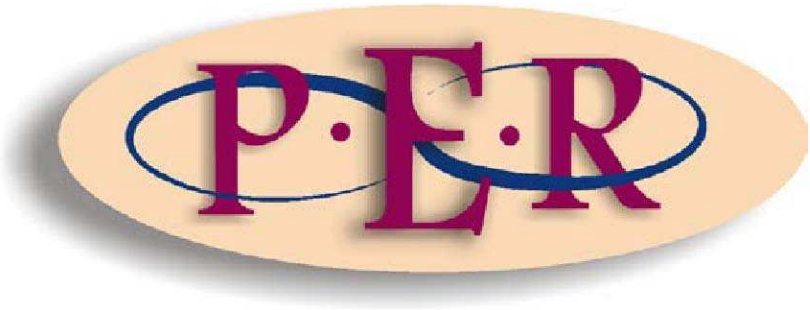
FORMULATING SPECIALISED LEGISLATION TO ADDRESS THE GROWING SPECTRE OF CYBERCRIME: A COMPARATIVE STUDY

ISSN 1727-3781



2009 VOLUME 12 No 4

FORMULATING SPECIALISED LEGISLATION TO ADDRESS THE GROWING SPECTRE OF CYBERCRIME: A COMPARATIVE STUDY

F Cassim*

Summary

The article looks at cyber legislation formulated to address cybercrime in the United States of America, the United Kingdom, Australia, India, the Gulf States and South Africa. The study reveals that the inability of national laws to address the challenges posed by cybercrime has led to the introduction of specialised cyber legislation. It is advocated that countries should amend their procedural laws to include intangible evidence of cybercrime, as opposed to tangible evidence of traditional crimes. It is possible that new forms of cybercrime will often emerge with evolving technology; therefore new cyber laws should be introduced to respond to these rapid changes. There should also be continuous research and training of IT security personnel, financial services sector personnel, police officers, prosecutors and the judiciary to keep them abreast of the evolving technology. International co-operation between countries is also required to address the global nature of cybercrime. To this end countries such as South Africa should ratify the Council of Europe's Convention on Cybercrime (COECC) to serve as a deterrent against international cybercrime. A balanced approach that considers the protection of fundamental human rights and the need for the effective prosecution of cybercrime has been mooted as the way forward.

Keywords

Cyber legislation; cybercrime; inability of national laws; specialised cyber legislation; comparative law; procedural laws; intangible evidence; traditional

* Prof Fawzia Cassim, Associate Professor, Department of Criminal and Procedural Law, University of South Africa, admitted attorney and conveyancer.

crimes; tangible evidence; evolving technology; international co-operation; global nature of cybercrime; COECC; international cybercrime; balanced approach; fundamental human rights; effective prosecution.

1 Introduction

There appears to be no precise definition for cybercrime or 'computer crime'. Computer crime has been described as "any violation of criminal law that involves knowledge of computer technology by the perpetrator, investigator or prosecution".[1] Cybercrime (online misdemeanour) has been defined as including any crime carried out primarily by means of a computer on the Internet; for example, hacking into or damaging a computer network, accessing and stealing electronic data without authorisation, and cyberstalking (via e-mail threats of violence or extortion).[2] Thus, on the one hand, a computer may be the 'object' of the crime when there is theft of computer hardware or software, or a computer may be the 'subject' of a crime when it is used as an 'instrument' to commit traditional crimes such as fraud, theft, extortion, or 'new' types of criminal activity such as denial of service attacks and malware, identity theft, child pornography, copyright infringement, mail or wire-fraud.[3]

Recently the face of cybercrime has changed as a result of the emergence of new Internet environments, organised cybercrime groups and new 'smart'

1 See Bazelon *et al* 2006 *ACLR* 260. It should be noted that the terms 'computer crime', 'cybercrime', 'information technology crime', 'high tech crime' and 'IT crime' are used interchangeably. Also see Van der Merwe 2007 *JCRDL* 309-310 regarding attempts by academic writers to define 'computer crime'.

