CHAPTER 4

UNAUTHORISED MODIFICATION

4.1 INTRODUCTION

The 21st century introduced an era of violence filled with acts of terrorism and religious wars. These wars and terrorist activities have also taken on a new form with the assistance of information technology.[1] Political and religious propaganda are easily distributed and accessible on websites on the Internet. These websites can be defaced or altered. Of greater concern is that in a modern era most first world powers' infrastructure is computerised and facilitates electronic attacks of war and terrorism. For example air traffic control, power grids and the floodgates of dams are all computerised and can be targeted by cyber terrorists. The interference with these systems can result in chaos and can be an effective tool in crippling the infrastructure of the opposition or those sympathetic to the opposition. Channels of communication can also be targeted. Viruses, worms and distributed denial of service attacks are just some of the methods that can be used to achieve such results.

Attacks need not be political or religious in nature and are frequently launched against corporations by disgruntled employees or persons.

[1] See in general the CSIS Report entitled *Cyber Threats and Information Security (Meeting the 21st Century Challenge)* (2001) ix *et seq*. and Hutchinson & Warren *Information warfare (corporate attack and defence in a digital world)* (2001).

There have been many instances of rogue code[2] being released on information and computer networks and the Internet, some harmless, others disastrous. Internationally there were the *Michelangelo* virus[3], *Melissa* virus[4], the *I love you* virus[5] and very recently the *Sobig.F* virus[6], the *MyDoom* virus[7] and *Sasser* worm[8], to name but a few.[9] The *Italian* (or *ping pong*) virus bounced ping-pong balls across the computer screen[10] and the *cookie monster* requested the user for a cookie and the message would only disappear after the word *cookie* had been entered into the computer[11]. Some of these early viruses were actually classified as harmless computer games.[12] The *Aldus Peace* virus displayed a peace message on thousands of Apple MacIntosh computers on 2 March 1988,

[2] See Anne W Branscomb *Rogue computer programs and computer rogues: tailoring the punishment to fit the crime* (1990) Rutgers Computer and Technology Law Journal Vol. 16 No. 1 1 *et seq*. Also see paragraph 4.2 *infra*.

[3] See Glenn D Baker *Trespassers will be prosecuted: Computer crime in the 1990s* (1993) Computer Law Journal Vol. xii No. 1 61, Bernard P Zajac, Jr *The Michelangelo virus – was it a failure* (1992) The Computer Law and Security Report 137 reported that there were few reported incidents in the UK and USA of actual damage caused by the virus. This was attributed to the warnings issued in the media before the date the virus was actually triggered.

[4] The *Melissa* virus infected and disrupted e-mail services around the globe.

[5] See paragraph 4.4.6 *infra* for a detailed discussion of the virus.

[6] *Sobig.F virus: now brace for the second wave* The Citizen 25/08/03 page 2; *SoBig virus – 'may have commercial motivation'* The Citizen 26/08/ 03 page 2.

[7] *Mydoom 'the biggest yet'* The Citizen 29/01/2004 page 27; *'Mydoom' to continue till Feb 12* The Citizen 31/01/2004 page 4; *Computer worm claims its first blood* The Citizen 02/02/2004 page 9; *Virus to get personal after Microsoft Bid* The Citizen 02/02/2004 page 17; *Computer gurus ponder possibility of information highway robbery* The Star 03/02/2004 page 4.

[8] Themba Sepotokele *Sasser worm stalls civil service* The Star 06/05/2004 front page. Also see *Cyber crime syndicates and Sasser* where it is reported that an 18 year old German student recently confessed to writing the Sasser worm (accessible at http://www.expresscomputeronline.com/20040531/technology01.shtml.

[9] D P van der Merwe *Computers and the Law* (2000) 165 *et seq*.

[10] John C Buyers *Computer viruses – 'AIDS' of the computing world* (1989) 62 Computers and Law 12 at 14; Ian J Loyd *Information Technology Law* (2000) 243; Dr. Alan Solomon *PC Viruses Detection, Analysis and Cure* (1991) 56 *et seq*.

[11] Loyd (footnote 10 *supra*) 242.

[12] Branscomb (footnote 2 *supra*) 21.

the anniversary of the launch of the MacIntosh personal computer.[13] There was the *stoned* virus that infected a computer and the following message would appear on the screen: “Your PC is Now Stoned! LEGALIZE MARIJUANA!”[14] In 1988 Robert T Morris released the *INTERNET* worm[15] on various networks and computer systems and was subsequently convicted in the United States of a federal computer charge.[16] The creator of the *Melissa* virus[17], one David L. Smith, pleaded guilty to a State computer-related theft charge as well as a statutory federal charge[18] and was sentenced on the federal conviction to 20 months in a federal prison and community service.[19] It is reported that Kevin David Mitnick[20] modified and mangled the credit record of a judge who sentenced him to a term in the reformatory.[21]

South Africa did not escape the onslaught of malicious cyber criminals either. Some of these international viruses infected South African

[13] Branscomb (footnote 2 *supra*) 13 *et seq*.; James Tramontana *Computer viruses: Is there a legal “antibiotic”?* (1990) Rutgers Computer & Technology Law Journal Vol. 16 No. 1 259.

[14] Branscomb (footnote 2 *supra*) 24; D P Van der Merwe *Onlangse ontwikkelinge op die raakvlak tussen rekenaars en die reg* (1991) 54 THRHR 103; Solomon (footnote 10 *supra*) 59.

[15] Also referred to as the *Cornell* virus or worm. See Bernard P Zajac Jr *Virus hits major US computer network* (1988-89) The Computer Law and Security Report 34.

[16] See discussion at 4.4.1.1 *infra*.

[17] David J Marchette *Computer Intrusion Detection and Network Monitoring* (2001) 236 *et seq*.

[18] According to a press release by the US Department of Justice entitled *Creator of “Melissa” Computer Virus Pleads Guilty to State and Federal Charges* accessible at http://www.usdoj.gov/criminal/cybercrime/melissa.htm. Also see S S Kennedy *et al Computer Crimes* in American Criminal Law Review (2002) Vol. 39 No. 2 footnote on p276; John Christopher Anderson *Transmitting legal documents over the Internet: How to protect your client and yourself* (2001) Rutgers Computer and Technology Law Journal Vol. 27 No. 1 9.

[19] According to a press release by the US Department of Justice entitled *Creator of Melissa Computer Virus Sentenced to 20 Months in Federal Prison* accessible at http://www.usdoj.gov/criminal/cybercrime/melissaSent.htm.

[20] See paragraph 3.4.1.1 *supra*.

[21] Branscomb (footnote 2 *supra*) 19.

networks and computers and caused damage in our country. There was also the disgruntled employee that released a virus into the Edgars Consolidated Stores computer system, crashed computers at more than 600 stores nationwide and caused extensive damage.[22] The virus caused trading losses of about R19m over a period of four days.[23] He was convicted[24] of malicious damage to property[25] in the Specialised Commercial Crime Court Johannesburg and subsequently sentenced to a term of imprisonment[26].[27]

4.2 DANGEROUS OR ROGUE CODE

Data can be modified through a myriad of ways. Hackers could for instance hack into a network and deface a website. The most well known form of modification of data is computer viruses. The term *computer virus* is commonly used in laymen terms to describe software programs primarily designed to disable computer systems. However there are various different forms of software programs that can affect computers and cause damage. The term *rogue code or programs* are used to refer to the group of different software programs that "disable or distort computer

[22] B Jordan *Hackers set to get the chop* at http://www.sundaytimes.co.za/2001/05/20/politics/po101.htm *Edcon says it lost R19m to a virus in its software* Business Report 06/112003 page 4.

[23] *Edcon says it lost R19m to a virus in its software* Business Report 06/11/2003 page 4. It was reported that the "virus caused a massive computer crash and sales had to be entered manually".

[24] *Man guilty of computer virus sabotage* The Star 18/05/2004 and *IT man costs Edgars R20m* The Citizen 18/05/2004 pages 1 and 2.

[25] At the time the offence was committed there were no statutory provisions that criminalised his actions (such as the Electronic Communications and Transactions Act). He was therefore charged with malicious damage to property. See paragraph 4.6.1 *infra*.

[26] Aphiwe Boyce *Man jailed for Edcon computer sabotage* Saturday Star 23/10/2004 page 3; Marthinus van Vuuren *Rekenaarvirus lei tot tronkstraf (Edgars verloor R19 miljoen; man moet 4 jaar sit)* Naweek-Beeld 23/10/2004 page 7.

[27] The State versus Berend Howard; Case number: 41/258/2002.

functioning".[28] Gordon uses the term *dangerous code* and it refers to "any computer program that causes destruction or harm to a computer system".[29] The most comprehensive definition is found in the Minnesota Statute in which it is referred to as a *destructive computer program.*[30] Some of the most well known forms of dangerous code or programs are discussed below.

