CHAPTER 3

UNAUTHORISED ACCESS

3.1 INTRODUCTION

The motion picture *WarGames*[1] about a teenage hacker that accidentally hacks into the Pentagon's computer system romanticised the phenomenon of hacking but also induced fear in many as to the possibility of a computer induced nuclear war.[2] The widely publicised *414 Gang* was a group of young people from Milwaukee (414 is the area code for Milwaukee) that gained unauthorised access to computers in the United States and Canada in the early 1980s.[3] The *414 Gang* managed to hack into a cancer institute's computer system that stored records of cancer patient's radiation treatment. The publicity attached to the *414 Gang* placed computer security and ethics in the limelight. In 1985 Hugo Cornwell[4] published his notorious book *The Hacker's Handbook*.[5] As a self-proclaimed hacker he ventures onto dangerous ground with his romanticised version of the hacking phenomenon and even attributes a short paragraph to so-called hackers etiquette. He states:

---

[1] Metro Goldwyn Mayer 1983.

[2] Jay BloomBecker *Computer Crime update: The view as we exit* (1984) Western New England Law Review Vol. 7 628. Also see Chris Reed(ed) *Computer Law* (1990) 163.

[3] Jay BloomBecker, Esq *Modem macho in Milwaukee* published in Computer Crime Digest (1983) Vol. 1 No.13 1 *et seq*.; BloomBecker (footnote 2 *supra*) 630 *et seq*.; *Balancing the scales: Computer Crime Legislation* (1985) Datapro Research Corporation USA.

[4] This is an alias. The author's real name is Peter Sommer and he wrote the first three editions of the book. The fourth edition was written by Steve Gold who was unsuccessfully prosecuted for the *Presstel* hack [See Computer Law and Practice (1989) Vol. 6 No. 1 31 and paragraph 3.4.2 *infra*].

[5] Published in 1985 by Century Communications Ltd. London.

> "don't manipulate files unless you are sure a back-up exists; don't crash operating systems; don't lock legitimate users out from access; watch who you give information to; if you really discover something confidential, keep it to yourself. Hackers should not be interested in fraud."[6]

It is not surprising that authorities called for a ban on this publication. There is even a hacker's manifesto in which it is claimed that a hacker's only crime is that of curiosity. Locally there are many instances of hacking although very few are actually reported and publicised.

3.2 WHAT IS HACKING?

Hacking is probably the first type of new computer offence that emerged with the advent of the computer and the most well known. Originally the term *hacker* referred to a computer programmer or specialist that designed software and pushed computer programs beyond their limits. The term also refers to computer fanatics.[7] The term *hacker* was later used by the media to label computer criminals who abuse computers and computer systems.

The formal description is unauthorised access and occurs when a person[8] gains access to a computer or computer system without authority to do so.[9] Bainbridge defines computer hacking as

---

[6] Page 4.

[7] Deirdre Black *The computer hacker – electronic vandal or scout of the networks* (1993) Journal of Law and Information Science Vol. 4 No. 1 67.

[8] There seems to be a perception that hackers are mostly male. See B Gordon *Internet Criminal Law* in Buys (ed) *Cyberlaw @ SA* (2000) footnote 7 on page 447.

[9] Gordon (footnote 8 *supra*) 425.

> "the accessing of a computer system without the express or implied permission of the owner of that computer system".[10]

A hacker uses a computer terminal to access sometimes a much larger computer system that may even be situated in a different part of the world.[11] It is a type of *electronic trespassing*[12] or *virtual breaking and entering*[13]. As Gordon points out the problem is not the access but rather the *unauthorised* access to a computer system.[14] It has also been referred to as *browsing*.[15]

Hacking should be distinguished from the term *cracking*.[16] A hacker penetrates a system for the glory or fun of it or for educational purposes (by conquering security measures), but a cracker accesses a computer system with an ulterior motive for example obtaining credit card numbers for subsequent fraudulent use, to cause damage or perhaps to crash the system.[17] The latter can cause considerable damage and are feared in the

---

[10] David I Bainbridge *Introduction to Computer Law* (2000) 307.

[11] Adv B Gordon *Computer Crime – An Introduction* (2002) February Servamus 35.

[12] See Martin Wasik *Crime and the Computer* (1991) 69; Martin L Forst *Cybercrime: Appellate Court Interpretations* (1999) 13 *et seq*.; Neil Ulrich *Wetgewing teen elektroniese betreding* (1998) UNISA (Magister Legum dissertation).

[13] F Lawrence Street & Mark P Grant *Law of the Internet* 2000 Edition (1999) 656.

[14] Gordon (footnote 11 *supra*) 35. The hacker 'breaks into' the system.

[15] Christopher D Chen *Computer Crime and the Computer Fraud and Abuse Act of 1986* (1990) Computer Law Journal Vol. X No. 1 79.

[16] See Buys(ed) *Cyberlaw @ SA* (2000) 425 and Buys(ed) *Cyberlaw @ SA II* (2004) 327.

[17] Eric J Sinrod & William P Reilly *Hacking your way to hard time: application of computer crime laws to specific types of hacking attacks* (2000) Journal of Internet Law Vol. 4 No. 3 3.

corporate world. Crackers usually have malicious intent.[18] It is said that hacker purists do not condone damage to computer systems.[19]

Hackers are usually young, intelligent people with an interest in information technology and computers.[20] There seems to be a perception that hackers are mostly male most probably due to the fact that the most well known hackers are male.[21] Hackers usually have interesting nicknames. Convicted hacker Kevin David Mitnick[22] used the name *Condor* and was listed in the telephone directory as *James Bond*.[23] Some hackers gain unauthorised access to computers in order to overcome extremely specialised computer security measures and some are actually used as computer security consultants.[24] Hackers that use their abilities for personal gain or with malicious intent are referred to in hacker circles as *Black Hats* and those "reformed" hackers that use their hacker knowledge and abilities for a good cause are referred to as *White Hats*.[25] Many corporations and security companies are actually of the view that it takes one cyber criminal to catch another.[26]

---

[18] Sinrod & Reilly (footnote 17 *supra*) 3; Jeff Crume *Inside Internet Security* (2000) 20 *et seq*.

[19] Sinrod & Reilly (footnote 17 *supra*) 3.

[20] See P Carstens & A Trichardt *Computer Crime by Means of the Automated Teller Machine – Just Another Face of Fraud* (1987) SACC 122 *et seq*. and C M B Naude *Rekenaarmisdaad: 'n Skewe beeld?* (1983) 7 SACC 168.

[21] The male personal pronoun will be used in the text.

[22] See paragraph 3.4.1.1 *infra*.

[23] Glenn D Baker *Trespassers will be prosecuted: Computer crime in the 1990s* (1993) Computer Law Journal Vol. XII No. 1 72 *et seq*.; Jeff Crume *Inside Internet Security* (2000) 27 – 28.

[24] Black (footnote 7 *supra*) 73.

[25] Sinrod & Reilly (footnote 17 *supra*) 2. Also see the National Geographic Special entitled *Cyberwars*.

[26] Don Robertson *Reformed hackers turn the tables* Sunday Times (Business Times) 12/10/2003 page 1.

Unauthorised access can be gained to a system through a myriad of ways. Some hackers guess the password or do investigation in order to obtain the password to a computer, network or system. Some computer users write down their passwords or use very-easy-to-guess passwords. Computer users often write down their passwords or pin codes and store them in an easy accessible area. The jargon term *scavenging* refers to the searching of physical areas such as trash bins to obtain information such as passwords as well as searching in an information system for residual pieces of data.[27] This information is sometimes used or assists to secure access to a computer or network. The term *piggy-backing* involves "gaining access to a computer by 'riding in' on the password of an authorised user".[28] System programmers sometimes leave *back doors* in order to gain easy access to a computer in order to repair the computer at a later stage. *Back doors* are occasionally used by hackers to secure unauthorised access to computers and computer systems. There are many software applications and devices that facilitate the unauthorised access to data.[29]

3.3 SHOULD HACKING BE CRIMINALISED?

One of the key debates was whether offences like hacking should be criminalised. Hugo Cornwall wrote in the first edition of *The Hacker's Handbook* that hacking is a re-assertion of the concepts of freedom, individuality and human worth.[30] It is quite clear that many hackers don't

---

[27] Dana van der Merwe *Computers and the Law* (2000) 170; Irving J Sloan *The Computer and the Law* (1984) 14.

[28] Van der Merwe (footnote 27 *supra*) 169.

[29] See chapter 7 *infra*.

[30] Hugo Cornwall *The Hacker's Handbook* (1985) 111.

believe that hacking is a crime, but rather refer to it as a "recreational and educational sport".[31] Hackers believe that information should be accessible to every person and pride themselves in the distribution of "free" software. After an evaluation of some of the arguments, Coldwell concludes that hacking exists in a state of *anomie*[32].[33]

At the centre of this debate locally are the rights to freedom of expression[34], access to information[35] and privacy[36], all rights protected by the South African Constitution[37]. The South African Law Commission concluded that unauthorised access to data or computer systems should be criminalised or sanctioned with a criminal penalty.[38] The invasion of a person's right to privacy may lead to a criminal sanction.[39] People value their privacy and this constitutionally entrenched right should be vigorously protected. Similarly this protection should be extended to information that is of personal or economic value and in electronic format.[40] Unauthorised access to data contained in a computer system

---

[31] Cornwall (footnote 30 *supra*) vii.

