronic content stored on a computer or uses a malicious computer program that modifies electronic files, such conduct constitutes malicious injury to property in that -

- a) Damage will be present where due to the modification the owner has to spend time, money and labour to repair the file or to restore it to its original form. Where an electronic file is modified it interferes with the owner's use of these files. Furthermore, where the file is rendered unusable due to the modification, the file is for all purpose permanently damaged.
- b) Such conduct is clearly unlawful.
- c) The *hacker* or the computer programmer caused such damage/prejudice.
- d) Intent is present in that the *hacker* has *dolus directus* and the computer programmer (who created the virus) has *dolus indeterminatus*.
- e) They caused damage to electronic content and thus incorporeal (immaterial) property. They also infringed the owner's legal interest he enjoys with regard to the immaterial content.

⁸³¹ 469 N.W. 2d 735 (Minn. App 1991):737.

⁸³² 469 N.W. 2d 735 (Minn. App 1991):737.

3.6.4. Bacteria and malicious injury to property

As noted earlier,⁸³³ bacteria are computer programs programmed to replicate *ad infinitum* within a computer system. This causes system resources (memory as well as hard drive space) to be consumed and eventually the computer will stop functioning. Such conduct clearly constitutes malicious injury to property in that -

- a) The computer program interferes (substantially) with the use of the computer. Normally the computer owner (or his system administrator) has to spend time and money to remove the malicious computer program and to repair the computer system. Therefore damage is present.
- b) Unlawfulness as well as causation is present.
- c) *Dolus indeterminatus* is present in that the program creator knew that his program has this potential but did not care who suffered the consequent prejudice.
- d) The computer system (as corporeal property) is damaged: it is rendered inoperable.

3.6.5. Denial-of-service attacks and e-mail bomb attacks

As previous noted,⁸³⁴ a denial-of-service attack (DoS attack) entails the situation where one or more computer users overwhelm a web server with millions of "false" requests, which, in turn, causes the computer to deny access to legitimate users of that particular web site. The DoS attack may be so overwhelming that it causes the computer to crash. E-mail bombs, as explained,⁸³⁵ entails the instance where one or more computer users overwhelm a computer with so many e-mail messages that it causes that particular computer to crash. Thus both e-mail bomb attacks and DoS attacks interfere with the operation or functioning of a particular computer.

Bearing in mind the general principles of malicious injury to property,⁸³⁶ it is submitted that both these attacks constitute malicious injury to property in that property, in this case the computer which includes its operating system (such as MS Windows), is damaged:

⁸³³ See par 2.6 of chapter 4.

⁸³⁴ See par 3 of chapter 5.

⁸³⁵ See par 3 of chapter 5.

⁸³⁶ Discussed in par 3.5.1 of this chapter.

- a) It will either cost the owner money or labour and effort to restore the computer to a working condition; and
- b) It interferes with the usage of the computer to such an extent that the computer owner cannot enjoy his subjective rights;

and the *hacker* clearly had *dolus directus* in that his actions were specifically directed against the targeted computer user. Of necessity, the elements unlawfulness and causation are present.

3.6.6. Defacement of a web page by a hacker or computer program

Under this heading the question whether the defacement of a web page, either by a *hacker* himself or by using a malicious computer program, constitutes malicious injury to property, is addressed.

Defacement of a web page can occur in one of two ways: a) When a *hacker* gains access to a web site and defaces a particular web page or b) When a person employs an insidious computer program to infect the computer hosting a web site and the program defaces a web page.⁸³⁷ The defacement of a web page can refer to various aspects of which the following are mere examples:

- The wording of an online news report can be changed (e.g. to read that Bill Gates hacked into NASA's computer system) or the prices of an online inventory can be modified (e.g. to read R2.99 instead of R299); or
- A message can be displayed on the web page, in addition to the normal contents of this particular page (e.g. stating that "Mafiaboy was here" or that "your network security sucks"); or
- The entire original web page is deleted and replaced with the *hacker's* web page, which, in turn, can include pornographic material, defamatory statements or non-relevant content.⁸³⁸

It is submitted that where a *hacker* defaces a web page by deleting the content of the web page and then replacing it with his own content, such conduct constitutes malicious injury to property in that he infringes the web page owner's immaterial

⁸³⁷ For instance, in 2001 an Internet worm penetrated computer systems and automatically attacked web sites, by defacing their home pages. See Boisteel 2001.

⁸³⁸ See www.antonline.com/achives/pages/ for examples of defaced web pages.

property rights: he “destroyed” the owner’s incorporeal property. Furthermore it will normally cost the owner time and labour to “rebuild” the web page or to recompile the information displayed on the previous web page.

Where text or pictures are added to a web page, such conduct is tantamount to graffiti. Only where the removal of the text or content added to the web page costs the owner labour, time and/or money to restore the page to its original condition, does such conduct constitute malicious injury to property.⁸³⁹

The *de minimis non curat lex* rule should be kept in mind at all relevant times. Whether this rule applies to a given scenario depends upon the facts of the particular scenario.⁸⁴⁰ The general criterion seems to be, in the case of malicious injury to property: was the damage done, if any, of such a trifling nature that the matter should never have come to court.⁸⁴¹

3.6.7. Mental copying or writing down of confidential information

The next issue to be addressed is whether a *hacker* who gains access to confidential information (including trade secrets) and either memorises the information or writes it down on a piece of paper, is guilty of malicious injury to property?

It was concluded in paragraph 3.1.8 of this chapter that the same *hacker* is guilty of theft of incorporeal property. It is submitted that it can also be argued that the *hacker* may also be guilty of malicious injury to property in that when he obtains knowledge of B’s confidential information (such as a confidential client list), which constitutes incorporeal property, he in effect either destroys B’s incorporeal property or immaterial property rights in that the law does not recognise the information as “confidential information” any longer or he damages the incorporeal property in that he diminishes the value of the incorporeal property and the benefits the owner enjoys in respect thereof. This will especially be the position where the *hacker* obtains the knowledge and then publishes it on a web page. This must also be seen as a type of “constructive

⁸³⁹ See *R v Bowden* 1957 3 SA 147 T:150F-G.

⁸⁴⁰ See par 3.1.7 of this chapter.

⁸⁴¹ *R v Dane* 1957 2 SA 472 N:473B-C. In *Mbala v S* 1969 1 PH H44 E the court confirmed this view by stating that “[i]t is certainly not a case in my view which should take up the time of the court.” However, the court continued to state that “There are, of course, cases in which a technical offence may be a serious one.”

malicious injury to property"⁸⁴² in that the *hacker* did not physically touch the incorporeal property but destroyed or diminished its value.

Geldenhuis, in his doctoral thesis, propounds a very unique theory and perspective which runs along the following lines: an owner of a corporeal object enjoys, by means of his ownership rights in regard to such object, the power to control the object to such an extent that information regarding the object be kept secret.⁸⁴³ Where the owner keeps such information secret, any act by a third party by means of which he acquires knowledge concerning the object infringes the owner's ownership rights, irrespective whether such impingements have any physical effect upon the corporeal object.⁸⁴⁴ The owner's interest in keeping such information secret is consequently protected by the subjective right he enjoys in regard to such property.⁸⁴⁵

Therefore where a *hacker* gains access to A's computer he infringes A's subjective right that the latter enjoys in regard to his computer: The *hacker* acquires knowledge, against A's wishes, of the password that grants access to the system and/or acquires knowledge about other information stored on A's hard drive. It is, therefore, submitted that such conduct constitutes malicious injury to property.

3.6.8. Attempt to commit malicious injury to property

Under this heading it is ascertained whether someone can be found guilty of an attempt to commit malicious injury to property where he intentionally releases sinister computer programs but such programs are either defective (and cannot cause any

⁸⁴² See par 3.6.2.3 of this chapter where this concept is discussed.

⁸⁴³ On p 119 he states: "Hierdie bevoegdheid [om sulke verbandhouende informasie geheim te hou] wat voortspruit uit die eienaar se gebruiks- en beskikkingsbevoegdheid oor die saak [die rekenaar], kan beskryf word as die bevoegdheid tot *absolute geheimhouding van inligting met betrekking tot die saak.*" [own translation: This power to keep such related information, which emerges from the owner's enjoyment and disposal powers over the property [the computer], secret, can be described as the power to keep information, in regard to the property, absolutely secret.]

⁸⁴⁴ Geldenhuis 1993:127-128. On p 119 he observes: "Indien 'n persoon in so 'n geval stappe sou doen om die inligting in stryd met die wil van die eienaar te bekom, en daarin slaag, sal sodanige optrede neerkom op 'n feitelike inwerking op die gemelde bevoegdhede van die eienaar ten aansien van die saak. Sodanige sal dus *prima facie* onregmatig wees." [own translation: Where a person in such a case takes steps to procure information contrary to the owner's wishes, and succeeds, such conduct constitutes a factual infringement upon the mentioned powers of the owner in regard to the property. This would be *prima facie* unlawful.]

⁸⁴⁵ Geldenhuis 1993:533.

prejudice) or the programs are discovered before they can cause any prejudice. Therefore in these instances no actual prejudice was caused.

3.6.8.1. Virus discovered prior to causing prejudice

Where A intentionally sends a malicious computer program as an e-mail attachment to B, intending to cause the latter either inconvenience or financial loss, but B discovers in time that the attachment contains a malicious program and consequently suffers no prejudice, the question of law arises whether A can be prosecuted for attempted malicious injury to property?⁸⁴⁶ In the example above it is assumed that if the computer program was not discovered and subsequently removed by B, it would either have deleted, modified or corrupted information stored on B's hard drive or would have rendered B's computer inoperable or inaccessible.

A court will find an accused guilty for an attempt to commit a crime where a) the accused had the intent to commit the particular crime and b) an overt act (*actus reus*) is present.⁸⁴⁷ With regard to the various types of "attempts" that exist in our law, the Supreme Court of Appeal enunciated in *R v Schoombie*⁸⁴⁸ that:

"Attempts seem to fall naturally in two classes: (a) Those in which the wrongdoer, intending to commit a crime, has done everything which he set out to do but has failed in his purpose either through lack of skill, or of foresight, or through the existence of some unexpected obstacle, or otherwise, (b) those in which the wrongdoer has not completed all that he set out to do, because the completion of his unlawful acts has been prevented by the intervention of some outside agency."⁸⁴⁹

The stated example can be compared with the facts in *S v Laurence*.⁸⁵⁰ The accused dispatched an envelope (containing an article, which, if published in South Africa, would have rendered the accused liable in terms of the *Suppression of Communism Act*) to A in London requesting him to forward the article to B, a publisher of a newspaper which would in the normal course of events have been circulated in South

⁸⁴⁶ In March 2001 a UK businessman was found guilty of contravening the UK *Computer Misuse Act* in that he sent a virus, out of jealousy, as an attachment to one of his business rivals. See De Bruxelles 2001.

⁸⁴⁷ *S v Du Plessis* 1981 3 SA 382 A:401C; Snyman 1999:293; LAWSA 1996:vol 6, par 141.

⁸⁴⁸ 1945 AD 541.

⁸⁴⁹ 1945 AD 541:547.

⁸⁵⁰ 1975 4 SA 825 A.

Africa. The envelope was intercepted and the accused was subsequently charged with attempt to contravene this Act. The Supreme Court of Appeal simply stated that:

"Thus he did everything which he set out to do; he could do no more and dropped out of the picture after he had completed his self-imposed task. On a realistic, common sense view the role played by the appellant clearly constituted a completed attempt".⁸⁵¹

The stated example can also be compared to the facts in *R v Lionda*.⁸⁵² The South African government had by means of a government notice stipulated that local businesses were prohibited from conducting business with firms in (*inter alia*) Switzerland. The accused dispatched a letter to a firm situated in Switzerland offering its services. This letter was intercepted and the accused was charged with attempting to contravene the above-mentioned notice. The accused contended that his conduct did not constitute an attempt to commit this offence seeing that the letter was intercepted. The Supreme Court of Appeal maintained that the accused's conduct constituted an attempt⁸⁵³ and that the interception did not change the character of the offence:

"But in my opinion here again the contention fails. The case is far more analogous to cases such as *Rex v Ransford* (13 Cox 9) and *Rex v Cope* (38 TLR 243), where it was held that the interception of a letter before it reached the addressee did not prevent the overt act of posting it from constituting an attempt."⁸⁵⁴

Therefore, it may safely be stated that in our given example the frustration of the completion of the offence was beyond A's control. There was no further step that the accused could have taken towards the consummation of the offence.⁸⁵⁵ The accused also had the necessary intent to commit the crime: either *dolus directus* or *dolus eventualis*. Therefore, it is submitted that he is guilty of attempted malicious injury to property.

⁸⁵¹ 1975 4 SA 825 A:827H-828A.

⁸⁵² 1944 AD 348.

⁸⁵³ 1944 AD 348:355.

⁸⁵⁴ 1944 AD 348:356-357.

⁸⁵⁵ See *S v Mlambo* 1986 4 SA 34 E:41G-H. See also 41J-42B: "In the present case the conduct of the accused had passed the stage of mere mental contemplation of wrongdoing. There had been an essential overt act in the chain of events leading to the consummation of the offence, and which commenced such chain of events in a manner which would, in the natural course of events and unless there was some interruption outside the control of the accused, result in consummation."

3.6.8.2. Target computer not vulnerable to computer program

The question that arises is: What would the position be if a malicious program is designed to delete or corrupt specific files, such as files ending with “.gif”, and the computer of the complainant contains no such files. Even if the complainant fails to detect the malicious program he will not suffer prejudice. The question therefore is whether such conduct constitutes attempted malicious injury to property?

It is clear that the accused did everything he could to commit the crime. It follows that this is a completed attempt but the question remains whether it is possible to hold an accused liable for an attempt to commit an offence where the offence that he attempted to commit was impossible – the computer program could not cause prejudice to B seeing that he had no files that could be deleted or corrupted by the program.

In *R v Davies & Another*⁸⁵⁶ the Supreme Court of Appeal dealt with an attempt to commit the impossible. The accused (a doctor) had attempted to conduct an illegal abortion, but unknown to him the foetus was already dead. The court maintained that -

“it seems that on principle the fact that an accused’s criminal purpose cannot be achieved, whether because the means are, in the existing or in all conceivable circumstances, inadequate, or because the object is, in the existing or in all conceivable circumstances, unattainable, does not prevent his endeavour from amounting to an attempt.”⁸⁵⁷

Furthermore, the court noted that -

“it would obviously be reasonable to treat as attempts all cases where an endeavour, going beyond preparation, has been made to procure an abortion, *whether or not the woman was pregnant, the foetus alive or the means capable of achieving the purpose aimed at.*”⁸⁵⁸ (own emphasis)

Therefore, it is submitted that in the given scenario either the means the accused used was inadequate (he should have used another computer program to delete files) or the object at which he directed his acts was unattainable (he could not cause prejudice to

⁸⁵⁶ 1956 3 SA 52 A.

⁸⁵⁷ 1956 3 SA 52 A:64A-B.

⁸⁵⁸ 1956 3 SA 52 A:64H.

the B in that his hard drive, the object, contained no such files).⁸⁵⁹ He also has the necessary intent to commit the crime. Therefore, it is submitted that he is guilty of attempted malicious injury to property.

3.6.8.3. Defective malicious programs

Another question that can be posed is what is the legal position where A, a computer programmer, creates a malicious computer program, releases it onto the Internet to wreak havoc, but it turns out that the program is defective and cannot cause prejudice to anyone. B contracts the virus.

It is submitted that this is also an example of a completed attempt where A did everything he could to commit the crime, but failed to succeed in that the means he used to commit the crime was not capable of committing the crime.⁸⁶⁰ A also had the necessary intent to commit the crime. It is submitted that a court will probably hold that *dolus indeterminatus* was present.

3.7. The offences of housebreaking and trespassing

The South African Law Commission correctly observes that unlawful access to a computer cannot amount to housebreaking with the intent to commit a crime due to the requirement of a person's presence in a physical structure and furthermore, the access (of a computer) must be connected to the intent to commit another offence.⁸⁶¹

The *Trespass Act*⁸⁶² is also not relevant to computer-related crimes in that it only applies to perpetrators that trespass on any land or building.⁸⁶³

3.8. The offence of sabotage

In layman's terms, it may be stated that the following acts amount to sabotage:

⁸⁵⁹ See *R v Davies & Another* 1956 3 SA 52 A:61H-62A; Snyman 1999:288; LAWSA 1996:vol 6, par 146.

⁸⁶⁰ See the discussion in para 3.6.8.1 & 3.6.8.2 of this chapter.

⁸⁶¹ www.lawcomm.co.za/CHP2DRAFT618.HTM. See also LAWSA 1996:vol 6, par 353 & 354.

⁸⁶² Act 6/1959.

⁸⁶³ S 1.

- Accessing a computer system to spread or insert a malicious computer program.
- Accessing the computer and deleting files or making the computer inaccessible.⁸⁶⁴

Sabotage is regulated by means of section 54(3) of the *Internal Security Act*⁸⁶⁵ which, for all purposes, targets acts of terrorism against the state or public.⁸⁶⁶ The only instance where a *hacker* can be prosecuted under this section is where he e.g. crashes the computer networks of a power, water or telecommunication station, or employs a malicious program to crash these networks.⁸⁶⁷ However such conduct can also be prosecuted as malicious injury to property.⁸⁶⁸

3.9. *Crimen iniuria* – violation of privacy as a common law offence

Under this heading it will be assessed whether the following conduct constitutes *crimen iniuria*:

- a) Penetrating the computer system or any part of the computer system of another user, without his authorisation.
- b) Intercepting or eavesdropping on e-mail communications.
- c) Installing a Trojan horse to intercept information or communications.
- d) Obtaining private information concerning third parties from a *hacker*.
- e) Disseminating “hacked” or intercepted information.

It will also be determined whether an unsuccessful hacking attempt constitutes attempted *crimen iniuria*.

3.9.1. General principles

Crimen iniuria is the unlawful, intentional and serious violation of the dignity or privacy

⁸⁶⁴ Van der Merwe 2000:153 &193.

⁸⁶⁵ Act 74/1982.

⁸⁶⁶ See the definition of sabotage in s 54(3).

⁸⁶⁷ S 54(3)(c) criminalises the following instances: “Any person who with intent to interrupt, impede or endanger at any place in the Republic the manufacture, storage, generation, distribution, rendering or supply of fuel, petroleum products, energy, light, power or water, or of sanitary, medical, health, educational, police, fire-fighting, ambulance, postal or telecommunication services or radio or television transmitting, broadcasting or receiving services or any other public service in the Republic or elsewhere commits any act” commits an offence of sabotage.”

⁸⁶⁸ As shown in par 3.6 of this chapter.

of another.⁸⁶⁹ The offence is committed where A's privacy is infringed, irrespective of whether he knows that his privacy is being or has been infringed⁸⁷⁰ and irrespective of whether it injures his feelings.⁸⁷¹ In *Financial Mail (Pty) Ltd & Others v Sage Holdings Ltd & Another*⁸⁷² the Supreme Court of Appeal held that both individuals and legal persons are the holders of the right to privacy.⁸⁷³

Hence there are four requirements for conduct to constitute this offence: a) an infringement of privacy, b) unlawfulness, c) intent and d) the infringement must be serious.⁸⁷⁴

3.9.1.1. The right to privacy and its infringement

The law recognises the right to privacy⁸⁷⁵ as an independent personality right.⁸⁷⁶ The right to privacy has been expressed and/or recognised as the right to privacy of one's home,⁸⁷⁷ premise,⁸⁷⁸ office⁸⁷⁹ and private quarters;⁸⁸⁰ the right to private communications;⁸⁸¹ the right to not be subjected to publicity⁸⁸² and the right to not have

⁸⁶⁹ Snyman 1999:466; LAWSA 1996:vol 6, par 275; Hunt-Milton 1990:525.

⁸⁷⁰ Snyman 1999:471; LAWSA 1996:vol 6, par 276 & 279; Hunt-Milton 1990:539. D 47.10.3.2 (translated by Mommsen *et al* 1985) reads: "Thus, someone can suffer an [iniuria] even though unaware".

⁸⁷¹ Neethling *et al* 1999:331.

⁸⁷² 1993 2 SA 451 A.

⁸⁷³ 1993 2 SA 451 A:462E.

⁸⁷⁴ Snyman 1999:466; Hunt-Milton 1990:526. In *R v Umfaan* 1908 TS 62 the court noted (at 66) that "[t]he act complained of must be wrongful; it must be intentional; and it must violate one or other of those real rights, those rights *in rem*, related to personality, which every free man is entitled to enjoy."

⁸⁷⁵ *Janit & Another v Motor Industry Fund Administrators (Pty) Ltd & Another* 1995 4 SA 293 A:303F-G; *Motor Industry Fund Administrators (Pty) Ltd & Another v Janit & Another* 1994 3 SA 56 W:60H; *S v Hammer & Others* 1994 2 SACR 496 C; *O'Keeffe v Argus P & P Co Ltd & Another* 1954 3 SA 244 C:249B-D; *R v R* 1954 2 SA 134 N:135F.

⁸⁷⁶ Neethling *et al* 1996:240, 242 & 255. In *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk* 1977 4 SA 476 T the court noted (at 383H-384A) that "[d]ie reg op privaatheid is een van die verskyningsvorme van die breër groep persoonlikheidsregte. In ons regspraak is erkenning aan sowel persoonlikheidsregte as die reg op privaatheid as beskermde regte verleen." [own translation: the right to privacy is a *specie* of a broader category of personality rights. Our judgments have recognised both personality rights as well as the right to privacy as protected rights.] See also *Janse van Vuuren & Another NNO v Kruger* 1993 4 SA 842 A:849F.

⁸⁷⁷ *R v S* 1955 3 SA 313 SWA:316A-B.

⁸⁷⁸ *R v Schonken* 1928 AD 36:45; *Ho Si v Vernon* 1909 TS 1074:1080 & 1088.

⁸⁷⁹ *Reid-Daly v Hickman and Others* 1981 2 SA 315 ZAD.

⁸⁸⁰ *De Fourd v Town Council of Cape Town* 1898 SC 399:402.

⁸⁸¹ *S v Hammer & Others* 1994 2 SACR 496 C:498c.

your private documents subjected to an unlawful search.⁸⁸³ Even Roman law recognised a forceful entrance into a house as an *iniuria*⁸⁸⁴ and further stipulated that even an unlawful intrusion upon a farm constituted an *iniuria*.⁸⁸⁵

Both US as well as local courts employ a two part test to determine the scope of an individual's or a business' right to privacy:

- a) The person must have a subjective expectation of privacy; and
- b) Such expectation must be one that society recognises as reasonable.⁸⁸⁶

In *National Media Ltd & Another v Jooste*⁸⁸⁷ the Supreme Court of Appeal described the right to privacy as follows:

"A right to privacy encompasses the competence to determine the destiny of private facts ... The individual concerned is entitled to dictate the ambit of disclosure, for example to a circle of friends, a professional adviser or the public ... He may prescribe the purpose and method of the disclosure ... Similarly, I am of the view that a person is entitled to decide when and under what conditions private facts may be made public. A contrary view will place undue constraints upon the individual's so-called 'absolute rights of personality'."⁸⁸⁸

Local courts have maintained that the right to privacy can be infringed in the following

⁸⁸² *Rhodesian Printing & Publishing Co Ltd v Duggan and Another* 1975 1 SA 590 RA:593-594C.

⁸⁸³ *Reid-Daly v Hickman and Others* 1981 2 SA 315 ZAD.

⁸⁸⁴ D 47.10.5 (translated by Mommsen *et al* 1985) reads: "The *lex Cornelia* on [iniuriis] applies to one who wishes to bring the action for insult on the ground that he declares himself to have been beaten or thrashed or *his house to have been entered by force* ... And so the *lex Cornelia* gives an action on three grounds: that a person was beaten or was thrashed or that his house was entered by force." (own emphasis) D 47.10.5.2 (translated by Mommsen *et al* 1985) reads: "House we must interpret not in terms of ownership but as one's place of residence. Hence, whether a person lives in a house which he owns or one he rents or has free or by hospitality, the statute applies."

⁸⁸⁵ D 47.10.5.4 (translated by Mommsen *et al* 1985) reads: "And if the owner has let a farm which is invaded, it is the tenant, not the owner, who can take proceedings." See also D 47.10.5.5.

⁸⁸⁶ See *Katz v United States* 389 US 347 (1967):361: "first that a person has exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable'." In *Bernstein & Others v Bester & Others NNO* 1996 2 SA 751 CC the Constitutional Court, after it referred to the *Katz*-case, noted (792F-I) that "it seems to be a sensible approach to say that the scope of a person's privacy extends *a fortiori* only to those aspects in regard to which a legitimate expectation of privacy can be harboured." In *Protea Technology Ltd & Another v Wainer & Others* 1997 9 BCLR 1225 W the court held (1239H) that such a "legitimate expectation" "requires a subjective expectation of privacy which society recognises as objective reasonable." See also Steytler 1998:83.

⁸⁸⁷ 1996 3 SA 262 A.

⁸⁸⁸ 1996 3 SA 262 A:271G-272A.

circumstances that will constitute *crimen iniuria*:

- a) Where a listening-in device is planted in the complainant's apartment without his knowledge or authorisation.⁸⁸⁹
- b) Where private detectives recorded private conversations of the complainant by means of a bugging device.⁸⁹⁰
- c) Where private documents are taken from a private safe and copied.⁸⁹¹ Such conduct, according to the court in *Reid-Daly v Hickman and Others*⁸⁹² could be equated with trespassing: "They are in no different category from a trespass upon the plaintiff's house in which damage is done, committed in order to examine the plaintiff's papers which it might be thought would assist in the inquiry."⁸⁹³
- d) Where someone without authorisation intercepts and reads another person's correspondence.⁸⁹⁴
- e) Where someone gains unauthorised access to another person's home, office, apartment or premise.⁸⁹⁵

In *Motor Industry Fund Administrators (Pty) Ltd & Another v Janit & Another*⁸⁹⁶ the court maintained that an "invasion of the right to privacy may take two forms: (i) the unlawful intrusion upon the privacy of another; and (ii) the unlawful publication of private facts about a person."⁸⁹⁷

Neethling *et al* state that "[a] violation of privacy by means of an act of intrusion takes

⁸⁸⁹ *Reid-Daly v Hickman and Others* 1981 2 SA 315 ZAD:323A-H; *S v A* 1971 2 SA 293 T:297C-D.

⁸⁹⁰ *S v A* 1971 2 SA 293 T:299C.

⁸⁹¹ *Reid-Daly v Hickman and Others* 1981 2 SA 315 ZAD:323D-H.

⁸⁹² 1981 2 SA 315 ZAD.

⁸⁹³ 1981 2 SA 315 ZAD:323F-G.

⁸⁹⁴ *S v Hammer & Others* 1994 2 SACR 496 C:497h-l & 500a-b. See also Snyman 1999:471.

⁸⁹⁵ *Reid-Daly v Hickman and Others* 1981 2 SA 315 ZAD; *R v S* 1955 3 SA 313 SWA:316A-B; *R v Schonken* 1928 AD 36:45; *Ho Si v Vernon* 1909 TS 1074:1080 & 1088; *De Foud v Town Council of Cape Town* 1898 SC 399:402.

⁸⁹⁶ 1994 3 SA 56 W.

⁸⁹⁷ 1994 3 SA 56 W:60H-l. See also *Janit & Another v Motor Industry Fund Administrators (Pty) Ltd & Another* 1995 4 SA 293 A:303G-H. Neethling *et al* 1996 maintain (at 243) that "privacy can be infringed only by acquaintance with personal facts by outsiders contrary to the determination and will of the person whose right is infringed, and such acquaintance can take place in two ways only, namely through intrusion (or acquaintance with private facts) and disclosure (or revelation of private facts)." Rautenbach 2001 also submits (at 119) that one's constitutional right to privacy, as enshrined in s 14 of the *Constitution*, protects "one's actions to control (i) access to personal matters ... and (ii) the obtaining, dissemination and use of information in respect of these matters."

place where an outsider himself acquires knowledge of private and personal facts relating to the plaintiff, contrary to the plaintiff's determination and wishes."⁸⁹⁸ This position exists, according to them, where either the private or personal facts are totally excluded from or limited to specific persons.⁸⁹⁹ They also maintain that where an employee discloses his employer's confidential information to third parties, without the employer's consent, he is guilty of an infringement of privacy.⁹⁰⁰

In *S v A*⁹⁰¹ the court noted that *crimen iniuria* "consists simply in the fact that there was a wrongful and intentional breach of the complainant's right to privacy."⁹⁰² In that particular case (where a listening-in device was secreted without authorisation) it was irrelevant, according to the court, "whether the complainant was overheard to say something shameful, something of which he could or would have been ashamed."⁹⁰³

Therefore, it may be concluded that the right to privacy protects an infringement of one's privacy sphere ("*privaatheidsfeer*").⁹⁰⁴ Put differently, it protects an individual's (or juristic person's) privacy domain.

3.9.1.2. Wrongfulness and seriousness

No South African court has yet stated that hacking into a computer constitutes an *iniuria* and thus *crimen iniuria*. Therefore we have to examine how the South African law assesses these aspects.

Hunt-Milton maintain that "[t]he concept both of what is an *injuria* and of what is a serious *injuria* 'depends to a great extent upon the modes of thought prevalent

⁸⁹⁸ Neethling *et al* 1996:244-245.

⁸⁹⁹ Neethling *et al* 1996:245, 247-248.

⁹⁰⁰ Neethling *et al* 1996:251, especially fn 90.

⁹⁰¹ 1971 2 SA 293 T.

⁹⁰² 1971 2 SA 293 T:298C-D.

⁹⁰³ 1971 2 SA 293 T: 298C-D.

⁹⁰⁴ Neethling 1971 states that "[d]ie privaetheid van 'n persoon omvat primêr sy persoonlikheidsgoed om in sy private lewe in 'n mate afgesonderd van die inmenging van buitelanders te leef." (at 326) [own translation: a person's privacy encompasses primarily the aspects of his personality to live his private life secluded from third party interference.] Snyman 1999 correctly submits (at 471) that an individual's right to privacy is infringed where "op 'n ongeoorloofde manier in 'n ander se private sfeer in te dring deur gebruikmaking van verkykers, kameras of meganiese afliesterapparate." [own translation: someone's privacy sphere is intruded upon in an unlawful way by utilising binoculars, cameras or mechanical eavesdropping apparatus.]

amongst any particular community or at any period of time, or upon those of different classes or grades of society, and the question must to a great extent therefore be left to the discretion of the court'.⁹⁰⁵ Stated differently, the *boni mores* (convictions of the community) serve as criterion.⁹⁰⁶

In the previous century local courts expanded the parameters of *crimen iniuria* to such an extent that "an exact precedent for what is today considered criminal *injuria* may be lacking in the old authorities."⁹⁰⁷ Furthermore, in determining whether particular conduct constitutes an *iniuria*, "the courts will have to give careful consideration to the provisions of the Constitution regarding the Bill of Rights."⁹⁰⁸ Section 14 of the *Constitution* provides explicitly for a right to privacy.