4.2.1 Viruses

It is said that in 1983 Frederick B Cohen constructed the first computer virus.[31] He defined a virus as … *a program that can infect other programs by modifying them to include a, possibly evolved, version of itself.* [32] A computer virus is a software program that attaches or copies itself to "infect" a program and has the ability to infect other programs on the system. Each infected program acts as a computer virus and copies itself to infect other programs and can spread through a computer system

[28] Anne W Branscomb *Rogue Computer Programs and Computer Rogues: Tailoring the punishment to fit the crime* (1990) Rutgers Computer and Technology Law Journal Vol. 16 No. 1 4 *et seq*.

[29] Barrie Gordon *Internet Criminal Law* in Buys(ed) *Cyberlaw @ SA* (2000) 426.

[30] "'Destructive computer program' means a computer program that performs a destructive function or produces a destructive product. A program performs a destructive function if it degrades performance of the affected computer, associated peripherals or a computer program; disables the computer, associated peripherals or a computer program; or destroys or alters computer programs or data. A program produces a destructive product if it produces unauthorized data, including data that make computer memory space unavailable; results in the unauthorized alteration of data or computer programs; or produces a destructive computer program, including a self-replicating computer program." Section 609.87(12) of the Minnesota Statute.

[31] See Bernard P Zajac Jr *Computer viruses can they be prevented?* (1989-90) The Computer Law and Security Report 18. Michael Alexander *The Underground Guide To Computer Security* (1996) 26 *et seq*. Fred Cohen is now an anti-virus expert. A virus called *papa* also 'pings' the website of Fred Cohen (DP van der Merwe *Computers and the Law* (2000) 165).

[32] Michael Alexander *The Underground Guide to Computer Security* (1996) 27. Also see S S Arkin and others *Prevention and prosecution of computer and high technology crime* (1990) 3A-2 *et seq.*; Robert P Bigelow *Computer security, crime and privacy – US status report* (1988-89) 6 Computer Law and Security Report 11 *et seq*. See in general Kit Burden & Creole Palmer *Cyber Crime – A new breed of criminal?* (2003) Computer Law and Security Report Vol. 19 No. 2 222 *et seq*.

like a virus.[33] The most important characteristic of a virus is replication, its ability to spread from one machine to another.[34] Recently a computer virus was defined as:

> "A virus is a very well known form of dangerous code. It is simply a small computer program that attaches itself to a computer application or other file, and copies itself onto the user's system. It then replicates itself to 'infect' many of the host's computer files to such an extent that it causes the computer to malfunction." [35]

Buys refers to the *I love you* virus that caused damage estimated at billions of dollars worldwide and infected millions of computers. Fites *et al* refers to a definition that a computer virus is "*malicious* software which replicates itself".[36] Many authors refer to viruses as *malicious* software programs because viruses are seen to be malicious in nature and some do have disastrous consequences. However, some authors argue that one could also have viruses that are not malicious in nature but are harmless or benign.[37] Viruses are often incorrectly referred to as *bugs.* A bug is merely a mistake in a computer system that is a result of human error.

[33] See Branscomb (footnote 2 *supra*) 4; Tramontana (footnote 13 *supra*) 254 *et seq.*; Fites *et al The Computer virus crisis* (1989) 23; Peter J Denning (ed) *Computers under attack intruders, worms, and viruses* (1990) 288.

[34] See Darryl C Wilson *Viewing Computer Crime: Where does the systems error really exist?* (1991) Computer Law Journal Vol. XI 278.

[35] Barrie J Gordon *Internet Criminal Law* in Buys(ed) *Cyberlaw @ SA* (2000) 426. Also see Reinhardt Buys *Love Hurts … Computer, network and e-mail security* (2000) July De Rebus 33, where he defines a computer virus as a small piece of software (or code) that attaches itself to a computer application, file or e-mail. It is called a virus because it generally infects a computer and replicates itself.

[36] Philip Fites *et al The Computer Virus Crisis* (1989) 6.

[37] Branscomb (footnote 2 *supra*) 46.

According to a BNA special report entitled *Computer data security* viruses move form computer to computer through electronic communications (i.e. electronic mail), on floppy diskettes, or on magnetic tapes.[38] Viruses can spread rapidly via the Internet through electronic mail messages.[39] According to the report the Computer Virus Industry Association divided viruses into three basic types: boot infectors[40], system infectors[41] and generic application infectors[42].[43]

4.2.2 Worms

A clear distinction between a *worm* and a computer *virus* is found in a footnote by Martin L Forst:

> "A 'worm' is a program that travels from one computer to another but does not attach itself to the operating system of the computer it 'infects'. It differs from a 'virus', which is also a migrating program, but one that attaches itself to the operating system of any computer it enters and can infect any other computer that uses files from the infected computer."[44]

[38] *Computer data security: A legal and practical guide to liability, loss prevention, and criminal & civil remedies* A BNA Special Report (1989) 7.

[39] See G J Ebersöhn *A common law perspective on computer-related crimes (1)* (2004) 67 THRHR No. 1 23

[40] Boot infectors attach themselves to boot sectors of hard and floppy disks and move or overwrite the original boot sector.

[41] System infectors attach themselves to at least one operating system module or system device driver. When a system diskette is inserted into a floppy drive, the virus replicates and attaches itself to system files.

[42] Generic application infectors can infect any application program. They may reside in memory and infect all programs, or be part of an infection selection algorithm that is invoked by certain types of commands. This is the most widespread type of virus.

[43] *Computer data security: A legal and practical guide to liability, loss prevention, and criminal & civil remedies* A BNA Special Report (1989) 7 *et seq*.

[44] Martin L Forst *Cybercrime: Appellate Court Interpretations* (1999) 133.

A worm makes copies of itself and does not spread like a virus by infecting files.[45] A worm is a software program that "lives" in a computer system and prevents the system from functioning properly.[46] It targets certain functions or resources, erases information needed by the computer and disables the proper functioning of the computer.[47] It does not have the ability to reproduce or copy itself and therefore does not spread like a virus.[48] A worm hides itself in the computer system.[49]

4.2.3 Trojan horse

The term *Trojan horse* was inspired by the wooden horse that the Greeks used to secretly gain access to Troy where the Greek soldiers were hiding inside the horse.[50] It is a useful software program that contains a secret or hidden undetectable code. When the useful software program is used the hidden code is also triggered and performs unwarranted mischievous functions.[51] A Trojan horse is a form of code that infects from within.[52] Trojan horse applications are sometimes used by cyber criminals to

[45] David J Marchette *Computer Intrusion Detection and Network Monitoring* (2001) 232.

[46] Branscomb (footnote 2 *supra*) 4; Tramontana (footnote 13 *supra*) 257.

[47] See Susan C Lyman *Civil remedies for the victims of computer viruses* (1992) Computer Law Journal Vol. XI footnote 27 on page 609.

[48] Michael Alexander *The Underground Guide to Computer Security* (1996) 41. Ebersöhn, however, states that "new generation worms can, like any virus, replicate themselves within machines and across networks" (footnote 39 *supra*) 23.

[49] Barrie Gordon *Internet Criminal Law* in Buys(ed) Cyberlaw @ SA (2000) 427.

[50] Fites at al *The computer virus crisis* (1989) 23; Darryl C Wilson *Viewing Computer Crime: Where does the systems error really exist* (1991) Computer Law Journal Volume X1 265 on 278.

[51] Tramontana (footnote 13 *supra*) 257; Branscomb (footnote 2 *supra*) 4 *et seq*.; Denning (ed) (footnote 33 *supra*) 117.

[52] Barrie Gordon *Internet Criminal Law* in Buys(ed) *Cyberlaw @ SA* (2000) 427.

spread viruses.[53] It is a trapdoor that programmers use in order to gain access to a system in order to spread other forms of malicious code. The user, under the impression that it is an ordinary application, runs the application and a virus or logic bomb is triggered. For example the virus is hidden in an e-mail message and once the user opens the electronic mail message the virus infects the computer system. Another definition of a Trojan horse is found in the BNA special report:

> "This method covertly places software commands into the system so that it will execute unauthorized functions in the background, while the authorized program continues to execute its instructions"[54]

4.2.4 Logic bombs

A logic bomb or a time bomb is an infection in the form of a software application designed to come into operation when a specific event takes place or at a specific preset time.[55] The "bomb" or rogue program is triggered when certain logical conditions are met or when a specific event happens.[56] For example a specific date can trigger the rogue software application to come into operation such as Friday the thirteenth.[57] The *Friday the 13th* virus deleted programs on Friday the thirteenth.[58] The

[53] Tramontana (footnote 13 *supra*) 257.

[54] BNA special report (footnote 38 *supra*) 6.

[55] Branscomb (footnote 2 *supra*) footnote 16 on page 5; Michael Alexander *The Underground Guide to Computer Security* (1996) 42; Irving J Sloan *The Computer and the Law* (1984) 13.