2 Berg 2007 *Michigan Bar Journal* 18.

3 The focus has thus shifted to the different categories of offences, such as fraud by computer manipulation, computer forgery and child pornography. Cybercrime also involves the use of a computer or computer technology to commit illegal access, illegal interception, data interference, system interference, misuse of devices, forgery and fraud. See further Cybercrime Law 2007 www.cybercrimelaw.net/; Brenner and Clarke 2005 *John Marshall JCIL* 665-666; Miquelan-Weissmann 2005 *John Marshall JCIL* 331, and Brenner and Koops 2004 *JHTL* 7. Regarding pirated software programmes, see DPA 2009 www.thepeninsulaqatar.com/ 14, which addresses the proliferation of pirated goods in the Philippines.

viruses.[4] Thus, the development of new accessible technologies and the expansion of the Internet have led to a number of new criminal behaviours.[5] This has led to a call for specialised legislation to combat these new criminal behaviours. The profile of the cybercriminal has also changed from the 'nerdy loner' to one who is now a syndicate member.[6] However, cybercrime knows no borders.[7] It is irrelevant for the perpetrator and the victim of a crime to meet, as the unlawful actions committed by a perpetrator in one country may have a direct and immediate effect in another country.

Computer crimes also impact *inter alia* on the protection of privacy, the prosecution of economic crimes, the protection of intellectual property and procedural provisions that assist in the prosecution of computer crimes. Many governments are adopting computer-specific criminal codes that address unauthorised access and manipulation of data. However, countries that regulate political discourse find it difficult to regulate freedom of expression, as what constitutes acceptable speech in one country is unacceptable in another country.[8]

---

4 Berg (n 2) 18.

5 The development of the Internet and the advancement of computer technology have also resulted in the creation of new opportunities for those who engage in illegal activity. See Brenner 2001 *Murdoch Univ EJL* 1. Brenner argues that law enforcement officials (police officials) should be equipped with the necessary legal tools to pursue cybercriminals. To this end, every legal system should take adequate measures to ensure that its criminal and procedural laws can meet the challenges posed by cybercrimes.

6 Berg (n 2) 20.

7 The perpetrator who is physically located in one country can wreak havoc in other countries as the 'love bug' episode illustrates. The 'love bug' virus emanating from the Philippines, launched during May 2000, affected twenty countries and caused $10 billion in damage. As there were no relevant computer offence laws in the Philippines, the creator of the virus escaped punishment due to the lack of appropriate laws with which to charge him (the perpetrator). This virus illustrates the problems that this type of activity poses for law enforcement (the police) in cross-border prosecution, such as the lack of cybercrime-specific criminal laws, the inadequacy of criminal laws, the lack of international agreements, the difficulties with jurisdiction and the difficulty in determining the number and effect of cyber offences. Brenner (n 5) 3. Also see Wilson 2006 *Aust LJ* 700 and Goodman and Brenner 2002 *IJLIT* 140-141, for further discussion about the 'love bug' virus.

8 Eg, the dissemination of Nazi propaganda denying that the Holocaust existed is illegal in Germany, and it is also a crime to display, exchange or sell Nazi paraphernalia in France. However, such material is easily accessible on the World Wide Web. It should be noted that the US is regarded as a haven for those who create and maintain web sites that disseminate hate speech, racist views, and Nazi and Neo-Nazi philosophies, because of its strong First Amendment protection for free speech, whilst these viewpoints or acts are outlawed in other countries. Germany has also revised its computer crime laws to provide

The article looks at cyber legislation formulated to address cybercrime in the United States of America (USA), the United Kingdom (UK), Australia, India and the Gulf States. The South African position is also examined. The study reveals that the inability of national laws to address the challenges posed by cybercrimes has led to the introduction of specialised cyber legislation. It is advocated that countries should amend their procedural laws to include intangible evidence of cybercrimes, as opposed to tangible evidence of traditional crimes. A balanced approach that considers the protection of fundamental human rights and the need for effective prosecution of cybercrimes has been mooted. International co-operation between countries is also required to address the global nature of cybercrime.