Numerous South African courts have stated that only serious *iniuria* constitute *crimen iniuria*.⁹⁰⁹ With regard to the criterion whether the conduct in question constitutes a serious *iniuria*, the courts have asked the following questions:

- (i) Whether the conduct is "likely to have results that may detrimentally affect the interests of the State or the community".⁹¹⁰
- (ii) Whether the *iniuria* is of such a reprehensible character that it should be punished in the interests of society.⁹¹¹
- (iii) Whether the conduct constitutes a real and substantial impairment of the complainant's *dignitas*.⁹¹² In the past, local courts treated the right to privacy as an aspect of *dignitas*.⁹¹³

⁹⁰⁵ Hunt-Milton 1990:529. See also *Rhodesian Printing & Publishing Co Ltd v Duggan and Another* 1975 1 SA 590 RA:594G-H; *S v A* 1971 2 SA 293 T:299A-B; *O'Keeffe v Argus P & P Co Ltd & Another* 1954 3 SA 244 C:248D-E; *R v Terblanche* 1933 OPD 65:69; Burchell & Milton 2000:514; Snyman 1999:472; LAWSA 1996:vol 6, par 280.

⁹⁰⁶ *Motor Industry Fund Administrators (Pty) Ltd & Another v Janit & Another* 1994 3 SA 56 W:60I-J; Neethling *et al* 1996:244; Hunt-Milton 1990:524.

⁹⁰⁷ Hunt-Milton 1990:524.

⁹⁰⁸ Neethling *et al* 1996:239.

⁹⁰⁹ *S v Jana* 1981 1 SA 671 T:676A; *S v A* 1971 2 SA 293 T:299A-B; *S v Momberg* 1970 2 SA 68 C; *R v Walton* 1958 3 SA 693 SR:694H-695A; *R v Olakawu* 1958 2 SA 357 C:359C; *R v Xabanisa* 1946 EDL 167:170; *R v Muller* 1938 OPD 141:142; *R v Terblanche* 1933 OPD 65; *R v Meer* 1923 OPD 77:80-81.

⁹¹⁰ *S v Momberg* 1970 2 SA 68 C:71H. See also *S v Jana* 1981 1 SA 671 T:676A

⁹¹¹ *R v Terblanche* 1933 OPD 65:71. In *S v A* 1971 2 SA 293 T the court maintained (at 299C-D) that the *boni mores* determine the reprehensibility of the conduct. See also LAWSA 1996:vol 6, par 280.

⁹¹² In *S v Bugwandeem* 1987 1 SA 787 N the court noted (at 796A-D) that "[t]he test requiring the *injuria* to be 'serious', in so far as it can be called a test at all, is so nebulous as to lead to arbitrariness in its application. While *injuriae* of a trivial nature should not engage the attention of the courts (they can be

Hunt-Milton contend that “new *mores* may lead the courts to regard as serious *injuriae* acts which in Roman-Dutch law were not regarded seriously.”⁹¹⁴ Put differently, “the court’s conception of contemporary *boni mores*” determines whether conduct constitutes a serious *iniuria*.⁹¹⁵ They further contend that “[t]he need to protect the community or sections of it from conduct of the kind which has occurred and the possible consequences of a failure to punish it criminally is often taken into account in determining whether X’s conduct” is serious enough to constitute *crimen iniuria*.⁹¹⁶

3.9.1.3. Intent

The intention must be *animus iniuriandi*.⁹¹⁷ The courts have ruled that *animus iniuriandi* is present where the invasion of privacy is secret and thus the complainant is unaware of this intrusion upon his privacy, provided the accused knows that he is infringing the complainant’s privacy (“if there is an intention to do the act”).⁹¹⁸ Furthermore, some courts have noted that such intent “may be gathered from the nature of the act which is done by the person accused of a *crimen iniuria* ... He must be taken to have intended the natural consequences of his act, and to have known that those consequences would follow.”⁹¹⁹

In *S v A*⁹²⁰ the court maintained, with regard to the question whether there existed proof that the accused had the intention to impair the privacy of the complainant, that

excluded on the principle *de minimis non curat lex*), any real and substantial impairment of a person’s *dignitas* should merit punishment, irrespective of whether it is of such a nature that it should be punished in the interests of the State ... In deciding whether the *injuria* in the circumstances of a particular case merits a conviction of *crimen iniuria*, the Court has to some extent to pass a value judgment in regard to the reprehensibility of the offending conduct, viewed in the light of the principles of morality and conduct generally accepted as the norm in society.” This view was endorsed in *S v Steenberg* 1999 1 SACR 594 N:596f-g.

⁹¹³ See Burchell & Milton 2000:510, fn 2; Neethling *et al* 1996:240. In *S v A* 1971 2 SA 293 T the court maintained (at 297D-H) that “an infringement of a person’s privacy *prima facie* constitutes an impairment of his *dignitas* ... the right to privacy is included in the concept of *dignitas*”.

⁹¹⁴ Hunt-Milton 1990:529.

⁹¹⁵ Hunt-Milton 1990:530. See also Burchell & Milton 2000:515.

⁹¹⁶ Hunt-Milton 1990:533.

⁹¹⁷ *R v Walton* 1958 3 SA 693 SR:697E-F; *R v Terblanche* 1933 OPD 65:67; *R v Holliday* 1927 CPD 395:402.

⁹¹⁸ *R v Holliday* 1927 CPD 395:402.

⁹¹⁹ *R v Terblanche* 1933 OPD 65:67-68.

⁹²⁰ 1971 2 SA 293 T.

intent in the form of *dolus eventualis* was present: "They must have foreseen the possibility that the complainant could or would be hurt and insulted by their conduct, but they acted in reckless disregard of his feelings."⁹²¹

3.9.2. Hacking and *crimen iniuria*

Before the question can be answered whether a successful hacking instance constitutes *crimen iniuria*, the question whether an individual's or juristic person's privacy encompasses electronic data or content stored on his/its computer, must first be dealt with.

As noted above, the law by means of *crimen iniuria* punishes the mere unauthorised intrusion upon an individual's privacy sphere.⁹²² Various kinds of private or business-related information can be located on any computer user's hard drive or company's computer system, such as business-related confidential information (e.g. client lists constituting trade secrets), personal or confidential e-mail messages and letters or unpublished articles (which the *Copyright Act* protects as immaterial property).

It is submitted that when local courts are afforded the opportunity, they will hold that all information or content stored on a computer (or any medium capable of storing electronic content) is protected by the right to privacy. The nature of the data or content stored on the computer should not determine whether the right to privacy protects it. As noted above, in *S v A*⁹²³ the court maintained that the mere intrusion of someone's privacy constitutes *crimen iniuria*, irrespective of the nature of the communications overheard (in that particular instance). Identical considerations should apply to electronic information or content stored on a computer.

Therefore it is submitted that where a *hacker* gains access to A's computer system and copies, deletes or modifies data, he commits *crimen iniuria*. It is further submitted that where a *hacker* merely gains access to a computer system, without deleting, copying or modifying data, he is also guilty of *crimen iniuria*. As the court observed in *R v Muller*.⁹²⁴ "In its application to facts [*crimen iniuria*] cannot be static in time or in relation

⁹²¹ 1971 2 SA 293 T:299F-G.

⁹²² *Snyman* 1999:471; *LAWSA* 1996:vol 6, par 279; *S v A* 1971 2 SA 293 T.

⁹²³ 1971 2 SA 293 T.

⁹²⁴ 1938 OPD 141.

to persons.”⁹²⁵ Furthermore, such content is protected by the *Constitution* which enshrines every individual’s and juristic person’s right to privacy. It is submitted that electronic content stored on a computer is protected by a “veil of privacy”.

Furthermore, such invasion into a computer user’s privacy is serious in that it is against the convictions of the community that Internet users should gain unauthorised access to other computer systems and therefore, it is submitted, of such a reprehensible character that it should be punished. Hacking instances are to the detriment of the state as well as the community, as is evident from chapter three. Similar considerations apply where employees gain unauthorised access to restricted electronic data stored on their employers’ computers.

In all these instances, *dolus eventualis* is present. Similar to what the court stated in *S v A*,⁹²⁶ the *hackers* must have foreseen the possibility that the complainants could or would regard such instances as an invasion of their privacy, but they, the *hackers*, acted in reckless disregard of that privacy.

Therefore, this study is not proposing an extension of legal principles but is advocating that vested principles are applied to new types of conduct, that occur due to new technology. The courts will merely have to apply two privacy rights to these new scenarios, namely the right to “not to have your documents subjected to an unlawful search” as well as the right to privacy to one’s home and office.

3.9.3. Eavesdropping by means of the Internet and *crimen iniuria*

It is abundantly clear, from the general principles discussed above⁹²⁷ as well as the conclusions reached in the previous paragraph, that where a *hacker* installs a Trojan horse on A’s computer, either to gain access to data or to engage in espionage, he infringes A’s right to privacy and, as stipulated above,⁹²⁸ this constitutes a serious *iniuria*.

In *S v A*⁹²⁹ the court maintained that “[t]he placing of the transmitting device in the complainant’s room and the listening-in to his private conversations undoubtedly

⁹²⁵ 1938 OPD 141:143.

⁹²⁶ 1971 2 SA 293 T.

⁹²⁷ See par 3.9.1 of this chapter.

⁹²⁸ See par 3.9.2 of this chapter.

⁹²⁹ 1971 2 SA 293 T.

constituted *wrongful acts*.⁹³⁰ (own emphasis). It therefore appears from this *dictum* that the court considered both the planting of the device and the listening to the private conversations to constitute separate wrongful acts.⁹³¹

Hence, where an Internet user installs *via* the Internet a computer program⁹³² on A's computer to engage in espionage⁹³³ and he subsequently uses this computer program to do his bidding (which includes instances where the program e-mails this information to its creator), he is guilty of two separate wrongful acts.

Similar considerations apply to instances where a *hacker* intercepts or eavesdrops on electronic conversations. This amounts to a wrongful, intentional and serious infringement of the complainant's common law as well as constitutional right to privacy and specifically his right to privacy of private communications. This constitutes an invasion of his private domain. In *Sage Holdings Ltd & Another v Financial Mail (Pty) Ltd & Others*⁹³⁴ the court held that:

"To my mind it is clear that the ordinary conduct of business postulates the need that, included in the right to conduct business without unlawful interference, is the right of a company that its internal communications will not be eavesdropped upon, nor recorded, nor intercepted. In exercising the right to trade and carry on a lawful business, a company or other juristic person would be entitled to regard the confidential oral or written communications of its directors and employees as sacrosanct and would in appropriate circumstances be entitled to enforce the confidentiality of the aforesaid oral and written communications. To my mind, such right would in appropriate circumstances be enforceable against whosoever is in possession thereof and whosoever seeks to utilise it. The fact that the person who is in possession thereof was not party to the unlawful conduct in obtaining it does not exclude the right which the applicants would have."⁹³⁵

When the matter went on appeal, the Supreme Court of Appeal noted that the "telephone-tapping which occurred was manifestly an unlawful invasion of the privacy of Sage and its corporate executives".⁹³⁶

⁹³⁰ 1971 2 SA 293 T:299E.

⁹³¹ This submission is confirmed by *Reid-Daly v Hickman and Others* 1981 2 SA 315 ZAD:323B.

⁹³² E.g. by sending the computer program as an e-mail attachment to A.

⁹³³ By searching for specific information such as passwords.

⁹³⁴ 1991 2 SA 117 W.

⁹³⁵ 1991 2 SA 117 W:132H-133A.

⁹³⁶ *Financial Mail (Pty) Ltd & Others v Sage Holdings Ltd & Another* 1993 2 SA 451 A:463B-C.

Hence it is abundantly clear that where a *hacker* eavesdrops on electronic communications, either by intercepting communications⁹³⁷ or by installing computer programs that engage in electronic espionage on his behalf, he is guilty of an infringement of the complainant's right to privacy and such conduct constitutes *crimen iniuria*.

3.9.4. Obtaining information from a hacker

Where a *hacker* copies data or content, without authorisation, stored on X's computer and divulges a copy of this information or content to a third party, the latter knowing that such information was unlawfully obtained by the *hacker* from X, the third party is also guilty of an infringement of X's right to privacy. In *Janit & Another v Motor Industry Fund Administrators (Pty) Ltd & Another*⁹³⁸ the Supreme Court of Appeal held that:

"When Murray stole the tape recordings of respondents' board meetings and offered them to Janit, he readily helped himself to the information they contained, despite the fact that he knew that the tapes had been unlawfully obtained and that they contained the private and confidential discussions of respondents' directors. In so doing he violated and infringed their legal right to privacy."⁹³⁹

3.9.5. Disseminating unlawfully obtained private information

Where a *hacker* or a third party divulges private information (i.e. any information or content stored on A's computer system that is not available to other Internet users), for instance by posting the information or content onto a web site where all computer users can see or download it, the *hacker* or third party is guilty of a separate act of *crimen iniuria*, in addition to the unlawful procurement of such information:

"There can be no doubt that if a person acquires knowledge of private facts through a wrongful act of intrusion, any disclosure of those facts by such a person, or by any other person, in principle constitutes an infringement of the right to privacy."⁹⁴⁰

However, Neethling *et al* contend that these instances only constitute *crimen iniuria*

⁹³⁷ For instance by means of DNS spoofing: see par 3 of chapter 5.

⁹³⁸ 1995 4 SA 293 A.

⁹³⁹ 1995 4 SA 293 A:305C

⁹⁴⁰ Neethling *et al* 1996:248. See also p 255 & 260; *Janit and Another v Motor Industry Fund Administrators (Pty) Ltd and Another* 1995 4 SA 293 A:303F-G & 303H-I.

where the "plaintiff is identified with the disclosed facts."⁹⁴¹

3.9.6. Attempted hacking and attempted *crimen iniuria*

The next question to be addressed is whether an attempt to gain access to a computer, without authorisation, constitutes attempted *crimen iniuria*.

The offence of attempted *crimen iniuria* obtains in the South African criminal law. In *R v R*⁹⁴² the accused tried to peep at the complainant while she was undressing, but failed because her curtains were drawn and her room was dark. The court found him guilty of attempted *crimen iniuria* and held further that -

"in general, a stranger who designedly stations himself close to the window of a dwelling-house, and from that position attempts to see or peep into the room from outside even if he does not know whether the window is that of a bedroom or of some other room in the house, runs the risk of committing the *offence of criminal injuria* if by such conduct he in fact infringes the rights of privacy ... of those within the room."⁹⁴³
(own emphasis)

Bearing this judgment in mind, it is submitted that where a *hacker* attempts to gain access to a computer system but fails to, he is guilty of attempted *crimen iniuria*. It is of no avail to him to allege that he had no prospect of obtaining access to the computer system. He clearly did everything he could do to gain access to the computer system. His attempt thus constitutes a completed attempt.

3.9.7. Insertion of a computer program

The question that is addressed under this heading is whether the insertion of a malicious computer program, by a *hacker* or by means of another computer program, that will either interfere with the operation of a computer or enable the computer programmer to engage in electronic espionage, constitutes *crimen iniuria*?

As noted above,⁹⁴⁴ when a *hacker* gains access to a computer system he infringes the computer owner's right to privacy and is consequently guilty of *crimen iniuria*.

⁹⁴¹ Neethling *et al* 1996:248.

⁹⁴² 1954 2 SA 134 N.

⁹⁴³ 1954 2 SA 134 N:135G-H.

⁹⁴⁴ In par 3.9.2 of this chapter.

Therefore when a *hacker* gains access and he inserts a malicious computer program (such as a virus, a Trojan horse or a password sniffer) he is guilty of *crimen iniuria*. The fact that he inserted a computer program will, it is submitted, be seen as aggravating circumstances.

However, a more difficult scenario arises where a worm or a virus is contracted, for instance by means of an infected e-mail attachment, and it installs another program such as a password sniffer, Trojan Horse or a virus. Is the computer programmer guilty of *crimen iniuria*?

It is submitted that where a computer program installs a Trojan horse (that embarks on espionage) or a password sniffer, such conduct constitutes an infringement of privacy in that it is tantamount to installing a bugging device or a camera in an office. The courts will regard the first computer program as a mere instrument in the hands of the computer programmer and therefore it is submitted that the programmer is guilty of *crimen iniuria*.

Where the first computer program installs a virus or any computer program that will delete or modify electronic files or interfere with the operation of a computer or a computer program and such virus or program is discovered before it can cause any damage, such conduct constitutes attempted malicious injury to property.⁹⁴⁵ This can be equated with the scenario where something throws a bomb, through an open window, into an office or an apartment. It was set to explode the 20th of August but is discovered prior to that date.

It is submitted that such conduct does not constitute *crimen iniuria* in that the computer programmer did not acquire any personal facts or knowledge nor does the second malicious program have the capabilities to acquire such facts or knowledge.

3.10. Inchoate crimes

Next, the application of two inchoate crimes namely complicity ("*medepligtigheid*") and incitement are discussed in the context of computer-related crimes.

The first question that is addressed is whether trafficking in passwords constitutes an offence in terms of our common law. Trafficking in passwords can be defined as

⁹⁴⁵ See par 3.6.8.1 of this chapter.

trading in or distributing illegally obtained passwords. Some *hackers* penetrate computer systems in order to obtain passwords that allow access to either other computers or to critical business information. For the purposes of this study, trafficking in illegally obtained private keys, used for encryption or decryption, is equated with the trafficking in illegally obtained passwords.

These *hackers* subsequently either -

- ⇒ sell these illegally obtained passwords, or
- ⇒ provide it to other *hackers* (for instance by e-mailing the passwords to them); or
- ⇒ make it available for distribution by posting these passwords on their own or so-called *hacker heaven* web sites.⁹⁴⁶

Such conduct can be equated with the following scenario: X steals or duplicates Y's key which allows Y access to his office. X then sells or distributes this key, or the duplicate, to A. The question of law is whether the selling, trading or distribution of the key constitutes an offence?

The second scenario that this paragraph deals with is the following: Some computer users create password sniffers that *hackers* use to obtain illegal access to any computer. The password sniffer attempts to discover the relevant password that allows access to the computer system. Furthermore, some computer users create hackers' tools that less experienced computer users (called *script kiddies*) utilise to either obtain illegal access to any computer or to interfere with the functioning of a computer by, for instance, launching a denial-of-service attack or an e-mail bomb attack.

The question of law is twofold: a) does the creation of such sniffers or hackers' tools constitute an offence in terms of our common law and b) does the distribution, for instance by making these sniffers or tools available for downloading on a web site, constitute an offence?

It is submitted that none of the above-mentioned acts constitutes a completed offence in terms of our common law. However, the question arises whether the distribution of hackers' tools, password sniffers or illegally obtained passwords constitutes an inchoate crime, such as complicity or incitement.

⁹⁴⁶ www.2600.com is an example of a *hacker* web site.

3.10.1. Accomplice

Under this heading the general principles of complicity ("*medepligtigheid*"), as a common law offence, are discussed. Thereafter it is determined whether specific forms of cyber-abuse, as outlined in paragraph 3.10, constitute complicity.

3.10.1.1. General principles

South African courts have maintained that before A can be found guilty as an accomplice, five requirements have to be met:⁹⁴⁷ (a) a third party must have committed the crime;⁹⁴⁸ (b) A must have facilitated (e.g. aided or assisted) the third party by means of his conduct, which can be the furnishing of advice or helping the third party to commit the crime or by giving the latter the opportunity, information or means to facilitate the commission of the crime;⁹⁴⁹ (c) A's facilitating conduct must be unlawful; (d) A must intentionally facilitate the third party and must know that his assistance is unlawful⁹⁵⁰ – *dolus eventualis* suffices;⁹⁵¹ and (e) there must be a causal connection between the A's assistance and the commission of the crime by the third party.⁹⁵²

⁹⁴⁷ Snyman 1999:271-274.

⁹⁴⁸ *S v Williams en 'n Ander* 1980 1 SA 60 A:63A.

⁹⁴⁹ In *S v Williams en 'n Ander* 1980 1 SA 60 A the Supreme Court of Appeal noted (at 63B-C) that: "n Medepligtige vereenselwig hom bewustelik met die pleging van die misdaad deur die dader of mededaders deurdat hy bewustelik behulpsaam is by die pleging van die misdaad of deurdat hy bewustelik die dader of mededaders die geleentheid, die middele of die inligting verskaf wat die pleging van die misdaad bevorder." [own translation: An accomplice knowingly identifies him with the commission of the offence, by the perpetrator or co-perpetrators, by intentionally assisting the commission of the offence or by intentionally providing the perpetrator or co-perpetrators with the opportunity, means or information and thereby facilitating the commission of the offence.] See also *S v Maxaba en 'n Ander* 1981 1 SA 1148 A:1156H. In *R v Jackelson* 1920 AD 486 the Supreme Court of Appeal noted (at 491): "But if a person assists in or facilitates the commission of a crime ... if he gives counsel or encouragement, or if he affords the means for facilitating the commission, if in short there is any co-operation between him and the criminal, then he 'aids' the latter to commit the crime." In *R v Peerkan & Lalloo* 1906 TS 798 the court maintained (at 804) that "[e]verybody who, in the opinion of the judge, does something to further the purpose of a criminal is a person who assists or helps at the crime."

⁹⁵⁰ *S v Williams en 'n Ander* 1980 1 SA 60 A. Some courts have stated that the alleged accomplice must "have had actual or constructive knowledge of 'all the essential or material facts which constitute the offence'." See *S v Tshwape & Another* 1964 4 SA 327 C:331H. In *R v Essop* 1918 TPD 275 the court noted (at 276) that "a person is only an aider and abettor in the sense of being criminally liable if he had knowledge that an offence was being committed or about to be committed." See also *Tommy & Others v R* 1931 NPD 317:323. In *S v Mahlangu & Andere* 1995 2 SACR 425 T the court held (at 436b-c) that an accused must intentionally identify him with the perpetrators. See also Burchell & Milton 2000:413.

Furthermore, mutual co-operation between the perpetrator and the accomplice is not required⁹⁵³ and neither does the law require that the accomplice and the perpetrator must be *ad idem*.⁹⁵⁴ Where the third party is unsuccessful in committing the intended crime and therefore guilty of an attempt to commit a crime, the accused (A) is guilty as an accomplice to this incomplete crime.⁹⁵⁵

Note should be taken of the fact that the law does not require that the perpetrator must be charged or convicted before someone can be held liable as an accomplice.⁹⁵⁶

⁹⁵¹ See Burchell & Milton 2000:413.

⁹⁵² In *S v Williams en 'n Ander* 1980 1 SA 60 A the Supreme Court of Appeal noted (at 63F) that "[v]olgens algemene beginsels moet daar 'n kousale verband tussen die medepligtige se hulpverlening en die pleging van die misdaad deur die dader of mededaders bestaan." [own translation: According to the general principles, a causal connection must exist between the accomplice's assistance and the commission of the offence by the perpetrator or co-perpetrators.] In *S v Khoza* 1982 3 SA 1019 A Justice Botha, in his minority judgment, stated (at 1054H) that "the Court in *Williams*' case could not have been postulating a causal connection between the conduct of the accomplice and the death of the deceased. What was stated to be required was a causal connection between the conduct of the accomplice and *the commission of the offence* by the perpetrator(s) ("die pleging van die misdaad deur die dader of mededaders"), which connotes no more than a causal connection between the conduct of the accomplice and the conduct of the perpetrator or co-perpetrators."

⁹⁵³ Snyman 1999:273.

⁹⁵⁴ In *S v Ohlenschlager* 1992 1 SACR 695 T the court maintained (at 768g) that "[o]oreenstemming tussen die hoofdader en die medepligtige ... is egter nie 'n vereiste van aanspreeklikheid as medepligtige nie." [own translation: Agreement between the principal and the accomplice is not set as a requirement for holding the accomplice liable.]

⁹⁵⁵ *R v Dettbarn* 1930 OPD 188:191: "for I understand the law to be that a person can only be convicted on the ground of aiding and abetting in the commission of an offence if the offence is actually committed, whether it be a completed offence, or an attempt which is in itself an offence ... a person can only be convicted on the ground of aiding and abetting if it is proved that an offence has been committed by someone". See also *De Wet en Swanepoel* 1985:199. Burchell & Milton 2000 takes this line of argument one step further and state (at 412) that "[i]f a person tries unsuccessfully to further or assist another in the perpetration of a crime ... then at most that person can be convicted of attempted complicity."

⁹⁵⁶ *S v Lamont* 1977 2 SA 679 RAD:683G-H; *Alper & Alper v R* 1931 NPD 431:436 & 442; LAWSA 1996:vol 6, par 131. In *R v Mlooi & Others* 1924 AD 131 the Supreme Court of Appeal stated (at 135) that the liability of an accomplice does not depend upon the liability of the principal offender. Snyman 1999 states (at 271) that "[d]ie dader hoef egter nie verhoor en skuldig bevind te wees nie. Dit hoef slegs vas te staan dat iemand anders as dader die misdaad gepleeg het, al kan die polisie hom nie vang nie, of al het hy intussen geestesongesteld geword, of al het hy 'n staatsgetuie geword." [own translation: the law does not require that the perpetrator must be tied and convicted. The sole requirement is that someone else must have committed the offence, as a perpetrator, even if the police

However, where the alleged perpetrator did not commit an offence or where he is acquitted of the alleged offence or where the prosecution cannot prove the commission of the alleged offence, any assistance by the accused (alleged accomplice) to the alleged perpetrator does not constitute an offence.⁹⁵⁷

Our common law authorities state that "a person who lends any aid whatsoever to a criminal is himself a criminal ... not only that lending aid consists in being actively helpful to the criminal, as, for instance, where a person holds down the man who is being murdered, but that anybody who lends assistance indirectly towards the commission of the crime is also to be regarded as assisting at the crime, as, for example, where a person sells poison, knowing that the poison will be used for a criminal purpose, or who gives another a weapon with which to commit a crime".⁹⁵⁸ Likewise, in *R v Jackelson*⁹⁵⁹ the Supreme Court of Appeal noted that "[t]here is ample authority in our writers on crimes for the proposition that the person who lends, say, a knife knowing the purpose for which it is to be used is criminally liable".⁹⁶⁰ The following passage of the Supreme Court of Appeal in *R v Longone*,⁹⁶¹ dealing with the *actus reus* as well as *dolus eventualis*, deserves full quotation. The court maintained that -

"there is ample authority in Roman-Dutch writers for the proposition that he who supplies another with poison or an instrument with which a murder is committed is himself guilty of the crime of murder *provided he had knowledge of the murderer's purpose* ... therefore ... when accused gave the poison to [the perpetrator] knowing that [the latter] intended to poison his wife, he committed an unlawful act and is criminally responsible for the direct consequences of such act and within limits for the indirect consequences. The difficulty which arises is that of determining such limits. If the [perpetrator] had succeeded in poisoning his wife accused would have been guilty of

is incapable of finding him, or even if he had become mentally deranged, or even if he had turned a state witness.] See also Burchell & Milton 2000:413; De Wet en Swanepoel 1985:198.

⁹⁵⁷ See *S v Gordon* 1962 4 SA 727 N:729H; *R v Sejosengoe* 1935 EDL 474:481; *Steward v R* 1934 NPD 340:344; *R x Rasool* 1924 AD 44:47 & 48; *R v Van Rooy & Another* 1920 CPD 695:696. See also Burchell & Milton 2000:408; LAWSA 1996:vol 6, par 131; De Wet en Swanepoel 1985:198.

⁹⁵⁸ *R v Peerkan & Lalloo* 1906 TS 798:804.

⁹⁵⁹ 1920 AD 486.

⁹⁶⁰ 1920 AD 486:490.

⁹⁶¹ 1938 AD 532. The facts were that A (the perpetrator) informed the accused that he wanted to kill his wife and the accused gave A poison to kill his wife. A put the poison in water which B drank and succumbed. A did not foresee, nor intent, that B would drink the water. The question of law was whether the accused could be liable for B's death as an accomplice.

murder. Equally clearly if [the perpetrator] had changed his mind and deliberately poisoned a third party, then accused would not have been guilty of the murder of such third party. What is the reason for the distinction? It seems to lie in the accused's state of mind relative to the act done by [the perpetrator]. In the one case he knew what [the perpetrator] proposed to do and assented to it; he foresaw what was likely to happen and it did happen. In the other case he did not know and could not foresee what would happen ... Here [the perpetrator], in attempting to poison his wife, took certain steps which resulted in the poisoning of [B], but the exact nature of the steps he took were not planned by or known to the accused beforehand. These steps, therefore, were not assented to or authorised by him. But it does not follow that accused escapes criminal responsibility for any act done by [the perpetrator] not expressly assented to or authorised by him. He is also responsible for such steps as in the circumstances he should reasonably have contemplated or foreseen as likely to be taken by [the perpetrator]. For example, if [the perpetrator] had poisoned his wife's food and if it was customary for [the perpetrator's] wife to share her food with her child, and accused knew this and knew that [the perpetrator] probably intended to poison the food, then accused would have been criminally responsible for the death of the child if the child was poisoned. On the other hand, if [the perpetrator] in order to poison his wife, had, unknown to the accused, poisoned the drinking water of the whole community and a large number of people had been poisoned, including [the perpetrator's] wife, then accused would have been guilty of the murder of the wife but not of the murder of the others. Applying these principles, it is clear that [the perpetrator's] action which resulted in the death of [B] was not assented to or authorised by the accused, and his guilt depends upon whether he should have foreseen that, [the perpetrator] was likely to do what he did. Now it was always possible that [the perpetrator] in carrying out his purpose would by mistake or accident or design kill someone other than his wife, but the test is not possibility but reasonable probability which should have been foreseen."⁹⁶² (own emphasis)

Finally, it should be mentioned that an accomplice is liable as if he himself committed the crime.⁹⁶³

⁹⁶² 1938 AD 532:537-539.

⁹⁶³ *R v Jackelson* 1920 AD 486:490; *R v Peerkan & Laloo* 1906 TS 798:802. In *R v Mlooi & Others* 1924 AD 131 the Supreme Court of Appeal explained (at 134) the liability of an accomplice as follows: "The actual perpetrator of a crime is not necessarily the only person liable to punishment. Anyone who procures or assists the commission of the offence ... is also liable to penal sanctions ... The position of a man who associates himself with the crime beforehand is well settled. Whoever instigates, procures or assists the commission of the deed is a *socius criminis*, and may be indicted, convicted and punished as if he were the principal offender."

3.10.1.2. Making passwords, password sniffers and hackers' tools available

Three possible scenarios, relevant to this study, arise:

- a) A makes a password available on the Internet or by means of the Internet and states that this password allows access to, for example, Microsoft's computer system. B obtains this password from A and uses it to gain access to Microsoft's computer system.
- b) A makes a password sniffer⁹⁶⁴ available on the Internet or by means of the Internet. He may, for example, state that this sniffer can be used against any Windows operating system. B obtains this sniffer from A and employs it to gain access to C's computer system.
- c) A makes a hackers' tool available on the Internet or by means of the Internet and states or claims that this program can be used to interfere with the operation of any computer system. B obtains this tool from A and uses it to launch a denial-of-service attack against C's computer system.

It is submitted that in all these instances A is guilty as an accomplice to an offence committed by B, where he employed the password, hackers' tool or password sniffer. All five elements posed for the liability of an accomplice are present:

(1) B committed an offence. Where B used the illegally obtained password or the password sniffer to gain access to a third party's computer system, he is guilty of fraud and *crimen iniuria*. Where B copied, mentally or by means of his computer, private information located on the third party's computer system, he is also guilty of theft. Where B, after he gained access to the third party's computer system, deleted or corrupted information, he is guilty of malicious injury to property. Where B used the hackers' tool to interfere with the functioning of a third party's computer system, he is guilty of malicious injury to property.

(2) A facilitated/aided B in the commission of the offences mentioned in (1). A's conduct is synonymous with the scenario where X provides Y with a weapon to kill or injure Z. In the postulated scenario, A furnishes a weapon to B to either gain access to a third party's computer system or to interfere with the operation of the latter's computer system. Identical considerations apply to the scenario where A provides B

⁹⁶⁴ As an example of a hackers' tool.

with advice on how to gain unlawful access to C's computer system. In all these instances, it is submitted, A indirectly facilitated the crime committed by B by making the password, password sniffer or hackers' tool available.