[32] Refers to a society with unclear or conflicting value systems or norms.

[33] R A Coldwell *Hacking into computer systems, anomie and computer education* (1998) Acta Criminologica Vol. 11 No. 1 15-18. For a detailed discussion of the arguments in favour and against the criminalisation of hacking see Brenda Nelson *Straining the capacity of the law: The idea of computer crime in the age of the computer worm* (1991) Computer Law Journal Vol. XI 299-321.

[34] Section 16 of Act 108 of 1996.

[35] Section 32 of Act 108 of 1996.

[36] Section 14 of Act 108 of 1996.

[37] Constitution of the Republic of South Africa, Act 108 of 1996.

[38] SA Law Commission Discussion Paper 99 Project 108 *Computer-related crime: Preliminary proposals for reform in respect of unauthorised access to computers, unauthorised modification of computer data and software applications and related procedural aspects* (2001) pages 3-5.

[39] Such as the offence of *crimen iniuria*.

[40] SA Law Commission Report (footnote 38 *supra*) 4.

infringes upon the constitutionally protected right to privacy.[41] One cannot just enter a bank and demand access to the confidential files of other bank customers. The emphasis is further on the *unauthorised* access to systems. The integrity of computer systems is greatly depended upon in our modern society and should be jealously guarded and protected. In a modern technological world computer systems should be protected against the intrusions of computer criminals.

Every person has the right to access to information held by the State and any information that is held by a person and that is required for the exercise or protection of any rights.[42] The Promotion of Access to Information Act[43] however specifically prescribes the procedure that must be followed in order to secure access to certain information. In light of these provisions it is clear that a person may not merely hack into a system in order to obtain such information.

3.4 COMPARATIVE LAW ANALYSIS IN RESPECT OF HACKING[44]

3.4.1 United States of America

The United States of America was probably the first country to criminalise hacking by enacting legislation at federal as well as state level. Federal legislation operates at federal level, governs the entire

[41] See M M Watney *Die strafregtelike en prosedurele middele ter bekamping van kubermisdaad (deel 2)* (2003) TSAR 256.

[42] Section 32(1) of Act 108 of 1996.

[43] Act 2 of 2000.

[44] There are many countries that have criminalised hacking. The discussion below however is only directed at certain countries.

United States and is generally applicable. Individual State Laws are only applicable in a specific State.

3.4.1.1 Federal Laws

The Computer Fraud and Abuse Act[45] is the most important federal legislation in respect of unauthorised access to computers and inserted computer crimes into the Federal Code. The goal of the Act is to "protect the confidentiality, integrity, and availability of computer data and systems".[46] There have been quite a few amendments to the Federal Code in respect of computer-related offences.[47] Section 1030(a) of the United States Code states:

> "Whoever
> (1) 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 defence 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 wilfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated,

[45] 1986.

[46] Jonathan B Wolf *Chasing 21st Century Cybercriminals With Old Laws and Little Money* (2000) American Journal of Criminal Law Vol. 28 No. 1 109.

[47] Shani S Kennedy & Rachel Price Flum *Computer Crimes* (2002) American Criminal Law Review Vol. 39 No. 2 279.

delivered, or transmitted the same to any person not entitled to receive it, or wilfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) 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;

(3) intentionally, without authorization to access any non-public 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;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, 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

(5) ….

shall be punished as provided in subsection (c) of this section."[48]

[48] United States Code, 2000 Edition.

The offences created by this section are very detailed and complex in nature. The mere accessing of any computer is not an offence in terms of these provisions. There are additional elements that have to be met before this constitutes an offence. They are firstly directed at certain categories of data or information. Certain categories of computers or computer systems are protected by the Act such as government computer systems.[49] These provisions initially excluded computers of individuals (personal computers), most businesses and companies and limited the scope of application of the Code.[50] The original text of section 1030(a)(4) referred to a *federal interest computer* but was subsequently amended by the National Information Infrastructure Protection Act (NIIPA)[51] to read *protected computer*. A *protected computer* will now include government computers, financial institution computers and any computer which is used in interstate or foreign commerce or communications.[52] Computers that are connected to the Internet are now protected. The USA PATRIOT Act[53] amended the provisions further providing for protection against terrorism through a cyber war.[54] Secondly, a specific intent is also required, for example the intent to defraud or the obtaining of an advantage or the furtherance of a fraud.

---

[49] See section 1030 (e) (2) of the United States Federal Code.

[50] Steve Shackelford *Computer-Related Crime: An International Problem in Need of an International Solution* (1992) Texas International Law Journal Vol. 27 No. 2 488; Christopher D Chen *Computer Crime and the Computer Fraud and Abuse Act of 1986* (1990) Computer Law Journal Vol. X No. 1 79.

[51] 1996. In general see the legislative analysis by the US Department of Justice in respect of the NIIPA accessible at http://www.usdoj.gov/criminal/cybercrime/1030-anal.html .

[52] Section 1030(e)(2) of the United States Federal Code.

[53] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorist Act 2001. This Act was promulgated after the 9/11 terrorist attacks in the USA.

[54] Kennedy (footnote 47 *supra*) 280.

One of the main criticisms against the Act is that key concepts such as *without authorisation*, *use*, *affects* and *access* were not defined.[55] The Act was further criticised on the basis that large corporations and businesses that are often targeted by computer criminals, were initially not protected by the Act.[56] The mere access, trespass or browsing in respect of a computer or system is not an offence in terms of the Act.[57]

One of the first persons that were charged with contraventions of the Act was Kevin David Mitnick.[58] Mitnick gained unauthorised access to Digital Equipment Corporation's computer systems and billed the cost of telephone calls to another account. He was convicted *inter alia* of contravening section 1030(a)(6) which criminalises access to an interstate computer network for criminal purposes. He received one of the harshest sentences a hacker has ever received in the United States and was sentenced to one year's imprisonment, six months in a residential treatment program and three years probation.[59] Mitnick was also convicted of unauthorised access to the computer system of Tsutomu Shimomura, a well-known computer security expert.[60]

---

[55] Bart D Cohen *Computer Crime* (1988) American Criminal Law Review Vol. 25 No. 3 368; Steve Shackelford (footnote 50 *supra*) 488; Glenn D Baker *Trespassers will be prosecuted: Computer Crime in the 1990s* (1993) Computer Law Journal Vol. XII No. 1 71.

[56] Chen (footnote 50 *supra*) 79. The position is now different due to all the amendments to the Code.

[57] Chen (footnote 50 *supra*) 79 *et seq*.

[58] Dana van der Merwe *Computer crime – recent national and international developments* (2003) 66 THRHR 36 *et seq*.

[59] See Glenn D Baker *Trespassers will be prosecuted: Computer Crime in the 1990s* (1993) Computer Law Journal Vol. XII No. 1 72 *et seq*.

[60] Michael Fraase *Information eclipse (privacy and access in America)* (1999) 226 *et seq.*

3.4.1.2 Individual States

The United States of America consists of fifty States, each with its own laws that govern them. All of these states have enacted legislation criminalising computer offences and some form of unauthorised access or hacking. Some of these Acts criminalise computer trespass[61], whilst others focus on unauthorised access[62]. In some instances the mere unauthorised access are criminalised[63], whilst others criminalise unauthorised access with the intent to commit further offences such as fraud[64].

The California Comprehensive Data Access and Fraud Act inserted certain computer offences into the California Penal Code and section 502(c)(7) states that any person that "knowingly and without permission accesses or causes to be accessed any computer, computer system or computer network" is guilty of an offence. Access with the intent to commit further actions or offences are also criminalised in California.[65] An interesting prosecution was the Californian case of *People v Lawton*[66] where a computer programmer obtained access to private files stored in a local public library system. Lawton was convicted and on appeal contended that he had permission to use the computer just like any other library user. The Court held that the lawful use of a public computer to

[61] For instance the criminal codes in Arkansas, New York and Washington.

[62] For instance the criminal codes in Alabama, California, Connecticut, Delaware and Florida.

[63] For example section 53a-251 of the Connecticut statutes.

[64] For example section 30-45-3 of the New Mexico Statutes.

[65] Section 502(c) of the California Penal Code.

[66] (1996) 56 Cal.Rptr.2d 521.

obtain unauthorised levels of data not open to the public falls within the ambit of unauthorised access.[67]

In New York the offence of *computer trespass* criminalises the mere unauthorised access to computer material as well as the unauthorised access with the intent to " commit or attempt to commit or further the commission of any felony".[68] Washington has a crime of *computer trespass in the first degree* that consists of the intentional and unauthorised access to a computer system or electronic database where the access is secured with the intent to commit another crime or the access involves a computer or database maintained by a government agency.[69] In the case of *State v Olsen*[70] the accused was convicted of *computer trespass* after he had accessed a Washington Police Department computer in violation of departmental policy.[71] The defendant contended that he was authorised to access the computer. The Court held on appeal that there was insufficient evidence to find that the access was indeed unauthorised.

