

**CYBER CRIME IN SOUTH AFRICA:
INVESTIGATING AND
PROSECUTING CYBER CRIME
AND THE BENEFITS
OF
PUBLIC-PRIVATE PARTNERSHIPS***



**ADV JACQUELINE FICK
SENIOR MANAGER: ADVISORY
RISK AND COMPLIANCE MANAGEMENT
PWC SOUTHERN AFRICA**

MARCH 2009

EXECUTIVE SUMMARY

With the advent of advanced technology has come a new breed of criminals: criminals who are well-organised, well-resourced and have technological savvy.

These cyber criminals commit their crimes with great speed, in an environment of cyber-anonymity and in most instances, in multiple legal jurisdictions.

Traditional criminals are turning away from crime such as cash-in-transit robberies to an easy and well-paying life of cyber crime, which offers far greater rewards for less risk.

Law enforcement agencies are left playing *catch-up* with criminals. Traditional law enforcement tools, methodologies and disciplines do not successfully address the detection, investigation and prosecution of cyber crime. This type of crime calls for a pro-active approach, for timely international cooperation, and for effective public-private partnerships to ensure the upper-hand over criminals.

This paper aims to provide a broad overview of the South African legal context governing cyber crime, practical examples of cyber investigations and the benefits of public-private partnerships to the prevention, detection and prosecution of cyber crime in South Africa.



TABLE OF CONTENTS

Executive Summary	1
Introduction	2
Legislative framework governing cyber crime in South Africa	3
■ Introduction	3
■ Definitions relating to cyber law.....	4
■ Categories of cyber crime	5
■ Specific provisions of the ECT Act	7
■ Unauthorised access (section 86(1))	7
■ Unauthorised modification of data and various forms of malicious code (section 86(2)).....	7
■ Denial of service attacks (section 86(5)).....	8
■ Unauthorised interception (section 86(1)).....	8
■ Devices (section 86(4)).....	9
■ Extortion (section 87(1)).....	9
■ Computer-related fraud (section 87(2)).....	9
■ Theft.....	9
■ Pornography, Cyber Obscenity and Stalking.....	10
■ Council of Europe’s Convention on Cyber crime.....	11
Investigation and prosecution of cyber crime in South Africa	13
■ Practical applications.....	18
Public-private partnerships: The layered defence	21
Conclusion	27
Bibliography	29

“With the Internet’s global reach, the temptation is irresistible for these criminal entrepreneurs. The value of information and transactions on computer networks has grown to the point where cyber crime has become an organised, professional activity. Cyber criminals take advantage of vulnerabilities in networks and computers to gain access to valuable information, such as personal identification information, financial data, or intellectual property.

Criminals now use the Internet for extortion, fraud, money laundering, and theft. Information technology lets them carry out these crimes more efficiently and with less risk. Victims can be found automatically. The use of pseudonyms or online identities provides an anonymity that is attractive to criminals. Some sources estimate that perhaps only 5 percent of cyber criminals are ever caught and convicted. The internet provides criminals a way to move money rapidly among bank accounts and countries. The nature of the Internet makes it difficult for police to follow transactions to gather evidence, and national laws differ enough to make prosecution difficult.”

**McAfee Virtual Criminology Report:
North American Study into Organised Crime and the Internet**



INTRODUCTION

In this exciting cyber era, information technology and computers have invaded our every day lives to such an extent that we cannot cope without them.

Traditional shopping malls have been replaced by virtual shopping malls and one can acquire almost anything through the Internet. Information superhighways have made a virtual borderless world possible. One can have access to information located anywhere in the world, within seconds and on the click of a mouse.

Computers and information technology are used in business, industry, medicine, science, engineering, education and government, to name but a few fields.

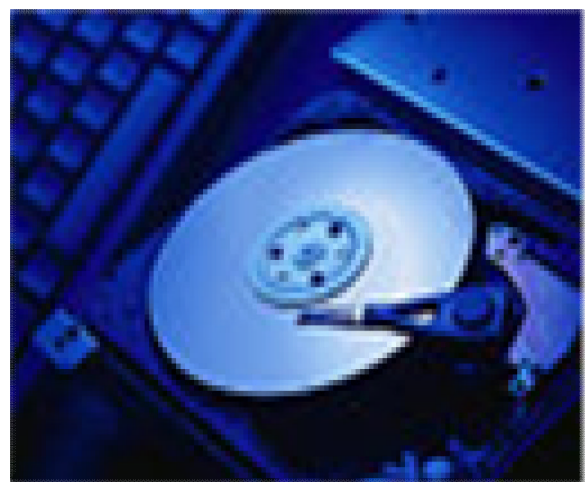
It is hard to imagine what the world would be like without it. The advantages of computers are countless and they have a profound effect on society.

But the same rings true when it comes to criminals: computers and

information technology has also revolutionised the commission of various crimes, leading to a situation where investigators more often than not, have to play catch-up with sophisticated and well-organised criminals.

This paper aims to provide a broad overview of the legislative framework governing cyber crime in South Africa, the investigation and prosecution of these crimes and the benefits of public-private partnerships.

The paper was written for the Council of Europe's Octopus Interface Conference 2009, 10 – 11 March 2009, Strasbourg, France. The author was a presenter at the Workshop on *Following criminal money on the Internet*, 10 March 2009.¹



LEGISLATIVE FRAMEWORK GOVERNING CYBER CRIME IN SOUTH AFRICA

INTRODUCTION

The South African criminal law originates from Roman law and legal principles that were developed centuries ago.

These legal concepts were hardly designed to cope with today's advancing technology, nor were the traditional methods of detection, investigation and prosecution of crime designed to bring cyber criminals to book.

Early in 2001 the South African Law Commission released a discussion paper on computer-related crime and also recommended that legislation should be considered to introduce new cyber offences.

This led to the Electronic Communications and Transactions Act, No. 25 of 2002 (hereinafter



referred to as the ECT Act), which was assented to on 31 July 2002 and has been in operation since 30 August 2002.

The ECT Act eradicated several of the *lacunae* that previously existed in the South African law, in respect of the emergence of various types of cyber crime, such as hacking and the creation of malicious computer code.