(3) A intentionally facilitated/aided B in committing the offences indicated in (1). Where A states that the password in question allows access to e.g. Microsoft's computer system, A definitely has the intent (*dolus directus*) to facilitate B in gaining access to Microsoft's computer system. It is submitted that where A renders a hackers' tool available, stipulating that it can be employed to gain access to any computer system or to interfere with the functioning of any computer system, A knows and/or foresees the possibility that if any Internet user (B) downloads the tool, he downloads it with the purpose of either gaining access to or interfering with the functioning of a computer system, and if B subsequently employs it against a third party's computer system, B will commit an offence, be it fraud, theft, *crimen iniuria* or malicious injury to property. Therefore either *dolus directus* or *dolus eventualis* is present.

(4) A's facilitation is unlawful. It is submitted that it is against the *boni mores* to help, aid or assist another to gain access to a third party's computer or to interfere with the functioning of a computer system.

(5) A causal connection exists between A's making available of the password, password sniffer or the hackers' tool and the commission of the offence by B. B used A's program or password to gain access to, or to interfere with, a third party's computer system.

It is submitted that A will be liable, as an accomplice, not only for B's unlawful gaining access to a third party's computer (which therefore entails that B is guilty of fraud) but also for other foreseen acts done by B, after he gained access to the latter's computer system (thus entailing that B may be guilty of *crimen iniuria*, theft and/or malicious injury to property). In *R v Barry*⁹⁶⁵ the accused incited two individuals to steal tyres. The latter stole two cars and subsequently abandoned the cars, after they had removed the tyres. The accused contended that he could only be held liable as an accomplice with regard to the theft of the tyres and not the cars. The court rejected this argument, stating that:

"On the facts of this case it is obvious that the appellant must have known that when he instigated [the accused] to steal tyres and tubes from motor cars, one way, if not the

only way, of doing so would be for them to take the cars in circumstances amounting to theft, and then to remove the tyres and tubes ... it is clear to my mind that as the instigator the appellant must have foreseen that one of the natural results of his instigation would be that the thieves would have to steal the cars before they could remove the tyres and tubes."⁹⁶⁶

Furthermore, many South African courts have held that where the accused made his premises available for the purpose of crime, he was guilty as an accomplice.⁹⁶⁷ On the same basis it may be contended that where A makes his hackers' tools available for download, knowing and/or foreseeing the possibility that it can be used for illegal purposes, he is guilty as an accomplice, where the person who downloaded the hackers' tool used it to commit an offence.

Finally, two further aspects must be highlighted:

- If B copies the password, password sniffer or hackers' tool and does not attempt to gain access to, or interfere with the operation of, a third party's computer, then A cannot be held liable as an accomplice.
- If B employs the program or password, obtained from A, and he fails to gain access to, or interfere with the functioning of, a third party's computer system, because the hackers' tool or password sniffer is defective or because it is the incorrect password,⁹⁶⁸ B is guilty of attempted fraud or attempted malicious injury to property. Therefore, it is submitted that A is an accomplice to B's attempted fraud or attempted malicious injury to property: A attempted to facilitate B in gaining access

⁹⁶⁵ 1932 TPD 312.

⁹⁶⁶ 1932 TPD 312:315. However, in *R v Toni* 1949 1 SA 109 A the Supreme Court of Appeal stated (at 114-115) that: "It is, at any rate, open to doubt whether the maker of a burglarious implement who delivers it to a housebreaker for the purposes of his nefarious profession becomes a party to every housebreaking in which the implement is subsequently used ... it may well be that the provider of the implement would not be criminally responsible as a party to housebreakings effected by means of the implement, except those of which he knew, or perhaps ought to have known, as specifically in the contemplation of the burglar when he gave it to him; and if this is so the same might apply to the forger who delivers the dangerous product of his crime in order that it may be used at large by the recipient." Burchell & Hunt 1970, however, state that, on the basis of the *Toni* judgment, "it is not inconceivable that X who supplies Y with a jemmy could be liable for all the housebreakings Y commits with it". (At 361, fn 106).

⁹⁶⁷ See *S v Levy & Another* 1967 1 SA 351 W:356C-D; *R v Scholtz* 1942 CPD 118:121-123; *R v Wiese & Another* 1928 TPD 149:154.

⁹⁶⁸ E.g. Microsoft, in the postulated example, could since have changed its password access.

to, or interfering with, the computer system of a third party.

3.10.2. Incitement

Under this heading the general principles of the offence of incitement are first discussed. Thereafter it is determined whether specific cyber-conduct constitutes incitement.

3.10.2.1. General principles

Incitement is both a common law⁹⁶⁹ as well as a statutory offence. Section 18(2)(b) of the *Riotous Assemblies Act*⁹⁷⁰ criminalises incitement by providing that -

“[a]ny person who ... incites, instigates, commands, or procures any other person to commit, any offence, whether at common law or against a statute or statutory regulation, shall be guilty of an offence and liable on conviction to the punishment to which a person convicted of actually committing that offence would be liable.”

The Act fails to explain the meaning of the word incite.

Incitement, as a common law or a statutory offence, is committed where A intentionally incites another person or persons to commit a crime.⁹⁷¹ Therefore three elements must be present before A's conduct can constitute incitement: He must (a) intentionally,⁹⁷² (b) attempt to move/induce B, either by means of words or conduct,⁹⁷³ to (c) do

⁹⁶⁹ LAWSA 1996:vol 6, par 152. In the following cases, the courts recognised incitement as a common law offence: *R v Wolff* 1930 TPD 821:824; *R v Fortuin* 1915 CPD 757:758 & 759; *R v Ungwaja* 1891 12 NLR 284:286; *R v Nihovo* 1921 AD 485:493: “In my opinion we should definitely lay down that it is an offence to incite a person to commit a crime even though nothing has been done by him in furtherance of its commission.” See also p 503. In *R v Silburn & Shearing* 1903 24 NLR 527 the court held (at 529) that “*soliciting or inciting* to the commission of crime is an indictable offence under our law.” (own emphasis).

⁹⁷⁰ Act 17/1956.

⁹⁷¹ Snyman 1999:298.

⁹⁷² *Dolus eventualis* suffices. See Burchell & Milton 2000:448. At p 448-449 the authors maintain that “it must be shown that the accused must have foreseen, and hence by inference did foresee, at least the possibility that his communication would influence the incitee's mind and result in his doing an act which amounted to a crime.”

⁹⁷³ *S v Nathie* 1964 3 SA 588 A:595A; *R v Palane*; *R v Frans* 1947 3 SA 270 T:271: “to commit the crime the inciter must ... do or say something in furtherance of [his] criminal intent.” See also Burchell & Milton 2000:446.

something which A knows, or reasonably foresees,⁹⁷⁴ is a crime.⁹⁷⁵

The law does not require that the incitee must respond to, or act upon, the incitement, before liability can follow.⁹⁷⁶ All that is required, for a completed incitement, is that the communication, constituting the alleged incitement, must have reached the incitee.⁹⁷⁷

The question of law that arises is what type of conduct is, as a minimum, required to constitute the offence of incitement. In *R v Zeelie*⁹⁷⁸ the Supreme Court of Appeal enunciated that the purpose of section 15(2)(b), the precursor of section 18(2)(b), was: "Wat die Wetgewer klaarblyklik in gedagte gehad het was dit: die gemenerereg sowel as die wetterereg bedreig sekere misdrywe met straf. Die dader self word dus ontmoedig deur daardie strafaandreiging. Dikwels word persone - ewentuele daders of andersins - deur ander aangehits, aangepor of opgerui om misdrywe te begaan. Tot ontmoediging van sulke aanhitters en ter beskerming van moontlike daders word die inwerking op die gees van die moontlike dader met daardie oogmerk self met straf bedreig."⁹⁷⁹ Keeping this passage in mind, the Supreme Court of Appeal maintained in *S v Nkosiyana & Another*⁹⁸⁰ that -

⁹⁷⁴ Burchell & Milton 2000:451.

⁹⁷⁵ In *R v J* 1958 4 SA 488 A the Supreme Court of Appeal stated (at 493A-B), with regard to the question whether the accused solicited the complainant and the allegation that the complainant did not understand the words used by the accused, that "[t]he law is concerned with what the appellant did and if, as appears to have been the position, he was making a serious proposal which so far as he knew would be understood by [the complainant] the crime was committed". The court found the accused guilty of incitement regardless of the fact that the complainant, due to her age, did not understand the accused. Burchell & Hunt 1970 state (at 399) that "[o]n principle, since the liability of the inciter and not that of the incitee is in question, the presence or absence of *mens rea* on the latter's part is immaterial, the state of mind of the inciter alone being relevant." For a contrary view, see *R v Milne & Another* 1951 1 SA 791 A:821H-822D.

⁹⁷⁶ LAWSA 1996:vol 6, par 152. In *R v Wolff* 1930 TPD 821 the court maintained (at 826) that "[i]f the person does nothing to further the commission of the crime, the inciter is non the less guilty, provided the crime solicited is one that is capable of being committed."

⁹⁷⁷ LAWSA 1996:vol 6, par 153.

⁹⁷⁸ 1952 1 SA 400 A.

⁹⁷⁹ 1952 1 SA 400 A:405C-D. [own translation: What the legislature apparently had in mind was the following: the common law as well as statutory law penalise certain offences. The perpetrator is, therefore, discouraged by these penalties. Often persons – eventually perpetrators or otherwise – are incited, solicited or instigated by third parties to commit offences. For the purpose of discouraging these inciters as well as to protect potential perpetrators, the law punishes the influencing of the mind of a potential perpetrator.]

⁹⁸⁰ 1966 4 SA 655 A.

"in criminal law, an inciter is one who reaches and seeks to influence the mind of another to the commission of a crime. The machinations of criminal ingenuity being legion, the approach to the other's mind may take various forms, such as suggestion, proposal, request, exhortation, gesture, argument, persuasion, inducement, goading, or the arousal of cupidity. The list is not exhaustive. The means employed are of secondary importance; *the decisive question in each case is whether the accused reached and sought to influence the mind of the other person towards the commission of a crime ... it is the conduct and intention of the inciter which is vitally in issue; and I reiterate that the purpose of making incitement a punishable offence is to discourage persons from seeking to influence the minds of others towards the commission of crimes.* Hence, depending on the circumstances, there may be an incitement irrespective of the responsiveness, real or feigned, or the unresponsiveness, of the person sought to be so influenced."⁹⁸¹ (own emphasis)

The court further stated that the act of inciting did not require any form of persuasion or urging.⁹⁸²

Other courts have stated that the accused's conduct or words must be examined in their proper context to determine whether the accused intended to incite someone.⁹⁸³

The test to determine whether the accused unlawfully incited someone to commit a crime has been held to be "whether the reasonable man would hold that the [accused's conduct] in the circumstances is an incitement to [commit a crime]."⁹⁸⁴

Finally, it should be borne in mind that local courts hold the view that where the incitement was successful, the inciter should not be charged with incitement but should be charged for his contribution to the offence which he has incited either as a perpetrator or an accomplice.⁹⁸⁵

⁹⁸¹ 1966 4 SA 655 A:658H-659B.

⁹⁸² 1966 4 SA 655 A:658D-H.

⁹⁸³ *S v Nathie* 1964 3 SA 588 A:595A.

⁹⁸⁴ *R v Maxaulana* 1953 2 SA 252 E:253E-F.

⁹⁸⁵ In *R v Milne & Another* 1951 1 SA 791 A the Supreme Court of Appeal enunciated (at 823G-H) that "[t]he construction of [s 18(2)(b)] is irrelevant in cases where the incitee does the act which he was incited to do, for if that act is a crime the inciter should not be charged under that section but should be charged with the substantive offence. In practice, therefore, the construction of that section is only of real importance in cases where the incitee does not do the act which he has been incited to do." See also *R v Bedhla* 1929 TPD 276:280; *R v Ungwaja* 1891 12 NLR 284:286.

3.10.2.2. Making passwords, password sniffers and hackers' tools available

It would be a fallacy to attempt to postulate all the possible circumstances that may arise where either password sniffers or other hackers' tools or illegally obtained passwords are posted on web sites and thus available for downloading, either for free or after paying the prescribed amount of money. For this reason, it is only assessed whether the following four instances constitute the offence of incitement:

- (1) A posts an illegally obtained password, that renders access to e.g. Microsoft's or MWeb's⁹⁸⁶ computer system, on a web site where he states that this password grants the possessor thereof illegal or free access to that particular computer system.
- (2) A makes a hackers' tool or a password sniffer available on a web site and states that "This program allows you to hack into any computer system ... It works ... proven technology!! Click here, try it out."⁹⁸⁷ When the user clicks on the message or banner, he is given the option of downloading the program.
- (3) The heading on one of A's web pages reads: "MAILBOMBER". Below this heading, the following message appears: "Ghost Mail 5.1. Facilitating mailbombing." Next to the message an icon of a stiffy is displayed. When the user clicks on this icon, he is given the option of downloading the program.⁹⁸⁸
- (4) Similar to (3) above, on A's web site the following heading appears: "Microsoft Windows hacks". When the user clicks on this link, another web page is displayed and one of the many headings reads "Windows password cracker – for cracking win passwords". When the user clicks on this heading, he is taken to another web page where the names of many hackers' tools and password sniffers are listed. When the user clicks on the name of one of these programs, he is given the option of downloading the program.⁹⁸⁹

Three observations should be made. Firstly, it is not incumbent upon the state to prove that the password, which the accused alleged would grant access to a specific computer, can actually render access to a particular computer. Likewise, the state

⁹⁸⁶ A South African ISP.

⁹⁸⁷ A similar message is displayed on www.uhackit.com with regard to a downloadable hackers' tool.

⁹⁸⁸ See <http://www.diabolo666-security.de/WelcomebyDiabolo2.htm>.

⁹⁸⁹ See e.g. <http://the-hack.net>.

does not have to prove that the hackers' tool, which the accused made available for downloading and which he averred could grant access or could interfere with the functioning of any computer system, actually possessed those capabilities. In *R v Panter*⁹⁹⁰ and in *R v Swart*⁹⁹¹ the accused attempted to incite the complainant to purchase diamonds, while the accused was not authorised to trade in diamonds. In both cases the accused alleged that the prosecution failed to prove that what they incited the complainants to purchase were real diamonds. In both cases the courts maintained that in the absence of any evidence by the accused in regard to the nature of the material in question, the court was entitled to rely on the accused's statements which they made to the complainant.⁹⁹²

Secondly, it will be sufficient for the prosecution to allege and prove that the incitement was directed towards the entire Internet community. The prosecution is, therefore, not obliged to allege or prove that the accused incited any particular computer user.⁹⁹³

Thirdly, in *R v Fortuin*⁹⁹⁴ the court stated that "[t]here is no special reason why, if inciting to commit a crime of murder or violence or assault is a crime, inciting to commit any other common law offence should not also be a crime."⁹⁹⁵ Therefore South African courts should be willing to extend the offence of incitement to computer-related crimes.

By means of the following two questions, namely (i) did A incite and (ii) did A have the necessary *mens rea* when he incited, the four postulated scenarios can be answered.

It is submitted that the accused in scenario (1) above is guilty of incitement: A incites a

⁹⁹⁰ 1932 TPD 121.

⁹⁹¹ 1932 TPD 168.

⁹⁹² 1932 TPD 121:123; 1932 TPD 168:170. See par 3.10.2.3 for an answer to the scenario where the computer program or password is defective.

⁹⁹³ In *R v Segal & Others* 1960 1 SA 721 A the Supreme Court of Appeal noted (at 731A) that the indictment does not have to allege incitement of particular persons. It was sufficient if it alleged incitement of the "whole of the non-European labour force of the Witwatersrand." Snyman 1999 states (at 298) that "[d]aar word aan die hand gedoen dat uitlokking nie noodwendig altyd aan 'n bepaalde persoon or persone gerig hoef te wees nie. Uitlokking teenoor mense in die algemeen behoort ook strafbaar te wees, soos waar 'n opruiende geskrif in 'n artikel in 'n koerant of in 'n vlugskrif vervat is." [own translation: It is submitted that incitement does not necessarily have to be directed towards a specific person or persons. Incitement of people in general ought to be punishable, e.g. where an instigating article is published in a newspaper or a pamphlet.]

⁹⁹⁴ 1915 CPD 757.

⁹⁹⁵ 1915 CPD 757:758.

computer user that visits this web site because he informs the computer user that this particular password can be used successfully to gain access to a specific computer system. He thereby seeks to influence the mind of a (potential) *hacker* to employ this password to gain access to the above-mentioned computer system.⁹⁹⁶ It is further submitted that A has *dolus directus* in that he knows that any *hacker* who downloads this password, will be able to gain unlawful access to Microsoft's or MWeb's computer system. This scenario can be equated with the following instance: X displays a jemmy in his shop with a poster next to the jemmy stating that this implement can be used to specifically gain access to Y's office.

With regard to scenario (2), it is submitted that A is also guilty of incitement. A incites a computer user, viewing this message, in that A makes an effort to draw the attention of the user to this particular program and by stating "click here, try it out" it can be argued that he, not only seeks to influence the mind of the viewer but, in fact urges the user to download and employ the said program. In *R v Panter*⁹⁹⁷ the court held that: "it seems to me clear that the accused incited Schoeman; there was not merely the mere proposal [to purchase diamonds from him, contrary to the law] but an effort on the part of the accused to bring Schoeman into contact with the native [who allegedly possessed the diamonds]."⁹⁹⁸ On the same premise, it may be stated that where A posts hackers' tools on a web site and states that the user should try out these tools, he not only solicits the computer user to employ these programs, but also makes an "effort" by making these programs available to the Internet community. This particular message can also be regarded as an electronic gesture to commit a crime.⁹⁹⁹ It is further submitted that A has the necessary intent in that he, at least, foresees the

⁹⁹⁶ See further the argument with regard to scenarios (3) and (4) as to the type of web pages where these types of programs and passwords are posted.

⁹⁹⁷ 1932 TPD 121.

⁹⁹⁸ 1932 TPD 121:125.

⁹⁹⁹ It would appear from the judgment in *R v Zeelie* 1952 1 SA 400 A that the Supreme Court of Appeal was of the opinion that a gesture can constitute an incitement. Hoexter JA noted (at 409H-410A) that "[d]it word wel deur Miriam ontken dat sy gewink het [vir die beskuldigde], maar met die oog op haar beroep en karakter is haar ontkenning van min waarde. Ek meen dus dat die saak behandel moet word op die grondslag dat Miriam wel in die verbyloop 'n aanlokkende handgebaar gemaak het." [own translation: Miriam denies that she winked [at the accused], but bearing in mind her profession as well as her character her denial is of little value. I am therefore of the opinion that the case must be dealt with on the basis that Miriam, in passing the accused, made an inciting hand movement."] In *R v Sibiyi* 1957 1 247 T the court, referring to Hoexter JA's statement, noted (at 249E-F) that "[t]he case of *Zeelie*,

possibility that these programs may be used for unlawful purposes and that his message may influence the minds of visitors (potential *hackers*) to commit offences. This scenario can be equated with the instance where X displays a jemmy in his shop and a poster next to this implement states: "This jemmy can be used for the purpose of breaking into houses. Try it!"

With regard to scenarios (3) and (4), there is no clear-cut answer. The answer depends greatly upon the circumstances of each particular case. However, it is submitted that A is guilty of incitement. These scenarios can be equated with the instance where A displays a jemmy in his store and a poster, next to it, stipulates that this implement can be used to break into houses. Furthermore, this store is located in a very criminal part of a hypothetical city. With regard to the postulated scenarios (3) and (4), it should be added that the type of web sites where these messages are displayed and where these types of programs can be downloaded, serve no purpose to ordinary Internet-surfers. These web pages only contain programs that can be used to hack into computer systems or to interfere with the operation of computer systems or to intercept electronic communications. Therefore these types of web sites are, generally speaking, only visited by, and of use to, *hackers*. In this context it can be argued that A seeks to influence the mind of a (potential) *hacker*, who visits his web site, to both download the program and to employ it. The program serves only one purpose namely to assist the *hacker* to hack into the computer system of a third party or to interfere with the functioning of the latter's computer system.¹⁰⁰⁰ It is submitted that, under these circumstances, a court would hold that A, beyond any reasonable doubt, incited web site visitors to employ these tools.¹⁰⁰¹ It can further be argued that

supra, is, however, interesting for the fact that it would seem that an incitement can be constituted by means of a gesture."

¹⁰⁰⁰ This submission is based upon the *dictum* of the Supreme Court of Appeal in *S v Nkosiyana & Another* 1966 4 SA 655 A. The accused approached the complainant to borrow R100 from him for the purpose of hiring an assassin to kill A. The complainant was an opponent to A. The accused's defence was that they merely requested the complainant for a loan and therefore no incitement occurred. The court rejected this contention, stating (at 660A-C) that "the Attorney-General was right in his submission that it goes much further than a mere request for a loan. It was a request to a fellow opposition member of the Assembly, and it was persisted in after he demurred, that he assist in the payment of the blood money in order to compass a political assassination. It was intended that he should start thinking in the direction of assistance, with a view to his compliance."

¹⁰⁰¹ In *R v Milne & Another* 1951 1 SA 791 A the Supreme Court of Appeal held (at 821A-B) that, where the accused instructed A to draw up a broker's note, which to the knowledge of the accused was false, and which note was subsequently used by B, an employee of the accused, to make an entry in the

by stating that the tool can be used for unlawful purposes, A makes, in effect, a proposal that the visitor should download the tool and use it. It can also be argued that A instigates the web site visitor to use this tool, after he downloaded it.¹⁰⁰²

It is furthermore submitted that A foresees that he may influence the mind of the (potential) *hacker* to download the program and to use it to hack into the computer system of a third party or to interfere with the proper operation of the latter's computer system.¹⁰⁰³ Therefore, it is submitted, A has the necessary *mens rea* in the form of *dolus eventualis*.¹⁰⁰⁴

books of the accused's company, the accused "may be said to have incited or instigated [B] to make that [false] entry." The accused did not request nor instruct B to make the false entry. B made the book entry in his normal course of employment.

¹⁰⁰² In *R v Fortuin* 1915 CPD 757 the court held (at 758) that "to incite" include "to solicit" and "to instigate". In *R v Sibiyi* 1957 1 SA 247 T the court held (at 250F-G) that "no technical meaning should be assigned to the word 'incite' ". In *R v Zeelie* 1952 1 SA 400 A Schreiner JA stated (at 402F) that he regarded an offer or a proposal to be the minimum required for an incitement.

¹⁰⁰³ Burchell & Milton 2000 maintain on p 448-449 that "it must be shown that the accused must have foreseen, and hence by inference did foresee, at least the possibility that his communication would influence the incitee's mind and result in his doing an act which amounted to a crime."

¹⁰⁰⁴ In *S v Lungile & Another* 1999 2 SACR 597 SCA the accused participated in an armed robbery. As a result of these events, one person was shot dead. The prosecution alleged that the accused, even though he was not armed but was aware of the fact that two of his co-robbers were armed, foresaw the possibility that someone might be killed in the process of the intended robbery, but proceeded recklessly. Stated differently, that *dolus eventualis* was present. The Supreme Court of Appeal held (at 602e-603d) that: "But this Court has cautioned, on several occasions, that one should not too readily proceed from 'ought to have foreseen' to 'must have foreseen' and hence to 'by necessary inference in fact did foresee' the possible consequences of the conduct inquired into. *Dolus* being a subjective state of mind, the several thought processes attributed to an accused must be established beyond any reasonable doubt, having due regard to the particular circumstances of the case ... In the present case, the crucial question therefore is whether the State proved beyond reasonable doubt that the first appellant in fact did foresee ('inderdaad voorsien het') that the death of a person could result from the armed robbery in which he participated. In this case, as in many others, the question whether an accused in fact foresaw a particular consequence of his acts can only be answered by way of deductive reasoning. Because such reasoning can be misleading, one must be cautious. Generally speaking, the fact that the first appellant had prior to the robbery made common cause with his co-robbers to execute the crime, well-knowing that at least two of them were armed, would set in motion a logical inferential process leading up to a finding that he did in fact foresee the possibility of a killing during the robbery and that he was reckless as regards that result ... In my view the inference is inescapable that the first appellant did foresee the possibility of the death of an employee of Scotts: he knew that at least two of his co-conspirators were armed with firearms; he knew that Scotts is in the main street of Port Elizabeth, and that it is immediately opposite a police station; and he knew that the robbery would take place in broad daylight. He nevertheless participated in the robbery, helping to subdue some of the victims. The State has consequently proved the necessary *mens rea* in the form of *dolus eventualis* beyond

It is imperative that the prosecution, by means of the indictment, informs the accused of how it alleges that the incitement was made. The indictment must contain statements reasonably sufficient to enable the accused to know the nature of the charge he faces.¹⁰⁰⁵ The indictment must, therefore, clearly stipulate how the prosecution alleges A to have incited web site visitors to, not only download the program or passwords, but also to employ it illegally.

Finally, it should be borne in mind that incitement to employ illegally obtained passwords or hackers' tools to penetrate computer systems' security measures or to interfere with their proper functioning can only constitute an offence, where the courts are willing to recognise that the unlawful breaking into computer systems as well as unlawful interference with computer systems constitute offences in terms of the South African criminal law.¹⁰⁰⁶

3.10.2.3. Attempted incitement

It is submitted that where A posts hackers' tools or illegally obtained passwords on a web site and these passwords and/or hackers' tools are defective, he is guilty of attempted incitement. In *R v Dick*¹⁰⁰⁷ the accused incited X to kill a third party. For this purpose the accused handed a certain quantity of powder to A. However, the quantity was not a lethal dose and therefore would not have killed the third party. The court stated that:

"The means that what was provided by accused for executing the act incited was inadequate to accomplish that purpose. It is well settled, however, that the fact that the means used are inadequate to accomplish the crime attempted would not prevent the endeavour from constituting an attempt. See *R v Davies and Another* ... the evidence does establish that the accused believed in the efficacy of the quantity of powder he

reasonable doubt." Similar reasoning can be applied to scenarios (3) and (4): A knows that, generally speaking, only *hackers* visit his web site; A knows that these *hackers* are searching for tools that can be used to either interfere with the functioning of computer system or to hack into computer systems; thus by necessary inference he must have foreseen that these *hackers* would employ his tools for the above-mentioned purposes, but recklessly posted the programs, together with the messages accompanying them, on the web site in question.

¹⁰⁰⁵ *R v Moilwanyana & Others* 1957 4 SA 608 T:613C-D; *R v D'Arcy & Others* 1934 GWL 8:10.

¹⁰⁰⁶ See *R v Nbakwa* 1956 2 SA 557 SR:560E.

¹⁰⁰⁷ 1969 3 SA 267 R.

anded over to compass his purpose, namely, the death of Eneresi."¹⁰⁰⁸

Consequently, the court convicted the accused of attempted incitement. Likewise, the Supreme Court of Appeal held in *S v Nkosiyana & Another*¹⁰⁰⁹ that the South African law recognises, although in a different context, the offence of attempted incitement. It noted that "[w]here the intended influencing does not reach the mind of the prospective incitee, the crime may be one of attempted incitement, e.g. where an inflammatory letter is sent but goes astray."¹⁰¹⁰

4. CONCLUSION

After a careful study of the common law as well as statutory offences recognised in South African law, it is submitted that -

- (a) where a *hacker* intercepts an electronic communication (such as e-mail), he is guilty both of *crimen iniuria* as well as of an offence in terms of the *Interception and Monitoring Prohibition Act*. Where the *hacker* intercepted such communication or conversation by means of spoofing, he is also guilty of fraud;
- (b) where a *hacker* monitors (eavesdrops on) electronic communications, he is guilty of *crimen iniuria*. Likewise, where a computer user uses a malicious computer program (such as a Trojan horse) to engage in espionage, he is guilty of *crimen iniuria*. In both instances he is also guilty of an offence in terms of the *Interception and Monitoring Prohibition Act*;
- (c) where a *hacker* gains access to a computer without authorisation, he is guilty of *crimen iniuria* as well as fraud;
- (d) where a *hacker* himself or by using a computer program copies electronic content, which includes passwords, information as well as other digital content, he is guilty of theft;
- (e) where a *hacker* mentally copies or writes down confidential information or passwords, he is guilty of theft;
- (f) where a *hacker* himself or by using a computer program modifies or deletes electronic content, he is guilty of malicious injury to property;
- (g) where a *hacker* himself or by using a computer program (such as bacteria) renders

¹⁰⁰⁸ 1969 3 SA 267 R:269B-G.

¹⁰⁰⁹ 1966 4 SA 655 A.

¹⁰¹⁰ 1966 4 SA 655 A:659A.

- a computer inaccessible or inoperable, he is guilty of malicious injury to property;
- (h) where a *hacker* interferes with the operation of a computer, for instance by means of a denial-of-service attack or an e-mail bomb attack, he is guilty of fraud and malicious injury to property;
 - (i) where a *hacker* himself or by means of a computer program defaces a web page to such an extent that it costs the owner of the web site time and labour or money to restore the web page, he is guilty of malicious injury to property;
 - (j) where a *hacker* installs a computer program (usually a "backdoor") on a computer in order to use it as part of a distributed denial-of-service attack or for whatever means, he is guilty of fraud in that he represents that he is authorised to install computer programs on the computer. Only where the *hacker* examined the electronic files stored on that computer, does he commit *crimen iniuria*;
 - (k) where a *hacker* spoofs the address of his e-mail message, he is guilty of fraud;
 - (l) where a computer user sends a virus hoax to other Internet users, he is guilty of fraud. Where such virus hoax subsequently causes damage to third parties' computers, he is guilty of malicious injury to property.
 - (m) where a third party receives copied electronic content (including passwords) from A, knowing that such content is stolen, the third party is guilty of receiving stolen property knowing it to be stolen. Where such stolen information consists of private facts, the third party is also guilty of *crimen iniuria*;
 - (n) where A intentionally sends a malicious computer program as an attachment to B, but the latter discovers this program before it causes any prejudice, A is guilty of attempted malicious injury to property;
 - (o) where A releases a malicious computer program onto the Internet, programmed to cause prejudice, but the program is defective and cannot cause financial prejudice, A is guilty of attempted malicious injury to property;
 - (p) where a *hacker* attempts to gain access to a computer system but fails to succeed, he is guilty of attempted *crimen iniuria* as well as fraud (or attempted fraud);
 - (q) where B instructs A (a third party) to gain access to X's computer system and to copy electronic content, and A does this, B is guilty of theft. An identical position exists where B assists A in disposing of the illegally obtained digital content;
 - (r) where A makes a hackers' tool or an illegally obtained password available, by means of the Internet, and B subsequently employs this password or hackers' tool to hack into a third party's computer system or to interfere with the latter's computer system, A is guilty as an accomplice to the offence committed by B; and

(s) where A makes a hackers' tool or an illegally obtained password available, by means of the Internet, and states that this password or hackers' tool renders access to, or interferes with the operation of, a specific or any computer system, A is guilty of incitement, either as a common law offence or as a statutory offence.

It is also submitted that the mere creation of malicious computer programs, password sniffers as well as hackers' tools does not constitute a criminal offence according to the South African criminal law.