The definition of *access* in most State criminal codes is similar. Access is defined in the Alabama Code as "to instruct, communicate with, store data in or retrieve data from a computer, computer system or computer

---

[67] Martin L Forst *Cybercrime: Appellate Court Interpretations* (1999) 181 *et seq*.

[68] Article 156 of the New York Penal Law. Also see the BNA Special Report *Computer data security* (1989) C47 – C52.

[69] Section 9A.52.110 of the Washington Criminal Code. Also see Martin L Forst *Cybercrime: Appellate Court Interpretations* (1999) 173 *et seq*.

[70] (1987) 47 Wash.App 514.

[71] Forst (footnote 67 *supra*) 173 *et seq*.

network".[72] In terms of the Hawaii Revised Statutes *access* means "to make use of any resources of a computer, computer system or computer network". Some state codes contain a mixture of definitions for example access is defined in the New Mexico statutes as "to program, execute programs on, intercept, instruct, communicate with, store data in, retrieve data from or otherwise make use of any computer resources, including data or programs of a computer, computer system, computer network or database".[73]

3.4.2 United Kingdom

The Scottish Law Commission produced a working paper in 1987 in respect of computer-related crimes.[74] The ruling by the House of Lords in the case of *R v Gold and Schifreen* [75] that computer hacking was not a criminal offence under the British Forgery and Counterfeiting Act of 1981 highlighted the need for legislative intervention to *bring the criminal law up to date with technology.*[76] In 1988 the Law Commission for England and Wales produced a working paper dealing with computer

---

[72] Also see the Alaska statutes, State of Arkansas Code, Arizona Revised Statutes, Connecticut Statutes, Delaware Code, Georgia Code and Minnesota Statutes.

[73] Also see North Carolina General Statutes, North Dakota Century Code and Washington Criminal Code.

[74] See Colin Tapper *"Computer Crime": Scotch Mist?* (1987) The Criminal Law Review 4.

[75] [1988] 2 WLR 984.

[76] Andrew Charlesworth *Legislation against Computer Misuse: The trials and tribulations of the UK Computer Misuse Act 1990* (1993) Journal of Law and Information Science Vol. 4 No. 1 82. See Ian J. Lloyd *Information Technology Law* (2000) 218 *et seq*.; Martin Wasik *Crime and the Computer* (1991) 69 *et seq*.; Richard Dedman *The Computer Misuse Bill 1990* (1990-91) 1 The Computer Law and Security Report 13 *et seq*. Also see David I Bainbridge *Computer misuse: what should the law do?* (1989) Solicitors Journal Vol. 133 No. 15 466 *et seq*. The author argues that hacking could constitute an offence of abstracting electricity in terms of section 13 of the Theft Act 1968. Small amounts of electricity are used when a hacker gains access to a computer system. However the required *mens rea* would be difficult to prove since a hacker might not realise that he is unlawfully using electricity.

misuse.[77] Another working paper was released by the Law Commission in October 1989 entitled *Criminal law: Computer misuse*.[78] The Computer Misuse Bill was introduced[79] and in August 1990 the Computer Misuse Act[80] came into effect.[81] The Act created three new computer-related offences.[82] The hacking offence is found in section 1 of the Act and reads as follows:

> "A person is guilty of an offence if-
> (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 that at the time when he causes the computer to perform the functions that that is the case."

The term *computer* is not defined in the Act.[83] In fact the British Law Commission was of the opinion that it would be unwise or unnecessary to

---

[77] Law Commission Working Paper No. 110 *Computer Misuse*, 1988. HMSO. See in general Martin Wasik *Law Reform Proposals on Computer Misuse* (1989) The Criminal Law Review 257 *et seq*.; Martin Wasik *The Law Commission Working Paper on Computer Misuse* (1988-89) 5 Computer Law and Security Report 2 *et seq*.; Jeffrey Chapman *Computer misuse – a response to Working Paper No. 110* (1989) Computer Law & Practice Vol. 5 115 *et seq*.; Michael Heather *Law Commission Working Paper No. 110* (1989) Computer Law & Practice Vol. 5 171 *et seq*.; Morag Macdonald *Hacking* (1989) Computer Law & Practice Vol. 5 195 *et seq*.

[78] Law Commission Working Paper No. 186 *Criminal law: Computer misuse*, 1989. See in general Martin Wasik *Tackling technocrime: The Law Commission Report on Computer Misuse* (1989) Computer Law & Practice Vol. 6 No. 1 23 *et seq*.

[79] For a broad overview of the Bill see Richard Dedman *The Computer Misuse Bill 1990* (1990-91) 1 Computer Law and Security Report 13 *et seq*.; Peter Cooke *Computer Misuse Bill* (1990) Computers and Law Vol. 1 Issue 3 5 *et seq*.

[80] The Computer Misuse Act 1990.

[81] See Martin Wasik *The Computer Misuse Act 1990* (1990) Criminal Law Review 767 *et seq*.; Steve Shackelford *Computer-Related Crime: An International Problem in Need of an International Solution* (1992) Texas International Law Journal Vol. 27 No. 2 490 – 493; Chris Reed *Electronic Finance Law* (1991) 212 *et seq*.

[82] See A T H Smith *Property Offences* (1994) 355 *et seq*.

[83] Shackelford (footnote 81 *supra*) 492.

define the term *computer* and proposed that it be afforded its ordinary meaning.[84] This may prove to be problematic when one deals with instances such as *Cox v Riley*[85] where a computerised saw was the object of the crime. It may be argued that a computerised saw does not fall within the ordinary meaning of the term *computer*.[86]

Section 1 of the Computer Misuse Act, 1990 criminalises hacking and the elements are: (1) access to computer or data, (2) unlawfulness i.e. unauthorised access and (3) intention.[87] Interestingly the *actus reus* consists in causing a computer to perform any function with the intent to secure access and appears not to be limited to the actual accessing of a computer.[88] Section 17(5) of the Act states that access of any kind by any person to any program or data held in a computer is unauthorised, if he is not himself entitled to control access of the kind in question to the program and data, and he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled.[89] Unauthorised access includes instances where authorised users deliberately exceed their authority.[90]

---

[84] Law Commission Working Paper (footnote 77 *supra*) 87. Also see Mark Tantum *Hacking: drafting the law* (1989) Computer Law & Practice Vol. 5 193.

[85] (1986) 83 Cr App R 54 (DC).

[86] Shackelford (footnote 81 *supra*) 492. Also see Smith and Hogan *Criminal Law* 725.

[87] In general see Lloyd (footnote 76 *supra*) 228 *et seq*.; Smith and Hogan (footnote 86 *supra*); Clive Gringras *The Laws of the Internet* (1997) 213 – 225; Tony Elbra *A practical guide to the Computer Misuse Act 1990* (1990) 4 *et seq*.

[88] Smith and Hogan *Criminal Law* 725.

[89] See Tony Elbra *A practical guide to the Computer Misuse Act 1990* (1990) 37 *et seq*.; A T H Smith *Property offences* (1994) 362 *et seq*.

[90] Tony Elbra *A practical guide to the Computer Misuse Act 1990* (1990) 5.

According to British authors Smith & Hogan the *mens rea* element[91] consists therein that the perpetrator must cause a computer to perform a function with the intent to secure access to any program or data held in any computer, knowing that the access he intends to secure is unauthorised.[92] The Act also contains a specific provision as to the required intent and states that the intent need not be directed at any particular program or data, a program or data of any particular kind, or a program or data held in any particular computer.[93] Section 1(2) seems to introduce a kind of *dolus generalis*[94], which is useful since some hackers tackle whatever constitutes a challenge.[95]

The maximum penalty for hacking is a fine of 2000 pounds or 6 months imprisonment. The British Law Commission in fact thought it inappropriate for a hacking offence to be punishable with imprisonment.[96]

There have been some prosecutions in terms of section 1 of the Computer Misuse Act.[97] Paul Bedworth was charged with various offences under the Computer Misuse Act and raised the "*addiction defence*".[98] The defence argued that Bedworth suffered from a psychological disorder

---

[91] Also see A T H Smith *Property offences* (1994) 363 *et seq*.

[92] Smith and Hogan *Criminal Law* 726.

[93] Section 1(2) of the Computer Misuse Act, 1990.

[94] General intent.

[95] D P van der Merwe *Computers and the Law* (2000) 179.

.

[96] Law Commission Working Paper No. 110, Computer Misuse, 1988 page 94.

[97] See Rupert Battcock *Prosecutions under the Computer Misuse Act 1990* (1996) Computers and Law Vol. 6 22 *et seq*.