[56] BNA special report (footnote 38 *supra*) 6.

[57] Bernard P Zajac, Jr *US Focus: Friday the 13th worm hits DEC* (1988-89) The Computer Law and Security Report 32 *et seq*.

[58] A variant of this virus is also known as the *South African virus* since it first appeared in South Africa in 1987. See Denning (ed) (footnote 33 *supra*) 346.

Michelangelo virus was triggered on 6 March 1992, the artist's birthday.[59]

4.2.5 Bacterium

Bacteria are software programs that are primarily designed to *crash* computer systems.[60] A definition of a bacterium is "a program that replicates itself and feeds off the host system by pre-empting processor and memory capacity"[61] A bacterium does not attach itself to other programs and therefore unlike a virus does not have the ability to spread. However the bacterium repeatedly replicates itself in the same system to the point where the system reaches capacity and is unable to process further information. It therefore ultimately causes the system to crash. A system crash is defined as " a system failure that requires at least operator intervention and often some maintenance before system running can resume".[62]

4.2.6 Crab

A crab can be defined as a software program designed to destroy screen displays.[63] In other words the software program is designed to affect the visual screen display of a computer. For example it sometimes looks as if

[59] See Bernard P Zajac, Jr *The Michelangelo virus – was it a failure?* (1992) The Computer Law and Security Report 137; D P van der Merwe *Computers and the Law* (2000) 165.

[60] Tramontana (footnote 13 *supra*) 256; Branscomb (footnote 2 *supra*) footnote 17 on page 5.

[61] Branscomb (footnote 2 *supra*) footnote 17 on page 5.

[62] Dictionary of Computing 1986, footnote 4 in Tramontana (footnote 13 *supra*) 253.

[63] Branscomb (footnote 2 *supra*) footnote 17 on page 5.

something has eaten part of the visual screen display.[64] *Fites et al* is of the view that a crab software program is closer to a worm than a virus.

4.2.7 Hoaxes or virtual viruses

A hoax or virtual virus is a warning about a malicious code or program that does not exist.[65] The recipient is requested to forward the warning message to as many persons he or she knows. This causes the network to be flooded with traffic which in turn will slow it down or cause it to be shut down.

4.3 SHOULD UNAUTHORISED MODIFICATION BE CRIMINALISED?[66]

Computers are used in *inter alia* hospitals, national security, aviation and financial institutions and the interference with these computers and related data may have disastrous consequences. Interference with these types of computer systems is potentially dangerous and very serious.[67] For instance air traffic control depends greatly on computer systems and the interference with those systems may result in aviation disasters and loss of life. Computers and information networks are increasingly

[64] Fites et al *The Computer virus crisis* (1989) 26.

[65] Ronald B Standler *Computer Crime* accessible at http://www.rbs2.com/ccrime.htm; Ebersöhn (footnote 39 *supra*) 24 *et seq*.

[66] For a comprehensive discussion of the question posed 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 *et seq*.

[67] South African 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) 3.

vulnerable to interference.[68] The South African Law Commission was of the view that unauthorised modification of data should be criminalised or sanctioned with criminal penalty.[69]

4.4 COMPARATIVE LAW ANALYSIS IN RESPECT OF UNAUTHORISED MODIFICATION OFFENCES

4.4.1 United states of America

4.4.1.1 Federal statutes

Section 1030(a)(5) of the Federal Code states:

> "(a) Whoever
>
> (5)
>
> (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, and as a result of such conduct causes, recklessly causes damage; or
>
> (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage"[70]

Viruses and other forms of rogue code could also be the basis of a criminal prosecution in terms of section 1030(a)(3) of the Computer Fraud and Abuse Act. Section 1030(a)(3) prohibits the intentional unauthorised access to United States government computers when such

[68] SA Law Commission Report (footnote 67 *supra*) 3-4.

[69] SA Law Commission Report (footnote 67 supra) 3-4.

[70] United States Code, 2000 Edition.

conduct affects the use of the computer by the government.[71] There has been much criticism against the Computer Fraud and Abuse Act, especially in relation to viruses.[72] Tramontana is of the view that the federal legislator did not foresee the advent of computer viruses when the Act was drafted.[73]

Section 1030(a)(3) is limited to computers used by the United States government.[74] Large non-governmental computer networks do not fall within the scope of protection of this section. The scope of section 1030(a)(5) was broader than section 1030(a)(3) since it applied to federal interest computers. Federal interest computers were defined in section 1030(e)(2) as computers used by and for the US government as well as computers used by and for financial institutions. Federal interest computers included a computer "which is one of two or more computers used in committing the offence, not all of which are located in the same State."[75] The National Information Infrastructure Protection Act[76] and the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorist Act ("USA PATRIOT" Act)[77] amended the federal code in respect of computer crime quite

[71] Lyman (footnote 47 *supra*) 609.

[72] See in general Steve Shackelford *Computer-Related Crime: An International Problem in Need of an International Solution* (1992) Texas International Law Journal Vol. 27 No. 2 487 *et seq*.; Tramontana (footnote 13 *supra*) 266.

[73] Tramontana (footnote 13 *supra*) 266.

[74] Shackelford (footnote 72 *supra*) 488.

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

[76] 1996.

[77] 2001. This Act was signed into law during October 2001 shortly after the "September 11" attacks.

considerably.[78] The NIIPA extended the scope of application of section 1030(a)(5) of the Code to include any *computer used in interstate commerce or communications* and will include any computer that is attached to the Internet.[79] A protected computer now also includes computers attached to the Internet.[80]

Secondly both sections 1030(a)(3) and 1030(a)(5) of the Act initially required *access* to the specific computer. It is very seldom that a perpetrator actually accesses the specific computer in order to insert the virus onto the computer. Viruses can spread through a variety of means. The perpetrator does not necessarily access the computers to which the virus spread.[81] It could happen that the virus program accesses a computer (and not the perpetrator). An unsuspecting person may come into possession of the virus and this person can innocently access a system and spread the virus.

Both sections 1030(a)(3) and 1030(a)(5) of the Act initially required that the perpetrator *intentionally* accesses the computer. The requirement of intentional access can be problematic to prove since a virus can easily spread to many computers via a network or electronic mail server, and the creator might not have intended for a specific computer to become infected.[82]

[78] Shani S Kennedy & Rachel Price Flum *Computer Crime* (2002) American Criminal Law Review Vol. 39 No. 2 280; D P van der Merwe *Computer crime – recent national and international developments* (2003) 66 THRHR 38.

[79] Kennedy (footnote 78 *supra*) 280. Also see Laura J Nicholson et al *Computer Crimes* (2000) American Criminal Law Review Vol. 37 No. 2 207 *et seq*.

[80] Kennedy (footnote 78 *supra*) 280 (amended by the National Information Infrastructure Protection Act of 1996).

[81] Shackelford (footnote 72 *supra*) 488.

[82] Lyman (footnote 47 *supra*) 609 *et seq*.

The case of *United States v Morris*[83] is indicative of two problematic areas of the American federal legislation, in particular the meaning of the concepts *access*[84] and *intent.*[85] Robert Tappan Morris, an IT student at Cornell University created the *INTERNET worm*[86] and released it into federal interest computer networks and caused significant damage. He was prosecuted of a computer virus crime under section 1030(a)(5) of the Computer Fraud and Abuse Act of 1986.[87] The *worm* replicated itself and infected computers at a very fast rate. Even efforts by Morris to contain the worm were unsuccessful. Morris alleged that he did not have the intent to inflict harm or damage, but that his motives were to test the vulnerability of the system in order to improve security.[88] His defence that a programming error caused the worm to go out of control and infect so many computers was rejected.[89] Morris further contended that he did not have the intent to access certain of the computers or systems and that he did not program the worm in such a manner. Morris was authorised to access the Cornell University computer system where it would appear the

[83] (1991) 928 F.2d 504.

[84] Shackelford (footnote 72 *supra*) 488.

[85] Christopher D Chen *Computer Crime and the Computer Fraud and Abuse Act of 1986* (1990) Computer Law Journal Vol. X No. 1 81 – 82.

[86] See 4.2.2 *supra*. See in general F Lawrence Street and Mark P Grant *Law of the Internet* 2000 edition (1999) 664 – 665; 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 *et seq*.; Bernard P Zajac Jr. *Virus hits major computer network* (1988-89) 5 The Computer Law and Security Report 34-35.

[87] Martin L Forst *Cybercrime: Appellate Court Interpretations* (1999) 16 *et seq*. Also see Glenn D Baker *Trespassers will be prosecuted: Computer crime in the 1990s* (1993) Computer Law Journal Vol. XII No. 1 74; Branscomb (footnote 2 *supra*) 6 – 12; Lyman (footnote 47 *supra*) 609 – 613; Nelson (footnote 86 *supra*) 301 – 302.

[88] At the time Morris' father was a well-known and respected expert on computer security (Nelson footnote 86 *supra* 302).