CHAPTER SEVEN

COMPARATIVE LAW STUDY

1. INTRODUCTION

In the previous chapter it was argued that the South African criminal law system can adequately deal with most hacking and virus instances as either fraud, theft, malicious injury to property, *crimen iniuria* and/or receiving stolen property knowing it to be stolen. However, it was also noted that certain forms of Internet abuse do not constitute criminal offences. In chapter eight it is assessed how computer-related crimes can be criminalised, should South African courts refuse to extend the application of criminal law principles, as contended for in chapter six. For this reason, it must be assessed in this chapter how foreign countries criminalise hacking as well as virus instances.

2. FOREIGN LEGISLATION

The federal legislation of America, the legislation of the states Georgia and Virginia in the US, the Canadian *Criminal Code*, the UK *Computer Misuse Act*, the Singapore *Computer Misuse Act* as well as legislation in the Netherlands are discussed under this heading. Finally, the new EU *Convention on Cybercrime* is discussed and scrutinised.

2.1. United States of America

2.1.1. Computer Fraud and Abuse Act

According to federal law in the USA, section 1030(a) in the *United States Code* (USC) Title 18 (also known as the *Computer Fraud and Abuse Act of 1984*),¹⁰¹¹ the following hacking and virus instances constitute federal offences:

□ Paragraph 1 penalises a *hacker* (either an external *hacker* or an employee who

¹⁰¹¹ As amended. A copy can be downloaded from www4.law.cornell.edu/uscode/18/1030.html. For a historical analysis of this Act, see *Shurgard Storage Centers Inc v Safeguard Self Storage Inc* 119 F.Supp.2d 1121 (W.D. Wash. 2000) and *North Texas Preventive Imaging LLC v Eisenberg* 1996 US Dist. LEXIS 19990 (C.D. Cal. 1996). Copies of these judgments can be downloaded, respectively, from www.privacysecuritynetwork.com/Library/docs/Shurgard%2Ehtm and www.loundy.com/CASES/NTPI_v_Eisenberg.html.

exceeds his authorised access¹⁰¹²) who intentionally accesses a computer¹⁰¹³ and obtains information that can be used to the peril of the US national defence or its foreign relations or to the advantage of any foreign nation, and either holds such information for himself or communicates it to another person, also not entitled to such information.¹⁰¹⁴

This paragraph, therefore, deals with *hackers* gaining access to specific computer systems, namely computers owned by the US defence and foreign relations department. Mere unauthorised access does not suffice. Conduct is solely penalised by this paragraph if the *hacker* also copied the information stored on these computers. The Act merely stipulates that the *hacker* must obtain information which thus includes instances where he electronically copies the information or makes a mental note or writes it down on a piece of paper.¹⁰¹⁵

□ Paragraph 2 penalises a *hacker* who intentionally accesses a computer and obtains a) information contained in a financial record¹⁰¹⁶ of a financial institution,¹⁰¹⁷ or of a

¹⁰¹² The term "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." S 1030(e)(6).

¹⁰¹³ The term "computer" means "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device." S 1030(e)(1).

¹⁰¹⁴ S 1030(a)(1) provides that "Whoever having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it".

¹⁰¹⁵ See US Department of Justice 1998: " 'obtaining information' includes merely reading it; i.e., there is no requirement that the information be copied or transported. This is critically important because, in an electronic environment, information can be 'stolen' without asportation, and the original usually remains intact."

¹⁰¹⁶ The term "financial record" means "information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution." S 1030(e)(5).

card issuer or contained in a file of a consumer reporting agency on a consumer; or b) information from any department¹⁰¹⁸ or agency of the US; or c) information from any *protected computer* "if the conduct involved an interstate or foreign communication".¹⁰¹⁹ The term "*protected computer*" means -

"a computer (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or (B) which is used in interstate or foreign commerce or communication."¹⁰²⁰ (own emphasis)

"Interstate commerce", in turn, is defined to include "commerce between one State, Territory, Possession, or the District of Columbia and another State, Territory, Possession, or the District of Columbia" and "foreign commerce" is defined to include "commerce with a foreign country."¹⁰²¹

Two court cases, illustrating unauthorised usage, are briefly examined. *America Online Inc v LCGM Inc*¹⁰²² is an example of a contravention of this provision. The defendants were members of the plaintiff's (AOL's) subscription service. The plaintiff's *Unsolicited Bulk E-mail Policy* and its *Terms of Service Policy* barred its members from sending

¹⁰¹⁷ The term "financial institution" means "(A) an institution, with deposits insured by the Federal Deposit Insurance Corporation; (B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank; (C) a credit union with accounts insured by the National Credit Union Administration; (D) a member of the Federal home loan bank system and any home loan bank; (E) any institution of the Farm Credit System under the Farm Credit Act of 1971; (F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934; (G) the Securities Investor Protection Corporation; (H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and (I) an organization operating under section 25 or section 25(a) US of the Federal Reserve Act." S 1030(e)(4).

¹⁰¹⁸ The term "department of the United States" means "the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5." S 1030(e)(7).

¹⁰¹⁹ S 1030(a)(2) provides that "Whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains (A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); (B) information from any department or agency of the United States; or (C) information from any protected computer if the conduct involved an interstate or foreign communication".

¹⁰²⁰ S 1030(e)(2).

¹⁰²¹ S 10 of Title 18.

bulk e-mail through plaintiff's computer systems. Defendants used their membership accounts to harvest the e-mail addresses of AOL members, to whom they eventually sent spam e-mail messages. Defendants acquired these e-mail addresses by using software programs. The court concluded that the defendants' conduct violated plaintiff's *Terms of Service Policy*, and therefore was unauthorized. Furthermore the addresses of AOL members were, according to the court, "information" within the meaning of the Act because such information was proprietary in nature. The court was of the opinion that the defendants contravened paragraph 2.

*In Shurgard Storage Centers Inc v Safeguard Self Storage Inc*¹⁰²³ the plaintiff and defendant were competitors. The defendant solicited the plaintiff's employees to cease their employment at the plaintiff and to work for him. One of the solicited employees, while still employed by the plaintiff, but acting as an agent for the defendant, sent e-mails to the defendant containing various trade secrets and proprietary information belonging to the plaintiff. The plaintiff alleged that the employee violated section 1030(a)(2)(C). The question of law was whether the employee acted without authorisation. The court answered in the affirmative:

"[T]he authority of the plaintiff's former employees ended when they allegedly became agents of the defendant. Therefore ... they lost their authorization and were 'without authorization' when they allegedly obtained and sent the proprietary information to the defendant via e-mail."

This paragraph, therefore, offers protection to three types of computers: a) computers used by financial institutions; b) computers used by US departments and agencies and c) computers used either for (Internet) communication or commerce. This provision penalises instances where a *hacker* gains access to any government computer or any private computer, used for commercial and communicational purposes, including those of ISPs,¹⁰²⁴ and obtains information.¹⁰²⁵ In *America Online Inc v National Health Care*

¹⁰²² 46 F. Supp. 2d 444 (E.D. Va. 1998). A copy of this judgment can be downloaded from <http://legal.web.aol.com/decisions/dljunk/lcgmopin.html>.

¹⁰²³ 119 F.Supp.2d 1121 (W.D. Wash. 2000). A copy of this judgment can be downloaded from www.privacysecuritynetwork.com/Library/docs/Shurgard%2Ehtm.

¹⁰²⁴ In *America Online Inc v National Health Care Discount Inc* 121 F.Supp. 1255 (N.D. Iowa 2000) the court held that the computers of America Online, an ISP, fall within the definition of "protected computers". A copy of this judgment can be downloaded from www.law.asu.edu/HomePages/Karjala/cyberlaw/AOLv.NatHealthCare9-29-00.html.

¹⁰²⁵ See US Department of Justice 1998.

*Discount Inc*¹⁰²⁶ the court observed that the purpose of this section is to protect privacy. It follows that where A, for example, hacks into Amazon.com's computer system and obtains, for instance, credit card information, he is guilty of an offence in terms of this provision. Mere unauthorised access does not suffice for this offence; the *hacker* must have made electronic, written or mental copies of the information stored on such computer system.¹⁰²⁷ Stated differently, he must have impinged on the confidentiality of data.¹⁰²⁸

It may further be concluded, from the above quoted judgments, that where a member of an electronic service employs his membership contrary to the service's user policy, his conduct is unauthorised. Further, where an employee uses his employer's computer system for unlawful purposes, his conduct is also unauthorised.

□ Paragraph 3 penalises a *hacker* who intentionally accesses any non-public computer¹⁰²⁹ of a US department or agency and where such conduct affects that use by or for the US Government.¹⁰³⁰

This paragraph only deals with hacking into government owned or controlled computers. Note however, that mere unauthorised access suffices for this offence: "Thus, an intruder who violates the integrity of a government machine to gain network

¹⁰²⁶ 121 F.Supp. 1255 (N.D. Iowa 2000). A copy of this judgment can be downloaded from www.law.asu.edu/HomePages/Karjala/cyberlaw/AOLv.NatHealthCare9-29-00.html.

¹⁰²⁷ The US Committee who drafted the amendment to s 1030(a)(2) noted in 1996 that "The proposed subsection 1030(a)(2)(C) is intended to protect against the interstate or foreign theft of information by computer This subsection would ensure that the theft of intangible information by the unauthorized use of a computer is prohibited in the same way theft of physical items are protected ... The crux of the offense under subsection 1030(a)(2)(C), however, is the abuse of a computer to obtain the information." Obtained from the judgment of *Shurgard Storage Centers Inc v Safeguard Self Storage Inc* 119 F.Supp.2d 1121 (W.D. Wash. 2000).

¹⁰²⁸ See US Department of Justice 1998.

¹⁰²⁹ The Act fails to define a "nonpublic computer". The US Department of Justice notes that "Congress added the word 'non-public' to make it perfectly clear that a person who has no authority to access any non-public computer of a department or agency may be convicted under (a)(3) even though permitted to access publicly available computers." Furthermore, it maintained that "[it] is intended to reflect the growing use of the Internet by government agencies and, in particular, the establishment of World Wide Web home pages and other public services." US Department of Justice 1998.

¹⁰³⁰ S 1030(a)(3) stipulates that "Whoever intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States".

access is nonetheless liable for trespass even when he has not jeopardized the confidentiality of data.”¹⁰³¹

□ Paragraph 4 penalises a *hacker* who knowingly and with intent to defraud, accesses a “protected computer”¹⁰³² and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period.¹⁰³³

*In Shurgard Storage Centers Inc v Safeguard Self Storage Inc*¹⁰³⁴ the plaintiff and defendant were competitors. The defendant solicited the plaintiff’s employees to cease their employment at the plaintiff and to work for him. A, one of the solicited employees, while still employed by the plaintiff, but acting as an agent for the defendant, sent e-mails to the defendant containing various trade secrets and proprietary information belonging to the plaintiff. The plaintiff alleged that employee A and the defendant (as his agent/employer) violated section 1030(a)(4). The question of law was whether “defraud” connotes common law fraud in this context. The court maintained that “defraud” merely connoted “wronging one in his property rights by dishonest methods of schemes.” Subsequently the court found that defendant and employee A had contravened this section.

This provision, therefore, also protects computers used for commercial and communicational purposes. Note that the section provides that mere unauthorised usage of a computer does not constitute an offence: searching through the electronic data of a third party’s computer, out of curiosity, does not violate this provision. The cyber-abuser must have obtained valuable information¹⁰³⁵ or such illicit usage

¹⁰³¹ US Department of Justice 1998.

¹⁰³² Thus a computer used by financial institutions or the US government or used for interstate or foreign commerce and communications.

¹⁰³³ S 1030(a)(4).

¹⁰³⁴ 119 F.Supp.2d 1121 (W.D. Wash. 2000). A copy of this judgment can be downloaded from www.privacysecuritynetwork.com/Library/docs/Shurguard%2Ehtm.

¹⁰³⁵ In *US v Czbinski* 106 F.3d 1069 (1st Cir. 1997) the accused worked for the IRS where he had access to income tax return information. His contract of service provided that he was only allowed to use such access for legitimate purposes. The accused, however, carried out numerous unauthorised searches of the IRS’ data, out of curiosity. For instance, he viewed the tax returns of a woman he had dated a few times. The court maintained that “[t]he plain language of section 1030(a)(4) emphasizes that more than mere unauthorized use is required: the ‘thing obtained’ may not merely be the unauthorized

(computer time) must be worth more than \$5 000.¹⁰³⁶ The Act does not provide how such value should be determined.¹⁰³⁷ Furthermore, from the above-mentioned court case it can be concluded that US courts interpret the word *defraud* very generously.

□ Paragraph 5 penalises a *hacker* who -

“(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization,¹⁰³⁸ and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage.”¹⁰³⁹

The term “damage” is defined to mean “any impairment to the integrity or availability of data, a program, a system, or information, that -

“(A) causes loss aggregating at least \$5,000 in value during any 1-year period to one or more individuals [or corporations¹⁰⁴⁰];

(B) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals;

(C) causes physical injury to any person; or

(D) threatens public health or safety¹⁰⁴¹.”¹⁰⁴²

use ... Congress intended section 1030(a)(4) to punish attempts to steal valuable data”. A copy of this judgment can be downloaded from www.law.emory.edu/1circuit/feb97/96-1317.01a.html.

¹⁰³⁶ US Department of Justice 1998.

¹⁰³⁷ The US Congress stated that “[a]s for the monetary threshold, any reasonable method can be used to establish the value of the information obtained. For example, the research, development, and manufacturing costs, or the value of the property ‘in the thieves’ market,’ can be used to meet the \$5,000 valuation.” US Department of Justice 1998.

¹⁰³⁸ In *Shurgard Storage Centers Inc v Safeguard Self Storage Inc* 119 F.Supp.2d 1121 (W.D. Wash. 2000) the court maintained that the phrase “without authorisation” includes instances where an employee exceeds his authorisation.

¹⁰³⁹ S 1030(a)(5).

¹⁰⁴⁰ In *US v Middleton* 231 F.3d 1207 (9th Cir. 2000) the court noted that “individuals” includes corporate bodies. The court maintained that “[i]t is highly unlikely, in view of Congress’ purpose to stop damage to computers used in interstate and foreign commerce and communication, that Congress intended to criminalize damage to such computers only if the damage is to a natural person.” A copy of this judgment can be downloaded from <http://laws.lp.findlaw.com/9th/9910518.html>.

¹⁰⁴¹ The US Department of Justice notes that “[a]s the NII and other network infrastructures continue to grow, computers will increasingly be used for access to critical services such as emergency response systems and air traffic control”. US Department of Justice 1998.

A few court cases need to be studied in order to put these provisions in perspective. In *North Texas Preventive Imaging LLC v Eisenberg*¹⁰⁴³ the plaintiff purchased a computer system from the defendant at the beginning of 1995. When several disputes arose between these parties, the defendant sent plaintiff "update disks" to update the computer systems. Unbeknown to the plaintiff, these disks contained disabling codes (a time bomb) that would have disabled the computer system, had plaintiff not discovered the time bomb. The plaintiff alleged that defendant violated section 1030(a)(5)(A). The question of law was whether this provision "prohibits a person from sending a disk containing disabling codes to an authorized person who then unwittingly loads the codes onto a computer." The court observed that it -

"found nothing in the statute or legislative history to suggest that Congress intended a blanket exemption for the use of time bombs from the CFAA's prohibitions. Rather, time bombs would appear to fall within the statute's proscription on the use of 'codes, information, programs, or commands' to cause harm to protected computer systems. Whether the use of a time bomb is illegal appears to require a case-by-case analysis of the defendant's intent, the type of computer involved, and the resulting harm ... The transmission of a disabling code by floppy computer disk may fall within the new language, if accompanied by the intent to cause harm."

In *America Online Inc v National Health Care Discount Inc*¹⁰⁴⁴ the court had to determine the meaning of the word "access", as used in paragraph 5. The employees of defendant sent spam e-mail messages to the members of the plaintiff (AOL). These employees obtained the e-mail addresses in question without authorisation. The court stated that:

"The [Act] does not define 'access,' but the general definition of the word, as transitive verb, is to 'gain access to.' ... As a noun, 'access,' in this context, means to exercise the 'freedom or ability to ... make use of' something. Id. The question here, therefore, is whether NHCD's e-mailers, by harvesting e-mail addresses of AOL members and then sending the members [spam] messages, exercised the freedom or ability to make use of AOL's computers. The court finds they did. For purposes of the [Act], when someone sends an e-mail message from his or her own computer, and the message then is

¹⁰⁴² S 1030(e)(8).

¹⁰⁴³ 1996 US Dist. LEXIS 19990 (C.D. Cal. 1996). A copy of this judgment can be downloaded from www.loundy.com/CASES/NTPI_v_Eisenberg.html.

¹⁰⁴⁴ 121 F.Supp. 1255 (N.D. Iowa 2000). A copy of this judgment can be downloaded from www.law.asu.edu/HomePages/Karjala/cyberlaw/AOLv.NatHealthCare9-29-00.html.

transmitted through a number of other computers until it reaches its destination, the sender is making use of all of those computers, and is therefore 'accessing' them. This is precisely what NHCD's e-mailers did with respect to AOL's computers."

The court further maintained that "when a large volume of [spam messages] causes slowdowns or *diminishes* the capacity of AOL to serve its *customers*, an 'impairment' has occurred to the 'availability' of AOL's 'system.'

In *US v Middleton*¹⁰⁴⁵ the court defined the term "loss" as follows: "The term 'loss' means any monetary loss that [the complainant] sustained as a result of any damage to [its] computer data, program, system or information that you find occurred. And in considering whether the damage caused a loss less than or greater than \$5,000, you may consider any loss that you find was a *natural and foreseeable* result of any damage that you find occurred. In determining the amount of losses, you may consider what measures were *reasonably necessary* to restore the data, program, system, or information that you find was damaged or what *measures were reasonably necessary to resecure* the data, program, system, or information from further damage." (own emphasis). The court further noted that excessive costs as well as "any costs that would merely create an improved computer system unrelated to preventing further damage resulting from [the accused's] conduct" were excluded from the term "loss" as envisaged by the Act. According to the court, losses only included those costs that were necessary to secure the system "as it was before, not making it more secure that it was before". The court further maintained that where an employer's employees spent time and labour to restore a computer system the losses could be calculated by multiplying the number of hours (it took the employees) by the hourly wage they receive. Moreover, "whether the amount of time spent by the employees and their imputed hourly rates were reasonable for the repair tasks that they performed are questions to be answered by the trier of fact." Note, however, that in *Moulton & Network Installation Computer Services Inc v VC3*¹⁰⁴⁶ the court maintained that time and money spent through the use of employees or third parties to *investigate* the accused's activities, do not fall within the ambit of the definition of damages.

¹⁰⁴⁵ 231 F.3d 1207 (9th Cir. 2000). A copy of this judgment can be downloaded from <http://laws.lp.findlaw.com/9th/9910518.html>.

¹⁰⁴⁶ (N.D. Ga. 2000). A copy of this judgment can be downloaded from <http://pub.bna.com/eclr/00434.htm>.

Lastly, in *Shurgard Storage Centers Inc v Safeguard Self Storage Inc*¹⁰⁴⁷ the court shed some light on the term "impairment". The court enunciated that "[t]he statute says damage is 'any impairment to the integrity ... of data ... or information.' ... The unambiguous meaning of 'any' clearly demonstrates that the statute is meant to apply to 'any' impairment to the integrity of data. However, the word 'integrity' is ambiguous in this context ... The word 'integrity' in the context of data necessarily contemplates maintaining the data in a protected state ... the defendant allegedly infiltrated the plaintiff's computer network [by means of employee A] and collected and disseminated confidential information ... an impairment of its integrity occurred."

Subparagraph (A), therefore, deals with instances where a computer programmer writes a malicious computer program and it subsequently causes damage to a computer of a financial institution, a US department or any computer used for commercial and communicational purposes. Furthermore, it encompasses instances where a *hacker* interferes with the functioning of any computer without accessing such computer, for instance by launching a denial-of-service attack against the computer: The *hacker* causes the transmission of a command (or many commands) that causes financial prejudice to the owner of the targeted computer system. Identical considerations apply where a *hacker* defaces a web site, maintained by a protected computer.

Subparagraphs (B) and (C) penalise instances where a *hacker* gains access to one of the above-mentioned computers and causes damage by, for instance, intentionally, recklessly or negligently deleting or corrupting information or modifying data or where he causes this computer to be inoperable or inaccessible.¹⁰⁴⁸ Note however, that mere unauthorised access does not constitute an offence in terms of these provisions.

Note further that the Act limits prosecution to instances where the financial losses suffered, due to the *hacker* or a malicious computer program, are at least \$5 000. The damage element consist of two aspects namely the conduct must (a) impair the integrity or availability of data, etc and b) such conduct must cause a loss of at least \$5

¹⁰⁴⁷ 119 F.Supp.2d 1121 (W.D. Wash. 2000). A copy of this judgment can be downloaded from www.privacysecuritynetwork.com/Library/docs/Shurgard%2Ehtm.

¹⁰⁴⁸ The US Department of Justice notes the following: "Essentially, this new statute provides that individuals who access protected computers without authority are responsible for the consequences of their actions ... damages are not limited to those caused by the process of gaining illegal entry. Rather, all damage, whether caused while gaining access or after entry, is relevant." US Department of Justice 1998.

000.¹⁰⁴⁹ Therefore, where a *hacker* gains access to Amazon.com's computer and does something trivial to annoy the owners, his conduct does not fall within the parameters of this offence if Amazon.com does not suffer at least \$5 000 prejudice. As can be seen from the judgments quoted above, US courts have been willing to hold that expenses incurred to recompile the lost information as well as to resecure the computer system, after the computer abuse occurred, constitute losses in terms of the Act. Furthermore, US courts have interpreted "impairment" to include viewing of electronic data.

□ Paragraph 6 penalises a *hacker* who "knowingly and with intent to defraud traffics (as defined in section 1029¹⁰⁵⁰) in any password or similar information through which a computer may be accessed without authorization, if (A) such trafficking affects interstate or foreign commerce; or (B) such computer is used by or for the Government of the United States."¹⁰⁵¹

This paragraph, therefore, deals with instances where *hackers* sell passwords that they unlawfully obtained from an institution. Seeing that this section relates to US government computers as well as to computers used for commerce, it criminalises the selling of passwords that will give anyone access to even a non-government computer such as Yahoo's computer server.

□ Paragraph 7 penalises anyone who "with intent to extort from any person, firm, association, educational institution, financial institution, government entity,¹⁰⁵² or other legal entity, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer."¹⁰⁵³

This provision, therefore, criminalises instances where a *hacker* e-mails A, threatening him that if he fails to pay, for instance, a \$100 000, he will either hack into A's

¹⁰⁴⁹ See *America Online Inc v National Health Care Discount Inc* 121 F.Supp. 1255 (N.D. Iowa 2000). A copy of this judgment can be downloaded from www.law.asu.edu/HomePages/Karjala/cyberlaw/AOLv.NatHealthCare9-29-00.html.

¹⁰⁵⁰ S 1029(e)(5) defines "traffic" to mean "transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of".

¹⁰⁵¹ S 1030(a)(6).

¹⁰⁵² The term "government entity" includes "the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country." S 1030(e)(9).

¹⁰⁵³ S 1030(a)(7).

computer and delete information or divulge A's passwords to the Internet community. It follows that this section encompasses Internet extortion: "The provision is worded broadly to cover threats to interfere in any way with the normal operation of the computer or system in question, such as denying access to authorized users, erasing or corrupting data or programs, or slowing down the operation of the computer or system."¹⁰⁵⁴ Note, however, that this section also contains a limitation in that the threat must relate to a computer used for interstate or foreign commerce or communication.

Section 1030(b) provides that an attempt to commit any of the offences listed above constitutes an offence. Section 1030(c) provides for the various penalties that may be imposed. The US Code also provides for civil liability by stipulating that -

"[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. Damages ... [of at least \$5,000 in value during any 1-year period to one or more individuals] are limited to economic damages".¹⁰⁵⁵

In conclusion it may be stated this Act has limited application. Generally speaking, the Act only applies to US government computers or computers used for foreign or interstate communication or commerce. The Act does not apply to normal home computers.¹⁰⁵⁶ Furthermore, the Act does not apply to instances where *hackers* merely gain access to non-governmental computers. It further transpires that defacing a web site does not constitute an offence, where the losses suffered do not amount to at least \$5 000. The mere creation of a virus hoax also does not constitute an offence. The Act further fails to deal with instances where a *hacker* attempts to gain access to a computer or to cause financial prejudice but fails to succeed. Also, the mere creation of malicious computer programs, password sniffers and hackers' tool is no offence. Finally, the Act fails to criminalise instances where hackers' tools or illegally obtained

¹⁰⁵⁴ US Department of Justice 1998. The US Department of Justice further notes that this provision "is designed to respond to a growing problem: the interstate transmission of threats directed against computers and computer networks ... These concerns are not theoretical. In one recent case, for example, an individual threatened to crash a computer system unless he was granted access to the system and given an account. Another case involved an individual who penetrated a city government's computer system and encrypted the data on a hard drive, thus leading the victim to suspect an extortion demand was imminent."

¹⁰⁵⁵ S 1030(g).

¹⁰⁵⁶ Unless the US courts are willing to hold that a home computer, used to communicate to other Internet users or to purchase goods or services by means of the Internet, constitute a computer used for foreign and/or interstate communication and/or trade.

password are made available by means of the Internet and other computer users are solicited to employ these tools or passwords.

2.1.2. More federal computer crimes legislation

A computer criminal can also be found guilty of stealing or embezzling records, money or things of value in terms of Title 18: "Anybody who either -

- a) embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, money, or thing of value of the United States or of any department or agency thereof, or
- b) receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted"

is guilty of an offence and punishable by a fine or imprisonment of not more than ten years, or both. The word "value" means "face, par, or market value, or cost price, either wholesale or retail, whichever is greater."¹⁰⁵⁷

It is clear that this section only deals with records, money and things of value belonging to the US government. This section, therefore, criminalises instances where a *hacker* penetrates a US government's computer system and obtains a valuable record by reason of the fact that it, for example, contains confidential information.

2.1.3. Georgia Computer Systems Protection Act

The *Georgia Computer Systems Protection Act*¹⁰⁵⁸ is an example of state legislation in the USA criminalising certain forms of computer abuse. The Act defines the word "use" to include causing or attempting to cause -

"(A) A computer or computer network¹⁰⁵⁹ to perform or to stop performing computer operations;¹⁰⁶⁰

¹⁰⁵⁷ S 641.

¹⁰⁵⁸ Title 16, ch 9, s 90 *et seq.* A copy of this act can be downloaded from www.clark.net/pub/rothman/gacode.htm.

¹⁰⁵⁹ The Act defines "computer network" as "a set of related, remotely connected computers and any communications facilities with the function and purpose of transmitting data among them through the Communications facilities." S 90(2).

¹⁰⁶⁰ The Act stipulates that "computer operation" means "computing, classifying, transmitting, receiving, retrieving, originating, switching, storing, displaying, manifesting, measuring, detecting, recording,

(B) The obstruction, interruption, malfunction, or denial of the use of a computer, computer network, computer program,¹⁰⁶¹ or data,¹⁰⁶² or

(C) A person to put false information into a computer."¹⁰⁶³

It will be noticed that (A) and (B) criminalise, amongst other criminal activities, denial-of-service attacks. The Act establishes six offences, namely computer theft, computer trespass, computer invasion of privacy, computer forgery, computer password disclosure and lastly transmitting misleading data. Each of these offences are discussed separately.

□ The offence "computer theft" is committed where "[a]ny person ... uses a computer or computer network with knowledge that such use is without authority¹⁰⁶⁴ and with the intention of:

- (1) Taking or appropriating any property [which includes computer programs, data, financial instruments¹⁰⁶⁵ and services¹⁰⁶⁶]¹⁰⁶⁷ of another, whether or not with the intention of depriving the owner of possession;
- (2) Obtaining property by any deceitful means or artful practice; or
- (3) Converting property to such person's use in violation of an agreement or other known legal obligation to make a specified application or disposition of such property".¹⁰⁶⁸

reproducing, handling, or utilizing any form of data for business, scientific, control, or other purposes." S 90(3).

¹⁰⁶¹ According to the Act, "computer program" means "one or more statements or instructions composed and structured in a form acceptable to a computer that, when executed by a computer in actual or modified form, cause the computer to perform one or more computer operations. The term 'computer program' shall include all associated procedures and documentation, whether or not such procedures and documentation are in human readable form." S 90(4).

¹⁰⁶² According to the Act, "data" includes "representation of information, intelligence, or data in any fixed medium, including documentation, computer printouts, magnetic storage media, punched cards, storage in a computer, or transmission by a computer network." S 90(5).

¹⁰⁶³ S 92(9).

¹⁰⁶⁴ Similar to all other computer crime legislation, this Act also provides that unauthorised use ("without authority") includes instances where a computer or computer network is used "in a manner that exceeds any right or permission granted by the owner of the computer or computer network." S 90(11).

¹⁰⁶⁵ The Act defines "financial instruments" to include "any check, draft, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction-authorizing mechanism, or marketable security, or any computer representation thereof." S 90(6).

¹⁰⁶⁶ According to the Act, the word "services" includes "computer time or services or data processing services." S 90(8).

¹⁰⁶⁷ According to the Act, "property" includes "computers, computer networks, computer programs, data, financial instruments, and services." S 90(7).

In *America Online Inc v LCGM Inc*¹⁰⁶⁹ the defendants (members of plaintiff) spoofed the heading information of their e-mail messages to create the impression that the e-mails originated from the plaintiff's computer system. Such conduct was against the plaintiff's e-mail policy and therefore unauthorised. The court found that "defendants intended to obtain services by false pretenses and to convert AOL's property ... defendants illegitimately obtained the unauthorized service of plaintiff's mail delivery system and obtained free advertising from AOL because AOL, not defendants, bore the costs of sending these messages."¹⁰⁷⁰

This offence, therefore, criminalises instances where a *hacker* gains unauthorised access with the intention to copy data, computer programs or electronic money or with the intention to use the hacked computer for some sinister purpose. Note that the Act does not require a successful attempt: the *hacker* must merely gain access with the intention to obtain information or services. Subsection (3) criminalises instances where a subscription member uses the subscription service's computer system contrary to the usage policy, for instance by harvesting the e-mail addresses of other subscription members for the purpose of sending spam e-mail messages.

□ The offence "computer trespass" is committed where "[a]ny person ... uses a computer or computer network with knowledge that such use is without authority and with the intention of:

- (1) Deleting or in any way removing, either temporarily or permanently, any computer program or data from a computer or computer network;
- (2) Obstructing, interrupting, or in any way interfering with the use of a computer program or data; or
- (3) Altering, damaging, or in any way causing the malfunction of a computer, computer network, or computer program, regardless of how long the alteration,

¹⁰⁶⁸ S 93(a).

¹⁰⁶⁹ 46 F. Supp. 2d 444 (E.D. Va. 1998). A copy of this judgment can be downloaded from <http://legal.web.aol.com/decisions/dljunk/lcgmopin.html>.

¹⁰⁷⁰ Even though this judgment concerned s 18.2-152.3 of the *Virginia Computer Crimes Act*, which provides that "[a]ny person who uses a COMPUTER or COMPUTER network without authority and with the intent to 1. Obtain property [tangible or intangible, including computer data, programs and software] or services by false pretenses; 2. Embezzle or commit larceny; or 3. Convert the property of another, shall be guilty of the crime of computer fraud", it can be used to illustrate the ambit of s 93(a) of the *Georgia Computer Systems Protection Act*.

damage, or malfunction persists".¹⁰⁷¹

It follows that this section criminalises instances where a *hacker* uses a computer with the intention to either a) delete or modify computer programs and data; or to b) cause a computer or a computer program to malfunction, or to c) interfere with the usage of a computer program or data, thereby including denial-of-service attacks and defacement of web sites. Note again, that the *hacker's* attempts do not have to be successful; only the intention is required. Note further that access is not required. Therefore, where a *hacker* employs a computer program to do the above, he is guilty of an offence, notwithstanding the fact that he did not access the computer system.