[98] Charlesworth (footnote 76 *supra*) 87 *et seq*.

known as *computer tendency syndrome.*[99] Bedworth pleaded not guilty and contended that he was addicted to computer hacking and therefore did not have the required intent. An addiction would not under normal circumstances be sufficient to evade criminal liability.[100] Surprisingly Bedworth was acquitted by a jury on the basis that he did not have the required intent, which decision was widely criticised.[101] An addiction should rather be a factor to be taken in account when sentence is considered.[102] His co-accused Strickland and Wood pleaded guilty to *inter alia* a conspiracy charge in terms of section 3 of the Act.[103]

The Computer Misuse Act also contains a provision in respect of unauthorised access with an ulterior motive.[104] Section 2(1) of the Act states:

> "A person is guilty of an offence under this section if he commits an offence under section 1 above with intent-
> (a) to commit an offence to which this section applies; or
> (b) to facilitate the commission of such offence (whether by himself or by any other person);
> and the offence he intends to commit or facilitate is referred to below in this section as the further offence."

---

[99] Shelley Hill *Driving a Trojan Horse and Cart through the Computer Misuse Act* (December 2003/ January 2004) Computers & Law Vol. 14 Issue 5 31.

[100] David I Bainbridge *Introduction to Computer Law* (2000) 311.

[101] Battcock (footnote 97 *supra*) 24; Charlesworth (footnote 76 *supra*) 89-90.

[102] Bainbridge (footnote 100 *supra*) 311; Charlesworth (footnote 76 *supra*) 89 *et seq.* states that the courts have been unsympathetic when addiction is used as a mitigating factor or as a defence.

[103] Battcock (footnote 97 *supra*) 24; Charlesworth (footnote 76 *supra*) 88.

[104] See in general Smith & Hogan *Criminal Law* 727 *et seq.*; A T H Smith *Property Offences* (1994) 365 *et seq.*; Gringras (footnote 87 *supra*) 225 – 227.

The offence consists therein that unauthorised access is gained to a computer system with the intent to commit or facilitate another offence such as theft.[105] It is immaterial whether the ulterior offence is committed at the time of access or in the future.[106]

3.4.3 Germany

Section 202a of the German Criminal Code provides for the offence of *data spying* and provides that any person who without authority procures data which are not meant for him and which are specifically secured against unauthorised access is guilty of an offence.[107] The German Criminal Code focuses on electronic data. It also states that the data should not be directly visible.[108] The element of procurement would in all probability require that the data be removed or that a copy at least be made. The mere unauthorised access to the data would in all probability not amount to procurement.[109] It is not clear whether mere unauthorised access to data has been criminalised.[110] It would appear that the German Criminal Code falls short as far as unauthorised access to data is concerned.

---

[105] Smith & Hogan *Criminal Law* 727.

[106] Smith & Hogan *Criminal Law* 727.

[107] See Vandenberghe(ed) *Advanced Topics of Law and Information Technology* (1989) 66 *et seq*.

[108] Ulrich Wuermeling *German and English Law against Computer Crime – A Comparative Survey* (1990-91) 3 The Computer Law and Security Report 16. For a discussion regarding the term *data* see Vandenberghe(ed) (footnote 107 *supra*) 57 – 59.

[109] See the South African Law Commission Report (footnote 38 *supra*) 32.

[110] Ulrich Wuermeling (footnote 108 *supra*) 15. Also see Sigmund P Martin *Controlling Computer Crime in Germany* (1996) Information & Communications Technology Law Vol. 5 No. 1 9 – the author is of the view that the mere unauthorised access to data (hacking) is not covered by this section.

3.4.4 Greece

The Greek Penal Code was amended in 1988 to include various computer crimes. Article 4(2) of Law number 1805 of 1988 inserted a new article in the Greek Penal Code in order to criminalise hacking offences. Section 370C(2) states:

> "Anyone who obtains access to data entered into a computer or peripheral computer memory or communicated by telecommunications systems, if these acts have been perpetrated without right, especially by breaching prohibitions or security measures taken by their lawful possessor, is punishable by imprisonment of up to three months or with a fine of at least 10 000 dra."[111]

The mere unauthorised access to data has been criminalised. The unauthorised access is not limited to a specific intent. The article contains an interesting provision where the perpetrator is in the service of the lawful possessor of the data. The unauthorised access to data will then only be criminally punishable if access to certain data is explicitly prohibited by an internal regulation or a written decision by the possessor or his qualified employee.[112] The Penal Code further provides that a prosecution can only follow when there is a formal complaint by the person whose system has been interfered with.[113] The penalty of a maximum of three months imprisonment for unauthorised access seems to be too lenient.

---

[111] Maria Stavropoulou & Chris Reed *Computer crime – the new Greek law* (1989) Computer Law & Practice Vol. 5 216.

[112] Article 370C(3) of the Greek Penal Code.

[113] Article 370C(4) of the Greek Penal Code.

3.4.5 Australia

In the early 1980s the Australian judiciary realised that Australian laws did not encompass certain forms of computer abuse. The Australian Crimes Act[114] (federal legislation) contains sections that criminalise unauthorised access to computers.[115] The provisions are detailed and relate mainly to Commonwealth computers under federal governmental control. Section 76B(1) focuses on intentional unauthorised access to data stored in a Commonwealth computer or data stored on behalf of the Commonwealth in a non-Commonwealth computer. The unauthorised access to data stored in a Commonwealth computer or computer containing Commonwealth data with the intent to defraud any person is criminalised in subsection (2). Section 76B(2) also categorises certain data that is stored in a Commonwealth computer on behalf of the Commonwealth such as trade secrets and records of financial institutions. Section 76D of the Australian Crimes Act[116] contains basically the same provisions as section 76B with the additional element that a government operated facility or a telecommunications service provider is used in order to obtain unauthorised access.[117] The federal legislation is government orientated and does not protect data contained in personal computers and computer systems of corporations, businesses and private institutions.

---

[114] 1914.

[115] Section 76B and section 76D of the Australian Crimes Act of 1914. In general see Gordon Hughes *Recent developments in Australian computer crime regulation* (1991) Computer Law & Practice 94 on page 95.

[116] 1914.

[117] SA Law Commission Report (footnote 38 *supra*) 24.

The various jurisdictions within Australia enacted and amended legislation to criminalise certain computer crimes. In Victoria section 9A of the Summary Offences Act 1966 introduced the offence of *computer trespass*. It states:

> "A person must not gain access to, or enter, a computer system or part of a computer system without lawful authority to do so"[118]

In New South Wales much more detailed legislation were included in the Crimes Act of 1900 by means of the Crimes (Computers and Forgery) Amendment Act of 1989 in respect of hacking offences.[119] Section 309(1)[120] made unlawful access to data in a computer a criminal offence. Where unlawful access was accompanied by the intent to defraud, to obtain financial advantage, or to cause loss or injury, the penalty was much more severe.[121] The unlawful access to certain categories of data for instance confidential government data also carried a more severe penalty.[122] The Cybercrime Act[123] however replaced the initial computer offences in the Crimes Act[124] with new cyber offences.[125] These crimes

---

[118] Gordon Hughes *Recent developments in Australian computer crime legislation* (1991) Computer Law & Practice Vol. 7 No. 3 94; Gordon Hughes *Disjointed Australian assault on hackers* (1989) Computer Law & Practice Vol. 6 No. 1 29.

[119] Gordon Hughes (footnote 118 *supra*) 94; Gordon Hughes (footnote 118 *supra*) 23 *et seq*.; Graham Greanleaf *Computers and Crime – The hacker's new rules* (1990-91) 2 The Computer Law and Security Report.

[120] The Crimes Act 1900.

[121] Section 309(2) of the Crimes Act 1900.

[122] Section 309(3) of the Crimes Act 1900.

[123] 2001.

[124] 1900.

[125] Yee Fen Lim *Cyberspace Law: Commentaries and Materials* (2002) 332.

include *inter alia* the unauthorised access to data with the intent to commit a serious offence and the unauthorised access to restricted data.[126]

3.4.6 Singapore and Malaysia

The Singapore Computer Misuse Act of 1993 and the Malaysian Computer Crimes Act of 1997 are both based on the United Kingdom Computer Misuse Act. The Singapore Computer Misuse Act criminalises unauthorised access to computer material.[127] Section 3 states:

> "(1) 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 both."

The section is widely defined and will include intentional unauthorised access to all types of data held in a computer or computer system. The Singapore Computer Misuse Act defines key concepts such as *computer*, *data*, *program* and *function*.[128] The Computer Misuse (Amendment) Act of 1998 increased the penalty to $ 5 000 and made provision for a stricter penalty for second offenders.[129] In the case of a second or subsequent offender the maximum penalty is a fine of $ 10 000 or three years

---

[126] Lim (footnote 125 *supra*) 333.