[89] David Davies *News and comment on recent developments in computer security* (1989-90) The Computer Law and Security Report 37; Nelson (footnote 86 *supra*) 301.

virus was first introduced.[90] His conviction[91] was upheld by the United States Court of Appeal[92] and he was sentenced to three years probation, 400 hours community service, a fine of $ 10 050 .00 and the cost of his supervision.[93]

The USA PATRIOT Act amended and re-designated section 1030(a)(5) of the Code.[94] A person who knowingly causes the transmission of a program, code or command and intentionally causes damage to a protected computer is guilty of an offence.[95] For purposes of this subsection it is irrelevant whether the perpetrator was authorised to access the computer.[96] Section 1030(a)(5)(A)(ii) of the code prohibits intentional access without authorisation that results in damage.[97] An intention to damage is not required and recklessness is sufficient.[98] Intentional access without authorisation that results in damage and where the perpetrator is negligent is governed by section 1030(a)(5)(A)(iii) of the Code.[99] The provision in respect of negligence is far reaching and in my view computer criminality should not be based on negligence.

[90] Chen (footnote 85 *supra*) 82.

[91] See Graham Greenleaf *Computers and crime – the hacker's new rules* (1990-91) The Computer Law and Security Report; David Davies *Jury convicts hacker whose worm turned nasty* (1989-90) 6 Computer Law and Security Report 37.

[92] United States v Morris (1991) 928 F.2d 504.

[93] Forst (footnote 87 *supra*) 122; Bernard P Zajac, Jr *Robert T Morris, jr. Convicted* (1989-90) The Computer law and Security Report 29 and (1990-91) The Computer Law and Security Report.

[94] Kennedy (footnote 78 *supra*) 281.

[95] Section 1030(a)(5)(i) of the Federal Code. See Kennedy (footnote 78 *supra*) 281.

[96] Kennedy (footnote 78 *supra*) 281.

[97] Kennedy (footnote 78 *supra*) 281.

[98] Kennedy (footnote 78 *supra*) 281 *et seq*.

[99] Kennedy (footnote 78 *supra*) 281 *et seq*.

After the terrorist attacks in America on 11 September 2001 the United States government directed the war on terrorism also at cyber crimes. It is possible that a terrorist attack can be launched through the Internet.[100] The USA PATRIOT Act also amended certain of the provisions of section 1030(a)(5) to include instances where the damage impaired the medical examination, diagnosis or treatment of an individual, caused physical injury to an individual, caused a threat to general public safety and health or affected a government computer system used for administration of justice, national defence or national security.[101] The School Website Protection Act[102] renders legislative protection to school computers that are interfered with.[103]

4.4.1.2 State laws

Section 502(c)(4) of the California Penal Code states that any person who "knowingly accesses and without permission adds, alters, damages, deletes or destroys any data, computer software or computer programs which reside or exist internal or external to a computer, computer system, or computer network" is guilty of a public offence.[104] The wording of the section is very wide and will include all forms of computer modification. The same problems might arise as with the Computer Fraud and Abuse Act in respect of the use of the term *knowingly access*.[105] However

[100] In a newspaper clipping entitled *US fear al-Qaeda Internet attack* it is reported that terrorist hackers could use the Internet to shut down American electricity grids or open the flood gates of dams – The Citizen 28/06/2002 page 2. Also see Burden & Palmer (footnote 32 *supra*) 226.

[101] Section 1030(a)(5)(B). Also see Kennedy (footnote 78 *supra*) 282.

[102] 2001.

[103] Kennedy (footnote 78 *supra*) 283 *et seq*.

[104] A BNA Special Report *Computer data security* (1989) C-13 – C-24.

[105] See paragraph 4.4.1.1 *supra*.

section 502(c)(8) of the California Penal Code stipulates that any person who “knowingly introduces any computer contaminant into any computer, computer system, or computer network” commits an offence.[106] The use of the word *introduces* would appear to refer to the planting of the virus. “Computer Contaminant” is defined as “any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer system or computer network without the intent or permission of the owner of the information”.[107] This section explicitly refers to viruses and worms.[108] It would appear that section 502(c)(8) focuses on the actual introduction of a rogue program into the computer, system or network.

The State of Arkansas criminalises these types of offences in the form of *computer trespass* that will include unauthorised altering, deletion damaging, destruction or disruption of a computer, system or network or data.[109] The State of Illinois refers to these types of offences as *computer tampering* and it includes instances where the computer is damaged or destroyed or when a computer program or data is altered, deleted or removed.[110] It is interesting to note that this section provides for damage to both the physical computer as well as incorporeal data contained in a

[106] See Lyman (footnote 47 *supra*) 614.

[107] Section 502 (b)(10) of the California Penal Code.

[108] Section 502 (b)(10) of the California Penal Code also states “they include, but are not limited to, a group of computer instructions commonly called viruses or worms, which are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some fashion usurp the normal operation of the computer, computer system, or computer network”.

[109] Section 5-41-104(a) of the State of Arkansas Code. Section 18.2-152.4. of the Virginia Computer Crimes Act also criminalises these types of offences as *computer trespass*.

[110] Section 16D-3(a)(3) of the Computer Crime Prevention Law. See Lyman (footnote 47 *supra*) 617.

computer system. The State of New York also contains provisions in respect of *computer tampering.*[111]

The crime *computer damage* in the State of Minnesota provides for the criminalisation of various damaging acts pertaining to computers. The unauthorised damaging or destruction of a computer, computer network, computer system, computer software and data as well as the unauthorised alteration with intent to injure or defraud is criminalised.[112] Section 609.88(1)(c) provides that whoever distributes a destructive computer program[113] without authorisation and with the intent to damage or destroy computers, networks or data is guilty of the statutory offence of computer damage.

4.4.2 United Kingdom

Section 1(1) of The Criminal Damage Act of 1971 states:

> " A person who without lawful excuse destroys or damages any property belonging to another intending to destroy or damage any such property or being reckless as to whether any such would be destroyed or damaged shall be guilty of an offence."

Property is described in section 10(1) of the Act as property of a tangible nature whether real or personal. Property will also include money. The

[111] Sections 156.20 and 156.25 of the New York Penal Law.

[112] Section 609.88 of the Minnesota Statute.

[113] See paragraph 4.2 *supra*.

damage need not be permanent.[114] In the case of *Cox v Riley*[115] an employee erased the circuit card that contained several programs for a computerised saw. The usefulness of the saw had been affected. It was held that by erasing the programs, the saw was in fact *damaged*.[116] The British Law Commission was also of the view that the erasure of a program or data (which is incorporeal in nature) constitutes damage to the hardware such as the magnetic tape or disc on which the data is stored (which is corporeal in nature).[117]

In the matter of *R v Whiteley*[118] a computer hacker[119] was charged with criminal damage. The accused gained unauthorised access to a computer network and altered data that was contained on disks in the computer system. The computers were unable to function properly and had to be shut down for certain time periods. The accused was charged of criminal damage to the computers on the basis that the accused impaired the usefulness of the computers. The accused was acquitted on this charge. The accused was secondly charged with criminal damage to the disks and was convicted. The accused altered the magnetic particles on the disks in order to change the information on the disks. The court found that the disks and the magnetic particles on them were one entity. They were therefore tangible in nature and capable of being damaged. The Act

[114] *Cox v Riley* (1986) 83 Cr App R 54 (DC). Also see Michael Molan *Hungerford – Welch & Taylor's Sourcebook on Criminal Law* (2001) 1114 *et seq*.; Shackelford (footnote 72 *supra*) 492; Lloyd (footnote 10 *supra*) 245 *et seq*.

[115] (1986) 83 Cr App R 54 (DC).

[116] Richard Dedman *The Computer Misuse Bill* (1990-91) 1 The Computer Law and Security report 14; John C Buyers (footnote 10 *supra*) 14.

[117] Law Commission Working Paper No. 110 *Computer Misuse* (1988) 40.

[118] (1991) 93 Cr App R 25 (CA). See Lloyd (footnote 10 *supra*) 246 *et seq*.

[119] He hacked under the pseudonym *The Mad Hacker* (Lloyd footnote 10 *supra* 246)

requires that tangible property should be damaged. The damage itself should not necessarily be tangible.[120] The court found that the discs had been damaged because the usefulness of the discs had been impaired.[121]

The British Law Commission also dealt with the unauthorised alteration or destruction of data.[122] Damage to computers however are now governed by the Computer Misuse Act[123] and section 3(1) of the Act states:

> "A person is guilty of an offence if –
> (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 requisite intent and the requisite knowledge."

The requisite intent is described in detail in section 3(2):

> "The requisite intent is an intent to cause a modification of the contents of any computer and by so doing –
> (a) to impair the operation of any computer;
> (b) to prevent or hinders 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."