The unauthorised access and unauthorised modification of data, as well as the possession and distribution of hardware devices and software programs that facilitate the commission of these offences have now been criminalised (e.g. spyware, key loggers and spy software).

DEFINITIONS RELATING TO CYBER LAW

It is interesting to note that the Convention on Cybercrime uses the terms computer system² and computer data³ and appears to limit the application of the Convention to computers, computer systems and computer-related data⁴.

Computer hardware refers to the mechanical components of a computer system and is physical in nature. Computer software refers to the instructions given to a computer in order to function in a certain way. These instructions consist of electronic data and are incorporeal in nature.⁵

It is furthermore important to note that computer components are used not only in computers, but also in various other devices such as cellular telephones.⁶

A smart card is a plastic card with a microprocessor chip embedded in it. This chip enables it to store data and to process information. A smart card has computer intelligence and can

perform various functions in respect of the stored data.⁷ Various crimes can be committed in respect of the smart card itself, as well as the functions and data contained in the microprocessor chip, which will make various forms of cyber crime equally applicable to smart cards.

All these devices essentially contain data that involves some form of computer and information technology and it is submitted will all fall within the scope and ambit of the ECT Act.

South African authors Credo and Michels⁸ defined computer crime as:

“...computer crime encompasses the use of a computer as a tool in the perpetration of a crime, as well as situations in which there has been unauthorised access to the victim’s computer, or data. Computer crime also extends to physical attacks on the computer and/or related equipment as well as illegal use of credit cards and violations of automated teller machines, including electronic fund transfer thefts and the counterfeit of hardware and software.”⁹

There has, however, been a move in South African law to use the term cyber crime which is wide enough to encompass all illegal activities in respect of computers, information networks and cyberspace.¹⁰

It is also important to bear in mind that computer-related crime can take on the form of traditional/conventional crimes in which computers are instrumental to the offence, such as child pornography and intellectual property theft, attacks on computer networks, as well as conventional criminal cases where the evidence that is to be used is in digital form.

The ECT Act sufficiently deals with jurisdiction, the admissibility of data messages, the admissibility of electronic signatures, as well as the regulation of cryptography.

Cyber inspectors are a new addition to law enforcement and their tasks include the monitoring of the Internet and ensuring that the provisions of the ECT are complied with. However, South Africa still does not have a recognised body that deals with electronic signatures, nor has the

provisions relating to cyber inspectors been implemented.

CATEGORIES OF CYBER CRIME

There are various different types of criminality where computers play a role, such as:

- Service disruption and/or the interference with lawful use of a computer.
- Dissemination of offensive materials such as pornography.
- Extortion and cyber-stalking.
- Reputational damage such as defacing a company website.
- Forgery/counterfeiting: IP offences, software piracy, copyright infringements, etc. Currently the best known form of cyber fraud is phishing that begins with an e-mail purporting to be from a bank, credit card company or retailer asking the user to go to a website and supply account information.
- Information theft is the most damaging category of Internet crime and can take on several forms, such as theft of personal identification information, credit

information from a company's database, financial information, intellectual property such as designs, etc.

- **Fraud:** Internet banking fraud, debit and credit card fraud, online auction fraud, online securities fraud, etc.
- **Illegal interception** of communications, espionage, etc.
- **Money laundering:** The growth of global financial services makes it easy to conduct banking operations across borders over the Internet. Although the use of the internet can provide law enforcement agencies with a greater ability to trace transactions through electronic records, the volume of transactions, the anonymity, the speed with which these transactions are concluded and the lack of consistent record-keeping still makes it very attractive to criminals and terrorists alike.

Many of these criminal activities mimic traditional crimes, but because most computer-related crimes are executed with great ease, speed and the impact is often felt across borders, the response to these types of crimes cannot be based on traditional investigative methodologies and tools alone.

“The success of cyber criminals poses new and difficult challenges for law enforcement. The anonymity and global connectivity of the Internet lets cyber criminals engage online in traditional crimes such as extortion, drug-running, or pornography on a greatly expanded scale. Crimes can be committed across national borders or from different continents. Criminals do not need to be physically present to commit the crime. This reduces the risk of capture and prosecution and makes the job of law enforcement that much harder.”

McAfee Virtual Criminology Report

SPECIFIC PROVISIONS OF THE ECT ACT



Unauthorised Access (section 86(1))¹¹

Section 86(1) has criminalised all forms of hacking. Section 88(1) of the ECT Act also criminalises an attempt to gain unauthorised access.¹² In other words, certain security measures have been overcome, but not all and access has also not been secured.¹³ It is submitted that the penalty clauses in the ECT Act are, however, far too lenient, given the impact of the crimes that can be committed in terms of the said Act.¹⁴

in comparison, section 40A(1)(d) of the National Prosecuting Authority Act, No. 32 of 1998, also provides for instances of unauthorised access and 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 a computer, or is *unauthorised*, at the *time* when the access is gained, to gain access to such computer, program or data.¹⁵

The penalty clause provides for a fine or imprisonment for a period not exceeding 25 years or to both¹⁶, which is considerably higher than the provisions of the ECT Act. It is submitted that these penalty provisions are more accurate and take proper cognisance of the dire implications of cyber crime.

Unauthorised modification of data and various forms of malicious code (Section 86(2))¹⁷

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. Damage is also not an essential element of the offence. The extent of the damage, however, can be an aggravating factor when sentence is considered.¹⁸

Denial of Service Attacks (Section 86(5))¹⁹

The act or conduct is very widely defined and consists of any of the actions criminalised in sections 86(1) to 86(4) of the ECT Act that result in a denial or partial denial of service to legitimate users.

These actions will, by implication, include unauthorised access, unauthorised modification or the utilisation of a program or device to overcome security measures. Examples would be where a cyber criminal interferes with or alters data in a computer system that prevents legitimate users access to the system.

A person that is convicted of contravening this subsection may be sentenced to a fine or imprisonment not exceeding 5 years.²⁰

Unauthorised Interception (Section 86(1))²¹

Cyber criminals often obtain valuable information by intercepting and monitoring communications sent via

the Internet or other information networks. Electronic mail messages can easily be intercepted by third parties, thereby enabling them to obtain bank account numbers, password, access codes and various other forms of data.