[127] In general see Katherine S Williams & Indira Mahalinngan Carr *The Singapore Computer Misuse Act – Better Protection for the Victims* (1994) Journal of Law and Information Science Vol. 5 No. 2 210 *et seq*.; Assafa Endeshaw *Computer Misuse Law in Singapore* (1999) Information & Communications Technology Law Vol. 8 No. 1 1 *et seq*.

[128] See Williams & Carr (footnote 127 *supra*) 211.

[129] Act 21 of 1998 published in Government Gazette No. 28 dated 24 July 1998.

imprisonment or both. Similarly in Malaysia it is an offence to cause any computer to perform any function with the intention to secure unauthorised access to computer material. [130]

Both Acts also contain a provision that criminalises unauthorised access to computer material to commit or facilitate a further offence.[131] The further offence is described as offences that involves property, fraud, dishonesty or offences that could cause bodily harm. [132]

3.5 INTERNATIONAL RESPONSES BY THE COUNCIL OF EUROPE

The Council of Europe released a report in 1990 focussing on computer-related crime and recommended that unauthorised access to data should be criminalised through legislative intervention[133] and suggested the following text: " The access without right to a computer system or network by infringing security measures".[134] The Council of Europe's Convention on Cybercrime[135] also recommended that unauthorised access to a computer system should be criminalised and states:

---

[130] Section 3 of the Malaysian Computer Crimes Act of 1997.

[131] Section 4 of the Singapore Computer Misuse Act of 1993 and section 4 of the Malaysian Computer Crimes Act of 1997.

[132] Section 4(2) of the Singapore Computer Misuse Act of 1993.

[133] Council of Europe *Computer-Related Crime. Recommendation No. R (89) 9 on computer-related crime and final report of the European Committee on Crime Problems* (1990) Strasbourg 49 – 53; Also see Bernard P Zajac Jr. *Transborder Data Flow and 1992* (1990-91) 2 The Computer Law and Security Report; Hans G Nilsson *The Council of Europe fights computer crime* (1989) Computer Law & Practice Vol. 6 No. 1 8 *et seq*.

[134] Council of Europe Report (footnote 133 supra) 51.

[135] Convention on Cybercrime ETS No. 185, Council of Europe, Budapest 2001. See paragraph 1.2 *supra*.

> "Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right."[136]

As has already been stated South Africa became a signatory to the Convention and now has to implement the provisions of the Convention. The Convention aims to implement similar provisions in respect of cyber crime in order to promote international conformity and co-operation as well as legal certainty. The main objective of the present article is to criminalise unauthorised access to a computer system. Whether the unauthorised access should be coupled with a specific dishonest intent is an issue that should be decided by the legislators of the individual signatory countries.

3.6 SOUTH AFRICAN OFFENCES BEFORE ENACTMENT OF THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT

It is important to deal with the law before the enactment of the Electronic Communications and Transactions Act. Certain common law crimes as well as statutory offences will be discussed to ascertain whether hacking falls within the ambit of the elements of these offences.

3.6.1 Housebreaking

Housebreaking with intent to commit a crime is defined as the unlawful and intentional breaking into and entering a building or structure, with the

[136] Article 2 of the Convention on Cybercrime.

intention of committing some crime in it.[137] The first element is that of breaking into the premises and it requires the displacement of an obstruction that forms part of the premises.[138] Physical damage is not essential. Entering the premises is the following element that should be present and is essential to prove the offence of housebreaking. Any part of the perpetrators body should be in the premises and it includes the instance where an instrument is inserted into the premises.[139]

The terms *building* or *structure* are important to establish whether unauthorised access to a computer system would have constituted the offence of housebreaking. The house, structure or premises can be any structure that is or may be used for human habitation or for the storage of property.[140] There are different views as to whether the structure or premises must be movable or immovable.[141] It is clear however that the premises or structure must be a *physical* structure. We are dealing with corporeal or tangible physical structures. A computer is not physically broken into in order to gain access to the information contained in its memory. Instead security measures are programmed on the computer and are part of the software and are intangible and incorporeal in nature. Unauthorised access or hacking in respect of a computer system is of an intangible electronic nature. The unauthorised access to incorporeal data contained in a computer system cannot be equated to the physical presence of a person in a physical structure.

---

[137] Snyman *Criminal Law* (2002) 539.

[138] *S v Ngobeza and another* 1992 (1) SACR 610 (T) on 614.

[139] Snyman *Criminal Law* (2002) 543.

[140] Snyman *Criminal Law* (2002) 541.

[141] See *S v Ngobeza and another* 1992 (1) SACR 610 (T) 613 *et seq*.

The Honourable Judge Smit stated in *S v Ngobeza and another*[142]:

> "*As in gedagte gehou word dat 'n persoon se reg op onverstoorde bewoning van sy woning en die reg op berging van sy goedere deur die misdaad huisbraak beskerm word, is dit moeilik te verstaan waarom toegelaat word dat tegniese (en soms gekunstelde) uitlegte van die misdaadselemente die misdaadomskrywing vertroebel.*"

However, the description and elements of a criminal offence have to be interpreted strictly. This would exclude the possibility of the judiciary extending the meaning and scope of *premises* or *structure*. It is difficult to imagine that the unauthorised access to a computer system could possibly be equated to the physical presence of a human being in a physical structure.

The housebreaking must be accompanied with the intention to commit another crime for instance theft.[143] A hacker who gains unauthorised access to data in a computer system does not necessarily have the intention to commit a further crime. A further problem arises where the hacker gains unauthorised access and then alters or deletes data contained in the computer system. The deletion or altering of the data may not constitute an offence in terms of our criminal law (before the enactment of the Electronic Communications and Transactions Act). It is clear that even if our courts are prepared to extend the meaning of premises and structure to include computer systems, the mere access to the system will not be sufficient to constitute the crime of housebreaking.

---

[142] 1992 (1) SACR 610 (T) on page 614.

[143] Snyman *Criminal Law* (2002) 545.

It is therefore clear that hacking would not fall within the ambit and elements of the offence of housebreaking.[144] The Law Commission was of a similar view and stated that it was unclear whether the courts would consider extending the scope of the offence.[145]

3.6.2 Trespassing Act

Section 1 of the Trespass Act[146] states as follows:

> "Any person who without the permission
> (a) of the lawful occupier of any land or any building or part of a building; or
> (b) of the owner or person in charge of any land or any building or part of a building that is not lawfully occupied by any person,
> enters or is upon such land or enters or is in such building or part of a building, shall be guilty of an offence unless he has lawful reason to enter or be in such a building or part of a building."

Hacking or unauthorised access can be described as a type of electronic trespassing. However, one of the elements of the statutory offence of trespassing is the entering or being present on any *land* or any *building* or *part of the building.*[147] This requires the physical presence of a person on fixed property. Since the unauthorised access to data contained in a computer system is of an incorporeal electronic nature, it will not fall within the scope of application of the Trespass Act. The wording of the

---

[144] Also see M M Watney *Die strafregtelike en prosedurele middele ter bekamping van kubermisdaad (deel 1)* (2003) 1 TSAR 59 in which a similar view is held by the author.

[145] SA Law Commission Report (footnote 38 *supra*) 8. Also see Buys(ed) *Cyberlaw @ SA II* (2004) 329.

[146] Act 6 of 1959.

[147] See in general Snyman *Criminal Law* (2002) 548.

Act is very specific and the courts cannot extend the scope of application of the Act. The Law Commission was also of the view that hacking offences will not fall within the ambit of the Trespass Act.[148]

3.6.3 Malicious injury to property

Snyman defines malicious injury to property as:

> " A person commits malicious injury to property if he unlawfully and intentionally damages
> (a) movable or immovable property belonging to another; or
> (b) his own insured property, intending to claim the value of the property from the insurer"[149]

The essential elements of the offence consist of 1) property; 2) damage; 3) unlawfulness and 4) intent.[150]

It is clear that the property must be corporeal in nature.[151] Computer data and software applications exist in an electronic digital world and are incorporeal in nature. The courts have extended the meaning of the item capable of being stolen to include incorporeal "property" in certain instances.[152] It is arguable whether the courts will extend the meaning of property to include items of an intangible nature.

---

[148] SA Law Commission Report (footnote 38 *supra*) 11-12. Also see M M Watney (footnote 144 *supra*) 63; Buys(ed) (footnote 145 *supra*) 330.

[149] Snyman *Criminal Law* (2002) 535.

[150] Snyman *Criminal Law* (2002) 535 *et seq*.

[151] Snyman *Criminal Law* (2002) 536.

[152] See chapter 11 *infra*..

The next element that presents a problem is the element of damage. The unauthorised access to data in a computer system does not necessarily cause damage to the computer or the data. Mere hacking offences will therefore not fall within the ambit of the offence.

3.6.4 Fraud

Ebersöhn argues that hacking will constitute the offence of fraud because the hacker misrepresents to the system administrator or person in control of a specific computer that he is an authorised user of the system or computer.[153] Hacking causes at least potential prejudice because security measures are breached or compromised.[154]

3.6.5 *Crimen Iniuria*

Snyman defines *crimen iniuria* as the unlawful, intentional and serious violation of the dignity or privacy of another.[155] The element of *dignitas* entails concepts of self-respect, mental tranquillity and privacy. The test is objective and that of the reasonable person, to establish whether the *dignitas* of the complainant has been impaired. According to Hunt[156] the complainant does not need to be aware of the impairment but subsequent conduct by the complainant is relevant.