2 Challenges deriving from cybercrime

Cybercrime differs from traditional crimes because it can be committed with relative ease, it requires few resources and it can be committed in a jurisdiction without the offenders being physically present.[9] The fact that cybercrime does not require physical proximity between a victim and perpetrator also compounds the problem of detection.[10] The challenges deriving from cybercrime arise in four main areas namely, logistics, combating anonymity, accessing electronic information and transnational enforcement.[11] Criminal laws regulating cyberspace tend to result in few prosecutions due to the jurisdictional difficulties and additional resources required in tracking down

that internet service providers such as *Compuserve* cannot be held liable for contents that they merely transmit. *Id* 149, 222. Also see Bazelon *et al* (n 1) 307-308.

9 Regarding examples of cybercrime, see Goodman and Brenner (n 7) 142, 146-150.

10 Other difficulties have been recognised: although cybercrime is committed by a small percentage of the population, the number of cybercrimes exceeds that of traditional crimes; there are also difficulties with gathering evidence and apprehending perpetrators; cybercrime patterns are not well documented; it is also difficult to categorise crimes; inaccurate cybercrime statistics exist because many cybercrimes go undetected and many are unreported. See Brenner and Clarke (n 3) 666-667.

11 Allan 2005 *NZLR* 150. Allan examines the problems posed by cybercrime, and notes that orthodox responses such as criminalisation, the enhancement of enforcement powers and the use of countering technology are ineffective in a virtual context. Allan advocates the use of alternative strategies such as those that encourage Internet users to share the burden of securing informational privacy.

cyber criminals in different countries (across different jurisdictional borders).[12] Criminal anonymity involves using sophisticated re-routing techniques and hacking incidents which remain anonymous. Privacy interests also compound the issue.[13]

An important challenge to state officials in prosecuting cybercrime is one of jurisdiction. Traditionally, crime and punishment were seen to be locally based, regional or national. However, this has changed today with the transnational character of cybercrime posing many problems.[14] The globally connected Internet has made cybercrime a trans-border problem with the result that "no island is an island".[15] The 'love bug' virus illustrates that the existence of cybercrime laws is a fundamental prerequisite for investigation as well as prosecution. The Philippine's failure to have cybercrime legislation in place meant that a Philippine national inflicted damage in twenty countries but suffered no consequences for his acts, This failure to have legislation impacted around the globe and illustrated the fragility of our modern networked world.[16] Therefore, the international character of cybercrime calls for international co-ordination and co-operation to address computer-related offences worldwide.

12 However, Brenner and Clarke advocate that criminal sanctions are preferable to civil liability in addressing cybercrime. They suggest that a system of administrative regulation backed by criminal sanctions will provide incentives to create a workable deterrent to cybercrime. They argue that prohibiting Internet access except through licensed Internet service providers, imposing certification and reporting requirements on larger organisations, requiring transparency regarding the security-related characteristics of information technology products and mandating cyber risk insurance are necessary if society is to control cybercrime. See Brenner and Clarke (n 3) 659-709.

13 See, eg, the Fourth Amendment in the US Constitution, which protects rights and freedoms against unreasonable search and seizure.

14 The 'love bug' virus is an example of this. See *inter alia* Goodman and Brenner (n 7) 140.

15 See Xingan 2007 *Webology* 2.

16 Onel de Guzman (a former computer science student) was identified as the person responsible for creating and disseminating the 'love bug' virus. However, Philippine law did not criminalise hacking or the distribution of viruses. The Philippine officials struggled with the question of how to prosecute De Guzman. They finally charged him with theft and credit card fraud but the charges were dismissed. De Guzman could not be extradited for prosecution in other countries such as the US (which has cybercrime laws) because the conduct attributed to De Guzman was not a crime in the Philippines. Extradition treaties require 'double criminality', namely the act for which a person is extradited must be a crime in both the extraditing country and the country seeking the extradition. De Guzman could not be charged for disseminating the 'love bug' virus. This meant that no one was prosecuted for the 'love bug' virus. See Goodman and Brenner (n 7) 142.