□ The offence "computer invasion of privacy" is committed where "[a]ny person ... uses a computer or computer network with the intention of examining any employment, medical, salary, credit, or any other financial or personal data relating to any other person with knowledge that such examination is without authority".¹⁰⁷²

It appears from this section that when a *hacker* gains access with the intention to merely look at the information stored on the computer or computer network, he is guilty of this offence. Therefore, the mere unauthorised access to a computer constitutes this offence; the provision does not require the *hacker* to be successful in acquiring any knowledge.

□ The offence "computer forgery" is committed where "[a]ny person ... creates, alters, or deletes any data contained in any computer or computer network, who, if such person had created, altered, or deleted a tangible document or instrument would have committed forgery under Article 1 of this chapter ... The absence of a tangible writing directly created or altered by the offender shall not be a defense to the crime of computer forgery if a creation, alteration, or deletion of data was involved in lieu of a tangible document or instrument."¹⁰⁷³

This section, therefore, criminalises online fraud where, for instance, a *hacker* gains access to the computer system of a financial institution and subsequently transfers electronic money from one account to another or creates a false account to his own or someone else's benefit.

¹⁰⁷¹ S 93(b).

¹⁰⁷² S 93(c).

¹⁰⁷³ S 93(d).

□ The offence “computer password disclosure” is committed where “[a]ny person ... discloses a number, code, password, or other means of access to a computer or computer network knowing that such disclosure is without authority and which results in damages (including the fair market value of any services used and victim expenditure) to the owner of the computer or computer network in excess of \$500.00”.¹⁰⁷⁴

This offence is aimed at instances where a *hacker* or someone else discloses passwords to third parties. However, a limitation is set namely that the owner of the computer system must suffer damages in excess of \$500 as a result of such unlawful disclosure.

□ Finally, the Act¹⁰⁷⁵ criminalises passing-off and online fraud by providing that it is unlawful -

“for any person, any organization, or any representative of any organization knowingly to transmit any data ... for the purpose of setting up, maintaining, operating, or exchanging data with an electronic mailbox, home page, or any other electronic information storage bank or point of access to electronic information if such data uses any individual name, trade name, registered trademark, logo, legal or official seal, or copyrighted symbol to falsely identify the person, organization, or representative transmitting such data or which would falsely state or imply that such person, organization, or representative has permission or is legally authorized to use such trade name, registered trademark, logo, legal or official seal, or copyrighted symbol for such purpose when such permission or authorization has not been obtained”.¹⁰⁷⁶

Where someone contravenes this provision, he is guilty of an offence and the aggrieved party may institute a civil action for equitable and/or monetary relief.¹⁰⁷⁷

Therefore, where A for instance creates a web page misrepresenting that he is Microsoft or a Microsoft affiliate/franchisee, he violates this provision. Likewise, A contravenes this provision where he sends e-mail indicating the above-mentioned false information. Hence, where A spoofs his e-mail address to create the false impression that the message was sent by America Online or a subscription member of the latter, he is guilty of an offence.

¹⁰⁷⁴ S 93(e).

¹⁰⁷⁵ Under the heading “transmitting misleading data”.

¹⁰⁷⁶ S 93.1(a).

¹⁰⁷⁷ S 93.1(b) & (c).

The Act provides that anybody convicted of the crime of computer theft, trespass, computer invasion of privacy, or computer forgery may not be fined more than \$50 000 or be imprisoned for more than 15 years, or both.¹⁰⁷⁸ Where someone is convicted of computer password disclosure, the maximum penalties are a fine of \$5 000 and/or imprisonment of one year.¹⁰⁷⁹

The Act continues to provide for the recovery of civil damages: Any person whose property or person is injured by reason of a violation of the above-mentioned prohibited acts, may sue for such injury and recover any damages sustained, which includes loss of profits as well as victim expenditure,¹⁰⁸⁰ the latter entailing -

“any expenditure reasonably and necessarily incurred by the owner to verify that a computer, computer network, computer program, or data was or was not altered, deleted, damaged, or destroyed by unauthorized use.”¹⁰⁸¹

Any party to such an action may request the court to conduct all legal proceedings by reasonable means in such a way as to protect “the secrecy and security of any computer, computer network, data or computer program involved in order to prevent possible recurrence of the same or a similar act by another person and to protect any trade secrets of any party.”¹⁰⁸²

In conclusion it may be pointed out that the Act fails to criminalise the following instances: a) intentionally sending virus hoaxes to other Internet users; b) creating malicious computer programs; c) disseminating such malicious computer programs; d) the creation and dissemination of hackers' tools; e) instances where a computer program installs another program on that particular computer; f) where a *hacker* discloses a password but the owner of the compromised computer system does not suffer financial losses in excess of \$500; g) where a third party acquires the stolen digital data from the *hacker*, knowing that such data was unlawfully obtained; h) attempted hacking; i) instructing *hackers* to penetrate computer systems or assisting them in getting rid of illegally obtained digital data and i) making hackers' tools or illegally obtained password available by means of the Internet and soliciting other computer users to employ these tools or passwords.

¹⁰⁷⁸ S 93(h)(1).

¹⁰⁷⁹ S 93(h)(2).

¹⁰⁸⁰ S 93(g)(1).

¹⁰⁸¹ S 90(10).

The Act is, however, an improvement on the federal *Computer Fraud and Abuse Act*¹⁰⁸³ in that it does not distinguish between various "types" of computers, namely whether the computer is owned or used by the US government or not, nor does it limit offences to specific computers and further does not require the wrongful conduct to be successful.

2.1.4. Virginia Computer Crimes Act

The *Virginia Computer Crimes Act*¹⁰⁸⁴ contains unique provisions dealing with computer-related crimes. Generally speaking, the Act establishes four computer crimes namely (a) computer fraud, (b) computer trespass, (c) invasion of privacy by means of computers and (d) theft of computer services. Only the offence of computer trespass is relevant to this study.¹⁰⁸⁵

The Act states that it is "unlawful for any person¹⁰⁸⁶ to use a COMPUTER¹⁰⁸⁷ or COMPUTER network¹⁰⁸⁸ without authority¹⁰⁸⁹ and with the intent to:

1. Temporarily or permanently remove, halt, or otherwise disable any COMPUTER data,¹⁰⁹⁰ COMPUTER programs,¹⁰⁹¹ or COMPUTER software¹⁰⁹² from a COMPUTER or COMPUTER network;

¹⁰⁸² S 93(g)(2).

¹⁰⁸³ Discussed in par 2.1.1.

¹⁰⁸⁴ A copy can be downloaded from www.etext.org/CuD/Law/virginia.

¹⁰⁸⁵ Generally speaking, the other offences created by this Act correspond with the offences created by the *Georgia Computer Systems Protection Act*, discussed in par 2.1.3 of this chapter.

¹⁰⁸⁶ The Act defines "person" to include an "individual, partnership, association, corporation or joint venture."

¹⁰⁸⁷ The Act defines "computer" as "an electronic, magnetic, optical, hydraulic or organic device or group of devices which, pursuant to a computer program, to human instruction, or to permanent instructions contained in the device or group of devices, can automatically perform computer operations with or on computer data and can communicate the results to another computer or to a person. The term 'computer' includes any connected or directly related device, equipment, or facility which enables the computer to store, retrieve or communicate computer programs, computer data or the results of computer operations to or from a person, another computer or another device." S 18.2-152.2.

¹⁰⁸⁸ The Act defines "computer network" to mean "a set of related, remotely connected devices and any communications facilities including more than one COMPUTER with the capability to transmit data among them through the communications facilities." S 18.2-152.2.

¹⁰⁸⁹ The Act provides that a person is "without authority" whenever "he has no right or permission of the owner to use a COMPUTER, or, he uses a COMPUTER in a manner exceeding such right or permission". S 18.2-152.2.

2. Cause a COMPUTER to malfunction regardless of how long the malfunction persists;
3. Alter or erase any COMPUTER data, COMPUTER programs, or COMPUTER software;
4. Effect the creation or alteration of a financial instrument¹⁰⁹³ or of an electronic transfer of funds;
5. Cause physical injury to the property of another;
6. Make or cause to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of COMPUTER data, COMPUTER programs, or COMPUTER software residing in, communicated by, or produced by a COMPUTER or COMPUTER network; or
7. Falsify or forge electronic mail transmission information or other routing information in any manner in connection with the transmission of unsolicited bulk electronic mail through or into the computer network of an electronic mail service provider or its subscribers.

B. It shall be unlawful for any person knowingly to sell, give or otherwise distribute or possess with the intent to sell, give or distribute software which (i) is primarily designed or produced for the purpose of facilitating or enabling the falsification of electronic mail transmission information or other routing information; (ii) has only limited commercially significant purpose or use other than to facilitate or enable the falsification of electronic mail transmission information or other routing information; or (iii) is marketed by that person or another acting in concert with that person with that person's knowledge for use in facilitating or enabling the falsification of electronic mail transmission information or other routing information."¹⁰⁹⁴

¹⁰⁹⁰ According to the Act, "computer data" means "any representation of information, knowledge, facts, concepts, or instructions which is being prepared or has been prepared and is intended to be processed, is being processed, or has been processed in a COMPUTER or COMPUTER network. 'COMPUTER data' may be in any form, whether readable only by a COMPUTER or only by a human or by either, including, but not limited to, COMPUTER printouts, magnetic storage media, punched cards, or stored internally in the memory of the COMPUTER." S 18.2-152.2.

¹⁰⁹¹ According to the Act, "computer program" means "an ordered set of data representing coded instructions or statements that, when executed by a COMPUTER, causes the COMPUTER to perform one or more COMPUTER operations." S 18.2-152.2.

¹⁰⁹² The Act defines "computer software" as "a set of COMPUTER programs, procedures and associated documentation concerned with COMPUTER data or with the operation of a COMPUTER, COMPUTER program, or COMPUTER network." S 18.2-152.2.

¹⁰⁹³ According to the Act, "financial instrument" includes "any check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction authorization mechanism, marketable security, or any computerized representation thereof." S 18.2-152.2.

¹⁰⁹⁴ S 18.2-152.4.

Therefore this offence penalises the following unlawful conduct: a) modification or erasure of data, programs and software; b) causing a computer to malfunction, for instance, by means of viruses or by inserting malicious codes; c) copying of data, programs and software; d) transferring funds electronically without authorisation; creating or modifying electronic checks or electronic credit; and e) the dissemination of, as well as possession of, software that is primarily designed to enable computer users to *spoof* (forge) the header information of e-mail messages. Furthermore, the Act only penalises the spoofing of the header information of spam messages and does not prohibit the spoofing of normal e-mail messages or the transmission of spam.

This Act is further unique in that it refers to computer programs, computer software and computer data. Examples of computer software are MS Windows and MS Word. An example of computer data is a Word document. A computer program can for instance be computer software in development or a program such as a screen saver. Therefore neither the prosecutor nor the court is not required to bring computer software within the definition of computer data or computer programs, as is the case with the legislation dealt so far.

2.2. Canada

The *Canadian Criminal Code of 1985*¹⁰⁹⁵ creates three offences namely a) unauthorised use of a computer, b) possession of a device to obtain unlawful computer service and c) interference with the use of a computer. With regard to the offence "unauthorised use of a computer" the *Criminal Code* provides that:

"Everyone who, fraudulently and without colour of right,

(a) obtains, directly or indirectly, any computer service,¹⁰⁹⁶

(b) by means of an electro-magnetic, acoustic, mechanical or other device,¹⁰⁹⁷ intercepts or causes to be intercepted,¹⁰⁹⁸ directly or indirectly, any function¹⁰⁹⁹ of a computer system,¹¹⁰⁰

¹⁰⁹⁵ R.S. 1985, c.C-46. A copy of this legislation can be downloaded from <http://laws.justice.gc.ca/en/C-46/>.

¹⁰⁹⁶ S 342.1(2) provides that "computer service" includes "data processing and the storage or retrieval of data."

¹⁰⁹⁷ According to s 342.1 "electro-magnetic, acoustic, mechanical or other device" means "any device or apparatus that is used or is capable of being used to intercept any function of a computer system, but

- (c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system, or
- (d) uses, possesses, traffics¹¹⁰¹ in or permits another person to have access to a computer password¹¹⁰² that would enable a person to commit an offence under paragraph (a), (b) or (c)

is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction."¹¹⁰³

It appears that this provision criminalises the following abuses: 1) gaining access without authorisation and obtaining control of a computer, by for instance viewing electronic data; 2) intercepting of and/or listening to electronic communications – note that par (b) covers the instance where a *hacker* uses a computer program to intercept or listen to electronic communications; and 3) possessing, using, trafficking in or disseminating passwords or allowing others access to such passwords.

With regard to the second offence "possession of a device to obtain computer service" the *Criminal Code* provides that:

"Every person who, without lawful justification or excuse, makes, possesses, sells, offers for sale or distributes any instrument or device or any component thereof, the design of which renders it primarily useful for committing an offence under section 342.1, under circumstances that give rise to a reasonable inference that the instrument,

does not include a hearing aid used to correct subnormal hearing of the user to not better than normal hearing."

¹⁰⁹⁸ "Intercept" includes "listen to or record a function of a computer system, or acquire the substance, meaning or purport thereof." S 342.1(2).

¹⁰⁹⁹ "Function" includes "logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer system." S 342.1(2).

¹¹⁰⁰ S 342.1(2) provides that "computer system" means "a device that, or a group of interconnected or related devices one or more of which, (a) contains computer programs or other data, and (b) pursuant to computer programs, (i) performs logic and control, and (ii) may perform any other function." "Computer program" means "data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function." "Data" means "representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer system."

¹¹⁰¹ "Traffic" means, in respect of a computer password, to "sell, export from or import into Canada, distribute or deal with in any other way." S 342.1(2).

¹¹⁰² S 342.1(2) provides that "computer password" means "any data by which a computer service or computer system is capable of being obtained or used."

¹¹⁰³ S 342.1.

device or component has been used or is or was intended to be used to commit an offence contrary to that section,

(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years; or

(b) is guilty of an offence punishable on summary conviction."¹¹⁰⁴

This provision thus penalises the possession of or making, selling or distributing for sale any physical or electronic instrument or device allowing anyone to gain access to a computer or to intercept electronic messages.

The Act creates a third offence, namely where someone wilfully -

"(a) destroys or alters data; [or]

(b) renders data meaningless, useless or ineffective; [or]

(c) obstructs, interrupts or interferes with the lawful use of data; or

(d) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto."¹¹⁰⁵

This provision clearly penalises the erasure, corruption and modification of data as well as the interference with the usage of data and computers. It also includes instances where a *hacker* defaces a web page by replacing the original web page with his own content. This provision can probably be interpreted to include instances where a malicious computer program destroys or alters data.

In conclusion it may be noted that the *Criminal Code* fails to penalise the following instances: a) the creation and/or dissemination of malicious computer programs and hackers' tools used for interfering with computer systems and/or data; b) the intentional creation of virus hoaxes; c) attempts to commit computer-related crimes that were unsuccessful; d) instructing *hackers* or assisting them to get rid of or sell copied electronic data; e) defacing web pages, similar to graffiti.

2.3. United Kingdom - The Computer Misuse Act of 1990¹¹⁰⁶

The first offence created by this Act is the "usage of a computer to secure

¹¹⁰⁴ S 342.2.

¹¹⁰⁵ S 430(1.1). A maximum term of 10 years' imprisonment can be imposed upon anyone found guilty of this offence. S 430(5).

¹¹⁰⁶ Act 18/1990. A copy can be downloaded from www.legislation.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_2.htm#mdiv1.

unauthorised access to programs or data".¹¹⁰⁷ Section 1(1) provides that a person is guilty of this offence where -

- "(a) he causes a computer to perform any function with intent *to secure access to any program or data held in any computer*;
- (b) the access he intends to secure is unauthorised; and
- (c) he knows at the time when he causes the computer to perform the function that that is the case."

The Act further provides that *a person secures access to any program or data held in a computer* (which includes any program or data held in any removable storage medium which is for the time being in the computer) if by causing a computer to perform any function he -

- "(a) alters or erases the program or data;
- (b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;
- (c) uses it [which means the function he causes the computer to perform (a) causes the program to be executed; or (b) is itself a function of the program]; or
- (d) has it output from the computer in which it is held (whether by having it displayed or in any other manner)."¹¹⁰⁸

Access to any program or data held in a computer is unauthorised where the *hacker* (a) is not entitled to control access of the kind in question to the program or data *and* (b) does not have consent to access of the kind in question to the program or data from any person who is so entitled.¹¹⁰⁹ In *R v Bow Street Magistrates Court and Allison, Ex Parte Government of the United States of America*¹¹¹⁰ the House of Lords maintained that the word "control" in this context clearly means authorised.¹¹¹¹ It remarked further

¹¹⁰⁷ Van der Merwe 2000:178 maintains that this is the "basic hacking offence". See also Anonymous 2001(s).

¹¹⁰⁸ S 17(2), (3) & (6).

¹¹⁰⁹ S 17(5). Put otherwise, the Act identifies "two ways in which authority may be acquired - by being oneself the person entitled to authorise and by being a person who has been authorised by a person entitled to authorise": *R v Bow Street Magistrates Court and Allison, Ex Parte Government of the United States of America* 1999 4 ALL ER 1 HL:7f-g, par 25.

¹¹¹⁰ 1999 4 ALL ER 1 HL. A copy of this judgment can also be downloaded from www.bailii.org/cgi-bailii/disp.pl/uk/cases/UKHL/1999/31.html?query=~+hacker.

¹¹¹¹ 1999 4 ALL ER 1 HL:7e; par 24. It also maintained (at 8g-h; par 28) that "control" should not be interpreted as authorisation to cause the computer to function and that access to a program should likewise not be interpreted as access to a computer at a particular level. The court maintained (at 9a;

that where A has authorised access to one piece of data and he accesses other data, which he is not allowed to access (even if the other data is of the same kind), the latter access will constitute unauthorised access.¹¹¹² Likewise, where A has authority to view data, he will act in contravention of section 1(1) where he copies or alters that data.¹¹¹³ "The refinement of the concept of access requires a refinement of the concept of authorisation. The authorisation must be authority to secure access of the kind in question."¹¹¹⁴ Therefore the Act applies to both external as well as internal *hackers* (employees abusing/manipulating their position) who obtain unauthorised access.¹¹¹⁵

Section 1(1) notably criminalises instances where someone intentionally attempts to 1) use that computer or another computer,¹¹¹⁶ or 2) delete or modify data, or 3) copy or view electronic data. This is observed from the fact that only an intent to cause the above is required.¹¹¹⁷ The South African Law Commission (SALC) maintains that "this offence can be committed in a number of ways such as unauthorised use of a person's password, trying to guess a password or installing a program that will obtain a person's password without his or her knowledge."¹¹¹⁸ It is further submitted that where a computer user employs a computer program to do the above-mentioned acts, his conduct falls within the scope of this offence.

Section 1 further stipulates that the intent a person is required to have to commit such an offence need not be directed at -

- "(a) any particular program or data;
- (b) a program or data of any particular kind; or

par 30) that s 1 is only concerned with authority to access the actual data involved, and does not deal with access to different kinds of data.

¹¹¹² 1999 4 ALL ER 1 HL:7g-h; par 25.

¹¹¹³ 1999 4 ALL ER 1 HL:7f-g; par 25.

¹¹¹⁴ 1999 4 ALL ER 1 HL:7d; par 24.

¹¹¹⁵ See *R v Bow Street Magistrates Court and Allison, Ex Parte Government of the United States of America* 1999 4 ALL ER 1 HL:9j-10b; par 33 & 34.

¹¹¹⁶ In *Attorney General's Reference* (No1 of 1991) 1992 3 ALL ER 897 CA the Court of Appeal maintained (at 901d *et seq*) that the phrase "he causes a computer to perform any function with intent to secure access to any program or data held in any computer" entails two scenarios: a) where X uses one computer to gain access to another computer and b) where the data to which he gains access is located on the same computer that he accessed and used, without authorisation.

¹¹¹⁷ *R v Bow Street Magistrates Court and Allison, Ex Parte Government of the United States of America* 1999 4 ALL ER 1 HL:9a-b; par 30; Anonymous 2001(u).

¹¹¹⁸ SALC's Discussion Paper 99:26. See also Anonymous 2001(s); Anonymous 2001(u).

(c) a program or data held in any particular computer.”¹¹¹⁹

In other words, mere “sniffing” constitutes an offence in terms of section 1(1), without the crown having to prove that the alleged *hacker* knew where the computer was located or what information was stored on this particular computer or to whom the computer belonged or in whose control it was. The section further imposes a maximum term of imprisonment of six months, or a fine not exceeding £2 000, or to both.¹¹²⁰

The second offence created is the “unauthorised access with the intent to commit a further offence”.¹¹²¹ Section 2 stipulates that anyone is guilty of this offence where he commits the above-mentioned offence (unauthorised access or attempted unauthorised access) with the intent to -

- a) commit an offence for which the sentence is fixed by law [e.g. murder] or for which a first offender over 21 years of age may be sentenced to imprisonment for a term of 5 years [e.g. theft, blackmail, obtaining property or services by deception]; or
- b) facilitate the commission of such an offence whether by himself or by any other person,

and it is irrelevant whether the commission of the “further” offence is impossible,¹¹²² for example where there is no information stored on the computer accessed that can be used for blackmailing someone.¹¹²³ Furthermore, it is immaterial “whether the further offence is to be committed on the same occasion as the unauthorised access offence or on any future occasion.”¹¹²⁴

Three examples of this offence are (1) where someone engages in persistent hacking¹¹²⁵ or (2) where a *hacker* gains (or attempts to gain) access to a bank’s computer system with the intent to transfer funds from a third party’s account into his own or (3) where a *hacker* gains (or attempts to gain) access with the intent to obtain

¹¹¹⁹ S 1(2).

¹¹²⁰ S 1(3).

¹¹²¹ S 2(1). This offence is generally known as the “ulterior hacking offence”. See Anonymous 2001(t); Van der Merwe 2000:179.

¹¹²² S 2(1), (2) & (4). See also Anonymous 2001(t).

¹¹²³ Anonymous 2001(t).

¹¹²⁴ S 2(3). S 2(5) states that in the case of a summary conviction the *hacker* may be sentenced in the magistrate’s court to imprisonment not exceeding six months or to a fine not exceeding the statutory maximum or to both; or in the case of a trial upon indictment in the Crown court the *hacker* may be sentenced to imprisonment not exceeding five years or to a fine, or both.

¹¹²⁵ Anonymous 2001(r).

confidential and personal information in order to commit blackmail.¹¹²⁶ Where the accused is found guilty of this offence, a maximum imprisonment of five years or a fine or both can be imposed upon him.¹¹²⁷

The third offence established by this Act is the offence of "unauthorised modification of computer material". Section 3 provides that a person is guilty of this offence where a) he does any act which causes an unauthorised modification of the contents of any computer and b) at the time when he does the act he has the required intent and the required knowledge.¹¹²⁸ The Act provides that the contents of a computer are modified where (a) any program or data held in the computer concerned is altered or erased or (b) any program or data is added to its contents.¹¹²⁹ The required intent is an intent to cause an unauthorised modification, permanently or temporarily, of the contents of any computer and by so doing -

- "(a) to impair the operation of any computer;
- (b) to prevent or hinder access to any program or data held in any computer; or
- (c) to impair the operation of any such program or the reliability of any such data."¹¹³⁰

The SALC correctly observes that the Act sets two elements for the perpetrator's intent namely "to cause the unauthorised modification and for that modification to have certain consequences."¹¹³¹

Identical to the above-mentioned offences, the intent need not be directed at any particular computer, program or data or any particular modification.¹¹³² This section carries the same maximum penalty as section 2.¹¹³³

The SALC correctly notes that the intent, as described in this section, indicates *dolus indeterminatus*:

"this formulation can be applied, for example, to a case where a person develops a virus program which is distributed indiscriminately via the e-mail or the Internet."¹¹³⁴

¹¹²⁶ Anonymous 2001(u).

¹¹²⁷ S 2(5).

¹¹²⁸ S 3(1).

¹¹²⁹ S 17(7).

¹¹³⁰ S 3(2), (4) & (5).

¹¹³¹ SALC's Discussion Paper 99:40.

¹¹³² S 3(3).

¹¹³³ S 3(7).

¹¹³⁴ SALC's Discussion Paper 99:40.

It follows that the third offence created is aimed, in addition to *hackers* causing the above-mentioned, at people disseminating malicious computer programs such as virus, worms and Trojan Horses that actually cause damage.¹¹³⁵ The Act penalises all distributions of malicious computer programs and it is irrelevant that the perpetrator had no idea which computers would be effected by the computer program.¹¹³⁶ Note also that where a *hacker* changes a password that allows access to a computer system or where he changes information (such as a patient's prescription), he is guilty of this offence.¹¹³⁷ This section also encompasses instances where a *hacker* defaces a web page by either adding content or text to the web page or by deleting the original content.

Finally, the Act provides that where an accused is charged with contravening sections 2 or 3 and he is found not guilty in terms of those sections, he may be held guilty in terms of section 1 "if on the facts shown he could have been found guilty of that offence in proceedings for that offence brought".¹¹³⁸

In conclusion, it should be pointed out that the UK Act does not criminalise the following conduct: a) interference with the operations of a computer such as denial-of-service attacks; b) the creation of malicious computer programs and hackers' tools; c) trafficking, disseminating and making passwords and hackers' tools available for downloading; d) spreading virus hoaxes; e) receiving stolen [copied] data or programs knowing that such data or programs were illegally obtained; f) where a *hacker* spoofs his own e-mail (or Internet) address; g) an unsuccessful attempt to cause a modification of electronic data or an insertion of data by means of a computer program; h) instructing and/or assisting *hackers* and i) soliciting Internet users to download hackers' tools and to employ them.

2.4. Singapore Computer Misuse Act

The *Singapore Computer Misuse Act*¹¹³⁹ (Chapter 50A) of 1998 corresponds to a large extent with the *UK Computer Misuse Act* in that it also contains the offences of

¹¹³⁵ Anonymous 2001(u); Van der Merwe 2000:179-180; Akdemiz 1996; Nel 1990:34.

¹¹³⁶ Nel 1990:36.

¹¹³⁷ Anonymous 2001(t).

¹¹³⁸ S 12(1).

¹¹³⁹ A copy of this Act can be downloaded from www.lawnet.com.sg/freeaccess/CMA.htm.

“unauthorised access to computer material”,¹¹⁴⁰ “unauthorised access with intent to commit or facilitate commission of further offences”¹¹⁴¹ and “unauthorised modification of computer material.”¹¹⁴² However, the Singapore Act contains a further offence namely “unauthorised use or interception of computer service”. Section 6(1) stipulates that:

“Subject to subsection (2), any person who knowingly -

(a) secures access without authority to any computer for the purpose of obtaining, directly or indirectly, any computer service;

(b) intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer by means of an electromagnetic, acoustic, mechanical or other device; or

(c) uses or causes to be used, directly or indirectly, the computer or any other device for the purpose of committing an offence under paragraph (a) or (b),

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$2,000 or to imprisonment for a term not exceeding 2 years or to both.”

This section is clearly based on the Canadian *Criminal Code* and therefore the comment levied against the corresponding section in the latter Act applies with equal force.

2.5. The Netherlands

The Dutch law is an example of an EU member country regulating computer-related crimes. The Dutch *Wetboek van Strafrecht* (hereafter referred to as the *Criminal Code*)

¹¹⁴⁰ S 3(1) provides that: “Subject to subsection (2), any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$2,000 or to imprisonment for a term not exceeding 2 years or to both.”

¹¹⁴¹ S 4(1) provides that: “Any person who causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer with intent to commit an offence to which this section applies shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$50,000 or to imprisonment for a term not exceeding 10 years or to both.”

¹¹⁴² S 5(1) provides that: “Subject to subsection (2), any person who does any act which he knows will cause an unauthorised modification of the contents of any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$2,000 or to imprisonment for a term not exceeding 2 years or to both.”

provides for the offence, called "computervredebreuk"¹¹⁴³ (literally translated: disturbance of the peace by means of a computer), committed under the following circumstances:

The intentional and unlawful intrusion/penetration of a computer whenever someone -

- a) penetrates any security measure; or
- b) gains access by means of one technical intervention, with the help of false signals or one false password by taking up a false identity/capacity

which is punishable by a fine or a maximum imprisonment of six months.¹¹⁴⁴

In other words, unauthorised access constitutes an offence only whenever a security measure is penetrated/circumvented by whatever means. Therefore, where a *hacker* gains access to a home computer that has no security measures such as a firewall, he commits no offence.

Whenever someone exceeds his access authority; he is punishable by a fine or a maximum of four years imprisonment.¹¹⁴⁵

Where someone penetrates a computer's security system by the intervention of a public communication network [i.e. the Internet], if the perpetrator -

- a) uses the processing capacity of a computer with the aim to unlawfully enrich himself; or
- b) by means of the intervention of a computer, which he has penetrated, gains access to a computer of a third party,

¹¹⁴³ This offence is included in the Second Book, title V "Misdrijven tegen het openbaar orden" (translated: offences against the public order).

¹¹⁴⁴ S 138a(1) provides that: "Met gevangenisstraf van ten hoogste zes maanden of geldboete van de derde categorie wordt, als schuldig aan computervredebreuk, gestraft hij die opzettelijk wederrechtelijk binnendringt in een geautomatiseerd werk voor de opslag of verwerking van gegevens, of in een deel daarvan, indien hij a. daarbij enige beveiliging doorbreekt of b. de toegang verwerft door een technische ingreep, met behulp van valse signalen of een valse sleutel dan wel door het aannemen van een valse hoedanigheid." S 80 provides that: "Onder geautomatiseerd werk wordt verstaan een inrichting die bestemd is om langs elektronische weg gegevens op te slaan en te verwerken." Thus a computer.

¹¹⁴⁵ S 138a(2) provides that: "Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervredebreuk, indien de dader vervolgens gegevens die zijn opgeslagen in een geautomatiseerd werk waarin hij zich wederrechtelijk bevindt, overneemt en voor zichzelf of een ander vastlegt."

he is punishable by a fine or a maximum of four years imprisonment.¹¹⁴⁶

This offence penalises the copying of confidential information for the purposes of selling or using such information as well as instances where a *hacker* "hacks" into computer A and by means of this computer gains access to computer B.

Furthermore, the *Criminal Code* provides that:

☐ Anyone who intentionally and unlawfully deletes, copies or alters or makes data inaccessible or unusable by means of a computer is punishable by a fine or a maximum of two years imprisonment.¹¹⁴⁷

This clearly covers both instances where a *hacker* commits these acts by means of his computer as well as where he utilises malicious computer programs, resulting in loss or alteration of data or causing the hard disk or computer to be inaccessible or copying electronic data. It also encompasses instances where a *hacker* defaces a web page by deleting information or replacing the original content with his own content. Note that this provision also encompasses interference with computer systems for instance by means of denial-of-service attacks.

☐ Anyone who by means of a public communications network unlawfully penetrates a computer and causes serious damage in regard to the information stored on the computer, is punishable by a fine or a maximum of four years imprisonment.¹¹⁴⁸

This is a reiteration of the above-mentioned provision, namely penalising *hackers* who delete, corrupt or modify information or render it inaccessible.