---

[153] G J Ebersöhn *A common law perspective on computer-related crimes (2)* (2004) 67 THRHR No. 2 197.

[154] Ebersöhn (footnote 153 *supra*) 198.

[155] Snyman *Criminal Law* (2002) 453.

[156] Hunt *South African Criminal Law and Procedure* (1970) 486.

Before the enactment of the Electronic Communications and Transactions Act, the question was posed whether the unauthorised access to data in a computer system is not perhaps a form of *crimen iniuria.* A specific act is not prescribed. However any conduct that results in the complainant's dignity or privacy being impaired will fall within the ambit of the offence. According to Snyman the planting of a listening-in device in a persons apartment and then listening to the conversations will constitute an impairment of privacy.[157] In the case of *S v A and Another*[158] the court found that the installing of a listening device in order to eavesdrop on another person's private conversations constitutes the offence of *crimen iniuria*. Similarly will the opening and reading of private mail constitute an invasion of privacy.[159] The unauthorised prying into a person's personal data contained in a personal computer may very well constitute an impairment of a person's privacy and dignity.[160] It is submitted however that computer systems of large corporations are not personal in nature and therefore not capable of the concepts *dignitas* and personal privacy. It can be argued that a person's privacy and possibly dignity are impaired by the intrusion into a personal computer[161] and that hacking in these cases will fall within the ambit of the elements of *crimen iniuria*.[162] The crime of *crimen iniuria* can also be committed through new

---

[157] Snyman *Criminal Law* (2002) 457.

[158] 1971 (2) SA 293 (T).

[159] Snyman (footnote 157 *supra*). Also see Jacques Jansen *Criminal protection of online privacy* (2002) April De Rebus 30 *et seq*.

[160] Which may form the basis for a civil action.

[161] The computer however can be an instrument through which the crime of *crimen iniuria* can be committed. See in this regard Watney (footnote 144 *supra*) 62

[162] G J Ebersöhn *A common law perspective on computer-related crimes (3)* (2004) 67 THRHR No. 3 378 *et seq*.

technology, for example when a website publishes remarks about or photographs of a person that violates his or her dignity.

3.7 THE SOUTH AFRICAN ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT

It is clear from the discussion above that our criminal law was in dire need of legislative intervention to appropriately criminalise actions of unauthorised access or hacking. The Law Commission recommended that unauthorised access to computer data and software applications should be criminalised.[163] In the proposed Computer Misuse Bill the following provision was suggested: "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."[164]

Section 86(1) of the Electronic Communications and Transactions Act[165] states as follows:

> "Subject to the Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1992), a person who intentionally accesses or intercepts any data without permission or authority to do so, is guilty of an offence."[166]

---

[163] SA Law Commission Report (footnote 38 *supra*) 52 *et seq*.

[164] SA Law Commission Report (footnote 38 *supra*) 64.

[165] Act 25 of 2002.

[166] In general see M M Watney *Die strafregtelike en prosedurele middele ter bekamping van kubermisdaad (deel 2)* (2003) 2 TSAR 241 *et seq*.; Cliffe Dekker Attorneys *Commentary on the Electronic Communications and Transactions Act, 2002* at http://www.mbendi.co.za/cliffedekker/literature/commentary/ect2002.htm.

For the first time in South African history the legislature has criminalised all forms of hacking.

3.7.1 The criminal action (conduct)

The criminal action or conduct consists in the accessing of data. *Access* is not defined in section 1 of the Electronic Communications and Transactions Act. An ordinary interpretation of the term *access* would mean that one succeeds getting into the system. A rather lengthy definition of *access* is found in the proposed Computer Misuse Bill:

> "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"[167]

Another definition of *access* can be found in section 101A(1) of the Customs and Excise Act[168] and means "gaining entry into, instructing or communicating with the logical, arithmetical or memory function resources of a computer, computer system or computer network". *Access* should be widely interpreted and should not be restricted to specific forms of access. Any form of unauthorised access to data should be

[167] SA Law Commission Report (footnote 38 *supra*) 63.

[168] Act 91 of 1964.

sufficient.[169] All forms of hacking, regardless of the method or manner through which unauthorised access is gained, will fall within the ambit of this offence. The Act also makes provision for an extended meaning of the term *access* and stipulates that access includes the actions of a person who, after taking note of any data, becomes aware of the fact that he or she is not authorised to access that data and still continues to access that data.[170]

It is possible that a hacker that penetrates a computer system could only gain limited access (access to only a certain level) as a result of limited skills or security measures. The ultimate objective of a hacker is to get access to the so-called *root level* of the system because then the hacker would have access to and complete control of the entire system.[171] Unauthorised access to any level of the computer system would fall within the ambit of the offence and the term *access* is therefore not limited to certain levels of access.

Would *port scanning* for instance fall within the ambit of unauthorised *access* to data? *Ports* are communication channels between computers and networks that facilitate the sending and receiving of information and data when the computers are linked to the Internet or similar information networks.

---

[169] Also see Section 40A(1)(a) of The National Prosecuting Authority Act, 32 of 1998 which states 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 *prosecuting authority*".

[170] Section 85 of Act 25 of 2002.

[171] As opposed to so-called *user level* access which is limited access to the system [Sinrod & Reilly (footnote 17 *supra*) 6].

> "Port scanning checks the available ports on a computer or a computer network to see which communication channels (doors) are "open" (which means that they are being used) and therefore vulnerable to further exploitation."[172]

When ports are scanned to establish whether they are in use, the data contained in the computer are not accessed. Ports that are in use may provide valuable information for subsequent unauthorised access to the data, but the mere scanning of ports does not constitute access to the data contained in the computer.[173] The ports are merely scanned to establish which ports or services are in use. It would appear that *port scanning* would not fall within the ambit of this subsection of the Act.

Access requires a positive act (*commissio*) and it is submitted that this section cannot be contravened by way of an omission. The conduct must be voluntary, in other words the perpetrator must be capable of making a decision about his conduct and the conduct must be controlled by his will.[174] The voluntariness of an act can be excluded by absolute force and automatism.[175] It is however difficult to imagine an instance where a perpetrator would act involuntarily since hacking can be of a very technical nature, requiring human concentration.

---

[172] G J Ebersöhn *Internet law: Port scanning and ping flooding – a legal perspective* (2003) 66 THRHR No. 4 563 at 564. Also see Wesley Brandi *Hackers: The Techniques and the Tools (Security attacks and techniques employed by Hackers)* accessible at the website of the University of Cape Town.

[173] Ebersöhn (footnote 172 *supra*) 569.

[174] Snyman *Criminal Law* (2002) 55 *et seq*.

[175] Snyman (footnote 174 *supra*) 55 *et seq*.

Data is defined in section 1 of the Act as "electronic representations of information in any form".[176] It is interesting to note that the Act does not use the terms *computer* or *computer system*, but rather uses the term *data*. This is advantageous since the scope of the Act is not limited to a computer, especially in light of the revolution in information technology. The Law Commission recommended in the proposed Computer Misuse Bill that unauthorised access to *an application or data held in a computer system* should be criminalised.[177] The Electronic Communications and Transactions Act referred only to the term *data*. Data is contained in a computer or computer system, but are not restricted to a computer or computer system. It is clear however that data should be electronic in nature. *Electronic* is defined in the Electronic Communications and Transactions Bill as *digital or other intangible form*.[178] This definition, however, was not included in the Act, but it is submitted that the meaning thereof should be similar. Access to *any* data is prohibited and is similarly not restricted to specific categories of data in electronic form. Unauthorised access to data contained in the microprocessor chip of a smart card[179] would also fall within the ambit of this statutory offence.[180]

Each and every computer or computer system is owned or controlled by a certain individual, company or government. The data contained in a computer or computer system is similarly under the control of a certain

---

[176] This is clearly incorporeal in nature.

[177] SA Law Commission Report (footnote 38 *supra*) 55 *et seq.*

[178] Section 1 of the ECT Bill, 2002.

[179] See paragraph 2.1 *supra.*

[180] Access to the data in the chip is not that easy. See W Faul *Die 'smart' kaart – hoe werk dit?* (1989) 1 SA Mercantile Law Journal 389.

individual, company or government and falls within the proprietary rights of another.

Two ex-employees of a South African corporation that runs the back office of overseas online casinos were recently convicted of contravening section 86(1) of the Act in terms of a plea and sentence agreement[181] entered into at the Specialised Commercial Crime Court Johannesburg.[182] The accused gained unauthorised access to one of the confidential client databases of the corporation. One of the accused did work on the client database from his home computer with the knowledge of his employer. After he left the employ of the complainant he discovered the database that still existed on the hard drive of his personal computer at home. The accused accessed the data without authority and copied certain portions thereof with the view to sell the data. The accused were arrested during a trap operation in relation to the sale of the data. They were each sentenced to a fine of R 10 000 or 6 months imprisonment half of which were conditionally suspended.