Law enforcement officials cannot prosecute cyber criminals unless countries have adequate laws in place outlawing such criminal activities.

Cybercrime is said to be becoming easier to carry out as society becomes more dependent on the Internet. This increases the risk of a catastrophic attack. However, it has been suggested that certain types of cybercrime can create more benefits than costs.[17] Cybercrime differs from other crimes in that it operates within a highly organised system making it more likely to create beneficial effects that outweigh their costs, and the perpetrators usually possess a particular psychology that make them amenable to more innovative law enforcement methods.[18] The millions of computers which are connected to the Internet are vulnerable to the threat of cybercrime. This vulnerability is compounded by the combination of more creative hackers, the prevalence of powerful computers, and the existence of broadband Internet connections. Untrained and apathetic users have also created an environment which is vulnerable to damaging attacks on the information infrastructure.[19] Traditional law enforcement tools are regarded as ineffective in addressing these crimes. Therefore, it is suggested that a non-traditional response would be appropriate, such as securing the information infrastructure by working with industry and Internet users and by enlisting hackers to achieve greater security.[20] The assistance of hackers and users is regarded as important in securing the Internet because hackers are seen as a valuable resource for security knowledge. Therefore, it is advocated that cybercrime policy should encourage their co-operation and avoid alienating them.[21]

Another challenge facing the IT environment is the diverging interests of those affected by cybercrime: on the one hand, individuals have a right to free speech

17 See Anon 2006 *Harvard LR* 2442.
18 *Id* 2443.
19 The risk of a serious cyber attack by terrorists and the ease with which hacking is carried out further compound matters. Thus the prosecution of cybercrime is important not only to law enforcement officers (the police) but also to global security. *Id* 2445.
20 Anon (n 17) 2463.
21 It is advocated that hackers should be encouraged to work with vendors and co-operate with law enforcement. However, those hackers convicted of conducting the most destructive attacks should receive the harshest of punishments. *Id* 2457-2463.

and privacy and on the other hand there is society's need to combat crime and secure community networks and the interests of big business. Informational privacy is thus important. The assistance of third parties such as Internet service providers and telecommunication entities would assist law enforcement agencies in their fight against cybercrime.[22] Co-operation with the private sector is also encouraged. A balanced approach that considers privacy interests and the need for effective prosecution of cybercrime is the way forward.[23] The need to eradicate cybercrime also depends on reaching a consensus on minimal standards for securing fundamental procedural due process guarantees such as respecting the rights of citizens under search and seizure provisions.[24]

A need thus arises for worldwide criminalisation to address the cybercrime problem. However, some undeveloped countries may have inadequate investigative powers or technological capacities to address the problem. Attempts to adopt, harmonise and streamline international cybercrime laws by conventions such as the Council of Europe's Convention on Cybercrime (hereinafter the COECC) and the United Nations Convention against Transnational Organised Crime are lauded. However, international co-operation by countries is needed to comply with these Conventions to ensure the integrity of the Internet and address the global nature of cybercrime. The COECC, which was signed in Hungary on the 23rd of November 2001, aims at encouraging countries to combat cybercrime.[25] It criminalises certain computer actions such as the interception of non-public transmission of computer data, establishes corporate liability, calls for the production of stored computer data and

22 Allan (n 11) 163.
23 *Id* 178.
24 Also see Kerr 2005/2006 *Harvard LR* 532-585.
25 The Council of Europe has drawn up a convention to respond to the challenges posed by cybercrime. The Convention was adopted on 8 November 2001 by the Foreign Ministers of the Council's member states and non-member states, namely the United States, Canada, Japan and South Africa. It was opened for signature on 23 November 2001 in Budapest, Hungary. The Convention entered into force on 1 July 2004. The Additional Protocol to the Convention on Cybercrime requiring states to criminalise the dissemination of racist and xenophobic material through computer systems was adopted on 7 November 2002 by the Committee of Ministers. The two main objectives are to harmonise criminal law in the fight against racism and xenophobia on the Internet and to improve international co-operation in this area. It was opened for signature during January 2003. It should be noted that European Cybercrime law is based primarily on the COECC. See further, Cybercrime Law 2007 www.cybercrimelaw.net/

recommends mutual assistance between countries during investigations.[26] The COECC is said to be the first international treaty on crimes via the Internet and other computer networks dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. The main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation. Although the COECC aims at international co-operation in prosecuting cybercrime, it contains no provision for co-operation in securing networks.[27] Thus, the Convention's underlying premise that harmonising national laws will improve law enforcement's ability to react across national borders is laudable but the difficulty lies in its implementation.[28]