Section 2 of the Regulation of Interception of Communications and Provision of Communication-related Information Act²² provides as follows:

“Subject to this Act, no person may intentionally intercept or attempt to intercept, or authorise or procure any other person to intercept or attempt to intercept, at any place in the Republic, any communication in the course of its occurrence or transmission.”²³

There is clearly an overlap between the Interception Act and the ECT Act in respect of unauthorised interception offences.

The ECT Act, however, provides for a penalty of a fine or a term of imprisonment not exceeding 12 months.²⁴ The sentence is much more lenient than that provided for in the Interception Act.

Devices (Section 86(4))²⁵

Cyber criminals often use devices in order to gain unauthorised access to data or to commit cyber crimes.

These devices may consist of hardware devices and attachments, as well as software programs such as spy software.

South Africa has experienced a high volume of incidents where cards are swiped through a skimming device²⁶ or card reader. All the data contained on the magnetic strip is captured and can then be downloaded from the device, with the assistance of a computer terminal. These devices are also often installed in Automated Teller Machines (ATMs).



Section 86(4) also criminalises the actual use of such a software program or device that is designed to overcome security measures or to contravene

any of the rest of the actions criminalised in section 86.²⁷

Extortion (Section 87(1))²⁸

The act consists in the performing or threat of performing any of the acts described in section 86 of the ECT Act, such as unauthorised modification of data.

Computer-related Fraud (Section 87(2))²⁹

This section criminalises computer-related fraud, forgery and uttering, in that the data should be falsified/false data should be produced.

The illegal action will be founded in any of the actions mentioned in section 86 that will cause fake data to be produced.³⁰

THEFT

The evolution of information technology and computers has also heralded the emergence of new forms of theft, such as the theft of electronic information, data, electronic funds and

software programs.

One of the biggest concerns in South Africa, is the phenomenon of identify theft which entails the theft of a person's identify that is subsequently used to impersonate the victim for criminal actions, such as the commission of fraud.

Identity theft has largely remained undetected in government, compared to the rate of detection within the private sector. It is submitted that this can largely be ascribed to the fact that government(s) do not always apply the same stringent security measures to protect online identities and the integrity of their network security.

However, government has a big bank account too and criminals in South Africa have taken the route of least resistance: there has been an increase in reported crimes where user identities and passwords have been compromised and theft and fraud committed within various state departments.

Law enforcement has joined forces with several government departments, as well as private sector partners to

introduce new measures for the prevention detection and prosecution of these types of crime.

This multi-stakeholder cooperation will be discussed in more detail below.



PORNOGRAPHY, CYBER OBSCENITY AND STALKING

Pornography is widely distributed though the Internet and of concern is that the Internet is being used as a key tool and facilitator in the distribution of specifically online child pornography.

The South African Constitution protects the rights of children under the age of 18 years and *inter alia* provides that a child should be protected from degradation.³¹

In South Africa the criminalisation of

child pornography is governed by the Films and Publications Act, No. 65 of 1996.³²

The Internet has explicitly been included in the definition of publications and all forms of child pornography on the Internet will constitute criminal offences.

Upon conviction a perpetrator may be sentenced to a fine or imprisonment for a period not exceeding 5 years or to both such fine and imprisonment where the court finds that aggravating factors are present.³³

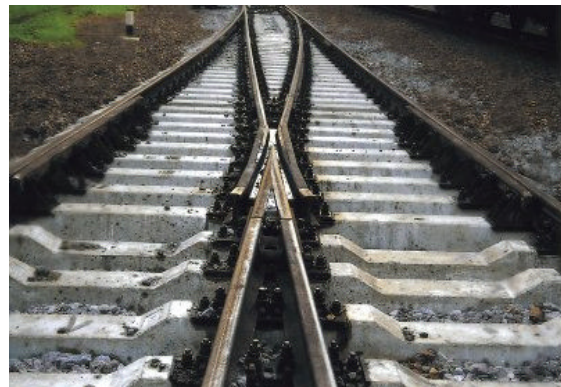
COUNCIL OF EUROPE'S CONVENTION ON CYBERCRIME

Until very recently it was not possible to talk about an international consensus on addressing cyber crime, specifically due to the trans-national nature of this type of crime.

The Council of Europe's Convention on Cybercrime has provided a sound basis for the essential cross-border law enforcement cooperation required to combat cyber crime.

So-called 'communities of shared fate' now have a purpose built mechanism on which they can fashion their own domestic legislation and enhance international cooperation on matters relating to cyber crime.

The Council of Europe's Convention on Cybercrime was opened for signature on 23 November 2001 at Budapest.³⁴ South Africa became a signatory on 23 November 2001, but has not ratified the Convention to date.



“Forensic specialists tasked with investigating computer-related crime also face new challenges. A shift away from ‘script kiddie’ releases of malicious software to bespoke code designed to steal information, especially personal identification data. The greater use of encryption and access protection also poses a growing challenge of extracting evidence from computers and servers. Another continuing problem was the reluctance of victims to report offences and that many victims are unaware that they or the computers had been compromised. The implications of such activity for infrastructure protection are ominous (Semple 2004). The online availability of source code and automated ‘easy to use’ hacking tools that act as system reconnaissance provide multiple exploit tools and deploy ‘spyware’ (i.e. keystroke monitoring or transmission); this had also increased the risks of computer intrusion activities as a predicate to other criminal activity such as extortion, financial or internet fraud, identity theft, telecommunications theft, and economic espionage.

Moreover, ‘patch’ counter-measures have proved inadequate because too many users failed to update (regardless of whether the software was licit or illicit) as ‘MS blaster’ demonstrated, despite the availability of an effective patch some months before the release of this particular malicious code.”

Broadhurst, R Developments in the global law enforcement of cyber-crime



INVESTIGATION AND PROSECUTION OF CYBER CRIME IN SOUTH AFRICA

The task of identifying, successfully investigating and prosecuting cyber criminals poses ever-increasing challenges to law enforcement agencies across the world.