[120] See Michael Molan *Hungerford-Welch & Taylor's Sourcebook on Criminal Law* (2001) 1114 *et seq*.; Deborah Fisch Nigri *Investigating computer crime in the UK* (1992) 8 The Computer Law and Security Report 132 on 133; Chris Reed *Electronic Finance Law* (1991) 220 *et seq*.; A T H Smith *Property Offences* (1994) 369.

[121] Smith and Hogan *Criminal Law* 729.

[122] In general see Martin Wasik *Law Reform Proposals on Computer Misuse* (1989) The Criminal Law Review 266 *et seq*.

[123] 1990. See Chris Reed *Electronic Finance Law* (1991) 222; A T H Smith *Property Offences* (1994) 367 *et seq*.; Clive Gringras *The Laws of the Internet* (1997) 227 – 239.

Section 3(3) introduces a general intent and further states:

> "The intent need not be directed at –
> (a) any particular computer;
> (b) any particular program or data or a program or data of any particular kind; or
> (c) any particular modification or modification of any particular kind."

The *actus reus* consists in any action which *causes* a modification of programs or data held in a computer. All forms of destructive or dangerous code will fall within the ambit of this provision. The modification should be unauthorised and is indicative of a lack of consent by the person entitled to prevent the modification.[124]

The perpetrator must know that his actions are unauthorised and should have the deliberate intent to impair the operation of the computer. It is immaterial if the modification is permanent or only temporary.[125] It is immaterial whether the damage is only effected at a later stage such as logic bombs which are triggered for example on a specific date. When a virus is released into a network or system it is not always known to the perpetrator exactly what data will be affected and the general intent provision in section 3(3) of the Act will apply.

[124] Tony Elbra *A Practicle Guide to the Computer Misuse Act 1990* (1990) 9.

[125] Elbra (footnote 124 *supra*) 10.

4.4.3 Germany

The German Criminal Code provides for various actions in respect of the unauthorised modification of data.[126] Section 303a(1) of the German StGB criminalises *alteration of data* and provides

> "Anybody who unlawfully deletes, suppresses, renders useless, or alters data shall be sentenced to imprisonment not exceeding 2 years or to a fine."

An attempt to commit the offence is also criminalised.[127] The data should be electronic in nature. The offence is broadly defined and therefore has a wide scope of application.

A further offence of *computer sabotage* is contained in section 303b of the German Criminal Code:

> "Anybody who interferes with a data processing activity which is of vital importance to another enterprise, another business or a public authority by
>
> 1. committing an offence under section 303a(1) or
> 2. destroying, damaging, rendering useless, removing or altering a data processing system or carrier
>
> shall be sentenced to imprisonment not exceeding five years or to a fine."[128]

[126] In general see Ulrich Wuermeling *German and English Law against Computer Crime – a comparative survey* (1990-91) 3 The Computer Law and Security Report 15; Sigmund P Martin *Controlling Computer Crime in Germany* (1996) Information & Communications Technology Law Vol. 5 No. 1 10.

[127] Section 303a(2) of the German StGB.

[128] Section 303b(1) of the German StGB. See Martin (footnote 126 *supra*) 11.

An attempt to commit the offence is criminalised in section 303b(2) of the German StGB. The provisions of section 303b are much more detailed and provide for more severe penalties.

4.4.4 Greece

Article 370B(1) of the Greek Penal Code[129] provides for the criminalisation of unauthorised modification and states:

> "Anyone who without right copies, prints, uses, discloses to a third party or in any way breaches computer data or programs which constitute state, scientific or professional secrets or secrets of a public or private enterprise is punishable by imprisonment of at least three months."

The words *or in any way breaches computer data* is widely formulated and would include most instances of rogue code. This section will also include instances where data is altered or destroyed.[130] A prosecution may only be instituted when there is a formal complaint by the person whose system has been breached.[131]

Section 370B(2) provides for a maximum penalty of imprisonment for one year when the perpetrator is in the service of the possessor of the data. Viruses can infect computers worldwide and cause widespread damage that could cost millions to repair. The maximum penalty of 3

[129] Inserted by article 3 of Law number 1805 of 1988.

[130] Maria Stavropoulou & Chris Reed *Computer crime – the new Greek law* (1989) Computer Law & Practice Vol. 5 215.

[131] Article 370B(4) of the Greek Penal Code.

months is certainly insufficient when one takes into account that millions of computers can be infected worldwide.

4.4.5 Singapore

The Singapore Computer Misuse Act of 1993 contains a provision that criminalises unauthorised modification of computer material.[132] Section 5(1) states:

> "Subject to subsection (2), any person who does any act which he knows will cause an unauthorised modification of the contents of a computer shall be guilty of an offence and shall be liable to a fine not exceeding $ 2 000 or to imprisonment for a term not exceeding 2 years or to both"[133]

The *actus reus* is very widely defined and will include all instances which result in modification. The term *contents of computer* presumably will include data and software programs. The Act further clearly stipulates that it is immaterial that the act is not directed at specific data, programs or computers.[134] A virus that spreads through the Internet will fall within the scope of the Act. It is further immaterial whether the modification is permanent or only temporary.[135] In Singapore if the damage caused by such offence exceeds $10 000, a harsher penalty is provided for: $20 000

[132] In general see Katherine S Williams & Indira Mahalingam 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.

[133] Section 5 of the Malaysian Computer Crimes Act of 1997 contains a similar provision.

[134] Section 5(3) of the Singapore Computer Misuse Act of 1993.

[135] Section 5(4) of the Singapore Computer Misuse Act of 1993.

fine or a maximum of 5 years imprisonment or both.[136] The Act requires that the perpetrator should know that his actions could cause an unauthorised modification.

4.4.6 Philippines

The *I love you* virus[137] originated in the Philippines and infected millions of computers worldwide and caused damage estimated at billions of dollars.[138] This virus was sent in the form of an electronic mail message to a user's system. Once opened the virus destroyed data on the user's computer system and contaminated all the e-mail addresses in the user's e-mail address list. It then sent a copy of the virus to all the listed e-mail addresses on the user's system and it was therefore classified as the fastest spreading virus ever created. The virus also sent dialup account names and passwords to a destination in the Philippines.[139] During an interview with the one of the perpetrator's lawyer, broadcast in a National Geographic Special entitled *Cyberwars*, it was alleged that he was unaware of how destructive the virus would be. This allegation was questioned since the perpetrator wrote a thesis on the subject.[140] The creators[141] of this virus could not be prosecuted of a crime since there was no specific sanctioning provision in the Philippine Criminal Code that

[136] Section 5(2) of the Singapore Computer Misuse Act of 1993.

[137] Also referred to as the *lovebug*.

[138] See Reinhardt Buys *Love Hurts… Computer, network and e-mail security* (2000) July De Rebus 33; Clair Coleman *Securing cyberspace - new laws and developing strategies* (2003) Computer Law and Security Report Vol. 19 No. 2 131 *et seq*.

[139] Marchette (footnote 17 *supra*) 238.

[140] Anderson (footnote 18 *supra*) 9.

[141] Two young computer programming students named Reonel Ramones and Onel de Guzman.

made provision for computer-related offences and viruses.[142] Shortly after the attack the Electronic Commerce Act[143] was enacted in the Philippines that criminalises unauthorised access and interference with computer systems.[144] The introduction of a virus into an information network such as the *I love you* virus is criminalised.

4.4.7 Australia

The Australian Crimes Act of 1914 provides for two offences in respect of unauthorised modification. Section 76C states:

> “A person who intentionally and without authority or lawful excuse:
>
> (a) destroys, erases or alters data stored in, or inserts data into, a Commonwealth computer;
>
> (b) interferes with, or interrupts or obstructs the lawful use of, a Commonwealth computer;
>
> (c) destroys, erases, alters or adds to data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer; or
>
> (d) impedes or prevents access to, or impairs the usefulness or effectiveness of, data stored in a Commonwealth computer or data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer;
>
> is guilty of an offence.”[145]

[142] Although no criminal charges could be brought, the creator could certainly face civil claims for the damage caused.

[143] 2000.

[144] *Prosecution of cyber crimes through appropriate cyber legislation in the Republic of the Philippines* accessible at http://www.acpf.org/WC8th/AgendaItem2/12%20Pp%20Gana,Phillipine.html; *Cyber Crime …and Punishment?* accessible at http://mcconnellinternational.com/services/cybercrime.htm

[145] In general see Gordon Hughes *Recent developments in Australian computer crime regulation* (1991) Computer Law & Practice 94 on page 95; Gordon Hughes *Disjointed Australian assault on hackers* Computer Law & Practice (1990) Vol. 6 28 on page 30.

The penalty that is provided for is quite strict since a maximum of ten years imprisonment may be imposed. The Act also contains criminal provisions in respect of damaging data in Commonwealth and other computers by means of a Commonwealth facility.[146] The Australian Crime Act operates at federal level and is limited to government computers and government data stored on non-Commonwealth computers.