3 Comparative perspective

Many countries have legal systems which involve a combination of English law, Roman Dutch law and constitutional law. These laws are promulgated to apply to traditional crimes such as murder, assault, theft and fraud. A problem therefore arises when these 'antiquated' procedural laws are confronted with infringements that arise in the IT environment. The inadequacy of existing criminal laws to address computer offences has led to the introduction of new legislation to keep abreast with modern technology.

3.1 United States of America

The *National Information Infrastructure Protection Act* of 1996 (hereinafter, the NIIPA or 'the 1996 Act') protects individuals against various crimes involving

26 See Jahankhani 2007 *IJESDF* 9 for further discussion.

27 Also see Miquelan-Weissmann (n 3) 329-361. It should be noted that SA has signed but not ratified the COECC. It is the only African country to have done so.

28 Brenner and Clarke (n 3) 671. The cyber crime treaty is also criticised for not providing adequate guarantees for fundamental due processes. See Miquelan-Weissmann (n 3) 356-357.

"protected computers".[29] Both the US Secret Service and the FBI have jurisdiction over offences committed under the NIIPA, the latter through the USA *Patriot Act*.[30] The *Electronic Communications Privacy Act* of 1986 (hereinafter the ECPA) is also aimed at non-traditional crimes such as hacking. It prohibits any obtaining, altering or preventing unauthorised access to electronic storage.[31]

Federal offences include cyber fraud, identity theft, spamming, cyber stalking, cyber fraud, making intentional false representations online, identity theft, the use of password sniffers, the decimation and creation of worms as well as the writing of viruses and Trojan horses, website defacements and web-spoofing.[32] Many states such as Arkansas and California have enacted anti-spam laws to regulate the use of Internet communications that send unsolicited advertisements for the purpose of promoting real property, goods, or services for sale or lease. Statutes have also been enacted in some states such as Arkansas and Georgia to provide civil compensatory damages so as to encourage the victims of computer crimes to come forward.[33]

Jurisdictional problems arise for state prosecutors when causes of action are committed in different states, because the jurisdictional rules of criminal law require the prosecutor to prove that the defendant intended to cause harm within his state. As a result, many states have amended their jurisdictional rules

---

29 See s 1030 of Title 18 of the NIIPA. This includes a computer involved in interstate commerce or communications or any computer attached to the Internet. Offences include the prohibition of access to information without authorisation or computer hacking. See s 1030(a) regarding the types of offences and definition of electronic storage. It should also be noted that s 1030 confers jurisdiction to prosecute when the conduct at issue impacts upon the federal government and where the USA is itself the victim. See Bazelon *et al* (n 1) 265. Also see Brenner and Koops (n 3) 25.

30 See s 1030 (d) of the NIIPA. It should be noted that the *Patriot Act* was introduced on 23 October 2001 to safeguard homeland security after the 9/11 attacks. Both the *Patriot Act* of 2001 and the *Cyber Security Act* of 2002 contain amendments to the NIIPA.

31 See s 2701(a) of the ECPA. In *US v Councilman* 385 F3d 793 (First Circuit 2005), the court found that the ECPA was enacted to increase government's powers to wiretap so as to include the digital transmission of electronic data.

32 The sale of non-prescriptive drugs, firearms, explosives, cigarettes, alcohol and visas on the Internet is strictly monitored. The *No Electronic Theft Act* regulates copyright offences and copyright management offences, while the *Digital Millennium Copyright Act* addresses piracy. For further information, see Snail and Madziwa 2008 *Without Prejudice* 30-31.