Due to the speed with which these crimes are committed and the difficulties posed by investigations of such a multi-jurisdictional nature, swift and speedy cooperation is required from law enforcement agencies across the globe: Something that would defy the traditional bureaucracy associated with international cooperation.

Cyber crime has resulted in the emergence of an alternative approach to traditional law enforcement (where traditionally means that the law should be enforced by the State alone). Co-operation and collaborating between the State and the private sector is necessary to effectively deal with the advent of cyber crime.

It is difficult to fathom what the true extent of cyber crime in South Africa is at this stage. Cyber crimes, if reported at all, are not always differentiated from other commercial crimes, fraud reports or criminal damage statistics. Thus the extent of computer-related crimes – even when reported – remains unclear. Police statistics about reported crime seldom reveals where a computer was used to facilitate the commission of a crime, where digital evidence was used as evidence of a particular crime or where specific types of cyber crime such as phishing, hacking, computer-related fraud and extortion, etc. was committed. The same applies to how many cases have successfully been prosecuted in court.



Due to the particular nature of cyber crimes, these offences are often difficult to investigate, are labour intensive and require specialised skills to successfully complete the

investigation, as well as the analysis of evidence gathered during the course of an investigation.

The trans-national aspect of cyber crime is further compounded by technological developments that pose new and difficult challenges for the identification of perpetrators and the collection of evidence.

Digital footprints are fragile and transient and swift action is required from all role players in a particular investigation. This becomes even more important when dealing with attacks that span across multiple jurisdictions. Traditional methods of law enforcement and investigations are no longer adequate.

The problem is further compounded by the fact that many law enforcement agencies still lack the capability to operate effectively in cyberspace. Even where there have been efforts to train law enforcement officials, cyber crime calls for specialisation and due to resource constraints, this is often not possible.

Sophisticated shareware tools for cybercrime available on hacker or

wares sites give even inexperienced cybercriminals the weapons they need to commit crime on the Internet.

During investigations in South Africa it has also been found that legitimate software is adapted or modified or used for illegal purposes such as identity theft.

There is also an increasing trend of traditional (or professional) criminals forming partnerships with their cyber counterparts due to the ease with which huge financial gains can be made from the Internet with relatively low risks. Traditional criminals bring with them the skills, knowledge and connections needed for a large scale, high-value criminal enterprise that, when combined with computer skills, form a winning *business strategy* to expand the scope and risk of cyber crime.

During the course of their investigations South African law enforcement agencies have, as is the case in most other countries, dealt with two basic avenues for cybercrime (or a combination of these two avenues):

- Exploiting vulnerabilities in

operating systems and other software programs; and/or

- Social engineering where the criminals have tricked a victim into providing access to their computer or network.

Criminals have also found their way into computers and networks by bribing officials within a business/department to load spy software onto a computer or to install a hardware key logger onto a system and then to remove it again and hand it over to the syndicate.

Criminals are more often than not, far better technically equipped and skilled than the law enforcement agencies that have to investigate their criminal conduct.

The speed at which these offences are committed, as well as the borderless nature thereof, also complicate investigations. Due to the fact that, for example, data can be deleted by the press of a button, it is vital that evidence, as well as the integrity of data be preserved, and that evidence be gathered and safeguarded as soon as possible.

The Directorate of Special Operations (DSO) in South Africa have demonstrated the vital importance of a prosecutor and investigator – both who are skilled and knowledgeable in cyber crimes and cyber law – working together from the onset of an investigation.



This ensures that legal requirements are always borne in mind and complied with at every stage of the investigation.

It also contributes to a speedier completion of the investigation and resultant prosecution.

When dealing with cyber crime in South Africa, one finds more often than not that these crimes are committed in an organised fashion by syndicates that conduct their activities with businesslike precision. This seems to be a phenomenon that is

occurring across the globe:

“E-crime now has a business structure that broadly mirrors that of legitimate business, and links in with other forms of organised crime. The structure includes software providers, information providers, hosting and service providers, consultants and people who provide services in the physical world, such as money couriers.”³⁵



Due to the relative scarcity of IT specialists that would be willing to render services to these syndicates, one also finds that a single specialist will operate within more than one syndicate. Due to the specialists' preference for particular software, malware or programming methods, one can often find valuable links within the specialists' digital fingerprint.

One might also want to focus on the arrest of such a specialist as he/she often can provide valuable links to several other criminals within a syndicate, or at least without their IT

specialist the syndicate would have to actively go out and recruit another (which might pose an opportunity for infiltration for law enforcement).

Cyber criminals cannot hide within the anonymity of their cyber world forever and eventually have to step out into the physical world, usually when they have to covert their cyber gains into real money. For example, when money has been siphoned-off into a bank account it would require a physical cash withdrawal, the purchase and/or sale of goods, issuing a cheque, etc.

These actions incur a significant risk of interception by law enforcement or loss due to the criminal having to rely on another criminal who turns out to be untrustworthy. But this has led to many a breakthrough for law enforcement agencies in South Africa that have patiently lain in wait and had been able to catch criminals in the act.

The successful investigation and subsequent prosecution of some cyber crimes will also largely depend on effective and timely international co-operation between countries.

COMBATING COMPUTER-RELATED CRIME

...The Cyber Crime Unit of the South African Police Service, for example, provides both reactive forensic and pro-active evidential intelligence services during the investigation of serious and organised crime. All operations of and analysis by the Unit are court-directed.

Members of the Cyber Crime Unit render supportive investigations where:

- Computers and networks (including the Internet) are the targets of an offence, e.g. damaging a computer or computer network.
- Computers and/or networks are the tools in the commission of an offence, e.g. creating and transmitting formulas for manufacturing home-made explosives; and
- Where computers and/or networks are incidental to an offence, e.g. criminals who store their records on computers and computing devices, which raises challenging evidential and forensic matters.

The primary clients of the Cyber Crime Unit is the South African Police Service, Interpol and authorised foreign Law Enforcement Agencies whilst training have also been provided to the Royal Swazi Police, the Botswana Police as well as delegates from other countries in the region. Support is also rendered to the victims of computer-related crime.