3.7.2 Unlawfulness

The element of unlawfulness lies in the absence of authority or permission. The Act does not define the term *unauthorised*. The absence of authority is an objectively determinable element and should be determined with reference to the circumstances and facts of each case.[183]

---

[181] Section 105A of the Criminal Procedure Act 51 of 1977.

[182] The State versus Shalika Maharaj and Kenneth Dolbey; case number SCCC 18/2004.

[183] SA Law Commission Report (footnote 38 *supra*) 54.

According to the Law Commission Report[184] the absence of authority consists of the absence of the permission of the owner or the person lawfully in charge of the computer data or software applications. It is important to note 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 the access, but rather the absence of permission by the person in charge of the affected computer data or software applications.[185] It is submitted that this approach to the absence of authority is correct and should be followed by our courts. Permission or the necessary authority could be grounds of justification. The State has the onus to prove the absence of authority or permission beyond a reasonable doubt.

An interesting question is whether access is unauthorised in terms of the Act if an authorised person exceeds the scope and limits of his authority. Will access be unauthorised if an authorised user uses the system for an unauthorised use such as accessing information out of the sphere of his normal duties? The Act does not define the term *unauthorised* and it is clear that the legislator left this aspect to the courts to define and develop.

In this regard it may be useful to consider a few foreign decisions. In the Washington case of *State v Olsen*[186] a police officer accessed a work computer and looked up information that was contrary to departmental policy. The Court of Appeal held that there was insufficient evidence to support a finding that the authorised defendant acted in an unauthorised

---

[184] SA Law Commission Report (footnote 38 *supra*) 54.

[185] Footnote 184 *supra*.

[186] (1987) 47 Wash.App. 514.

manner.[187] In the British case of *R v Bignall*[188] a police officer, who was authorised to access the police computer, accessed a work computer in order to obtain information for personal interest that was not connected with his duties. The Court held that since the accused was authorised to access the computer system, no offence was committed.[189] In the British case of *R v Bow Street Magistrates Court ex p Allison*[190] the accused misused information she obtained due to her authorised access to the computer system of American Express.[191] In this case, however, it was held (*contra* to the decision in *Bignall*[192]) that the court should consider the use or purpose with which access is gained rather than the data that was accessed.[193] The Court found that the access was unauthorised and the accused was convicted.

Section 40A(1)(d) of the National Prosecuting Authority Act[194] provides for instance 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

---

[187] Martin L Forst *Cybercrime: Appellate Court Interpretations* (1999) 173 *et seq*. Also see paragraph 3.4.1.2 *supra*.

[188] [1998] 1 Cr App Rep 1.

[189] Ian J. Lloyd *Information Technology Law* (2000) 234 *et seq*.; David I Bainbridge *Introduction to Computer Law* (2000) 312 criticised the *Bignell* decision and stated that it left an unsatisfactory gap in the Computer Misuse Act.

[190] [1999] 4 All ER 1.

[191] In this case the accused was authorised to access the computer system of American Express. She accessed the computer and obtained account information which was later used to encode fraudulent credit cards.

[192] Footnote 188 *supra*.

[193] Lloyd (footnote 189 *supra*) 235 *et seq*.

[194] Act 32 of 1998.

unauthorised, at the time when the access is gained, to gain access to such computer, program or data.[195]

In order to establish whether access was unauthorised the legal principles of *consent* must be considered. Authorisation is a form of consent in that the owner gives the user consent to access the system. There will be no legal consent if the conduct exceeds the scope and limit of the consent.[196] It was stated in *Rex v Leguabe*[197] in respect of certain statutory offences pertaining to the use of a motor vehicle without the consent of the owner that:

> "If in the course of driving a motor vehicle within the limits of the consent or the instructions of the owner a driver, by a change of intention, departs from the instructions or the terms of the consent of the owner and drives it for his own purposes he is, in my opinion, guilty of a contravention of the section."[198]

The Court states further:

> "Likewise, in the case of driving without the knowledge or consent of the owner, if the stage arises where the driver departs substantially from the instructions or terms of consent of the owner the guilty mind may be inferred from his conduct and he may be found guilty of a contravention of this section."[199]

---

[195] Section 71(1) of the South African Police Service Act 68 of 1995 and section 128(1)(e) of the Correctional Services Act 111 of 1998 have similar provisions.

[196] Also see S v Le Grange 1962 (3) SA 498 (A) at 503 where it is stated "*'n Toestemming wat alle bevoegdhede te buite gaan, is regtens geen toestemming nie*".

[197] 1949 (4) SA 871 (T).

[198] At page 872.

[199] At page 872.

The Court held in the case of *S v Le Grange*[200] that an authorised driver of a state vehicle cannot give himself permission to exceed the limits of his authorisation. It is submitted that a person may have authority to access certain data, but could exceed the nature and scope of the authority and would therefore act unlawfully. For example it may be argued that an employee, who is authorised to access certain data, who copies the data exceeds the scope of his authority. The authorisation limits an employee to access to data within the scope of his duties. When the employee accesses the system and copies the data, he actually exceeds the ambit and scope of the authorisation and the access becomes unauthorised. In this regard it is also important to note that the "authorised user" must knowingly exceed the ambit and scope of his authorisation (in other words the person must intentionally act in an unauthorised manner).[201]

In these types of cases it will be important to present evidence as to what procedures and company policies were in place in respect of the authority to access certain data. It would also be imperative to lead evidence to ascertain whether the accused was in fact aware of these policies and procedures.

In an unreported decision that came to my attention, the accused, an authorised user, was convicted of unauthorised access in terms of section 86(1) of the Act on the basis that she exceeded her authorisation to access certain data. The accused, a former employee of Rentmeester Insurance Company, gained access to confidential databases of Rentmeester that she

---

[200] 1962 (3) SA 498 (A).

[201] *Le Grange* (footnote 200 *supra*) at page 503 and *Leguabe* (footnote 197 *supra*) at page 872 where the court stated that intention can be inferred from the conduct. Also see paragraph 3.7.3 *infra*.

e-mailed to her fiancé.[202] The Court considered the nature of vicarious liability[203] as well as the legal principles of consent and authority and concluded that the accused did not have consent to act in such a manner and that she misused the information network. She was convicted of a contravention of section 86(1) of the Act.

3.7.3 Culpability and criminal capacity

The form of culpability is specifically prescribed in section 86(1) of the Act as intent (*dolus*). The Law Commission also recommended that the form of culpability should be limited to intent.[204] Negligence will therefore not suffice. The intent should be directed at all the elements of the offence.[205] Firstly the perpetrator must have the intent to secure access to data and secondly the perpetrator must have knowledge of the unlawfulness of the access i.e. knowledge of the absence of authority or permission. If the authorised user exceeds the scope and limits of his authorisation, he should also know that he is exceeding his authority or acting contrary to the limitations of his authorisation.

The prosecution must prove intentional conduct and the absence of grounds that exclude culpability. Intentional conduct can be inferred from the facts and circumstances of a specific case. The manner in which

---

[202] The State versus Magrieta Gloudina Douwenga. The Accused was tried and convicted in the Specialised Commercial Crime Court, Pretoria.

[203] Liability of the employer as a result of the delict committed by an employee in the course and scope of his employment (see *Absa Bank Ltd v Bond Equipment (Pretoria) (Pty) Ltd* 2001 (1) SA 372 (SCA) at 378.

[204] SA Law Commission Report (footnote 38 *supra*) 54.

[205] Footnote 204 *supra* and Snyman *Criminal Law* (2002) 179 *et seq*.

unauthorised access is secured could be useful to prove intent, especially when it is very technical in nature and calls for human concentration.

What forms of intent will suffice to establish culpability? It is submitted that all forms of intent should be sufficient enough to establish *mens rea*. *Dolus directus* will be present when a perpetrator's main objective is to gain unauthorised access to certain data. *Dolus indirectus* will be present when the unauthorised access is not the perpetrator's main objective but is a necessary action towards his main intention, which would be some other offence. For example a perpetrator unlawfully deletes certain data from a system. In order to delete the data he has to gain unauthorised access to the system. The perpetrator had *dolus directus* in respect of the deletion of the data[206] and has *dolus indirectus* in respect of the unauthorised access since this is necessary action in order to gain access to the data.

When a perpetrator foresees that he might not have the authority to gain access to the data and regardless proceeds with the access, there will be intent in the form of *dolus eventualis*. Intent in the form of *dolus eventualis* must be distinguished from negligence where a perpetrator did not foresee, but should have foreseen that he does not have authority to access the data. The negligent person will not have committed an offence, since intention is required.