33 See Bazelon *et al* (n 1) 304-305.

to address the new concerns that arise from the global nature of the Internet. To illustrate this, Wisconsin's criminal statutes confer jurisdiction even where the cause of action has no consequence in the state; some states such as Arizona, Kansas, New York and Missouri allow jurisdiction where a result of the offence occurs in the state whether or not an element occurs in the state, whilst Alabama, California and South Dakota have statutes conferring jurisdiction where an offence begins outside the state but "consummates within the state".[34] US Code section 1030 also considers the nationality of the victim and it confers jurisdiction to prosecute when the conduct at issue impacts upon the federal government, where the US is itself the victim. The Michigan statute confers criminal jurisdiction whenever the victim of the offence resides in Michigan or is located in Michigan at the time of the commission of the criminal offence. It has also been held that the nationality of the offender could support extraterritorial jurisdiction because the federal government can exert personal jurisdiction over American citizens and American corporations anywhere in the world.[35]

The case of *US v Gorshov*[36] raises controversy about a country's jurisdiction to enforce its law regarding cyberspace cases. The facts were that some Russian nationals were identified as hackers who had been breaking into the computer systems of American businesses. They were trapped by FBI agents into coming to an interview in the United States and were subsequently arrested. Information was retrieved from Russian computers by the FBI agents without a

34 Thus, in the US many states take a broad approach to the question of jurisdiction. For example, in Arkansas the computer crime legislation provides that a person is liable for prosecution if the offence originates in the state or has consequences in the state (Arkansas Code s 5-27-606(2003)). In Northern Carolina it is an offence where the electronic communication was originally sent from or where it was originally received in the state (North Carolina General Statute s 14-453.2 (2002)). Also see Audal *et al* 2008 *ACLR* 269-270.

35 See *US v Judd* 46 F3d 961, 967 (California Circuit 1995). The case decisions in all states also address the issue of personal jurisdiction in terms of due process considerations of the Fourth Amendment, which guards against unreasonable searches and seizures. The cases consider the question of whether a non-resident defendant has "minimum contacts with the jurisdiction and has purposefully availed himself of the privilege of conducting activities within the particular state, thus invoking the benefit and protection of its laws". See *Burger King Corporation v Rudzewicz* 471 US 462, 474-475 (1985). Also see Finlay 1999 *TBJ* 336 and Brenner and Koops (n 3) 38.

36 2001 WL 1024026. The question arose whether the actions of the FBI agents were justified or not as an exercise of enforcement of jurisdiction.

warrant. The District court found that there had been no violation of the Fourth Amendment, which did not encompass extra-territorial searches of non-US citizens, nor was there any violation of Russian law. However, the Russian authorities charged the FBI agents with hacking and requested their presence for trial in Russia, but the American government did not comply.[37]

In *United States v Thomas*[38] the court found that the Western District of Tennessee could prosecute a San Francisco bulletin board operator for transporting obscene material electronically. Courts are perceived by the internet community not to be the best place to develop policy on cyber law or resolve on-line disputes because of their expense, their slowness and their lack of expertise about computer technology. The introduction of the Virtual Magistrate in the United States is a first attempt at creating an on-line arbitration mechanism to resolve disputes.[39] Nevertheless, the establishment of a "real live" cyberspace jurisdiction is said to be remote in time, as local governments and courts will resist it.[40]

Valiant attempts are being made in the USA to respond to the increase in cybercrime, such as the Project Safe Childhood to combat child exploitation on the Internet, and the use of specialised prosecutors to fight cyber crimes in the US Attorney's Offices nationwide.[41] During August 2008 the US Senate passed a Bill on cybercrime to modernise the country's computer crime laws and to provide prosecutors with more leeway in pursuing cyber criminals. Current

37 See Brenner and Koops (n 3) 21-22 for differing views regarding the question of whether the actions of the FBI agents were justified.

38 74 F3d 70 (Sixth Circuit 1996). However, the effect of this case is uncertain for future litigation involving on-line jurisdiction because it is a criminal case (it involves child pornography).