The Cyber Crime Unit specialises in:

- Proactive evidential intelligence operations via the Internet and computer networks.
- Tracing of "on-line" suspects.
- Forensic search and seizure of memory resident data and computer-related information.
- Forensic analysis of seized material.
- Evidential Intelligence operations.
- Tracing and locating Internet based messages and information.
- Operations to identify and locate on-line suspects, criminal activities and contraband.
- Internet and networked based surveillance.

The Unit also provides evidential Intelligence (proactive support) via:

- Network forensics.
- Internet and Intranet based surveillance.
- On-line transactions and communication to identify suspects and criminal activities.
- Email messages, Web Sites, News Groups, Internet Relay Chat and Virtual Private Networks.

SAPS COUNTRY REPORT TO THE 11TH UNITED NATIONS CONGRESS ON CRIME

PRACTICAL APPLICATIONS

The Directorate of Special Operations (DSO) obtained the first conviction in South Africa for the possession and use of spy software and the use thereof to hack into various government computer systems in 2006.³⁶

The Directorate, also known as the Scorpions, were approached by various government departments to investigate fraudulent transactions that were being created on their computer systems, by making use of user id's and passwords of employees. These user identifications and passwords were in turn stolen by means of hardware key loggers and spy software that were installed on certain computers.

South Africa has seen a sharp increase over the last few years in the commission of these types of crime and the potential loss for the government has proven to be significant.

The commission of cyber crime in government spheres also tend to go hand in hand with crimes such as fraud, computer-related fraud, bribery and corruption.

In the same fashion, the DSO also deals with cyber crime committed in the private sector. It has had great success with a project involving cyber crime in the banking industry that is committed from the anonymity of internet cafés. In March 2007, the Gauteng office made a major breakthrough in the case by arresting an IT mastermind, involved in the acquisition and preparation of spyware that was being placed on South African banking systems.

The suspect also played a major role in moving the proceeds of these Internet frauds to bank accounts in New York and other parts of the world.

The NPA also received a certificate of recognition from Motorola Information Protection Services, USA and Sun Microsystems for its contribution to the fight against cyber crime in this project.

Other successful investigations and prosecutions dealt with issues ranging

CYBER CRIME IN SOUTH AFRICA

from contraventions of section 86(1) of the ECT Act where two ex-employees of a South African corporation that ran the back office of an overseas online casino, to where accused were installing hardware key loggers on computer systems to obtain information that was entered into a computer.

The phenomenon of advance fee fraud schemes, or more commonly referred to as 419 scams, have been widely reported on in South Africa.³⁷

South African law enforcement have successfully dealt with such prosecutions and have also embarked on joint initiatives with international partners (USA in particular) to address this type of crime.



CYBER CRIME IN SOUTH AFRICA

“In this context, the creation of a “global culture of security” is vital to preserve our core values of security and privacy and realise the potential of the digital age. But how do we create such a culture? Personal and national security are too important to allow such a culture to arise unplanned and reactively. Rather, we must develop a comprehensive approach to security in which both the public and private sectors play leading roles, share responsibility, and support one another. In particular, government and the private sector, with information technology companies in a leading role, should work together to ensure the development of strong criminal laws and the capability to enforce them, to share information that will enhance security, and to support the security education and training of citizens.”

**SCOTT CHARNEY
VICE PRESIDENT, TRUSTWORTHY COMPUTING
MICROSOFT CORPORATION**

MARCH 31, 2005



PUBLIC-PRIVATE PARTNERSHIPS: THE LAYERED DEFENCE

The effective control of cyber crime requires more than just cooperation between public and private security agencies.

The role of the communications and IT industries in designing products that are resistant to crime and that facilitate detection and investigation is also of critical importance.

To effectively address cyber crime also calls for a less re-active and more pro-active approach to the prevention, detection, investigation and prosecution of these crimes. One of the key success factors to such a pro-active approach lies in the combined forces of public and private partnerships.

Whilst it might be that only law enforcement can arrest criminals, service providers and private sector institutions can do much to investigate and prevent cyber crime.



The private sector is the first line of defence against financial crimes perpetrated by criminals. They operate and maintain the very systems criminal organisations seek to exploit for their illicit purposes. Regardless, if the crime is one of fraud against a financial institution or the use of a financial institution to move illicit funds – virtually every criminal scheme requires the use of a financial institution in the furtherance of criminal activity, i.e. the use of legitimate funds and seemingly legitimate financial transactions to further illicit activity.

In South Africa the Financial Intelligence Centre (FIC) plays an important role in this regard.³⁸

The FIC's mission is to establish and maintain an effective policy and compliance framework and operational

capacity to oversee compliance and to provide high quality, timely financial intelligence for use in the fight against crime, money laundering and terror financing, in order for South Africa to protect the integrity and stability of its financial systems, to develop economically and to be a responsible global citizen.

The FIC Act also sets up a regulatory anti-money laundering regime which is intended to break the cycle used by organised criminal groups to benefit from illegitimate profits. By doing this the Act aims to maintain the integrity of the financial system. Apart from the regulatory regime the FIC Act also creates the Financial Intelligence Centre.



The regulatory regime of the FIC Act imposes 'knowing your client'³⁹, record-keeping and reporting obligations on accountable institutions. It also requires accountable institutions

to develop and implement internal rules to facilitate compliance with these obligations.

There are several success stories in South Africa where effective multi-stakeholder cooperation has yielded positive results in dealing with cyber crime. Government departments have taken hands with law enforcement agencies, law enforcement agencies have formed partnerships with the private sector and the private sector industries have created forums for knowledge sharing and collaboration.

Some of these examples include:

- The Council for Scientific and Industrial Research (CSIR) in South Africa is one of the leading scientific and technology research, development and implementation organisations in Africa. It undertakes directed research, innovation and development in science and technology for socio-economic growth and to improve the quality of life of the country's citizens. Building local and international partnerships remains a key component of its endeavours to provide world-class technology.

The CSIR Defence, Peace, Safety and Security Unit has also made a valuable contribution to the fight against cyber crime by supporting departments and agencies which are primarily tasked with the prevention and combating of crime, by for example researching cyber forensics and delivering practical solutions through strategic partnerships with South African law enforcement agencies and role-players in the financial services industry.