Culpability may be excluded by mistake and coerced access. It is possible that a hacker may be forced by other criminals to hack into a system. If a perpetrator is under the impression that the access is authorised whilst he

[206] An offence in terms of section 86(2) of the Electronic Communications and Transactions Act, 25 of 2002. See chapter 4 *infra*.

is in fact not authorised, he does not have the intention to unlawfully access the data (no knowledge of unlawfulness).

Before a person can be said to have acted with culpability, he must have criminal capacity.[207] A perpetrator's capacity is determined firstly by his ability to distinguish between right and wrong, and secondly his ability to conduct himself in accordance with his insight into right and wrong.[208] Criminal capacity can be excluded by instances of mental illness and youth.[209] A child below the age of seven is irrebuttably presumed to lack criminal capacity. From the age of eight to just before the completion of the fourteenth year a child is rebuttably[210] presumed to lack criminal capacity. Hackers are often of very young age but will usually have criminal capacity. It might be that a hacker has diminished capacity due to a very youthful age that may serve as a mitigating factor in sentence.

A hacker will not evade criminal liability by raising the "*addiction defence*".[211] Whether hacking can actually be the subject of an addiction is arguable but for purposes of this discussion it is accepted that one can be addicted to hacking. Hackers are usually intelligent people with the ability to distinguish between right and wrong and to act in accordance with this insight. Due to a "hacking addiction" a hacker might find it more difficult than a normal person to resist temptation and to conduct himself in accordance with his insight into right and wrong. The hacker

---

[207] Snyman *Criminal Law* (2002) 158 *et seq*.

[208] Snyman (footnote 207 *supra*) 158.

[209] Snyman (footnote 207 *supra*) 158 *et seq*.

[210] The State must rebut the presumption.

[211] See paragraph 3.4.2 *supra*.

therefore has criminal capacity and should be convicted. However, it could be argued that his criminal capacity may be diminished[212] due to his addiction. Diminished capacity as a result of an addiction may arguably only serve as a mitigating factor in respect of sentence.

3.7.4 Related provisions

An *attempt* to gain unauthorised access is criminalised in section 88(1) of the Act.[213] For example when a person who intends gaining unauthorised access is still in the process of gaining access and gets caught, can be convicted of attempted unauthorised access in terms of section 88(1) of the Act. In other words certain security measures have been overcome, but not all and access has not been secured.

Section 88(2) of the Act provides for the criminalisation of aiding and abetting another to gain unauthorised access. In terms of the Riotous Assemblies Act[214] a person that conspires with another person, or incites, instigates, commands or procures any person to contravene this section (unauthorised access) will be guilty of an offence.[215] It often happens that an employee of a company, who is authorised to gain access to data, copies the data contrary to the scope and limits of his authority, and sells it to a competitor. The competitor is not authorised to gain access to the specific data. It can be argued that the authorised employee aids and abets

---

[212] Diminished capacity – see Snyman *Criminal Law* (2002) 161.

[213] Section 18(1) of the Riotous Assemblies Act 17 of 1956 also provides for the criminalisation of an attempt to commit a statutory offence.

[214] Act 17 of 1956.

[215] Section 18(2) of Act 17 of 1956. The same will apply in respect of all the South African offences discussed in this paper.

the competitor to gain unauthorised access to the data. The provisions of the Riotous Assemblies Act[216] may be equally applicable when these persons conspire to commit the statutory offence of unauthorised access.

3.7.5 Sentence

The penalty clause is found in section 89(1) of the Act and stipulates that a person is liable to a fine[217] or imprisonment not exceeding 12 months. It is submitted that the Act provides for far too lenient sentences. The Law Commission recommended a maximum sentence of a fine or a term of imprisonment not exceeding 5 years.[218] For instance section 41(4) of the National Prosecuting Authority Act[219] provides that a person that is convicted of contravening section 40A(2) of the Act (unauthorised access to NPA computers) shall be liable to a fine or to imprisonment for a period not exceeding 25 years or to both such a fine and such imprisonment. Clearly the penalty provided for in the NPA Act is inappropriate, but it is perhaps an indication of the seriousness with which these types of offences are viewed.[220] I am of the view that the penalty suggested by the Law Commission would have been more appropriate in cases of unauthorised access and would have been more in line with international provisions in respect of the sentencing of hackers.

---

[216] Act 17 of 1956.

[217] However an unlimited fine may not be imposed. See the provisions of the Adjustment of Fines Act 101 of 1991.

[218] Section 10(1) of the Proposed Computer Misuse Bill, SA Law Commission Report 67.

[219] Act 32 of 1998.

[220] Compare with the provisions of the Financial Intelligence Centre Act 38 of 2001 that provides for a maximum penalty of 15 years [section 68(1)] and the Defence Act 42 of 2002 that provides for a maximum penalty of 25 years [section 104(8)].

A further problem is that hackers are often youthful offenders and would usually not be in a position to pay a fine. If a fine is imposed the parents or guardians of the perpetrator will usually bear the brunt of the sentence. Hackers are usually multiple offenders and will not easily mend their ways. For some it can be equated to an addiction.

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

The Electronic Communications and Transactions Act is not the only legislation in South Africa that deals with unauthorised access to data and computer systems. There are various Acts that criminalise hacking offences but they are limited to computers that are *inter alia* under the control of certain governmental departments. Section 71(2) of the South African Police Services Act[221] criminalises unauthorised access to computers that belong to or are under the control of the South African Police Service.[222] The Act uses the term *wilfully* to indicate that intention is a requirement. *Access* is not restricted to a specific manner and includes all forms of access.[223] Unauthorised access includes instances where a person is authorised to use the computer but unauthorised to gain access to a certain program or data.[224] Upon conviction a person may be sentenced to a fine or to imprisonment not exceeding a period of two years.

---

[221] Act 68 of 1995.

[222] The section states: "Any person who wilfully gains unauthorised access to any computer which belongs to or is under the control of the Service or to any program or data held in such a computer, or in a computer to which only certain or all members have restricted access in their capacity as members, shall be guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding two years".

[223] Section 71(1) of Act 68 of 1995.

[224] Section 71(1) of Act 68 of 1995.

The Correctional Services Act[225] has similar provisions. Section 128(2) of the Act provides that unauthorised access to a computer or program or data belonging to or under the control of the Department of Correctional Services is a criminal offence. The scope of this Act is not restricted to a computer due to the inclusion of the term data. A person may be sentenced on conviction to a fine or imprisonment not exceeding two years or to both.

Unauthorised access to a computer belonging to or which is under the control of the National Prosecuting Authority is criminalised in section 40A(2)(a) of The National Prosecuting Authority Act[226]. Similar definitions as discussed *supra* are found in the Act. The penalty clause provides for a fine or imprisonment not exceeding 25 years or both.[227]

The Financial Intelligence Centre Act[228] (so-called Whistle Blowing Act) that was promulgated on 1 February 2002 has more detailed provisions in respect of computer crime that aims to protect the computers of the Financial Intelligence Centre. Section 65 of the Act states as follows:

> "(1) Any person who, without authority to do so, wilfully accesses or causes any other person to access any computer system that belongs to, or is under the control of, the Centre, or any application or data held in such a computer system, is guilty of an offence.

[225] Act 111 of 1998.

[226] Act 32 of 1998.

[227] Section 41(4) of Act 32 of 1998.

[228] Act 38 of 2001.

> (2) Any person who, without authority to do so, wilfully causes any computer system that belongs to, or is under the control of, the Centre, to perform or fail to perform a function, is guilty of an offence."

Access is defined in section 67(a) of the Act and the definition is similar to the definition used in the proposed Computer Misuse Bill.[229] *Application* is described as a set of instructions that, when executed in a computer system, causes a computer system to perform a function.[230] *Data* is defined as any representation of information, knowledge, facts or concepts, capable of being processed in a computer system.[231] The Act provides for instances where another person, perhaps without the necessary expertise, uses a hacker to gain access to data in which he is interested. This person as well as the hacker could be charged with a contravention of the Act. Upon conviction a person may be sentenced to imprisonment not exceeding a term of 15 years or to a fine not exceeding R 10 000 000.[232]

The Defence Act[233] provides that a person who gains unauthorised access to a computer system or computer database of the National Defence Force is guilty of an offence and may be sentenced to a fine or imprisonment not exceeding 25 years.[234]

---

[229] See paragraph 3.7.1 *supra*.

[230] Section 67(b) of Act 38 of 2001.

[231] Section 67(d) of Act 38 of 2001.

[232] Section 68(1) of Act 38 of 2001.

[233] Act 42 of 2002.

[234] Section 104(8) of Act 42 of 2002.

In terms of which Act should a cyber criminal be prosecuted when his actions fall within the ambit of both the Electronic Communications and Transactions Act and one of the aforementioned Acts that deals with specific groups of computers. According to a Latin maxim it is stipulated that when both general and specific provisions regulate a certain aspect the specific provisions should be followed. It is therefore submitted that such a perpetrator should be charged with contravening the specific provisions and as an alternative contravening the Electronic Communications and Transactions Act. This approach could however be constitutionally challenged due to the obvious disparity in sentencing provisions between the various Acts.