The intentional and unauthorised destruction, erasure or altering of data was initially criminalised in New South Wales.[147] The Cybercrime Act[148] replaced the existing computer crimes in the Crimes Act[149] with new cyber offences.[150] The unauthorised impairment of data or impairment to commit a serious offence, the unauthorised modification of data to cause an impairment, the unauthorised impairment of an electronic communication as well as the unauthorised modification of restricted data are criminalised in terms of the provisions of the new legislation.[151]

4.4.8 Canada

The Canadian Criminal Code contains the offence of *mischief*[152] that in essence criminalises the destruction of or damage in relation to property.

[146] Section 76E of the Australian Crimes Act of 1914.

[147] Section 310 of the Crimes Act 1900. Also see Graham Greenleaf *Computers and crime – the hacker's new rules* (1990-91) 2 The Computer Law and Security Report; Gordon Hughes (footnote 145 *supra*) 94; Gordon Hughes (footnote 145 *supra*) 30.

[148] 2001. The Act commenced on 21/12/2001.

[149] 1900.

[150] See Yee Fen Lim *Cyberspace Law – Commentaries and Materials* (2002) 332 *et seq*.

[151] Yee Fen Lim (footnote 150 *supra*) 333.

[152] Section 430 of the Canadian Criminal Code.

The offence is widely defined and includes instances where the lawful use of property is obstructed or interfered with.[153] *Mischief in relation to data* is specifically criminalised in section 430(1.1):

> "Every one commits mischief who wilfully
>
> (a) destroys or alters data;
>
> (b) renders data meaningless, useless or ineffective;
>
> (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."

The Act is widely defined and will include all instances of malicious code. The focus is on the result of the actions and not the manner in which it is achieved. The concept *data* is also defined in the Act as representations of information suitable for use in a computer system.[154] The Act uses the term *wilfully* and intention is therefore a requirement for a conviction. Upon conviction a perpetrator may be sentenced to a period of imprisonment not exceeding 10 years. This is an indication that offences of this nature are viewed in a serious light.

4.5 INTERNATIONAL RESPONSES BY THE COUNCIL OF EUROPE

The Council of Europe in a report on computer-related crime also dealt with the issue of *damage to computer data or programs* and suggested that these crimes should be included when drafting computer crime

[153] Section 430(1) of the Canadian Criminal Code.

[154] Section 342.1(2) of the Canadian Criminal Code.

legislation.[155] A draft text was recommended: “The erasure, damaging, deterioration or suppression of computer data or computer programs without right”.[156] The report further dealt with *computer sabotage* and recommended the following text:

> “The input, alteration, erasure or suppression of computer data or computer programs, or interference with computer systems, with the intent to hinder the functioning of a computer or telecommunications system.”[157]

It would appear that computer sabotage is directed at the criminalising of viruses and worms that cause damage to computer systems and hinders the proper functioning of the computer or system.

The Council of Europe’s Convention on Cybercrime[158] deals with the issue of data interference and system interference. Article 4 of the Convention provides that the signatory countries should adopt legislation that criminalises the intentional damaging, deletion, deterioration, alteration or suppression of computer data without right. Article 5 of the Convention deals with system interference and provides that the signatory countries should adopt legislation that criminalises the intentional serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or

[155] 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 43-46; 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*.

[156] Council of Europe Report (footnote 155 *supra*) 44.

[157] Council of Europe Report (footnote 155 supra) 47.

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

suppressing computer data. South Africa, to a certain extent, adhered to these provisions by the enactment of section 86(2) of the Electronic Communications and Transactions Act that will be discussed in more detail below.[159]

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

4.6.1 Malicious injury to property

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.[160]

The disgruntled employee that created a virus and caused a nationwide Edgars network failure was convicted of malicious injury to property in the Specialised Commercial Crimes Court, Johannesburg.[161] The offence was committed before the enactment of the Electronic Communications and Transactions Act. The charge sheet alleged that during April 1999 to May 1999 the accused unlawfully and intentionally created and loaded a

[159] See paragraph 4.7 *infra*.

[160] Snyman *Criminal Law* (2002) 535; Hunt defines malicious injury to property as: “unlawfully damaging property with intent to injure another” (*South African Criminal Law and Procedure* (1970) 778. In *Mnyandu* 1973 4 SA 603 (N) at 606A the crime was defined as the unlawful and intentional damaging of property belonging to another person or in which another person has a substantial interest.

[161] The State versus Berend Howard, case number 41/258/2002. See *Man guilty of computer virus sabotage* The Star 18/05/2004; *IT man costs Edgars R20m* The Citizen 18/05/2004 pages 1 and 2.

malicious software program using the central computer network of Edgars Consolidated Stores Limited, causing damage to the network servers throughout South Africa, centralised in Edgardale, resulting in a nationwide network failure. The prosecution argued firstly that the network or system is corporeal or tangible in nature and secondly that there is no requirement in law that the *property* should be tangible in nature.

In the *Howard* case data was erased and affected. Data and information are of an electronic incorporeal nature. The molecules are digital in nature and if one compares it with the decision in *S v Mintoor*[162] it is clearly incorporeal in nature. The main problem in this case is the requirement that *property* should be damaged. It is stated that the property should be corporeal in nature. The prosecution's argument that there is no legal requirement that *tangible* property should be damaged *appears* to be incorrect in view of all the reported decisions[163], literary works[164] and the Law Commission's Report[165]. However in the case of *R v Mavros*[166] the court held that *property* also includes rights that others have in that property.[167] The Court stated in *S v Mtetwa*[168] that "in regard to the crime

[162] 1996 (1) SACR 514 (C).

[163] See in general Snyman *Criminal Law* (2002) 535 *et seq*. All the South African cases deal with some form of corporeal property. See for example *R v Mandatela and another* 1948 (4) SA 985 (E); *R v Ncetendaba and another* 1952 (2) SA 647 (SR); *R v Bhaya* 1953 (3) SA 143 (N); *R v Bowden and another* 1957 (3) SA 148 (T); *R v Nyawo and others* 1966(2) SA 61 (Rhodesia); *S v Mnyandu* 1973 (4) SA 603 (N); *S v Kgware and another* 1977 (2) SA 454 (C) and *S v Swiegelaar* 1979 (2) SA 238 (C).

[164] Hunt *South African Criminal Law and Procedure* (1970) 778 *et seq*. and Snyman *Criminal Law* (2002) 536 and all the authorities cited by him in footnote 1 on page 535.

[165] SA Law Commision Report (footnote 67 *supra*) 6.

[166] 1921 AD 19.

[167] At page 23. Also see G J Ebersöhn *A common law perspective on computer-related crimes (2)* (2004) 67 THRHR No. 2 207.

[168] 1963 (3) SA 445 (N).

of malicious injury to property it is not necessary that the complainant should be the full and unencumbered owner of the property injured" and stated further that "what is required is that the intentional and unlawful act be an injury to the *rights of another person in that property*[169]".[170] It would therefore appear that *property* would also include rights that others have in respect of the property.[171] A right is incorporeal in nature and it could certainly be argued that the courts have expanded the scope of malicious injury to property to include incorporeal limited real rights. In the *Howard case* the court found in passing that the element of property does not necessarily have to be corporeal in nature. It should however also be borne in mind that the offence of malicious injury to property was developed in an era where intangible concepts such as data and information systems did not exist and that offences such as *crimen iniuria* and fraud sufficiently provide for the criminalisation of injury to incorporeal concepts such as dignity. Property rights are further limited to *things* that are corporeal in nature. Consequently it is submitted that the element of property has not been expanded to include all types of incorporeal or intangible "property" or concepts.

In the *Howard* matter the malicious code caused the deletion of files, which ultimately resulted in a denial of service and various cashiers could not access the system from point of sale terminals and computers. In the case of *R v Bowden and another*[172] the Court found that if property is affected in such a manner that it can be restored or repaired but reparation

[169] My emphasis.

[170] At page 449.

[171] Ebersöhn (footnote 167 *supra*) 207.

[172] 1957 (3) SA 148 (T).

causes expense and difficulty to the owner, then the element of damage would have been satisfied. In the current case therefore there is clearly damage.

The next aspect to consider is the prosecution's argument that the computer system is corporeal in nature. It could be argued that what really is affected or actually damaged with the introduction of malicious code is data and information that is entirely intangible in nature, and would not fall within the scope and ambit of the offence of malicious injury to property. If one looks at the courts' extension of the principle of theft of incorporeal items[173], one may by way of analogy argue that the position should be the same with malicious damage to property. However, the principle of legality or *nulum crimen sine lege* as well as section 35(3)(l) of the Constitution[174] which provides that every accused person has the right to a fair trial which includes the right "not to be convicted for an act or omission that was not was not an offence under either national or international law at the time it was committed or omitted", may prevent such an extension.[175] It should also be noted that recently the Court did not extend the meaning of property to include intangible electricity.[176] The Legislator deemed it fit to enact specific provisions in respect of the modification of data and arguably holds the same view that the common law should not be extended to include incorporeal items. It might have been better to prosecute *Howard* in the

[173] Discussed in more detail in paragraph 11.3 *infra*.