The CSIR has also provided valuable cyber training to law enforcement officials.

- **Business Against Crime South Africa (BAC)** is a section 21 company that seeks to support the South African Government's efforts to fight crime by complementing its resources with entrepreneurial, managerial and technological skills from the South African private sector.
- **The South African Fraud Prevention Service (SAFPS)** is a service which is committed to combating fraud in society and to offering the South African public a

means whereby they can protect themselves against impersonation and identity theft.

- **South African banking Risk Information Centre (SABRIC)** is a section 21 company established to combat crime in the banking industry. Its key stakeholders are the major banks in South Africa. Its principle business is to detect, prevent and reduce organised crime in the banking industry through effective public-private partnerships.

The company also provides crime risk information and consequence management to the banking industry and CIT companies.

To effectively deal with cyber crime also requires a change of mindset.

Security has to be understood in broad rather than narrow terms. It can no longer be the aspect that is considered after the business is up and running: It needs to form part of intelligence, planning and business strategy right from the onset. Public-private partnerships will assist in the sharing of information where businesses could then incorporate criminal threats in their risk assessment process.

It is law enforcement's responsibility to identify vulnerabilities and behaviours that are indicative of (cyber) criminal behaviour.

This information should then in turn be provided to the private sector for everyone's well being. The private sector and Government should use this information to protect themselves against fraudulent schemes.

An effective partnership between investigators, government and the private sector aids in implementing systems that protects against exploitation.

“Shannon and Thomas (2005) also stress ‘human security’ perspectives in dealing with complex threats posed by cyber crime and argue that over-reliance on the State, especially the public police, to address cyber-security issues would expose both markets and society to frequent low level but costly risks. Consequently the role of public-private police partnerships in the marketplace and the emergence of civil society on the Internet combined with public awareness has become essential to contain cyber crime amongst ordinary users.”

Broadhurst, R

A layered defence pushes criminals to seek more desperate schemes that can be more readily identified and countered by law enforcement.

Providing the private sector with red flag indicators of suspicious behaviour assists them in identifying actions that can be referred to law enforcement for investigation. These simple and timely investigative referrals can result in the identification and dismantling of an entire criminal network.

Cyber crime creates an unprecedented need for concerted action from government and industry, but also unprecedented challenges to effective international cooperation. Determining criminal jurisdiction can become a time-consuming exercise and costly exercise – often providing the criminals with added security and means to hide their crimes.

After an analysis of the instructive guidance and principles offered by the international community, Scott Charney⁴⁰ identified the following five elements of a sound, comprehensive public-private sector approach to cyber crime:

- The existence of strong laws and adequate resources for law enforcement.
- Proper training of law enforcement.
- Coordination among domestic and international law enforcement agencies and improved information sharing that is closely related to such coordination.
- Heightened public awareness of the risks of cyberspace and proper user practices.
- Improved technology.⁴¹

If this framework is applied to the South African context the following observations can be made:

- Although South Africa has signed the Convention on Cyber Crime, it has not ratified it. South Africa does have laws dealing with cybercrime but not in one framework. Especially the penalties in the ECT Act fail to recognise the seriousness of cyber offences.
- Training of law enforcement officials in cyber crime is very costly and heavy reliance has to be placed on assistance from the private sector and international

donors. However, one of the best forms of training is still *on-the-job*-training and a cross-pollination of skills.

- Domestically several industries have created forums for information sharing and creating awareness, e.g. SABRIC and BAC. Private and public sector partnerships are also on the increase and where in place, have led to great successes in the prevention and combating of cyber fraud especially.
- Public awareness raised for e.g. by banks on their websites provides valuable information to online customers. In comparison with some of their international counterparts, there is still much that South Africa can do to effectively raise public awareness regarding cyber crime (in all its forms).
- Improved technology should not only be the responsibility of the companies developing it, but government should also play an active role by, for example funding cyber security-related research and development, etc.

“In sum, the synergy between organised crime and the Internet is not only very natural but also one that is likely to flourish and develop even further in the future. The Internet provides both channels and targets for criminals and enables them to be exploited for considerable gain with a very low level of risk. For organised crime it is difficult to ask for more. It is critical, therefore, to identify some of the ways in which organised crime is already overlapping with cybercrime.”

Phil Williams, Organised Crime and Cyber crime: Implications for Business



CONCLUSION

Cyber crime is an international phenomenon that necessitates co-operation between multiple countries.

It is borderless, fast and even deadly in some instances and furthermore dictates that new and more effective prevention, investigation and prosecution strategies should be developed and employed on an almost daily basis.

The benefits and necessity for public-private partnerships to succeed in addressing cyber crime cannot be stressed enough. Cyber crime, however, remains under-reported and this must also be seen in light of the balance between reporting of crime and reputational damage to companies.

In the case of for example a bank, their online transactions must be perceived to be secure and there is a natural desire to avoid any disclosures that might undermine customer confidence and place a company at a competitive disadvantage.



Unfortunately this works in favour of the criminals. Disclosure of information relating specifically to cyber crime must be understood within the following three categories:

- Sharing of information between companies within a particular industry or market, e.g. banks, investment companies, etc.
- Sharing of information between businesses and law enforcement agencies.
- Full public disclosure.

However, the more developed the methods of information sharing between industry members, and between business and law enforcement agencies are, the less the need for a situation where full public disclosure will be called for.