¹¹⁴⁶ S 138a(3) stipulates that: "Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervredebreuk gepleegd door tussenkomst van de een openbaar telecommunicatienetwerk, indien de dader vervolgens; a. met het oogmerk zich wederrechtelijk te bevoordelen gebruik maakt van verwerkingscapaciteit van een geautomatiseerd werk; b. door tussenkomst van het geautomatiseerd werk waarin hij is binnengedrongen de toegang verwerft tot het geautomatiseerd werk van een derde."

¹¹⁴⁷ S 350a(1) states that: "Hij die opzettelijk en wederrechtelijk gegevens die door middel van een geautomatiseerd werk zijn opgeslagen, worden verwerkt of overgedragen, verandert, wist, onbruikbaar of ontoegankelijk maakt, dan wel andere gegevens daaraan toevoegt, wordt gestraft met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie."

¹¹⁴⁸ S 350a(2) provides that: "Hij die het feit, bedoeld in het eerste lid, pleegt na door tussenkomst van een openbaar telecommunicatienetwerk, wederrechtelijk in een geautomatiseerd werk te zijn binnengedrongen en daar ernstige schade met betrekking tot die gegevens veroorzaakt, wordt gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie."

□ Anyone who intentionally and unlawfully causes information to be available or distributed with the intent to cause losses by copying such information, is punishable by a fine or a maximum of four years imprisonment.¹¹⁴⁹ However, anyone that commits this offence with the aim to limit someone else's loss, is not guilty of this offence.¹¹⁵⁰

In other words, the provision penalises instances where a *hacker* copied confidential information and subsequently forwarded this information to other Internet users or made it available to third parties by uploading it to a web site where anyone could download and/or see the information. It can be argued that "information" includes, in this context, trafficking in illegally obtained passwords. Note that the accused must have the intent to cause losses by his conduct.

In conclusion it should be noted that the Dutch *Criminal Code* fails to penalise a) the creation and/or dissemination of malicious computer programs and hackers' tools; b) creating false virus hoaxes; c) gaining access to any computer that does not have security measures; d) memorising or writing down confidential information without making an electronic copy; e) inserting information (for instance where a *hacker* defaces a web page by the addition of text or content); f) where a third party receives copied data knowingly that such data was illegally obtained; g) attempted computer-related crimes; h) instructing or assisting hackers; and i) soliciting third party computer users to download and employ hackers' tools.

2.6. EU Convention on Cybercrime

One of the most recent developments concerning Internet related commercial crimes is the *Convention on Cybercrime*¹¹⁵¹ adopted by the *European Committee of Ministers of the Council of Europe* in November 2001. One of the purposes of this treaty is to ensure uniform legislation in the member-countries, criminalising a common minimum

¹¹⁴⁹ S 350a(3) provides that: "Hij die opzettelijk en wederrechtelijk gegevens ter beschikking stelt of verspreidt die bedoeld zijn om schade aan te richten door zichzelf te vermenigvuldigen in een geautomatiseerd werk, wordt gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie."

¹¹⁵⁰ S 350a(4) provides that: "Niet strafbaar is degen die het feit, bedoeld in het derde lid, pleegt met het oogmerk om schade als gevolg van deze gegevens te beperken."

¹¹⁵¹ A copy of this document can be downloaded from <http://conventions.coe.int/treaty/EN/projets/FinalCyberCrime.htm>. The first *Draft Convention on Cybercrime* was issued in April 2000 and the final version in June 2001.

standard of relevant offences:¹¹⁵² "This kind of harmonisation alleviates the fight against such crimes on the national and on the international level as well."¹¹⁵³

The provisions of the Convention can be divided into three categories: the first category deals with the proposed offences; the second category deals with procedural law aspects and the third category deals with international co-operation. The latter two categories are of no relevance to this dissertation. In November 2001 the *Explanatory Report*¹¹⁵⁴ was published to explain the provisions of the Convention.¹¹⁵⁵ The following offences are established by the Convention:

Offences against the confidentiality, integrity and availability of computer data and systems:

Under this heading, the Convention introduces five offences, which all parties to the convention must criminalise:

a) Illegal access: the intentional access¹¹⁵⁶ to the whole or any part of a computer system¹¹⁵⁷ without right¹¹⁵⁸ (therefore unauthorised).¹¹⁵⁹ Moreover, a "Party may

¹¹⁵² *Explanatory Report*: para 16 & 33.

¹¹⁵³ *Explanatory Report*: par 33.

¹¹⁵⁴ A copy can be downloaded from <http://conventions.coe.int/treaty/EN/projets/FinalCyberRapex.htm>.

¹¹⁵⁵ The *Explanatory Report* maintains (at par II) that "[t]he text of this explanatory report does not constitute an instrument providing an authoritative interpretation of the Convention, although it might be of such a nature as to facilitate the application of the provisions contained therein."

¹¹⁵⁶ According to the *Explanatory Report* "access" comprises "the entering of the whole or any part of a computer system (hardware, components, stored data of the system installed, directories, traffic and content-related data). However, it does not include the mere sending of an e-mail message or file to that system. 'Access' includes the entering of another computer system, where it is connected via public telecommunication networks, or to a computer system on the same network, such as a LAN (local area network) or Intranet within an organisation. The method of communication (e.g. from a distance, including via wireless links or at a close range) does not matter." (At par 46).

¹¹⁵⁷ According to the Convention "computer system" means "any device or a group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data". Article 1(a).

¹¹⁵⁸ The *Explanatory Report* stipulates (at par 38) that the expression "without right" refers to "conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences)." The *Explanatory Report* continues to state (at par 47-48) that "there is no criminalisation of the access authorised by the owner or other right holder of the system or part of it (such as for the purpose of

require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.”¹¹⁶⁰

This provision, therefore, criminalises mere unauthorised intrusion and consequently covers the “basic offence of dangerous threats to and attacks against the security (i.e. the confidentiality, integrity and availability) of computer systems and data.”¹¹⁶¹ The last stipulation enunciates that a member-state may pose additional requirements for the commission of the offence. For instance, a member-state may provide that this offence can only be committed *via* the Internet and does not include instances where someone physically accesses the computer without authorisation.¹¹⁶²

b) Illegal interception: the intentional unauthorised “interception ... made by technical means, of non-public¹¹⁶³ transmissions of computer data¹¹⁶⁴ to, from or within a

authorised testing or protection of the computer system concerned). Moreover, there is no criminalisation for accessing a computer system that permits free and open access by the public, as such access is ‘with right.’ ... The application of specific technical tools may result in an access under Article 2, such as the access of a web page, directly or through hypertext links, including deep-links or the application of ‘cookies’ or ‘bots’ to locate and retrieve information on behalf of communication. The application of such tools *per se* is not ‘without right’. The maintenance of a public web site implies consent by the web site-owner that it can be accessed by any other web-user. The application of standard tools provided for in the commonly applied communication protocols and programs, is not in itself ‘without right.’”

¹¹⁵⁹ Article 2.

¹¹⁶⁰ Article 2.

¹¹⁶¹ *Explanatory Report*, par 44. According to the *Explanatory Report* “[t]he mere unauthorised intrusion, i.e. ‘hacking’, ‘cracking’ or ‘computer trespass’ should in principle be illegal in itself. It may lead to impediments to legitimate users of systems and data and may cause alteration or destruction with high costs for reconstruction. Such intrusions may give access to confidential data (including passwords, information about the targeted system) and secrets, to the use of the system without payment or even encourage hackers to commit more dangerous forms of computer-related offences, like computer-related fraud or forgery.” (At par 44).

¹¹⁶² *Explanatory Report* states (at par 50) that “[t]he last option allows Parties to exclude the situation where a person physically accesses a stand-alone computer without any use of another computer system.”

¹¹⁶³ According to the *Explanatory Report*, the term “non-public” qualifies the nature of the transmission (communication) process and not the nature of the data transmitted: “The data communicated may be publicly available information, but the parties wish to communicate confidentially. Or data may be kept secret for commercial purposes until the service is paid ... Communications of employees, whether or not for business purposes, which constitute ‘non-public transmissions of computer data’ are also protected against interception without right under Article 3”. (At par 42).

computer system,¹¹⁶⁵ including electromagnetic emissions from a computer system carrying such computer data.”¹¹⁶⁶ A member-state may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.¹¹⁶⁷

This provision “aims to protect the right of privacy of data communication.”¹¹⁶⁸ It applies to all forms of electronic data transfer, whether by telephone, fax, e-mail or file transfer.¹¹⁶⁹ The *Explanatory Report* explains the phrase “interception by technical means” as follows:

“Interception by ‘technical means’ relates to listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices. Interception may also involve recording. Technical means includes technical devices fixed to transmission lines as well as devices to collect and record wireless communications. They may include the use of software, passwords and codes. The requirement of using technical means is a restrictive qualification to avoid over-criminalisation.”¹¹⁷⁰

Therefore this provision encompasses both the monitoring as well as interception of electronic communications. It also covers instances where a computer user intercepts electronic communications by means of a physical device or by means of a computer program. It further transpires from the *Explanatory Report* that this provision is also intended to encompass instances where a *hacker* accesses a computer and obtains data without authorisation.

c) Data interference: the intentional and unauthorised damaging, deletion,

¹¹⁶⁴ According to the Convention, “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 1(b).

¹¹⁶⁵ The *Explanatory Report* elaborates (at par 55) upon this provision: “The communication in the form of transmission of computer data can take place inside a single computer system (flowing from CPU to screen or printer, for example), between two computer systems belonging to the same person, two computers communicating with one another, or a computer and a person (e.g. through the keyboard).”

¹¹⁶⁶ Article 3.

¹¹⁶⁷ Article 3.

¹¹⁶⁸ *Explanatory Report*: par 51.

¹¹⁶⁹ *Explanatory Report*: par 51.

¹¹⁷⁰ *Explanatory Report*: par 53.

deterioration, alteration or suppression of computer data.¹¹⁷¹ A member-state may pose the requirement that such conduct must cause serious harm.¹¹⁷² The *Explanatory Report* notes that member-states may provide that "alteration" includes "spoofing" activities.¹¹⁷³ Furthermore, the *Explanatory Report* maintains that modifications of traffic data for the purpose of facilitating legitimate anonymous communications or to ensure secure communications (e.g. encryption) "should in principle be considered a legitimate protection of privacy".¹¹⁷⁴ Anonymous communications refers, for instance, to web sites such as www.safeweb.com.

This provision, therefore, protects "the integrity and the proper functioning or use of stored computer data or computer programs."¹¹⁷⁵ The *Explanatory Report* notes that "alteration" not only includes the modification of data, but also the "input of malicious codes, such as viruses and Trojan horses".¹¹⁷⁶ Furthermore, the *Explanatory Report* stipulates that "[s]uppressing of computer data means any action that prevents or terminates the availability of the data to the person who has access to the computer or the data carrier on which it was stored."¹¹⁷⁷ Therefore, this provision encompasses denial-of-service attacks as well as e-mail bomb attacks. Furthermore, not only does it cover the deletion and modification of electronic data by *hackers* as well as malicious computer programs, but also the defacement of web page where the *hacker* suppresses or deletes the electronic content.

- d) System interference: the intentional, unauthorised and serious "hindering ... of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data."¹¹⁷⁸

The *Explanatory Report* provides that this provision protects the ability of a computer to function properly.¹¹⁷⁹ Each member-state determines what type of

¹¹⁷¹ Article 4.

¹¹⁷² Article 4.

¹¹⁷³ Par 62.

¹¹⁷⁴ *Explanatory Report*:par 62.

¹¹⁷⁵ *Explanatory Report*:par 60.

¹¹⁷⁶ Par 61.

¹¹⁷⁷ *Explanatory Report*:par 61.

¹¹⁷⁸ Article 5.

¹¹⁷⁹ *Explanatory Report*:par 65 & 66. It also refers to this type of computer abuse as "computer sabotage". See par 65.

hindering is considered as serious enough to fall within the scope of this provision.¹¹⁸⁰ This provision refers, it is submitted, to instances where sinister computer users render a computer (system) inoperable or virtually inoperable/inaccessible by for instance launching a denial-of-service attack or an e-mail bomb attack against the complainant's computer system; where a virus seriously interferes with the operation of a computer system, such conduct is also included:

"The drafters considered as 'serious' the sending of data to a particular system in such a form, size or frequency that it has a significant detrimental effect on the ability of the owner or operator to use the system, or to communicate with other systems (e.g., by means of programs that generate 'denial of service' attacks, malicious codes such as viruses that prevent or substantially slow the operation of the system, or programs that send huge quantities of electronic mail to a recipient in order to block the communications functions of the system.)"¹¹⁸¹

e) Cracking devices: the intentional and unauthorised -

"a) production, sale, procurement for use, import, distribution or otherwise making available of:

1) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Article 2 - 5;

2) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed

with intent that it be used for the purpose of committing the offences established in Articles 2 - 5;

b) the possession of an item referred to in paragraphs (a)(1) and (2) above, with intent that it be used for the purpose of committing the offenses established in Articles 2 - 5. A party may require by law that a number of such items be possessed before criminal liability attaches."¹¹⁸²

The Convention provides that where such production, sale, procurement for use, import, distribution, making available or possession is for the purpose of

¹¹⁸⁰ *Explanatory Report*:par 67.

¹¹⁸¹ *Explanatory Report*:par 67.

¹¹⁸² Article 6(1). The number of "items" possessed would bear directly upon the criminal intent of the accused. See *Explanatory Report* :par 75.

authorised testing or protection of a computer system, no crime is committed.¹¹⁸³

The *Explanatory Report* explains the terms “distribution” and “making available” as follows: “ ‘Distribution’ refers to the active act of forwarding data to others, while ‘making available’ refers to the placing online devices for the use of others. This term also intends to cover the creation or compilation of hyperlinks in order to facilitate access to such devices.”¹¹⁸⁴ In other words, if A puts a hyperlink on his web page that transfers a computer user to another web page where he can download these hackers’ tools or copy illegally obtained passwords, A commits an offence.

The *Explanatory Report* also provides that “computer program” refers to “programs that are for example designed to alter or even destroy data or interfere with the operation of systems, such as virus programs, or programs designed or adapted to gain access to computer systems.”¹¹⁸⁵ Hence hackers’ tools, including password sniffers. This provision, therefore, criminalises the trafficking in as well as possession of illegally obtained passwords or hackers’ tools¹¹⁸⁶ that allow the possessor to gain access to a computer system, to interfere with the functioning of a computer system, to monitor communications, to delete files or to render a computer (or data stored on such computer) inoperable or inaccessible.¹¹⁸⁷ This provision therefore criminalises the creation of hackers’ tools and malicious computer programs by providing that the mere possession of these programs constitute an offence. Furthermore, the Convention criminalises the soliciting of computer users to download these programs by providing that the making available of these programs constitutes an offence. The soliciting aspect will, of course, bear upon the sentence of the cyber-abuser.

¹¹⁸³ Article 6(2).

¹¹⁸⁴ *Explanatory Report*: par 72.

¹¹⁸⁵ *Explanatory Report*: par 72.

¹¹⁸⁶ According to the *Explanatory Report*, the court would have to determine objectively whether the computer program constitutes a hackers’ tool: “the Convention restricts its scope to cases where the devices are objectively designed, or adapted, primarily for the purpose of committing an offence.” (At par 73).

¹¹⁸⁷ The *Explanatory Report* states (at par 71) that “[a]s the commission of these offences often requires the possession of means of access (‘hacker tools’) or other tools, there is a strong incentive to acquire them for criminal purposes which may then lead to the creation of a kind of black market in their production and distribution. To combat such dangers more effectively, the criminal law should prohibit

Finally it should be mentioned that the requirement posed in (a) and (b) namely that the accused must traffic in, or possess, hackers' tools or illegally obtained passwords with the intent that it be used for criminal purposes ensures that where "devices are produced and put on the market for legitimate purposes, e.g. to counter-attacks against computer systems", such conduct does not fall within the scope of the prohibition.¹¹⁸⁸

Computer-related offences

Under this heading, the Convention introduces two offences which all member-states must criminalise – they are specific forms of manipulation of computer systems or computer data:¹¹⁸⁹

- (1) Computer-related forgery: the intentional and unauthorised "input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible."¹¹⁹⁰ A member-state may require by law an intent to defraud, or similar dishonest intent, before criminal liability attaches.¹¹⁹¹

The *Explanatory Report* states that the purpose of this provision is "to create a parallel offence to the forgery of tangible documents."¹¹⁹² It further explains this provision as follows:

"Computer-related forgery involves unauthorised creating or altering stored data so that they acquire a different evidentiary value and the course of legal transactions, which relies on the authenticity of information contained in the data, is subject to a deception. The protected legal interest is the security and reliability of electronic data which may have consequences for legal relations ... The unauthorised 'input' of correct or incorrect data brings about a situation that corresponds to the making of a false document. Subsequent alterations (modifications, variations, partial changes),

specific potentially dangerous acts at the source, preceding the commission of offences under Articles 2 – 5."

¹¹⁸⁸ *Explanatory Report*:par 76.

¹¹⁸⁹ See the *Explanatory Report*:par 80.

¹¹⁹⁰ Article 7.

¹¹⁹¹ Article 7.

¹¹⁹² Par 81.

deletions (removal of data from a data medium) and suppression (holding back, concealment of data) correspond in general to the falsification of a genuine document ... The term 'for legal purposes' refers also to legal transactions and documents which are legally relevant."¹¹⁹³

In other words, this provision criminalises, for example, instances where a *hacker* gains access to a bank's computer system and transfers money from or to accounts or creates fictitious accounts. This provision also encompasses instances where a computer user modifies his examination results by means of a computer.

(2) Computer-related fraud: the intentional and unauthorised causing of a loss of property to another by -

A) any input, alteration, deletion or suppression of computer data; or

B) any interference with the functioning of a computer or system,

with the fraudulent and dishonest intent of procuring an economic benefit for oneself or for another.¹¹⁹⁴ A member-state may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.¹¹⁹⁵

This provision refers to online fraud.¹¹⁹⁶ The aim of this provision is to "criminalise any undue manipulation in the course of data processing with the intention to effect an illegal transfer of property."¹¹⁹⁷ The *Explanatory Report* stipulates that "loss of property" includes the loss of money, tangibles and intangibles with an economic value.¹¹⁹⁸ Therefore, this provision refers to instances enumerated under (1) [computer-related forgery] as well as instances where a competitor penetrates A's computer system and destroys electronic data.

Content-related offences: these offences refer to child pornography and copyright infringements, which are of no relevance for purposes of this dissertation.¹¹⁹⁹

The Convention also makes provision for other criminal aspects. The intentional aiding

¹¹⁹³ *Explanatory Report*: para 81-84.

¹¹⁹⁴ Article 8.

¹¹⁹⁵ Article 8.

¹¹⁹⁶ *Explanatory Report*: para 86 & 88.

¹¹⁹⁷ *Explanatory Report*: par 86.

¹¹⁹⁸ *Explanatory Report*: par 88.

¹¹⁹⁹ See article 9.

or abetting the commission of any of the above-mentioned offences, with the intent that such offence be committed, constitutes an offence.¹²⁰⁰ Furthermore, the intentional attempt to commit any of the the above-mentioned offences, except those enunciated in article 6 (cracking devices) constitutes an offence.¹²⁰¹

Consequently, where A sends B a malicious computer program and B discovers the program before it causes any damage or where A releases a virus onto the Internet but it is defective and cannot cause any damage, his conduct is penalised as an attempt to commit a computer-related crime. The same principles apply where someone launches an unsuccessful denial-of-service attack. As noted, the person aiding or abetting the perpetrator must also have the objective to commit the crime. This ensures that ISPs are not guilty of this offence where their services are used as a conduit to assist the transmission of harmful data or malicious code.¹²⁰²

The Convention, in addition, makes provision for vicarious liability by providing that each member-state is obliged to adopt the necessary legislation to ensure that a "legal person can be held liable for a criminal offence established in accordance with this Convention, committed for its benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on:

- a. a power of representation of the legal person;
- b. an authority to take decisions on behalf of the legal person;
- c. an authority to exercise control within the legal person."¹²⁰³

This, more or less, refers to instances where directors and managers commit the above-mentioned offences.¹²⁰⁴ Furthermore, the Convention obliges member-states to

¹²⁰⁰ Article 11(1).

¹²⁰¹ Article 11(2). Note, however, that the Convention states that member-states may reserve the right not to criminalise attempts, or certain attempts, of the above-mentioned offences: Article 11(3).

¹²⁰² *Explanatory Report*:par 119. Consequently, ISPs do not have to actively monitor content to avoid criminal liability under this provision. See par 119.

¹²⁰³ Article 12(1).

¹²⁰⁴ See *Explanatory Report*:par 124. The *Explanatory Report* states (at par 124) that "four conditions need to be met for liability to attach. First, one of the offences described in the Convention must have been committed. Second, the offence must have been committed for the benefit of the legal person. Third, a person who has a leading position must have committed the offence (including aiding and abetting) ... Fourth, the person who has a leading position must have acted on the basis of one of these powers - a power of representation or an authority to take decisions or to exercise control - which

ensure that legal persons can also “be held liable where the lack of supervision or control by a natural person referred to [above] has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person under its authority.”¹²⁰⁵ This provision aims to render a legal person liable where a computer-related crime is committed by an individual, such as an employee or agent, under a director’s supervision, due to the latter’s “failure to take appropriate and reasonable measures to prevent employees or agents from committing criminal activities on behalf of the legal person.”¹²⁰⁶ It follows that the legal person is not liable for crimes committed by its customers or any other third person, seeing that they are not under its control.¹²⁰⁷ Finally, the Convention stipulates that the legal person’s liability does not affect the liability of the natural person who committed the crime.¹²⁰⁸

Conclusion

In conclusion it may be stated that this convention is the most comprehensive document on cyber-crime in existence. However, it fails to criminalise the following forms of conduct: a) the dissemination of virus hoaxes; b) the defacement of web pages by adding electronic content or information and c) receiving electronic content (e.g. data) from someone (the *hacker*) knowing that such content was illegally obtained.

demonstrate that such a physical person acted within the scope of his or her authority to engage the liability of the legal person.”

¹²⁰⁵ Article 12(2).

¹²⁰⁶ *Explanatory Report*: para 123 & 125. The *Explanatory Report* further states (at par 125) that “[s]uch appropriate and reasonable measures could be determined by various factors, such as the type of the business, its size, the standards or the established business best practices, etc. This should not be interpreted as requiring a general surveillance regime over employee communications”.

¹²⁰⁷ *Explanatory Report*: par 125.

¹²⁰⁸ Article 12(4).

CHAPTER EIGHT

PROPOSALS FOR AMENDING SOUTH AFRICAN CRIMINAL LAW

1. ACTIVITIES TO BE CRIMINALISED

In chapter six it was contended that should South African courts be willing to interpret the requirements of certain common law offences generously and furthermore be willing to apply these principles to computer-related conduct, then virtually all cyber-crime activities will fall within the definitions of common law offences, as discussed in that chapter. Should South African courts, however, be unwilling to extend the application of common law offences to cyber-crime activities, the following thirteen "transgressions" have to be criminalised, by means of legislation, in order to encompass the activities of *hackers* and computer programmers who write malicious programs and hackers' tools, namely:

1. Mere unauthorised access to a computer or any data stored on a computer. (This may be called *electronic trespassing*.¹²⁰⁹)
2. Unauthorised access to a computer and thereby -
 - a) rendering the computer or the information stored on the computer inaccessible or unusable;¹²¹⁰
 - b) manipulating information stored on a computer. (This would criminalise the unlawful alteration, deletion or corruption of electronic content stored on a computer as well as the insertion of words or numbers in computer files. This may be called *interference with the course of data processing*¹²¹¹);
 - c) unlawfully obtaining/procuring electronic content or bits of information (such as credit card numbers). "Obtaining" should include the electronic copying of content, displaying it on a computer screen or making a print out of electronic information;
 - d) causing a message or electronic content to be displayed on any computer screen, without authorisation. (This will encompass instances where *hackers* deface web pages);
 - e) transferring electronic funds or creating fictitious accounts, without

¹²⁰⁹ See Van der Merwe 2000:174.

¹²¹⁰ See Nel 1990:45.

¹²¹¹ See Van der Merwe 2000:174.

authorisation. (This may be called *electronic fraud* where a *hacker* for instance penetrates a bank's computer system.)

3. Causing malicious computer programs¹²¹² to enter a computer system with the intent to either -

- a) obtain information; or
- b) manipulate information (referring to instances where a computer program deletes, modifies, corrupts or inserts information); or
- c) interfere with the operation of a computer system; or
- d) render the operating system inaccessible or inoperable; or
- e) display some message.^{1213 1214}

4. The mere creation as well as possession of malicious computer programs and hackers' tools, with the intent that it be used for criminal purposes.¹²¹⁵ The same should apply to the possession of illegally obtained passwords, with the intent that it be used for criminal purposes.

5. Sending an e-mail message or attachment containing a malicious computer program to someone else, knowing or suspecting that the message or attachment contains a malicious program.

6. Interfering with the operation and/or use of a computer system. (This will penalise individuals responsible for denial-of-service attacks and e-mail bombs attacks.)

7. Trafficking in, or making available of, illegally obtained passwords, hackers' tools and malicious computer programs. The following conduct, in particular, should be

¹²¹² The definition of "malicious computer program" can, for instance, be a program that causes a computer to do something, or interferes with the functioning of the computer, without the computer owner's consent or the consent of the person who is lawfully in control of the computer.

¹²¹³ See also Nel 1990:44 who is also in favour of penalising the creation and distribution of "harmless" viruses. By harmless she means that the virus does not delete files, but merely displays some message.

¹²¹⁴ Legislation criminalising the dissemination of malicious computer programs should never require an intent to cause prejudice because instances have occurred where the program writer disseminated a program with the intention that it should spread as far as possible across computer networks, without causing any prejudice to the computer owners, in order to indicate how vulnerable the security of computer systems were. However, due to miscalculation and erroneous or negligent programming, these program have often duplicated at such a rate that the programs caused infected computers to malfunction. See *US v Morris* 928 F.2d 504 (2nd Cir. 1991). A copy of this judgment can be downloaded from www.loundy.com/CASES/US_v_Morris2.html.

¹²¹⁵ Nel 1992:151; Nel 1990:47.

criminalised:

- a) Selling or trading in passwords, hackers' tools or malicious computer programs.
- b) Rendering access to the above. (This will include instances where a *hacker* posts passwords, hackers' tools or virus programs on a web site where it can be downloaded.)
- c) Disseminating the above to other Internet users. (This will include instances where a *hacker* e-mails, for example, passwords to other Internet users.)
- d) Obtaining the above, knowing or suspecting that -
 - (i) the password was obtained without the lawful owner's permission; or
 - (ii) the program downloaded can be used to gain unauthorised access to a computer and/or to interfere with the operation or usage of a computer and/or to create malicious computer programs.

Therefore, in effect, the mere possession of hackers' tools, malicious computer programs and illegally obtained passwords will be penalised, if the accused acquired it with the required knowledge and/or intent.

8. Inciting other computer users to commit computer-related offences (by, for instance, publishing vulnerabilities of computer operating systems or programs such as MS Windows or MS Outlook on *hacker* orientated web sites or by inciting Internet users to embark on an e-mail bomb attack against a particular computer user).

9. Spoofing header information (such as changing the address of an e-mail message to appear as if the e-mail came from A instead of B).

10. To intercept or monitor any electronic communications between two or more computers. (The interception and monitoring of electronic communications between two or more computers should be regulated in a separate act and not in the *Interception and Monitoring Prohibition Act* or in its successor, the proposed *Interception and Monitoring Act*. It is submitted that all legislation dealing with computer and Internet-abuse should be contained in one act.)

11. Sending a false warning message to another computer user (or to computer users), knowing that the message is false and with the intent that the recipient of the message does something positive or refrains from doing something on account of this message. (This should criminalise the creation and distribution of virus hoaxes.)

12. Receiving electronic data or content from someone, either knowing, believing or

suspecting that such data or content was illegally obtained. (This will penalise receivers of copied ("stolen") digital information.)

13. Attempts to commit the above-mentioned computer-related offence.

A definition of "unauthorised access" is necessary. It can be defined as "access without the permission of the person who controls access to the computer." This would encompass the instance where an employee who only enjoys limited access to the computer, exceeds his authorisation.¹²¹⁶ It is advised that legislation should use the words "electronic content" instead of electronic information or data. "Electronic content" is neutral and encompasses digital information, data, programs and software. "Hackers' tools" can be defined as software or programs used to either create or assist in creating malicious computer programs or to assist in gaining access to a computer or to assist in interfering with the operation or functioning of a computer or electronic content stored on a computer.

Legislation prohibiting computer-related crimes should contain a provision stipulating that where someone is found guilty of such an offence, the court can order that the computer equipment used for committing the offence be forfeited to the state or to any non-profit organisation such as the SPCA.¹²¹⁷ Nel proposes that legislation should empower courts to order that -

- colleges and universities be prohibited from granting degrees and diplomas, for a specified period of time, to anyone found guilty of a computer-related crime; and
- all computer businesses be prohibited from employing anyone found guilty of a computer-related crime.¹²¹⁸

It is contended that courts should further be empowered to prohibit cyber-criminals from participating in any computer business, computer-related and computer-orientated business, which includes employment by businesses selling computers, computer software, etc or where the culprit incorporates his own "computer" company.

Most companies are reluctant to report computer-related crimes in that it may attract unwanted attention, adverse publicity or cause future attacks.¹²¹⁹ Furthermore, victims

¹²¹⁶ Malan 1989:231.

¹²¹⁷ Nel 1992:157; Nel 1990:59.

¹²¹⁸ Nel 1992:157; Nel 1990:60.

¹²¹⁹ eEurope 2001; Paar 2000: "such reports may encourage others to invade the company's computer network."

will not gain any direct benefit from reporting these offences.¹²²⁰ Bearing these reasons in mind, it is submitted that South African legislation should provide for remunerative punishments, where the *hacker* or virus writer is found guilty of a computer-related offence. In other words, a court should be empowered to order that the accused pay the victim (complainant) monetary damages, where he is found guilty.

Furthermore, such legislation should provide for secrecy: the court must, as far as possible, ensure that no trade secrets as well as confidential information concerning the victim or his computer system are revealed. In addition, the media should be barred from reporting such instances without the complainant's or the court's consent. The media would still be allowed to report that a new virus has, for instance, been released onto the Internet, but it would be prohibited from naming anyone that has been infected by such viruses, where the latter has made a complaint or laid a charge against the culprit. This would be in accordance with the media's right to freedom of speech, as enshrined in section 16 of the *Constitution*,¹²²¹ but limited by section 36.¹²²² To give effect to such a provision, it should be made an offence to report in the media, including the online media, the names of businesses who suffered prejudice from instances of hacking or malicious programs, where the latter instituted action against the culprits or reported the instance to the police. This would entail that the media shoulders a responsibility to check, whenever it wants to identify businesses, whether they have reported hacking or virus instances or instituted proceedings against the wrongdoers.

Legislation should also state that addiction to computers is no defence. The reason for such a provision is that in the UK the jury refused to convict a young *hacker* on the strength of the defense's submission that he was addicted to computers and was consequently "unable to form the necessary intent to be found guilty."¹²²³

¹²²⁰ Akdeniz 1996:8.

¹²²¹ S 16(1) provides that "[e]veryone has the right to freedom of expression, which includes (a) freedom of the press and other media."