[174] Act 108 of 1996.

[175] See paragraph 1.2 *supra*.

[176] *S v Mintoor* (footnote 162 *supra*).

High Court, since a Regional Court is merely a creature of statute and is bound by the *stare decisis* doctrine to the decisions of the High Court.

In most instances of the introduction of rogue code no damage is caused to the physical components of a computer, but operations are impaired which result in a denial of service. It could be argued that a computer system is damaged which means that the computer itself cannot operate properly and is therefore affected. The intangible data and tangible computer are interlinked and they operate as a unit. The intangible instructions and data exist in a computer or computer system and the computer cannot properly function without the intangible instructions and data. When data on a disk is altered or erased, the owner must repair the disk or restore the information. Malan is of the view that the disk and the information contained on it must be viewed as one entity and damage to the entity (the disc) will constitute malicious injury to property.[177] In other words the usefulness of the computers are affected when instructions of a computer system or computer are erased or interfered with. In relation to the impairment of the usefulness of the physical computer one can consider the British cases of *Cox v Riley*[178] and *Whitely*[179].[180] The Court stated in *Whitely*:

> “What the Act requires to be proved is that tangible property has been damaged, not necessarily that the damage itself is 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

[177] F R Malan *Oor inligting, rekenaarmisbruik en die strafreg* (1989) De Jure 225.

[178] (1986) 83 Cr App R 54 (DC). See Reed *Computer Law* (1990) 168 *et seq*.

[179] (1991) 93 Cr App R 25 (CA).

[180] Discussed in paragraph 4.4.2 *supra*.

> and 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."[181]

It appears that the Court found in the case of *Howard* that the physical computers were temporarily damaged as a result of the virus and convicted the accused of malicious injury to property. The Accused was recently sentenced to a term of imprisonment.[182] Leave to appeal and bail pending appeal were granted to the Accused.

4.6.2 Housebreaking with the intent to commit an offence

The offence of housebreaking with the intent to commit an offence has been discussed in great detail above.[183] The main problem is that data is incorporeal in nature and access thereto exists in an electronic world. Although the offence is called *housebreaking*, damage is not a prerequisite and would not assist when data is damaged or destroyed. The requirement that the perpetrator must further have the intention to commit an offence is problematic since it is debatable whether the modification of data was a criminal offence (before enactment of the Electronic Communications and Transactions Act).[184]

[181] (1991) 93 Cr App Rep 25 at 28. Ian I Lloyd *Information Technology Law* (2000) 247; David I Bainbridge *Introduction to Computer Law* (2000) 320 *et. seq*.

[182] Aphiwe Boyce *Man jailed for Edcon computer sabotage* Saturday Star 23/10/2004 page 3; Marthinus van Vuuren *Rekenaarvirus lei tot tronkstraf (Edgars verloor R19 miljoen; man moet 4 jaar sit)* Naweek-Beeld 23/10/2004 page 7.

[183] See paragraph 3.6.1 *supra*.

[184] SA Law Commission Report (footnote 67 *supra*) 7-9.

4.6.3 Trespass Act

The Trespass Act[185] was also discussed in detail above[186] and is limited to the unlawful entering or presence of a person on physical property or a building. Damage, interference or modification of the property is not a requirement and this offence can therefore not be applicable when computer data is modified.[187]

4.7 THE SOUTH AFRICAN ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT

It is clear from the discussions above that South African law was ill equipped to criminally deal with unauthorised modification of data and various forms of malicious code. The Law Commission's proposals included the statutory criminalisation of the unauthorised modification of computer data and software applications. In the proposed Computer Misuse Bill two offences are proposed in respect of the modification of data.[188] These offences include any unauthorised act that causes data to be modified, destroyed or erased or otherwise rendered ineffective as well as the unauthorised insertion of any application in a computer system.

Section 86(2) of the Electronic Communications and Transactions Act[189] states as follows:

[185] Act 6 of 1959.

[186] See paragraph 3.6.2 *supra*.

[187] Also see the SA Law Commission Report (footnote 67 *supra*) 11-12; M M Watney *Die strafregtelike en prosedurele middele ter bekamping van kubermisdaad (deel1)* (2003) 1 TSAR 63.

[188] SA Law Commission Report (footnote 67 *supra*) 64.

[189] Act 25 of 2002.

> "A person who intentionally and without authority to do so, interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective, is guilty of an offence."

The Act did not include the wording of the second suggested offence in the proposed Computer Misuse Bill.

4.7.1 The criminal action (conduct)

The conduct consists in the interference with data which interference causes the data to be modified, destroyed or otherwise rendered ineffective. The act is widely defined. Interference in any manner would therefore suffice as long as it results in the data being modified, destroyed or otherwise rendered ineffective. The focus is on the result caused by the interference. All forms of dangerous code such as viruses and worms will fall within the ambit of the offence. The actions of a hacker that hacks into a computer system and deletes or changes the data or defaces a website will similarly fall within the scope of this section.

To modify means to change data. The meaning of *destroy,* according to the Essential English Dictionary[190], is that so much damage is done that the data is completely ruined. Data is rendered ineffective if the normal functioning thereof has been impaired. The modification need not be permanent in nature and could only be temporary in nature. Damage is not an essential element of the offence.[191] The extent of the damage, however, can be an aggravating factor when sentence is considered.

[190] Collins Essential English Dictionary.

[191] See the SA Law Commission Report (footnote 67 *supra*) 56.

Ping flooding occurs when millions of pings[192] are sent from one computer to the port[193] of another computer. The latter computer responds to the pings of the first computer and due to the vast amount of pings it attempts to respond to, the system is crippled and may even result in a system crash.[194] According to Ebersöhn *ping flooding* interferes with the data in an indirect manner causing the data to be rendered ineffective, as the data or system is inoperable or inaccessible, and will constitute a contravention of section 86(2) of the Act.[195] He is of the view that *ping flooding* does not directly affect or interfere with the data, but as a result of the system failure the data also becomes ineffective.[196]

Data is defined as electronic representations of information in any form.[197] Data is again widely defined and not restricted to specific forms of data. This will include data stored in computers, the Internet and information networks. It is also submitted that the Act will also be applicable in respect of data contained in computerised devices, smart cards and even cellular phones. Nowadays access to the Internet can be gained from a cellular phone which makes cellular phones vulnerable and could easily affect the operation of the phone or cause the phone to perform certain unwarranted actions.[198]

[192] A *ping* is a signal sent from one computer to another computer. The latter computer responds to the ping. See G J Ebersöhn *Internet law: Port scanning and ping flooding – a legal perspective* (2003) THRHR 66 No. 4 563 at 565.

[193] A *port* is a communication channel from which one computer can sent information to another computer. See Ebersöhn (footnote 192 *supra*) 563.

[194] Ebersöhn (footnote 192 *supra*) 565.

[195] Ebersöhn (footnote 192 *supra*) 569.

[196] Footnote 195 *supra*.

[197] Section 1 of the Electronic Communications and Transactions Act 25 of 2002. The discussion in paragraph 3.7.1 *supra* is equally applicable.

[198] Hugo Hagen *Virus threatens cellphones* The Citizen 18/06/2004 pages 1 and 2.

If a person creates and loads a virus on the Internet and a lot of computers worldwide are infected, how many crimes does the person commit? Is the loading of the virus with the intention to indiscriminately “infect” a single act, or does every infected computer constitute an act or offence? It would appear that in South Africa the focus of the Act is more on the result caused by the offence and it could certainly be argued that each and every computer or computer system that falls within the authority of a certain individual or corporation and that is affected could constitute an offence. The intention of the perpetrator is also an important factor to take into account when deciding how many offences the cyber criminal actually committed.

4.7.2 Unlawfulness

The unlawfulness of the act lies in the absence of authority or permission to make the modification. The owner or person lawfully in charge of the affected data can give permission or authority to modify the data. The person in charge of the computer from where the modification is done cannot give such authority or permission (unless of course such person has the necessary authority).[199]

The element of unlawfulness can be excluded by means of grounds of justification. Permission or authority may justify a perpetrator’s actions. One could envisage that a perpetrator may act on instructions. Computer programmers may modify data in order to repair a problem with the computer system or network. It is equally possible that an authorised

[199] See SA Law Commission Report (footnote 67 *supra*) 56 *et seq*.

person may deliberately exceed the scope and ambit of his authority or consent.[200]

In an era of misuse of proprietary data some software engineers' program software in such a manner that a logic bomb (*software bombs*) will disable the software at a specific point in time when for instance the license expires.[201] Such a logic bomb that disables data will constitute an interference with data. The question is whether such interference is authorised. It is submitted that the person that uses the software are only legitimately doing so until the license expire. Once the license expires the user does not have any rights in relation to the data until such time that the license is renewed and the software developer is the person that has intellectual property rights in relation to such data. It is submitted that such interference could be authorised provided that additional interference to the system is not caused.