Sharing of information can also lead to

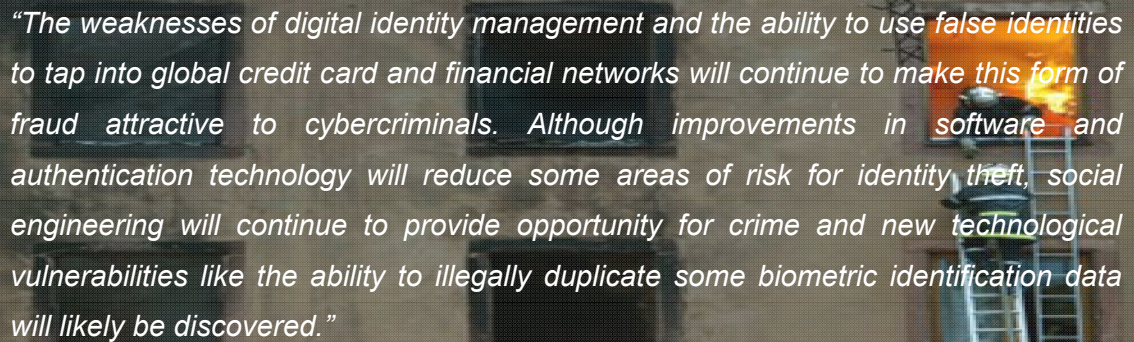
CYBER CRIME IN SOUTH AFRICA

the creation of similar and shared methods and tools for the detection and prevention of cyber crime and contribute to the effective (and pro-active) prevention of cyber crime within a particular industry.

The fight against cyber crime will remain an active battle between law enforcement agencies and cyber criminals.

The competitive advantage could remain on the right side of the law by means of fostering and nurturing effective public-private partnerships, as well as international cooperation and actively embarking on public awareness campaigns.

Prevention remains better than cure.



“The weaknesses of digital identity management and the ability to use false identities to tap into global credit card and financial networks will continue to make this form of fraud attractive to cybercriminals. Although improvements in software and authentication technology will reduce some areas of risk for identity theft, social engineering will continue to provide opportunity for crime and new technological vulnerabilities like the ability to illegally duplicate some biometric identification data will likely be discovered.”

McAfee Virtual Criminology Report

BIBLIOGRAPHY

Broadhurst, R Developments in the global law enforcement of cyber-crime accessed on 15 January 2009 on [citeseerx.ist.psu.edu \(10\[1\].1.1.88.7864.pdf\)](http://citeseerx.ist.psu.edu (10[1].1.1.88.7864.pdf))

Charney, S Combating Cybercrime: A Public-Private Strategy in the Digital Environment accessed on 21 January 2009 at web.reed.edu/nwacc/programs/confos/UNcrimeCongressPaper.doc

Council of Europe Convention on Cybercrime accessed on www.coe.org

Forman, M.M Combating terrorist financing and other financial crimes through private sector partnerships accessed on 17 January 2009 at www.emeraldinsight.com/insight/viewContentServlet?Filename=Published/EmeraldFullTextArticle/Articles/3100090109.html

McAfee Virtual Criminology Report: North American Study into Organized Crime and the Internet accessed on 17 January 2009 at www.mccafee.com/us/local_content/misc/mccafee_na_virtual_criminology_report.pdf

Titterington, G Taking the battle to the e-criminals 10 December 2008, www.ovum.com

Williams, P Organized Crime and Cyber-Crime: Implications for Business accessed on 15 January 2009 at www.cert.org/archive/pdf/cybercrime-business.pdf

BIBLIOGRAPHY

Broadhurst, R Developments in the global law enforcement of cyber-crime accessed on 15 January 2009 on [citeseerx.ist.psu.edu \(10\[1\].1.1.88.7864.pdf\)](http://citeseerx.ist.psu.edu (10[1].1.1.88.7864.pdf))

Charney, S Combating Cybercrime: A Public-Private Strategy in the Digital Environment accessed on 21 January 2009 at web.reed.edu/nwacc/programs/confos/UNcrimeCongressPaper.doc

Council of Europe Convention on Cybercrime accessed on www.coe.org

Forman, M.M Combating terrorist financing and other financial crimes through private sector partnerships accessed on 17 January 2009 at www.emeraldinsight.com/insight/viewContentServlet?Filename=Published/EmeraldFullTextArticle/Articles/3100090109.html

McAfee Virtual Criminology Report: North American Study into Organized Crime and the Internet accessed on 17 January 2009 at www.mccafee.com/us/local_content/misc/mccafee_na_virtual_criminology_report.pdf

Titterington, G Taking the battle to the e-criminals 10 December 2008, www.ovum.com

Williams, P Organized Crime and Cyber-Crime: Implications for Business accessed on 15 January 2009 at www.cert.org/archive/pdf/cybercrime-business.pdf

ENDNOTES

1. Although the author is employed by PwC, the practical research is largely based on experience during her employment in the Directorate of Special Operations.
2. *Computer system* means “any device or group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data Article 1A of the Convention on Cybercrime.
3. *Computer data* means “any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function Article 1B of the Convention on Cybercrime.
4. A description of *computer system* is found in the Financial Intelligence Centre Act, No. 38 of 2001: “...computer system means an electronic, magnetic, optical, electrochemical or other data processing device, including the physical components thereof, and any removable storage medium that is for the time being therein or connected thereto, or a group of such interconnected or related devices, one or more of which is capable of (i) containing data; or (ii) performing a logical, arithmetic or any other function in relation to data.”
5. The ECT Act does not deal with the concepts of *computer* or *computer system*, but rather with the concept *data*. *Data* is defined as “electronic representations of information in any form” and widens the scope of the application of the Act, because it is not limited to only computers. This is advantageous since it would include information systems, large computer networks, the Internet and cyberspace. Information technology necessitates the use of the term *data* rather than the term *computer*. One of the main purposes of the Act as stipulated in the Preamble is to prevent abuse of information systems. The term *information system* is defined in the ECT Act as “a system for generating, sending, receiving, sorting, displaying or otherwise processing data messages and includes the Internet.”
6. The programming and functions of these computerised devices are in the form of data. A cellular phone contains data in that it stores information in electronic format.
7. Traditional credit and debit cards are issued with magnetic strips that contain data. Bank account numbers and expiry dates are encoded on the magnetic strips through means of computer technology. These magnetic strips may also be the subject matter of various types of cyber crime. South African banks, however, are moving towards the use of microprocessor chips embedded in credit and debit cards.
8. Credo and Michels **Computer crime in South Africa** (1985) 2.
9. Prof. Dana van der Merwe in the second edition of his book *Computers and the Law* (2000) at p 188 defined computer crime as follows: “Computer crime covers all sets of circumstances where electronic data processing forms the means for the commission and/or the object of an offence and represents the basis for the suspicion that an offence has been committed.”