¹²²² S 36(1) provides that "[t]he rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including (a) the nature of the right; (b) the importance of the purpose of the limitation; (c) the nature and extent of the limitation; (d) the relation between the limitation and its purpose; and (e) less restrictive means to achieve the purpose."

¹²²³ Wing 2001. The case was *R v Bedworth* (1993). See www.som.hw.ac.uk/buslm1/ITlawcases.htm.

2. CURRENT DEVELOPMENTS

Under this heading current developments in South Africa, concerning the criminalisation of computer-related crimes, are discussed.

2.1. National Prosecuting Authority Amendment Bill

When this dissertation was written, attempts were made to amend the *National Prosecuting Authority Act*¹²²⁴ in order to criminalise hacking into computers of the National Directorate of Prosecutions, including computers of the Scorpions unit.¹²²⁵

The *National Prosecuting Authority Amendment Bill*¹²²⁶ proposes certain amendments, to the above-mentioned Act, which are virtually identical to the instances already criminalised by section 71 of the *South African Police Service Act*.¹²²⁷ The only difference is that the bill¹²²⁸ does not only penalise gaining unauthorised access, but also allowing or causing any other person to gain such access to any computer which belongs to or is under the control of the prosecuting authority or to any program or data held in such a computer, or in a computer to which only certain or all members of the prosecuting authority have access in their capacity as members.

The bill provides that where a computer offence, criminalised by the bill, is committed, the court is empowered to impose a fine or imprisonment for a period not exceeding 25 years or both such fine and imprisonment.¹²²⁹

2.2. South African Law Commission: Discussion Paper 99

In 2001 the South African Law Commission published "*Discussion Paper 99: computer-related crime: preliminary proposals for reform in respect of unauthorised access to computers, unauthorised modification of computer data and software*

¹²²⁴ Act 32/1998.

¹²²⁵ Stuart 2000:9; Hartley 2000:4.

¹²²⁶ B 39b/2000.

¹²²⁷ Discussed in par 2.2 of chapter 6.

¹²²⁸ These amendments will be promulgated as s 40A of the *National Prosecuting Authority Act*.

¹²²⁹ S 19.

applications and related procedural aspects".¹²³⁰ This document deals with¹²³¹ -

- ⇒ obtaining unauthorised access to or obtaining computer data and software applications;
- ⇒ unauthorised modification of computer data and software applications;
- ⇒ development and trafficking in devices or applications primarily used to obtain unauthorised access;
- ⇒ trafficking in computer passwords; and
- ⇒ interference with the use of a computer system.

This discussion paper includes a draft bill, titled the *Computer Misuse Bill*, and proposes five offences. The first offence established in section 2 of the draft bill is the "unauthorised access to or obtaining of applications or data in computer systems". It provides that:

"Any person who intentionally and without authority to do so, accesses or obtains any application or data held in a computer system, is guilty of an offence."¹²³²

Section 1 defines "access", "application", "computer system" and "data" as follows:¹²³³

Data:

"any representation of information, knowledge, facts or concepts, capable of being processed in a computer system, and includes such a representation held in any removable storage medium which is for the time being in a computer system."

Application:

"a set of instructions that, when executed in a computer system, causes a computer system to perform a function, and includes such a set of instructions held in any removable storage medium which is for the time being in a computer system."

Computer system:

"an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, one or more of which is capable of (a) containing data; or (b) performing a logical, arithmetic, or any other function in relation

¹²³⁰ A copy can be downloaded from www.law.wits.ac.za/salc/discussn/dp99.pdf or www.2600.co.za/articles/dp99.pdf.

¹²³¹ See Government Notice GG 938/2001 (18/5/2001), no 22281 p 64-6; SALC's Discussion Paper 99:x.

¹²³² SALC's Discussion Paper 99:64.

¹²³³ SALC's Discussion Paper 99:63-64.

to data.”

Access:

“access in relation to an application or data means rendering that application or data, by whatever means, in a form that would enable a person, at the time when it is so rendered or subsequently, to take account of that application or data and includes using the application or data or having it output from the computer system in which it is held in a displayed or printed form, or to a storage medium or by means of any other output device, whether attached to the computer system in which the application or data are held or not.”

The Law Commission notes the following:

“It is proposed that a wide description of the criminal action be adopted. This description should be aimed at protecting the computer data or software applications stored on a computer system without being limited by references to specific methods by means of which the access is to be obtained ... The access component of the criminal action should include any manner by means of which a person is enabled to take account of the computer data or use the software applications. Access should therefore be a wide concept and should include all means of taking account of computer data or software applications or of having it output from the computer in which it is held, including on a monitor, printer or storage medium. It should be irrelevant to the description of the criminal action whether the monitor, printer, storage medium or other output device is attached to the computer in which the data or software applications are held or not. In other words it should not only include all instances of copying, moving, or using computer data or software applications but also the mere becoming aware thereof ... The element of unlawfulness will be what distinguishes the lawful use of a computer from usage which should be subjected to criminal sanction. This element should be expressed by means of a reference to an absence of authority to obtain the access in question. The absence of authority is an objectively determinable element. It will be determined with reference to the circumstances of each case. An absence of authority should, in the first instance, entail absence of the permission of the owner or the person lawfully in charge of the computer data or software applications in question. In this regard it must be noted that it is not the absence of permission by the person in charge of the computer by means of which the access is obtained that determines the unlawfulness of that access, but rather the absence of permission by person in charge of the affected computer data or software applications ... The form of culpability of the unlawful access offence should be intent. The intent should be directed at all the elements of the offence. This implies that the accused must have had the intent to obtain access to the computer data or software applications in question, as well as that

he or she must have had knowledge of the unlawfulness thereof ... The element of intent should not be linked to a specific purpose or motive for which the unauthorised access is obtained.”¹²³⁴

This section, therefore, penalises instances where a *hacker* gains access to data or applications on a computer system or without gaining access to the computer obtains the data or application, for instance, by means of a computer program. It further transpires that merely viewing data suffices; the cyber-abuser is not required to make a copy before the provision is contravened.

The second offence which the draft bill proposes to establish is the “unauthorised modification of applications or data in computer system”. Section 3 stipulates that:

“(1) Any person who intentionally and without authority to do so, performs an act causing any application or data held in a computer system to be modified, destroyed or erased or otherwise rendered ineffective is guilty of an offence.

(2) Any person who intentionally and without authority to do so inserts any application or data in a computer system is guilty of an offence.”¹²³⁵

The Law Commission notes the following regarding this proposed offence:

“[I]t is proposed that the criminal action be widely defined. It should not be limited by any reference to specific methods by means of which the modification is made. The criminal action should therefore include any action which results in a modification of the computer data or software applications concerned ... The criminal action should not contain actual damage resulting from the modification as one of its components. The fact that a modification of computer data or software applications caused damage in any given case should be a factor to take into account upon sentencing ... [The element of unlawfulness] should be expressed by means of a reference to an absence of authority to make the modification in question ... The element of intent would naturally include knowledge of the unlawfulness of the modification. In other words the accused must have known that he or she had no authority to cause the modification of the computer data or software applications in question ... The element of intent should therefore not be linked with a specific purpose or motive for which the unauthorised modification is effected.”¹²³⁶

This provision, therefore, criminalises instances where a *hacker* himself or by means of

¹²³⁴ SALC's Discussion Paper 99:53-55.

¹²³⁵ SALC's Discussion Paper 99:64.

¹²³⁶ SALC's Discussion Paper 99:56-57.

a computer program deletes or modifies electronic files or inserts information (data) or a malicious computer program (an application) or causes an application to malfunction. This provision would also appear to criminalise instances where a *hacker* or a computer program defaces a web page by deleting data or by adding text.

The third offence, according to section 4 of the draft bill, is to develop and traffic in devices or applications primarily used to obtain unauthorised access:

“Any person who, without lawful justification, develops, manufactures, produces, imports, exports, procures for use, or makes available, a device or application designed or adapted to make it primarily useful for accessing or for modifying, destroying or erasing or otherwise rendering ineffective an application or data held in a computer system without authority to access, modify, destroy or erase or otherwise render ineffective that application or data, is guilty of an offence.”¹²³⁷ (own emphasis)

This section, therefore, penalises the creation, procurement and making available of hackers’ tools that assist in accessing computers (for instance password sniffers that obtain or guess the relevant password) or deleting or modifying information or causing applications to malfunction. It can also be argued that the section penalises the development, making available or intentional procurement of malicious computer programs.

The Law Commission also proposed that the “trafficking in computer passwords” should be an offence. Section 5 provides that -

“[a]ny person who makes available any password or similar information by means of which an application or data held in a computer system can be accessed without authority to access that application or data, is guilty of an offence.”¹²³⁸

According to section 6, the “interference with the use of [a] computer system” should also be an offence: Any person who -

- “(a) prevents or hinders access to any application or data in a computer system;
- (b) impairs the effectiveness or reliability of any application or data in a computer system, or
- (c) impairs the operation of a computer system, is guilty of an offence.”¹²³⁹

¹²³⁷ SALC’s Discussion Paper 99:65.

¹²³⁸ SALC’s Discussion Paper 99:65.

¹²³⁹ SALC’s Discussion Paper 99:65.

This section, therefore, criminalises denial-of-service attacks as well as e-mail bomb attacks. It also penalises *hackers* who by themselves or by means of malicious computer programs (such as micro viruses) impair the reliability of data and applications. It can also be argued that where a virus hoax is successful, in other words so many Internet users disseminated the message that one of more servers were rendered inoperable, such conduct falls within the scope of either impairing the operation of a computer system or preventing/hindering access to data or applications stored on a computer system.

Finally, the Law Commission proposes that where someone is convicted of an offence established in section 2 (unauthorised access), he should be liable to a fine or to a maximum imprisonment of 5 years.¹²⁴⁰ Where the accused is found guilty of another proposed offence, he should be liable to a fine or to a maximum imprisonment of 10 years.¹²⁴¹

3. COMMENTS AND RECOMMENDATIONS

The following comments and recommendations concerning the proposed *Computer Misuse Bill* can be furnished:

- (i) Section 2 appears to penalise instances where the *hacker* gains access to data or applications on a computer. It is advised that the section should provide that whenever someone gains access to a computer, or to any data or applications stored in such computer, without authorisation, he is guilty of an offence. The difference is that some *hackers* merely gain access to a computer to prove how good they are without necessarily accessing any application or obtaining any information. They merely attempt to penetrate the computer's security system. This section should also encompass such instances.¹²⁴² Otherwise the section should state that where someone gains unauthorised access to a computer he is deemed to have accessed a computer's applications or data.
- (ii) The proposed bill should also penalise:
 - a) The intentional dissemination of virus hoaxes, knowing that such electronic communications contain false information;

¹²⁴⁰ S 10(1). SALC's Discussion Paper 99:66.

¹²⁴¹ S 10(2). SALC's Discussion Paper 99:66.

- b) The receiving of electronic data or applications, knowing, suspecting or believing that such data or applications were illegally obtained;
- c) The creation, procurement or making available for use of applications used to interfere with the operations, functioning or accessing of a computer or computer system. (This will cover programs used to launch denial-of-service attacks);
- d) The possession of passwords to which the accused is not entitled;
- e) Attempts to commit a computer-related crime; and
- f) The fraudulent altering of header information. (This will include *spoofing* e-mail addresses or altering examination results.)
- g) Gaining access to data, stored on a removable medium, without authorisation. The proposed section 2 only penalises the instance where a *hacker* gains access to (e.g.) a floppy, inserted into the computer, to which he gained access. However, it does not encompass the scenario where someone gains unauthorised access to a room, takes a floppy (or any removable storage medium),¹²⁴³ and inserts it into his own computer and consequently gains access to the electronic information.

- (iii) The bill should stipulate that the interception and monitoring of electronic communications or data in transmission are prohibited.
- (iv) The bill should provide that either the Law Commission or a committee is obliged to report (at least) every three years to parliament examining the provisions of this bill in the light of the development of technology and addressing the question whether the Act should be amended to cover any loopholes.¹²⁴⁴
- (v) Finally, it is advised that the proposed section 4 should be amended to provide that linking to web sites/pages, that primarily make electronic applications or programs, used primarily for deleting, or modifying or interfering with computer systems, available for downloading, constitutes an offence where the owner of the linking web site/page knows this. Hence, where someone intentionally includes a hyperlink on his page that transfers Internet users to web sites where hackers' tools can be downloaded, he is guilty of an offence.

¹²⁴² It is submitted that under normal circumstances it will be difficult for the prosecution to prove that the *hacker* actually accessed any particular data or applications.

¹²⁴³ Which may or may not be inserted into the computer.

¹²⁴⁴ A similar provision is included in article 12(1) of the *EU Copyright Directive*.

CHAPTER NINE

SUMMARY

The purpose of this study was to determine whether there exists a need for legislation in South Africa criminalising Internet related commercial crimes and specifically computer-related crimes, which for all purposes refer to instances where computer experts (hackers) gain access to third parties' computers without authorisation or unlawfully interfere with the latter's computer systems as well as to instances where computer experts disseminate malicious computer programs that do the above. Collectively these instances are referred to as hacking and virus instances. The selling and/or distributing of hackers' tools (used to gain access to computer system or to interfere with the functioning of computer systems) and illegally obtained passwords are also examples of a computer-related crime, studied in this dissertation.

In search for an answer to the above-mentioned question, this study assessed whether computer-related crimes can be accommodated by the current definitions of common law as well as statutory offences, with specific reference to the offences of theft, receiving stolen property knowing it to be stolen, fraud, theft by false pretences, malicious injury to property and *crimen iniuria*.

After a thorough analysis of the current law obtaining in South Africa it was concluded that should local courts be willing to extend the application as well as the definitions of common law offences to computer-related crimes, then virtually all instances of computer-related crimes would be encompassed by the above-mentioned common law offences. Only the creation and possession of hackers' tools and illegally obtained passwords would not constitute offences in terms of the South African criminal law. It was further noted that should local courts refuse to extend the application of common law offences to computer-related crimes, then thirteen cyber-"transgression" have to be criminalised.

Further note was taken of the South African Law Commission's draft bill, the *Computer Misuse Bill*, as a proposal to criminalise computer-related crimes. In order to assess whether such proposed legislation is in line with foreign legislation criminalising the above-mentioned aspects, this study also scrutinised the legislation of the United States, the United Kingdom, Singapore, the Netherlands as well as the newly enacted *European Convention on Cybercrime*.

Certain recommendations were also made to the South African Law Commission with regard to the type of conduct that should be criminalised to bring foreseen South African legislation, dealing with cyber-related crimes, in line with foreign legislation.

OPSOMMING

Die doel van hierdie studie was om te bepaal of daar 'n behoefte aan wetgewing in Suid-Afrika is wat Internet verwante kommersiële misdade bestraf, met spesifieke verwysing na rekenaar-verwante misdade, wat vir alle doeleindes verwys na gevalle waar rekenaarkundiges ("*hackers*") toegang verkry to derdes se rekenaars sonder laasgenoemde se toestemming of waar hulle onregmatig inmeng met die funksionering van laasgenoemdes se rekenaarstelsels, asook gevalle waar rekenaarkundiges kwaadwillige programmatuur versprei wat die bogenoemde doen. Die handel in en/of die verspreiding van onwettig verkryde "*passwords*" en "*hackers' tools*" (wat gebruik word om onregmatige toegang tot rekenaars te bewerkstelling of om in te meng met die funksionering van rekenaarstelsels) is ook voorbeelde van rekenaar-verwante misdade wat bestudeer was in hierdie studie.

Ten einde 'n antwoord op bogenoemde probleemstelling te verkry het, het die studie bepaal of rekenaar-verwante misdade geakkommodeer kan word deur die huidige omskrywings van gemeenregtelike sowel as statutêre misdade, met spesifieke verwysing na diefstal, ontvangs van gesteelde goedere wetende dat dit gesteel is, bedrog, diefstal deur valse voorwendsels, saakbeskadiging en *crimen iniuria*.

Na 'n deeglike studie van die huidige regsposisie in Suid-Afrika, was tot die gevolgtrekking gekom dat sou ons howe bereid wees om die toepassing sowel as die definisies van gemeenregtelike misdade na rekenaar-verwante misdade uit te brei, dan sal dit beteken dat feitlik alle gevalle van rekenaar-verwante misdade bestraf sal word deur bogenoemde gemeenregtelike misdade. Slegs die skepping en besit van "*hackers' tools*" en onwettig verkryde "*passwords*" sal nie misdade daar stel in terme van die Suid-Afrikaanse strafreg nie. Daar was verder opgemerk dat sou ons howe nie bereid wees om die toepassing van gemeenregtelike misdade uit te brei na rekenaar-verwante misdade, moet dertien Internet-"misbruike" gekriminaliseer word.

Verder was daar kennis geneem van die Suid-Afrikaanse Regskommissie se konsep wetsontwerp, die *Wetsontwerp op Rekenarmisbruik*, as 'n voorstel om rekenaar-

verwante misdade te bestraf. Ten einde te bepaal het of die voorgestelde wetgewing in lyn is met buitelandse wetgewing wat bogenoemde aspekte kriminaliseer, het die studie ook die wetgewing van die Verenigde State van Amerika, Brittanje, Singapoer, Nederland asook die nuut gepromulgeerde Europese *Konvensie oor Internet Misdade* ("*Convention on Cybercrime*") bestudeer.

Sekere aanbevelings word ook gemaak aan die Suid-Afrikaanse Regskommissie met betrekking tot die tipe handeling wat bestraf moet word ten einde Suid-Afrikaanse wetgewing, wat handel met Internet-verwante misdade, in lyn te bring met buitelandse wetgewing.

BIBLIOGRAPHY

ABREU E

2000. Hackers, the Feds want you. *Computing SA* 7 Aug p17.

AKDENIZ Y

1996. Section 3 of the Computer Misuse Act 1990: an Antidote for Computer Viruses!
<http://webjcli.ncl.ac.uk/1996/issue3/akdeniz3.html>.

ANDRESS M

2000. CyberwallPlus-SV boosts security. *Computing SA* 12 June p26.

ANONYMOUS

2001(a). SSL. www.cs.umu.se.

2001(b). SSL basics for Internet users. www.rsasecurity.com/standards/ssl/basics.html.

2001(c). 'Mafiaboy' Sentenced to 8 Months. (13/09/2001)
www.wired.com/news/business/0,1367,46791,00.html.

2001(d). Hackers' crack at phone systems costs millions. (21/02/2001) www.iol.co.za/general.

2001(e). Networks Unlimited. *Smart Business Computing* March/April p38.

2001(f). Police net Kournikova-virus suspect. (14/2/2001) www.iol.co.za.

2001(g). US hit hard by hackers. (09/03/2001) www.news24.co.za.

2001(h). Hackers hit Microsoft again. (29/01/2001) www.news24.co.za.

2001(i). Easy to wiretap e-mail. (06/02/2001) www.news24.co.za.

2001(j) What are e-mail bombs? www.cs.tcd.ie/courses/baict/bac/jf/projects/99/mailbomb/.

2001(k). What is a Mail Bomb? www.valise.com/h_bombs.html.

2001(l). Email bombing and spamming.
www.cert.org/tech_tips/email_bombing_spamming.html.

2001(m). Hacker brings down White House website. (05/05/2001) www.iol.co.za.

2001(n). E-commerce hampered by fear of fraud. (02/03/2001) www.iol.co.za.

2001(o). Amazon branch breaks off after big hack. (06/03/2001) www.iol.co.za.

2001(p). Hacker siphons R2m from account in cyberspace scam. *The Star* (13/3/2001) p7.

2001(q). SA's first cybercrime kingpin arrested. (02/04/2001) www.iol.co.za.

2001(r). Computer Misuse Act 1990. (04/06/1996)
www.eeng.brad.ac.uk/help/.regulations/.cma90.html.

2001(s). Guidance on Computer Misuse Act. www.lancs.ac.uk/homepage/webmenus/e-security/cm misuse.htm.

2001(t). Computer Misuse Act. www.uclan.ac.uk/facs/destech/compute/staff/casey/integ/mscmisus.htm.

2001(u). Computer Misuse Act 1990. www.swan.ac.uk/law/staff/pntodd/statutes/stats_c/computer.htm.

2001(v). Crash! Boom! Bang! *SA Computer Magazine* May p34.

2001(w). Hoax emailers' nabbed in Cape Town. (15/9/2001) www.iol.co.za.

2001(x). Anna virus writer goes on trial. (14/9/2001) <http://news.cnet.com/news/0-1003-200-7164744.html?tag=lh>.

2001(y). Web attacks double, budgets frozen. *Finance Week* 19 Oct p73.

2000(a). Firewalls only the start of corporate security. *Computing SA* 13 March p27.

2000(b). ISA extends check point internet security. *Computing SA* 14 February p34.

2000(c). Internet banking. *SA Banker* Vol 97(1) p20.

2000(d). Security tip. *e-Business Advisor* Jan p48.

2000(e). Hacker's trial in Amazon ends in crop net. (19/4/2000) www.iol.co.za.

2000(f). Safeguards fall as hackers keep cracking. (9/5/2000) www.iol.co.za.

2000(g). Hackers hit US government email service. (17/7/2000) www.iol.co.za.

2000(h). Hacker attacks cop website with nude woman. (10/12/2000) www.iol.co.za.

2000(i). Teen hacker now regrets 'fun' cyberinvasion. (24/9/2000) www.iol.co.za.

2000(j). Cybercrime is huge growth industry – US. (2/16/2000) www.iol.co.za.

2000(k). New Yorker arrested for hacking into Nasa. (13/7/2000) www.iol.co.za.

2000(l). SouthPark virus worms way around world. (11/5/2000) www.iol.co.za.

2000(m). Microsoft admits hackers stole crucial code. (12/10/2000) www.iol.co.za.

2000(n). 'World's worst' parliamentary site hacked. (31/12/2000) www.iol.co.za.

2000(o). Email viruses to get deadlier in 2001. (31/12/2000) www.iol.co.za.

2000(p). From Trojan Horses to Worms: understanding various malicious threats. <http://enterprisesecurity.symantec.com/article.cfm?articleid=130&PID=2110062>.

2000(q). "ILOVEYOU" worm wreaks havoc worldwide. <http://enterprisesecurity.symantec.com/article.cfm?articleID=97&PID=2110062>.

- 2000(r). How to enhance your IT system's security. *Sunday Times* 1 Oct p3.
- 2000(s). Know your enemy: the tools and methodologies of the script kiddie. <http://project.honeynet.org/papers/enemy/>.
- 2000(t). Corporate hackers cause concern. *Business Day* 27 Jan p10.
- 2000(u). Email viruses to get deadlier in 2001. (31/12/2000) www.iol.co.za.
- 2000(v). Intrusion detection provides round-the-clock network surveillance. *Computing SA* 28 Aug p26.
- 2000(w). Tripwire prevents crash and burn. *Computing SA* 4 Sept p24.
- 2000(x). Cybercrime on the rise in US. *Computing SA* 18 Sept p19.
- 2000(y). What are stealth, polymorphic, and armoured viruses? (7/07/2000) <http://kb.indiana.edu/data/aehs.html>.
- 2000(z). Security the biggest hurdle to overcome. *F&T Net* Vol 4(5) p58.
- 2000(za). Firewalls 101: beat a hacker at his own game. (24/10/2000) www.iol.co.za.
- 2000(zb). Gates becomes a criminal in hacker's hands. (11/10/2000) www.iol.co.za.
- 2000(zc). Home Internet usage tops 295 million: survey. (08/09/2000) www.iol.co.za.
- 1999(a). The road to IP security. *Computing SA* 30 Aug p29.
- 1999(b). Virus Alert. *SA Computer* July p78.
- 1999(c). Hacking & cracking the heart of an organisation. *Computing SA* 30 Aug p36.
- 1999(d). Enforce security policy to keep corporate networks safe. *Computing SA* 30 Aug p38.
- 1999(e). Why firewalls are not enough. *Computing SA* 30 Aug p38.
- 1999(f). E-commerce and privacy: perception versus reality. *Computing SA* 30 Aug p43.
- 1998(a). Findings of the Heath Special Investigating Unit. *Local Government Digest* Vol 18(4) Nov p2.
- 1998(b). Electronic crime a reality. *Finance Week* 16 April p60.
1997. Hoe veilig is jou geheime. *Finansies en Tegniek* Vol 49 5 Dec p12.
- ASOKAN N
1997. The state of art in electronic payment systems. *Computer* Sept p28.
- ATKINS NG
1990. Computer Insurance – IV (Protection against uninsurable risks). *Businessman's Law* p79.
- BAERTLEIN L

2001. Kournikova virus lobs emails around the world. (13/2/2001) www.iol.co.za.
- BASS T, FREYRE A, GRUBER D & WATT G
1998. E-Mail Bombs and Countermeasures: Cyber Attacks on Availability and Brand integrity. www.silkroad.com/papers/html/bomb/n1.html.
- BEARD J
2001. E-mail Snoopers' powerful tools threaten electronic privacy. (26/3/2001) www.law.com.
- BEARZI J
2000. Robbery on the information highway. *The Star* 3 Oct p1.
- BEAVER T
2000. Countering the hackers. *Saturday Star* 15 Sept p8.
- BENNETTE R & LUBER P
1999. Securing the perimeter. *Computing SA* 28 June p16.
- BIDOLI M
2000. EEEK! Business beware of cybersuits. *Financial Mail* 12 May p76.
1999. In the new Wild Web West. *Financial Mail* 24 Sept p99.
- BOISTEEL S
2001. Automatic web-defacing worm on the loose, CERT says. (08/05/2001) www.newsbytes.com/news/01/165448.html.
- BORASKY DV
1999. Digital signatures: secure transactions or standard mess? *Online* July/August p47.
- BOTHA CR
1986. S v Myeza 1985 (4) SA 30 (T): oor blikringetjies en boetebessies – aspekte van bedrog. *SACJ (South African Journal of Criminal Justice)* p72.
- BRAUN U
1997. Headstart for virtual vaults. *Financial Mail* 19 Sept p56.
- BURCHELL JM & MILTON J
2000. *Principles of criminal law*. Revised Reprint. Juta:Cape Town.
- BURCHELL JM & HUNT PMA
1970. *South African Criminal Law and Procedure*. Juta:Cape Town.
- BUYS R
2000. Love hurts. *De Rebus* July p33.
- CAMERER L
1997. International fraud trends: South Africa at risk. *African Security Review* Vol 6(2) p45.
- CARR I *et al*
1994. *Computers and Law*. Oxford.

CARROLL C

2000. Loveletter virus catches the world off guard. *Computing SA* 8 May p1.

CARSTENS P & TRICHARDT A

1987. Computer crime by means of the automated teller machine – just another face of fraud. *SACJ* p122.

CHADWICK D

1999. Smart cards aren't always the smart choice. *Computer Dec* p142.

CHEN GCC

1999. International response to cyber crime: Asian perspective (6/12/1999)
www.oas.org/juridico/english/chen.htm.

CHIEN E

2000. The rise of the network Trojan. (20/12/2000)
<http://enterprisesecurity.symantec.com/article.cfm?articleid=535>.

CHRISTIANSON G & MOSTERT W

2000. Digital signatures. *De Rebus* May p26.

COBB M

1999. Virtual viruses. *e-Business Advisor* March p34.

1998. Confidentiality, authentication, and integrity for e-mail. *e-Business Advisor* October p52.

COETZEE JA

1970. Diefstal van onliggaamlike sake? *THRHR (Tydskrif vir Romeins-Hollanse Reg: Journal for Contemporary Roman-Dutch Law)* p369.

COETZER J

1985. Computer crime – a new tune on an old fiddle. *Accountancy SA* Vol 2(1) Jan p16.

COOKE SH & FRYER V

1998. Computer fraud – risks and implications. *Accountancy SA* Feb p4.

COPELING AJC

1968. *Dun and Bradstreet (Pty) Ltd v SA Merchants Combined Credit Bureau (Cape) (Pty) Ltd* – Unlicensed use by rival trader of confidential information compiled and distributed by fellow trader – nature of remedies available. *THRHR* p180.

CSINGER A & SIAU K

1998. The global public key infrastructure: terms and concepts. *Computer* Sept p30.

DANIELS M

2000. Viruses and virus countermeasures: principles and practice.
www.cs.uct.ac.za/courses/CS400W/NIS/papers00/mdaniels/.

DAVIDSON T

1998. For your eyes only. *Charter* Vol 69(3) April p48.

DAVIES L

1996. Internet and the elephant. *International Business Lawyer* April p151.

DE BRUXELLES

2001. Price war computer boss sent e-mail virus. *The Times* (31/3/2001) www.thetimes.co.uk/article/0,,2-107878,00.html.

DELIO M

2000. Hackers crack into MS system. www.wired.com/news/culture/012843977800.html.

DEVENISH GE

1992. *Interpretation of Statutes*. Juta:Cape Town.

DE WET JC & SWANEPOEL HL

1985. *Strafreg*. 4th Edition. Butterworths:Durban.

DISABATINO J

2000. Cyber extortionists arrested in Bloomberg case. *Computing SA* 21 Aug p13.

DITTRICH D

1999. The "stacheldraft" distributed denial of service attack tool. <http://project.honeynet.org/papers/enemy/ddos.txt>.

DOMANSKI A

1993. The nature of the right infringed in cases of unlawful competition in South African law. *SA Merc LJ (South African Mercantile Law Journal)* p127.

DOWD PW & McHENRY JT

1998. Network security: it's time to take it seriously. *Computer* Sept p24.

DRYER JW

1983. Computer Law in South Africa. *De Rebus* Nov p535.

DUTSON S

1997. The Internet, the conflict of laws, international litigation and intellectual property: the implications of the international scope of the Internet on intellectual property infringements. *JBL (Business Lawyer)* p495.

DYANTI A

2000. Cybercops hot on heels of virtual villains. (28/7/2000) www.iol.co.za.

ERDOZAIN JC

1999. Encryption technologies and digital signatures. *International Business Lawyer* June p275.

FINN M

1998. Keep an eye on your network. *e-Business Advisor* Nov p40.

FRANKE D

1999. E-business. *Accountancy and Finance Update* Dec p21.

FLEISHMAN G

2001. Broadband security. *Fortune* 14 May p117.

FURBER P

1998. IPSs suffer new wave of cracking attempts. *Computing SA* 6 July p1.

GALVIN J
2001. 'Cyberwars' bring real-world conflict to the Web. (16/02/2001)
www.zdnet.com/cdn/stories/news.

GARBER L
1999. Melissa Virus creates a new type of threat. *Computer* June p16.

1998. Antivirus technology offers new curses. *Computer* Feb p12.

GARDINER FG & LANSDOWN WH
1939. *South African criminal law and procedure*. 4th Edition. Juta:Cape Town.

GARFINKEL S & SPAFFORD G
1997. *Web security & commerce*. O'Reilly:US.

GELDENHUYS T
1993. *Die Regsbeskerming van Inligting*. LLD:UNISA.

GOLDMAN J
1996. E-mail bombs. (14/08/1996) www.kron.com/nc4/use/stories/ebombs.html.

GOLD S
2001. New e-mail worm SirCam causing consternation. (22/7/2001)
www.newsbytes.com/news/01/168120.html.

GORDON G
1999(a). Reliable systems to combat hackers and crackers. *Financial Mail* 3 Sept p125.

1999(b). Building the barricades. *Financial Mail* 12 Nov p92.

1998(a). Hacking law on the horizon. *Financial Mail* 6 Feb p67.

1998(b). Virtual wallets will be safe from real fraudsters. *Financial Mail* 6 March p76.

GOYAL RM
1994. *Computer Crimes (concept, control and prevention)*. Sysman Computers:Bombay.