4.7.3 Culpability

Mens rea is prescribed by the Act as intention. The South African Law Commission also recommended that the conduct should be intentional.[202] Negligence will therefore not suffice. The intent must be directed at all the elements of the offence.[203] Firstly the perpetrator should have the intent to interfere with data in such a way that the data is modified, destroyed or otherwise rendered ineffective. Secondly the perpetrator

[200] See the discussion in paragraph 3.7.2 *supra*.

[201] See in general Tim Sewart *Time to Drop the Bomb* (2003) Computers & Law Vol. 14 Issue 4 23 *et seq*.

[202] SA Law Commission Report (footnote 67 *supra*) 57.

[203] Snyman *Criminal Law* (2002) 179 *et seq*.

should have knowledge of the unlawfulness of his actions.[204] In other words he must know that he has no authority or permission to cause the modification.

Intent in the form of *dolus directus*, *dolus indirectus* and *dolus eventualis* will all be sufficient to establish *mens rea*. *Dolus directus* will be present when the perpetrator has the intent to interfere with data in such a way that it is modified, destroyed or otherwise rendered ineffective. One can perceive that *dolus indirectus* may be present when the perpetrator's main objective is to commit some other offence but in order to achieve this goal it is necessary to commit the present offence. When the perpetrator foresees that he might not have the authority to modify data and he proceeds with his actions, intent in the form of *dolus eventualis* is present.

If a perpetrator foresees that a virus may spread and infect certain computers and he proceeds with the actions, intent in the form of *dolus eventualis* will be present. An accused may argue that he or she did not have the required intent because he did not foresee that the virus or rogue program will spread in a certain manner or that it will infect certain computers. A virus may spread in a way that the perpetrator did not foresee at all. A person may innocently load the virus on a disc and then spread the virus to another computer or system. Whether the perpetrator in fact foresaw the possibility is a subjective test.[205] What must be established is the likelihood of the possibility viewed in the light of the particular circumstances of each case.[206] The fact that the perpetrator is a

[204] SA Law Commission Report (footnote 67 *supra*) 57.

[205] M M Loubser & M A Rabie *Defining dolus eventualis: a voluntative element?* (1988) 3 SACJ 415 on page 416.

[206] Loubser & Rabie (footnote 205 *supra*) 418.

computer programmer or very knowledgeable in the field of information technology may assist the court in finding whether the perpetrator in fact foresaw a certain result. It may be problematic to prove intent when one deals with an unintelligent accused who is not an expert in the field of computers and information technology.[207] A person must have criminal capacity and the sentiments expressed in respect of youthful offenders are equally applicable in these types of cases.[208]

4.7.4 Related provisions

An attempt to intentionally interfere with data without authority is criminalised in section 88(1) of the Act. Aiding and abetting a person to commit the offence is criminalised as a separate offence.[209] The provisions of the Riotous Assemblies Act[210] would also apply in respect to the offence of unauthorised modification for example where two or more persons conspire to release a virus on the Internet.[211]

It is further submitted that if a cyber criminal hacks into a system and then release a virus the person contravenes section 86(1) in respect of the unauthorised access as well as section 86(2) in relation to the interference of data. These offences have separate criminal actions and are clearly distinguishable.

[207] Cliffe Dekker Attorneys *Commentary on the Electronic Communications and Transactions Act, 2002* at http://www.mbendi.co.za/cliffedekker/literature/commentary/ect2002.htm

[208] See the discussion in paragraph 3.7.3 *supra*.

[209] Section 88(2) of the Electronic Communications and Transactions Act 25 of 2002.

[210] Act 17 of 1956.

[211] See paragraph 3.7.4 *supra*

4.7.5 Sentence

Section 89(1) of the Act provides that a person convicted of contravening section 86(2) of the Act may be sentenced to a fine or imprisonment not exceeding 12 months. The maximum fine falls within the jurisdiction of the district courts. Certain modifications such as viruses could have disastrous consequences and could cause huge amounts of damage. For example the *I Love You* virus caused damage estimated at billions of dollars.[212] Locally the virus that was loaded on the mainframe of Edgars caused damage to the value of R19m.[213] It is submitted that the penalty provided for in the Act is far too lenient especially in light of the advent of viruses and other forms of destructive code.[214] The Law Commission suggested a fine or a term of imprisonment not exceeding 10 years.[215] The National Prosecuting Authority Act[216] provides for a maximum penalty of a fine or 25 years imprisonment or both.[217] The Financial Intelligence Centre Act[218] provides for a fine not exceeding R 10 000 000 or a term of imprisonment not exceeding 15 years.[219] The penalty provided for by the Defence Act[220] is a maximum of 25 years imprisonment.[221] Although

[212] See paragraphs 4.1 and 4.4.6 *supra*.

[213] See paragraph 4.1 and 4.6.1 *supra*.

[214] The same view is held by M M Watney *Die strafregtelike en prosedurele middele ter bekamping van kubermisdaad (deel 2)* (2003) TSAR 241 on 242.

[215] Section 10(2) of the Proposed Computer Misuse Bill, SA Law Commission Report (footnote 67 *supra*) 67.

[216] Act 32 of 1998.

[217] Section 41(4) of Act 32 of 1998. See paragraph 4.8 *infra*.

[218] Act 38 of 2001.

[219] Section 68(1) of Act 38 of 2001. See paragraph 4.8 *infra*.

[220] Act 42 of 2002.

[221] Section 104(8) of Act 42 of 2002. See paragraph 4.8 *infra*.

some of these provisions are severe it is perhaps an indication of the serious light in which these types of offences should be viewed.

Crackers are often youthful offenders and would usually not be in a financial position to pay a heavy fine or to pay for the damages that has been caused. The parents of the perpetrator might end up paying the fine or damages and might not necessarily be in a financial position to do so. It is also not conducive to send a youthful first offender to prison. Many crackers are multiple offenders and will not easily change their ways. Treatment programs in the form of correctional supervision might be more effective under these circumstances.[222]

4.8 FURTHER SOUTH AFRICAN LEGISLATION IN RESPECT OF UNAUTHORISED MODIFICATION OFFENCES

The South African Police Service Act[223] provides that any person who performs an act that causes an unauthorised modification of the contents of a computer under the control of the South African Police Service is guilty of an offence.[224] The provisions of this section are limited to computers that belong to or are under the control of the South African Police Service. The modification may be of a temporary or permanent nature.[225] The perpetrator must have the intent to impair the operation of the computer or the reliability of the data held in the computer or to obstruct access to the data.[226] Upon conviction the perpetrator may be

[222] In terms of the provisions of section 276(1)(h) of Act 51 of 1977.

[223] Act 68 of 1995.

[224] Section 71(4) of Act 68 of 1995.

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

[226] Section 71(4) of Act 68 of 1995.

sentenced to a fine or a maximum period of 5 years imprisonment.[227] Section 128 of the Correctional Services Act[228] has similar provisions. The scope of application of this section is however limited to computers that belong to or are under the control of the Department of Correctional Services or a contractor of the Department.

The National Prosecuting Authority Act[229] provides for similar offences in respect of the computers that belong to or are under the control of the National Prosecuting Authority.[230] The penalty provided for by the Act is a fine or a period of imprisonment not exceeding 25 years or both.[231] The penalty provisions are severe and it is highly unlikely that it will be imposed in any circumstances.

Section 66 of the Financial Intelligence Centre Act[232] states:

> "Any person who, without authority to do so, wilfully causes a computer system that belongs to, or is under the control of, the Centre, or any application or data held in such a computer system, to be modified, destroyed, erased or the operation or reliability of such a computer system, application or data to be otherwise impaired, is guilty of an offence."

The Act focuses on the result of the actions and is broadly defined, which widens the scope of application of this section. However this chapter of

[227] Section 71(4) of Act 68 of 1995.

[228] Act 111 of 1998.

[229] Act 32 of 1998.

[230] Section 40A(2)(c) of Act 32 of 1998.

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

[232] Act 38 of 2001. The Act came into operation on 1 February 2002.

the Act is limited to computers that belong to or are under the control of the Financial Intelligence Centre. Upon conviction an accused may be sentenced to a maximum period of 15 years imprisonment or to a fine not exceeding R 10 000 000.[233]

The Defence Act[234] contains a provision in relation to the computers of the Department of Defence and provides that a person:

> "…. or who, without authority, changes, alters, corrupts, copies or withdraws data from any such systems or data bases, is guilty of an offence…."[235]

A maximum penalty of a fine or 25 years imprisonment is provided for.[236] The Act was assented to on 12 February 2003 and came into operation on 23 May 2003.

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

[234] Act 42 of 2002.

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

[236] Footnote 235 *supra*.