10. Watney uses the term *cyber crime* and defined it as all illegal activities pertaining to a computer system, irrespective of whether the computer is the object of the crime or the instrument with which the crime is committed. (Watney, MM **Die Strafregtelike en prosedurele middele ter bekamping van kubermisdaad** (Deel 1)(2003) 1 TSAR 56).
11. Subject to the Interception and Monitoring Prohibition Act, 1992 (Act 127 of 1992), a person who intentionally accesses or intercepts any data without permission or authority to do so, is guilty of an offence.
12. 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).
13. Section 88(2) of the Act provides for the criminalisation of aiding and abetting another to gain unauthorised access. It often happens that an employee of a company, who is authorised to gain access to certain data, copies the data contrary to the scope and limits of his/her authority, and sells it to a competitor. The competitor is not authorised to gain access to the specific data.
14. Section 89(1) provides for a sentence of a fine or imprisonment not exceeding twelve months.
15. Section 71(1) of the South African Police Service Act, No. 68 of 1995 and section 128(1)(e) of the Correctional Services Act, No. 111 of 1998, also have similar provisions.
16. Section 40A(2).
17. 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 render ineffective, is guilty of an offence.
18. An attempt to intentionally interfere with data without authority is criminalised in section 88(1) of the ECT Act. Section 89(1) of the ECT 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 South African district courts.
19. A person who commits any act described in this section with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users is guilty of an offence.
20. Section 89(2) of Act 25 of 2002. Section 88(2) also criminalises the aiding and abetting of another to commit the offence.
21. Section 86(1) provides that, subject to the Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1992), a person who intentionally accesses or intercept any data without authority or permission to do so, is guilty of an offence.
22. Act 70 of 2002, which repeals Act 127 of 1992.
23. Section 49(1) of the Act provides that such an intentional and unlawful interception is a criminal offence. The criminal conduct or *actus reus* will consist of the interception of a communication in the course of its occurrence or transmission.

24. Section 89(1).
25. Section 86(4) of the ECT Act provides as follows: “A person who utilises any device or computer program mentioned in subsection (3) in order to unlawfully overcome security measures designed to protect such data or access thereto, is guilty of an offence.”
26. An electronic card reader or *skimming device* is a physical device that can be used to *read* electronic data from the magnetic strip of a credit card.
27. Section 88(1) provides that a person that attempts to commit the offences referred to in sections 86(3) and 86(4) is guilty of an offence. The aiding and abetting of a person to commit such may be sentenced to a fine or a term of imprisonment not exceeding 5 years.
28. Section 87(1) of the ECT Act provides that: “A person who performs or threatens to perform any of the acts described in section 86, for the purpose of obtaining any unlawful proprietary advantage by undertaking to cease or desist from such action, or by undertaking to restore any damage caused as a result of those actions, is guilty of an offence.”
29. Section 87(2) of the ECT Act stated as follows: “A person who performs any of the acts described in section 86 for the purpose of obtaining any unlawful advantage by causing fake data to be produced with the intent that it be considered or acted upon as if it were authentic, is guilty of an offence.”
30. Section 88(1) of the ECT Act criminalised an attempt to commit the offence. Similarly section 88(2) criminalises the aiding and abetting to commit the offence as criminal conduct.
31. Section 28 of the Constitution of the Republic of South Africa, Act 108 of 1996.
32. Section 27(1)(a) of the Films and Publications Act provides that a person shall be guilty of an offence if he/she knowingly creates, produces, imports or is in possession of a *publication* that contains a visual representation of child pornography. Section 27(1)(b) provides that a person that knowingly creates, distributes, produces, imports or is in possession of a *film* that contains a scene of child pornography shall be guilty of an offence.
33. Section 30(1) of Act 65 of 1996.
34. The preamble to the Convention reads as follows: “Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation...” The Convention aims to harmonise laws in respect of cyber offences, procedure, investigation and prosecution thereof.
35. Titterington, G Taking the battle to the e-criminals.
36. The *State v Siphon Msomi*, case number 41/1320/2006.
37. In these cases the perpetrator sends an electronic message to another person in which certain misrepresentations are made, and in which the victim is requested to keep certain

CYBER CRIME IN SOUTH AFRICA

money in trust for the perpetrator. This usually includes a request for an advance or administration fee in order to facilitate the transaction.

38. The Financial Intelligence Centre (**FIC**) was established under the FIC Act No. 38 of 2001 in February 2002. The FIC started receiving reports on suspicious and unusual transactions on 3 February 2003. The FIC Act is the result of 5 years of investigation and development. It complements and works with the Prevention of Organised Crime Act, No. 121 of 1998 which contains the substantive money laundering offences.
39. Knowing your client (KYC) is also becoming more imperative by the day: Business and government departments alike can learn much from the banking sector where rigorous process of client acceptance has been at the order of the day. This practice is to guard not only against criminal syndicates infiltrating your business/government department but also to identify and prevent opportunities for money-laundering.
40. Charney, S Combating Cybercrime: A Public-Private Strategy in the Digital Environment.
41. Grabosky and Broadhurst (2005)(as referred to in Broadhurst, R **Developments in the global law enforcement of cyber crime**), also provide a very useful framework for effective regional cooperation to facilitate the combating of cyber crime. It includes the following basic elements:
 - Improve security awareness by providing adequate resources to secure transactions and equip system operators and administrators.
 - Improve coordination and collaboration by enabling systematic exchanges between the private sector and law enforcement including joint operations.
 - Take steps to ensure that technology does not outpace the ability of law enforcement to investigate and enact substantive and procedural laws adequate to cope with current and anticipated manifestations of cyber crime.
 - Broadly criminalise the conduct (including juvenile offenders) and focus on all violators big and small.
 - Strengthen international initiatives by updating existing treaties and agreements to recognise the existence, threats and transnational nature of high tech computer-related crimes and strive for legal harmonisation.
 - The development of forensic computing skills by law enforcement and investigative personnel and mechanisms for operational cooperation between law enforcement agencies from different countries, i.e. 24/7 points of contact for investigators.