GREEN J
2000. Crook nets thousands in Internet bank scam. (08/11/2000) www.iol.co.za.

HALL M
2000. IT panned for security 'complacency'. *Computing SA* 26 June p23.

HAMMOND G
1988. Theft of information. *The Law Quarterly Review* Oct p527.

HARRIS P
2000. The UK Computer Misuse Act 1990. www.crills.com/cyber.loi/393.htm.

HARRISON A
2000. Corporate security begins at home. *Computing SA* 13 March p27.

HARTLEY W
2000. Committee moves to short-circuit hackers. *Business day* 19 Oct p4.

HAYES F

2000. Wanted: security champion. *Computing SA* 24 Jan p20.

HEAVENS A

2000. Microsoft hacker's motive suspected to be espionage. *Business day* 31 Oct p11.

HEDBERG SR

1997. HP's International cryptography framework compromise or threat? *Computer* Jan p28.

HERRINGSHAW C

1997. Detecting attacks on networks. *Computer* Dec p6.

HEWITT G

2000. The Eurozone. *SA Banker* Vol 97(1) p20.

HOARE S

2000. Trojan Horse saddles you with losses.

<http://enterprisesecurity.symantec.com/article.cfm?articleid=350&PID=2110062>.

HUBER U

1742. *Heedendaegse Rechtgeleertheyt*. Amsterdam.

HUNT PMA

1967. The 'damage' element in malicious injury to property. *SALJ (South African Law Journal)* p142.

HUNT PMA & MILTON JRL

1990. *South African Criminal Law and Procedure*. Revised 2nd Edition. Juta:Cape Town.

HURTER E

2000. Dispute resolution in Cyberspace: a futuristic look at the possibility of online Intellectual property and e-commerce arbitration. *SA Merc LJ* p199.

JONES N

2000. Digital watermarks and protection of ownership. www.cs.uct.ac.za/courses/CS400W/NIS/papers00/njones/Digital_Watermarks.htm.

JOUBERT DJ

1985. Die reg en inligting. *De Jure* p34.

JOUBERT WA

1958. 'n Realistiese benadering van die subjektiewe reg. *THRHR* p98.

JURY K

2000. Are banks ready for the Internet quake? *Accountancy SA* April p7.

KEHOE L

2000. Cyberterrorism moves from science fiction reality. (14/2/2000) www.businessday.co.za.

KEPHART JO, SORKIN GB, CHESS DM & WHITE SR

1999. Fighting computer viruses. www.sciam.computer/1197issue/1197kephart.html.

KLEYN D

1993. Dogmatiese probleme rakende die rol van onstoflike sake in die sakereg. *De Jure* p1.

KNOBEL JC

1990. Die beskerming van handelsgeheime in die deliktereg. *THRHR* p488.

KUNER C

1996. Legal aspects of encryption in the Internet. *International Business Lawyer* April p186.

LABUSCHAGNE JTM

1990. Regsobjekte sonder ekonomiese waarde en die irrasionele by regsdenke. *THRHR* p557.

LAING R

1998. The cheque is in the e-mail. *Finance Week* 7 May p33.

LAWSA (THE LAW OF SOUTH AFRICA) – JOUBERT WA (Founding Editor).

1996. *LAWSA*. First Re-issue. Butterworths:Durban.

LAWTON G

2000. Intellectual-Property Protection opens path for e-commerce. *Computer* Feb p14.

1999. Explorer worm targets networks, deletes data. *Computer* Aug p15.

LEMOS R

2001. Hackers divided over response to terrorism. (14/9/2001) <http://news.cnet.com/news/0-1003-200-7166935.html>.

LE PAGE D

1999. Software – would you buy on these purchase conditions? *Accountancy SA* Sept p5.

LE ROUX F

2000. E-commerce – The legal framework. *De Rebus* Sept p25.

LES AOANA M

2000. A comparison of RSA and Elliptic Curve Encryption.

www.cs.uct.ac.za/courses/CS400W/NIS/papers00/mlesaoana/paper.htm.

LEWIS P

2001. Back to basic – Your hard drive is going to die. *Fortune* 25 June p75.

LLOYD T

1999. Pigeons in the spymaster's loft. *Financial Mail* 27 August p48.

LOUBSER MM

1978. *The theft of money in South African Law*. Annale:Universiteit van Stellenbosch.

LOURENS J

1998. Electronic commerce – the law and its consequences. *De Rebus* May p64.

MALAN FR

1989. Oor inligting, rekenaarmisbruik en die strafreg. *De Jure* p211.

MARITZ E

2000. Creating certainty over the Internet. *SA Treasurer* 14 Sept p11.

MARX A

2000. Anti-virus programs fail. *Computing SA* 21 Aug p25.

MATTHEAUS A

1672. *De Criminibus ad Lib. XLVII et XLVIII Dig. Commentarius*. Amsterdam.

MCLEOD D

2000(a). Symphony of destruction? *Financial Mail* 26 May p81.

2000(b). Under a virtual hammer. *Financial Mail* 25 Feb p122.

1999. Cybertrade takes off. *Financial Mail* 3 Sept p109.

MCNAMARA JD

1998. HI-Tech Security. *Vital Speeches of the Day* Vol 65(2) 1 Nov p55.

MEALL L

2000. Abcde-finance. *Accountancy* Sept p56.

MKHWANAZI S

2000. Hacker congests Medinfo e-mail. *The Star* 6 April p7.

MOMMSEN T, KRUEGER P & WATSON A

1985. *The Digest of Justinian*. University of Pennsylvania Press.

MOORMAN J

1764. *Verhandelinge over de misdaden en der selver straffen*. Amsterdam.

MORT S

2000. Predators stalk the Web for soft spots in e-commerce. *The Star* 2 Aug p 2.

MYERS G

2000. Hackers depend on the slackers for success. *Sunday Times* 1 Oct p3.

NEETHLING J

1983. Die aanwending van 'n mededinger se bedryfsidees: onregmatige mededinging? *Codicillus* May p24.

1971. Crimen iniuria – inbreuk op privaatheid – ernstige krenking van dignitas. *THRHR* p324.

NEETHLING J, POTGIETER JM & VISSER PJ

1999. *Law of Delict*. 3rd Edition. Butterworths:Durban.

1996. *Neethling's Law of Personality*. 3rd Edition. Butterworths:Durban.

NEL SS

1992. Die strafbaarstelling van rekenaarvirusbesmetting. *SACJ* p142.

1990. *Rekenaarbetreding met spesifieke verwysing na rekenaarvirusse*. LLM: UNISA.

NICCOLAE J

2000. 'South Park' Trojan can create e-mail storms. *Computing SA* 13 March p27.

OPPLIGER R

1998. Security at the Internet layer. *Computer* Sept p43.

OUTING S

1997. E-Mail Bombs and Journalists. (10/01/1997)

www.mediainfo.com/ephome/news/newshtm/stop/st011097.htm.

PAAR R

2000. Circle the wagons against cybercrime. *New York Law Journal* (04/12/2000)

www.legalinnovators.com/SeenInPrint/Publications/PDF/cybercrime.pdf.

PAYNE H

1998. Feeding on globalisation. *Financial Mail* 10 July p35.

PLANTING S

2000(a). Sneaks in the server. *Financial Mail* 7 April p80.

2000(b). Strike against SA companies. *Financial Mail* 21 April p77.

RAUTENBACH IM

2001. The conduct and interest protected by the right to privacy in section 14 of the Constitution. *TSAR (Tydskrif vir die Suid-Afrikaanse Reg: Journal of South African Law)* p115.

RUTHERFORD BR

2000. Well-known marks on the Internet. *SA Merc LJ* p175.

RYRIE T

1999(a). E-commerce: coming ready or not. *Charter* Vol 70(5) June p44.

1999(b). For your eyes only? *Charter* Vol 70(7) Aug p46.

SCALA G

2000. Edgars hacker faces prosecution. *Computing SA* 27 March p1.

SHEARMAN A

2000. Hack the planet. www.cs.uct.ac.za/courses/CS400W/NIS/papers00/andy/dos.htm.

SKEEN Q

1984. Computers and Crime. *SACJ* p262.

SNYMAN CR

1999. *Strafreg*. 4th Edition. Butterworths:Durban.

1975. Die begrip "toe-eiening" in die omskrywing van diefstal. *THRHR* p29.

1972. Die vereistes van contrectatio en lucrum by furtum in die Romeinse Reg. *Acta Juridica* p271.

STANLEY B

2000. Credit card hacker demands R60m ransom. (18/01/2000) www.iol.co.za.

STEENKAMP W

2001. Computer hackers leave gambling bosses red faced. *Saturday Weekend Argus* 6 May p9.

STEWART DJ

2000. Help, hackers stole our name! (21/11/2000) www.law.com.

STEYTLER NC

1998. *Constitutional Criminal Procedure – a commentary on the Constitution of the Republic of South Africa, 1996*. Butterworths:Durban.

STUART B

2000. New bill challenges hackers. *The Citizen* 19 Oct p9.

THIEL G

2001. Cyber-terrorists hack into Mbeki's credit card. *Cape Times* 7 Feb p4.

THOMAS JAC

1975. *The Institutes of Justinian*. Juta:Cape Town.

THOMPSON T

2000. Police cover blown by cyber-spies. *Mail & Guardian* 6 April p36.

UHLIG R & CAVE A

2000. Hackers open window on Microsoft's inner secrets. *Sunday Times* 29 Oct p1.

VAN DER LINDE J

1828. *Regtsgeleerd, Practicaal en Koopmans Handboek*. Amsterdam.

VAN DER MERWE DP

2000. *Computers and the Law*. 2nd Edition. Juta:Cape Town.

1999. Die regsimplikasies van elektroniese handeldryf. *THRHR* p226.

1987. Theft of incorporeals in the form of information. *Magistrate Dec Vol* 22(4) p38.

1985. Diefstal van onliggaamlike sake met spesifieke verwysing na rekenaars. *SACJ* p129.

VAN HEERDEN HJO & NEETHLING J

1995. *Unlawful Competition*. Butterworths:Durban.

VAN LEEUWEN S

1780. *Het Roomsche Hollandsche Recht*. Amsterdam.

1741. *Censura Forensis*. Amsterdam.

VAN NIEKERK R

2001. SA e-commerce at crucial point. (04/04/2001) www.news24.co.za.

VERLOREN VAN THEMAAT JP

1949. *Diefstal en, in verband daarmee, bedrog in die Romeins-Hollandse Reg*. LLD:Pretoria.

VOET J

1698. *Commentarius Ad Pandectas*. Amsterdam.

VOGES J

2001. Protect your web assets now! *Smart Business Computing* March/April p36.

WEBSTER C

1998. Legal rights and the Internet. *Juta's Business Law* Vol 6(1) p2.

WILLAN P

2000. Mafia caught attempting online bank fraud. *Computing SA* 9 Oct p13.

WING M

2001. Computer crime – ignorance is bliss? A practical guide to how to avoid being hacked.
<http://darby.butterworths.co.uk/articles/article2.htm>.

WHIPPLE LC

1999. To improve security, log system activity. *e-Business Advisor* March p10.

WOLF J

2000(a). FBI warns of new cyber attacks. (13/12/2000) www.news24.co.za/news24/.

2000(b). Love bug only tip of virus iceberg. (10/5/2000) www.iol.co.za.

LIST OF REPORTS

AMERICA

AMERICAN BAR ASSOCIATION

1996. *Digital Signature Guidelines*. www.abanet.org/scitech/ec/isc/dsgree.html.

US DEPARTMENT OF JUSTICE

1998. The National Information Infrastructure Protection Act of 1996. www.usdoj.gov/criminal/cybercrime/1030_anal.html.

EUROPE

COMMISSION OF THE EUROPEAN COMMUNITIES

2001. eEurope 2002 - Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime. (26/01/2001). <http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeCommEN.html>.

EUROPEAN COMMITTEE OF MINISTERS OF THE COUNCIL OF EUROPE

2001. *Explanatory Report to the Convention on Cybercrime*. <http://conventions.coe.int/treaty/EN/projets/FinalCyberRapex.htm>.

WORLD INTELLECTUAL PROPERTY ORGANISATION

2001. *Convention on Cybercrime*.

<http://conventions.coe.int/treaty/EN/projets/FinalCyberCrime.htm>.

2000. *Primer on Electronic Commerce and Intellectual Property Issues*. <http://ecommerce.wipo.international/primer/index.html>.

SOUTH AFRICA

DEPARTMENT OF TELECOMMUNICATIONS

2000. *Green Paper on Electronic Commerce*. www.ecomm-debate.co.za/greenpaper/index.html.

SOUTH AFRICAN LAW COMMISSION

2001. *Discussion Paper 99: 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*.

www.law.wits.ac.za/salc/discussn/dp99.pdf.

TABLE OF CASES

AMERICA

America Online Inc v LCGM Inc 46 F.Supp. 2d 444 (E.D. Va. 1998).
America Online Inc v National Health Care Discount Inc 121 F.Supp. 1255 (N.D. Iowa 2000).
American Guarantee & Liability Insurance v Ingram Micro Inc 2000 WL 726789 (D.Ariz. 2000).
Andersen Consulting LLP v UOP and Bickel & Brewer 991 F.Supp. 1041 (N.D. ILL. 1998).
Brookfield Communications Inc v West Coast Entertainment Corp 174 F.3d 1036 (9th Cir. 1999).
Corcoran v Sullivan 112 F.3d 836 (7th Cir. 1997).
Hotmail Corporation v Van\$ Money Pie Inc et al 47 USPQ 2D (BNA) 1020 (N.D. Cal. 1998).
International News Service v The Associated Press 248 US 215 (1918).
Katz v United States 389 US 347 (1967).
Moulton & Network Installation Computer Services Inc v VC3 (N.D. Ga. 2000).
North Texas Preventive Imaging LLC v Eisenberg 1996 US Dist. LEXIS 19990 (C.D. Cal. 1996).
Parker et al v C.N. Enterprises et al (Tex. Travis County Dist. Ct. Nov. 10, 1997).
Playboy Enterprises Inc v Webbworld Inc et al 968 F.Supp 1171 (N.D. Tex. 1997).
Retail Systems Inc v CNA Insurance Companies 469 N.W.2d 735 (Minn. Ct. Appl 1991).
Shurgard Storage Centers Inc v Safeguard Self Storage Inc 119 F.Supp.2d 1121 (W.D. Wash. 2000).
Sporty's Farm v Sportman's Market 202 F.3d 489 (2d Cir. 2000).
US v Czbinski 106 F.3d 1069 (1st Cir. 1997).
US v Middleton 231 F.3d 1207 (9th Cir. 2000).
US v Morris 928 F.2d 504 (2nd Cir. 1991).
Yournetdating LLC v Mitchell et al 88 F.Supp.2d 870 (N.D. ILL. 2000).

AUSTRALIA

Kennison v Daire 1985 38 SASR 404.

CANADA

R v Stewart 1988 1 SCR 963; 1988 (50) DLR (4th) 1 SCC.

SOUTH AFRICA

Alper & Alper v R 1931 NPD 431.

Badenhorst v Balju, Pretoria Sentraal, & Andere 1998 4 SA SA 132 T.
Bernstein & Others v Bester & Others NNO 1996 2 SA 751 CC; 1996 4 BCLR 449 CC.
Bruyns v R 1901 NLR 75.

Coolair Ventilator Co (SA) (Pty) Ltd v Liebenberg & Another 1967 1 SA 686 W.

De Fourd v Town Council of Cape Town 1898 SC 399.
De Wet v Santam Bpk 1996 1 SA 926 A.
Dun & Bradstreet (Pty) Ltd v SA Merchants Combined Credit Bureau (Cape) (Pty) Ltd 1968 1 SA 209 C.
Du Plessis & Others v De Klerk & Another 1996 3 SA 850 CC.

Easyfind International (SA) (Pty) Ltd v Instaplan Holdings & Another 1983 3 917 W.
Ex Parte Minister of Justice: in Re R v Gesa; R v De Jongh 1959 1 SA 235 A.
Ex Parte Minister of Justice: in Re R v Maserow & Another 1943 AD 164.

Financial Mail (Pty) Ltd & Others v Sage Holdings Ltd & Another 1993 2 SA 451 A.

Gordon Lloyd Page & Associates v Rivera & Another 2001 1 SA 88 SCA.

Harchris Heat Treatment (Pty) Ltd v ISCOR 1983 1 SA 548 T.
Hewlett v Minister of Finance & Another 1982 1 SA 490 ZSC.
Ho Si v Vernon 1909 TS 1074.

James Walter Hill-Cathrine (Appellant) v The Clerk of the Peace for the County of Klip River (Respondent) 1890 NPD 69.

Janit & Another v Motor Industry Fund Administrators (Pty) Ltd & Another 1995 4 SA 293 A.
Janse van Vuuren & Another NNO v Kruger 1993 4 SA 842 A.
Johannesburg Municipality v Cohen's Trustee 1909 TS 811.

Kohrs v R 1940 NPD 11.

Manamela & Another v S 1999 4 ALL SA 161 W.

Maswana v R 1909 EDC 253.

Mbala v S 1969 1 PH H44 E.

Meter Systems Holdings Ltd v Venter & Another 1993 1 SA 409 W.

Moodley v R 1914 NPD 514.

Motor Industry Fund Administrators (Pty) Ltd & Another v Janit & Another 1994 3 SA 56 W.
MV Snow Delta Serva Ship Ltd v Discount Tonnage Ltd 2000 4 SA 746 SCA.

National Media Ltd & Another v Jooste 1996 3 SA 262 A.

O'Keeffe v Argus P & P Co Ltd & Another 1954 3 SA 244 C.
Osman v Attorney-General of Transvaal 1998 1 SACR 28 T.

Padyachi v R 1919 NPD 145.

Petersen v R 1909 TS 263.

Premier Western Cape & Others v Parker & Mohammed & Others 1999 1 ALL SA 176 C.

Protea Technology Ltd v Wainer 1997 9 BCLR 1225 W.

R v Arbee 1956 4 SA 438 A.

R v Attia 1937 TPD 102.

R v Barry 1932 TPD 312.

R v Bazi 1943 EDL 222.

R v Bedhla 1929 TPD 276.

R v Bhardu 1945 AD 813.

R v Bowden 1957 3 SA 148 T.

R v Buffel Dikgat 1928 GWL 11.

R v Carelse and Kay 1920 CPD 471.

R v Cheeseborough 1948 3 SA 756 T.

R v Coertzen 1929 SWA 20.

R v Coovadia 1957 3 SA 611 N.

R v Correia 1958 1 533 A.

R v Dane 1957 2 SA 472 N.

R v D'Arcy & Others 1934 GWL 8.

R v Davies 1928 AD 165.
R v Davies & Another 1956 3 SA 52 A.
R v De Beer 1940 OPD 268.
R v De Jongh 1959 1 SA 235 A.
R v Dettbarn 1930 OPD 188.
R v De Vos 1898 EDC 145.
R v Dick 1969 3 SA 267 R.
R v Dier 1869 3 EDC 436.
R v Dhlamini 1943 TPD 20.
R v Essop 1918 TPD 275.
R v Fortuin 1915 CPD 757.
R v Frankfort Motors (Pty) Ltd & Others 1946 TPD 255.
R v Gordon 1916 CPD 69.
R v Gush 1934 AD 260.
R v Harlow 1955 3 SA 259 C.
R v Hedley 1930 CPD 113.
R v Henkes 1941 AD 143.
R v Heyne & Others 1956 3 SA 604 A.
R v Holliday 1927 CPD 395.
R v Hyland 1924 TPD 336.
R v Ismail & Another 1958 1 SA 206 A.
R v J 1958 4 SA 488 A.
R v Jackelson 1920 AD 486.
R v Jass 1965 3 SA 248 E.
R v Joffe 1925 TPD 86.
R v Jolosa 1903 TPD 694.
R v Jones and More 1926 AD 350.
R v Karolia 1956 3 SA 569 T.
R v Kinsela 1961 3 SA 519 C.
R v Kruse 1946 AD 524.
R v Kumana 1900 EDC 167.
R v Kwessa 1947 1 SA 428 C.
R v Laforte 1922 CPD 487.
R v Laubscher and Others 1913 CPD 123.
R v Lee 1952 2 SA 67 T.
R v Lionda 1944 AD 348.
R v Longone 1938 AD 532.
R v Macatlane 1929 TPD 708.
R v Malamu Nkatlapaan 1918 TPD 424.
R v Manuel 1953 4 SA 523 A.
R v Maritz 1944 EDL 101.
R v Markins Motors (Pty) Ltd & Another 1959 3 SA 508 A.
R v Maruba 1942 OPD 51.
R v Mashanga 1924 AD 11.
R v Mavros 1921 AD 19.
R v Maxaulana 1953 2 SA 252 E.
R v Medziso 1950 4 SA 282 R.
R v Meer 1923 OPD 77.
R v Milne & Erleigh 1951 1 SA 791 A.
R v Mlooi 1925 AD 131.
R v Mofokeng 1939 OPD 116.
R v Moilwanyana & Others 1957 4 SA 608 T.
R v Monyane en 'n Ander 1960 3 SA 20 T.
R v Muller 1938 OPD 141.

R v Naidoo 1949 4 SA 858 A.
R v Nbakwa 1956 2 SA 557 SR.
R v Ncetendaba and Another 1952 2 SA 647 SR.
R v Ncuba 1968 2 SA 18 R.
R v Nkomozombanzo 1959 1 SA 746 SR.
R v Nkwana 1953 2 SA 190 T.
R v Nlhovo 1921 AD 485.
R v Olakawu 1958 2 SA 357 C.
R v Oliver and Others 1921 TPD 120.
R v Patz 1946 AD 845.
R v Palane; R v Frans 1947 3 SA 270 T.
R v Panter 1932 TPD 121.
R v Peerkan & Lalloo 1906 TS 798.
R v Pretorius 1908 TPD 272.
R v R 1954 2 SA 134 N.
R x Rasool 1924 AD 44.
R v Rautenbach 1943 OPD 60.
R v Reikert 1874 Buch 142.
R v Renaud 1922 CPD 322.
R v S 1955 3 SA 313 SWA.
R v Saffy & Bennett 1944 AD 391.
R v Seabe 1927 AD 28.
R v Scholtz 1942 CPD 118.
R v Schonken 1928 AD 36.
R v Schoombie 1945 AD 541.
R v Segal & Others 1960 1 SA 721 A.
R v Sejosengoe 1935 EDL 474.
R v Shelembe 1955 4 SA 410 N.
R v Sibiya 1955 4 SA 247 A.
R v Sibiya 1957 1 247 T.
R v Siboya 1919 EDL 41.
R v Silburn & Shearing 1903 24 NLR 527.
R v Sipendu 1932 EDL 312.
R v Smulian 1928 TPD 762.
R v Swart 1932 TPD 168.
R v Teichert 1958 3 SA 747 N.
R v Terblanche 1933 OPD 65.
R v Thebeta 1948 3 SA 218 T.
R v Toni 1949 1 SA 109 A.
R v Umfaan 1908 TS 62.
R v Ungwaja 1891 12 NLR 284.
R v Vilakazi 1959 4 SA 700 N.
R v Van der Bank 1941 TPD 307.
R v Van Rooy & Another 1920 CPD 695.
R v Von Elling 1945 AD 234.
R v Walton 1958 3 SA 693 SR.
R v Weiss 1932 AD 41.
R v Wiese & Another 1928 TPD 149.
R v Witbooi Motaung 1954 2 PH H 116 O.
R v Wolff 1930 TPD 821.
R v Xabanisa 1946 EDL 167.
R v Zeelie 1952 1 SA 400 A.
Reid-Daly v Hickman and Others 1981 2 SA 315 ZAD.
Rhodesian Printing & Publishing Co Ltd v Duggan and Another 1975 1 SA 590 RA.

S v A 1971 2 SA 293 T.
S v Abrahams en 'n Ander 1998 1 SACR 314 K.
S v African Bank of South Africa Ltd & Others 1990 2 SACR 585 W.
S v Augustine 1986 3 SA 294 C.
S v Boesak 2000 1 SACR 633 SCA.
S v Botha 1970 1 SA 688 T.
S v Bolus & Another 1966 4 575 A.
S v Boshoff 1962 3 SA 175 N.
S v Bugwandeem 1987 1 SA 787 N.
S v Campbell 1991 1 SACR 503 Nm.
S v Cassiem 2001 1 SACR 489 SCA.
S v Daniels 1970 3 SA 96 E.
S v Dreyer 1967 4 SA 614 E.
S v Dube 2000 1 SACR 53 N.
S v Du Plessis 1981 3 SA 382 A.
S v Du Preez 1998 2 SACR 133 K.
S v Du Toit 1995 2 SACR 651 K.
S v Ganyu 1977 4 SA 810 RAD.
S v Gordon 1962 4 SA 727 N.
S v Graham 1975 3 SA 569 A.
S v Hammer & Others 1994 2 SACR 496 C.
S v Harper 1981 2 SA 638 D.
S v Heller 1971 2 SA 29 A.
S v Isaacs 1968 2 SA 187 D.
S v Jana 1981 1 SA 671 T.
S v Kariko & Another 1998 2 SACR 531 NmHC.
S v Karsen 1961 2 PH H176 T.
S v Kearney 1964 2 SA 495 A.
S v Kgware and Another 1977 2 SA 454 O.
S v Khoza 1982 3 SA 1019 A.
S v Khumalo 1964 1 SA 498 N.
S v Kidson 1999 1 SACR 338 W.
S v Kimmich 1996 2 SACR 200 C; 1996 2 ALL SA 403 C.
S v Kotze 1965 1 SA 118 A.
S v Kruger & Another 1961 4 SA 816 A.
S v Lamont 1977 2 SA 679 RAD.
S v Langa & Others 1998 1 SACR 21 T.
S v Laurence 1975 4 SA 825 A.
S v Levy & Another 1967 1 SA 351 W.
S v Lungile & Another 1999 2 SACR 597 SCA.
S v Luther en 'n Ander 1962 3 SA 506 A.
S v M 1982 1 SA 309 O.
S v Mahlangu & Andere 1995 2 SACR 425 T.
S v Mangquku 1971 2 SA 365 E.
S v Maxaba en 'n Ander 1981 1 SA 1148 A.
S v Mbokazi 1998 2 ALL SA 78 N.
S v Mintoor 1996 1 SACR 514 C.
S v Mkhize 1980 4 SA 37 N.
S v Mlambo 1986 4 SA 34 E.
S v Mnyandu 1973 4 SA 603 N.
S v Mohapie 1969 4 SA 446 C.
S v Moller 1990 3 SA 876 A.
S v Momberg 1970 2 SA 68 C.

S v Mtetwa 1963 3 SA 445 N.
S v Mtshali 1960 4 SA 252 N.
S v Myeza 1985 4 SA 30 T.
S v Naryan 1998 2 ALL SA 345 W.
S v Nathie 1964 3 SA 588 A.
S v Ncube en 'n Ander 1998 1 SACR 174 T.
S v Ndhlela 1964 4 SA 703 N.
S v Nedzamba 1993 1 SACR 673 V.
S v Nel 1970 4 SA 440 T.
S v Nkosiyana & Another 1966 4 SA 655 A.
S v Ohlenschlager 1992 1 SACR 695 T.
S v Ostilly & Others 1977 4 SA 699 D.
S v Ressel 1968 4 224 A.
S v Rheeder 2001 1 SA 348 SCA.
S v Salemane 1967 3 SA 691 O.
S v Schwartz 1980 4 SA 588 T.
S v Shepard 1967 4 SA 170 W.
S v Siswana 1968 4 SA 251 E.
S v Solomon 1973 4 SA 644 K.
S v Steenberg 1999 1 SACR 594 N.
S v Swarts en 'n Ander 1961 4 SA 589 OK.
S v Stevenson 1976 1 SA 636 T.
S v Ushewokunze 1971 2 SA 362 RAD.
S v Tekane en 'n Ander 1998 1 SACR 291 O.
S v Tshwape & Another 1964 4 SA 327 C.
S v Van Bijlon 1965 3 SA 314 T.
S v Van den berg 1979 3 SA 1027 NK.
S v Van der Berg 1991 1 SACR 104 T.
S v Verwey 1968 4 SA 682 A.
S v Vilakasi and Another 1999 2 SACR 393 N.
S v Visagie 1991 1 SA 177 A.
S v Willcocks Regional magistrate court case, no 41/273/83 (Durban).
S v Williams en 'n Ander 1980 1 SA 60 A.
S v Wilson 1962 2 SA 619 A.
S v Zuma 1992 2 SACR 488 N.
SA Historical Mint (Pty) Ltd v Sutcliffe & Another 1983 2 SA 84 C.
Sage Holdings Ltd & Another v Financial Mail (Pty) Ltd & Others 1991 2 SA 117 W.
Standard Bank of South Africa v Coetsee 1981 1 SA 1131 A.
Steward v R 1934 NPD 340.

Tie Rack plc v Tie Rack Stores (Pty) Ltd & Another 1989 4 SA 427 T.
Thompson & Strydom 1964 1 PH H4 N.
Tommy & Others v R 1931 NPD 317.

Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk 1977 4 SA 476 T.
Union Share Agency & Investment Ltd v Spain 1944 AD 74.

Van Castricum v Theunissen & Another 1993 2 SA 726 T.

Weber-Stephen products Co v Alrite Engineering (Pty) Ltd & Others 1990 2 SA 718 T.

UNITED KINGDOM

Attorney General's Reference (No1 of 1991) 1992 3 ALL ER 897 CA.

Morphitis v Salmon 1990 Crim LR 48.

R v Bow Street Magistrates Court and Allison, Ex Parte Government of the United States of America 1999 4 ALL ER 1 HL.

Re London & Globe Finance Corporation 1903 1 Ch 728.

R v Whiteley 1991 93 Cr App R 25.

TABLE OF STATUTES AND DRAFT LEGISLATION

AMERICA

Computer Fraud and Abuse Act of 1984.
Georgia Computer Systems Protection Act Title 16, ch 9, s 90.
Virginia Computer Crimes Act.

CANADA

Canadian Criminal Code R.S. 1985.

EU

2001. Convention on Cybercrime.
<http://conventions.coe.int/treaty/EN/projets/FinalCyberCrime.htm>.

SINGAPORE

Singapore Computer Misuse Act (Chapter 50A) of 1998.

THE NETHERLANDS

Wetboek van Strafrecht.

SOUTH AFRICA

Adjustment of Fines Act 101 of 1991.
Close Corporations Act 69 of 1984.
Constitution 108 of 1996.
Copyright Act 98 of 1978.
Correctional Services Act 111 of 1998.
Criminal Procedure Act 51 of 1977.
Electricity Act 41 of 1987.
General Law Amendment Act 62 of 1955.
General Law Amendment Act 50 of 1956.
Interception and Monitoring Bill 50 of 2001.
Interception and Monitoring Prohibition Act 127 of 1992.
Interim Constitution 200 of 1993.
Internal Security Act 74 of 1982.
Judicial Matters Amendment Act 62 of 2000.
Magistrates' Act 32 of 1944.
National Prosecuting Authority Act 32 of 1998.
National Prosecuting Authority Amendment Bill 39b of 2000.
Riotous Assemblies Act 17 of 1956.
South African Police Service Act 68 of 1995.
Trespass Act 6 of 1959.

UNITED KINGDOM

Computer Misuse Act 18 of 1990.
Criminal Damage Act of 1971.
Theft Act 60 of 1968.

KEY TERMS

Computer crimes; cybercrimes; computer-related crimes; hacking; viruses; denial-of-service attacks; theft; malicious injury to property; fraud; crimen iniuria.

D.O.V.S. BIBLIOTEK