39 The idea was to offer arbitration for quick resolution of disputes involving users of on-line systems and those who claim to be affected by illegal messages, postings, files and system operators. Canada has a similar experimental system called the Cybertribunal which is based at the University of Montreal. The Tribunal is investigating possible court action to curb the dissemination of hate literature from Canadian sites over the Internet. See Blackwell 1997 *Canadian Lawyer* 22-23.

40 *Ibid*.

41 Berg (n 2) 22. An initiative has also been launched by the US Electronic Crimes Task Force and the Federal Bureau of Investigations which brings law enforcement officers together with members of the private sector and academics in a collaborative effort against cybercrime. See Brenner and Clarke (n 3) 682. Regarding further attempts by the Department of Justice and FBI to address cybercrime, see Audal *et al* (n 34) 265-267.

federal cybercrime laws require prosecutors to demonstrate that the illegal activity caused at least $5,000 in damages before they can institute actions for unauthorised access to a computer. However, that threshold will now be eliminated under the new Bill. The new legislation contains the following amendments: it is a felony to install spyware or Keystroke-monitoring programmes on ten or more computers regardless of the amount of damages caused; the new legislation also enables identity theft victims to seek restitution for the loss of time and money spent restoring their credit; the Bill would also allow federal courts to prosecute cyber criminals who 'attack' computers located in the state in which they live;[42] and another new provision covers cyber extortion to address shortcomings in the existing law.[43] These new provisions will be added to a bill known as the *Former Vice President Protection Act*.[44] The new government under President Barack Obama is also presently reviewing cybercrime regulations.[45]

The above discussion demonstrates that the United States is taking the lead in addressing cybercrime. The collaborative initiative involving the police, the private sector and academics is an encouraging attempt to involve all role players in the fight against cybercrime. The advent of the new Bill also illustrates that the US is taking the lead in updating outdated computer laws to keep abreast with advancing computer technology. The ratification of the COECC by the United States has received much needed support in the global fight against cybercrime.[46]

---

42 Current law provides that federal courts have jurisdiction only if a thief uses interstate communication to access the victim's PC.

43 The existing law provides that the government can prosecute cyber extortionists who threaten to delete a victim's data or to damage a computer. There is no specific statute addressing cyber criminals who try to extort companies by publishing or releasing stolen information. However, this activity has now been criminalised. See Krebs 2008 blog.washingtonpost-com/

44 *Ibid*.

45 During February 2009, President Barack Obama instructed the National Security and Homeland Security Advisors to conduct a review of the plan, programmes and activities dedicated to cybersecurity including new regulations to combat cybercrime. See Cybercrime Law 2009 www.cybercrimelaw.net/

46 See Anon 2006 *Computer Fraud and Security* 2-3.

3.2 United Kingdom

There was widespread agreement in the 1980s that the United Kingdom's existing computer law was outdated.[47] The UK's ratification of the COECC also led to calls to amend the *Computer Misuse Act* 1990 (the CMA). The CMA was consequently amended on 1 October 2008[48] to clarify the meaning of "unauthorised access" to a computer.[49] The inclusion of a new provision also makes it an offence to to make, adapt, supply or offer to supply any item of hardware, software or data for use in the commission of an offence under the Act.[50] The maximum penalty for unauthorised access to a computer system has been increased from six months to two years in prison.[51] Denial of service attacks is also criminalised, and the maximum penalty is ten years' imprisonment. It is also an offence to distribute hacking tools for criminal purposes. Although the amendments are lauded, it has been suggested that alternative government mechanisms are required to better address the growing problem of computer misuse.[52] The Home Office has recently announced a proposal to make it harder for child sex-offenders to meet children online.[53]

47 It should be noted that the English courts concluded that their existing laws did not accommodate nor reflect the changes brought about by computer technology. See *inter alia R v Gold* (1988) AC 1063, where the defendant was acquitted because there were no laws to prevent unlawful access to a computer. This led to the enactment of the *Computer Misuse Act* 1990. However, this act was soon found to be ineffective in addressing cybercrime. See McKenna 2004 *Infosecurity Today* 5.

48 See Leyden 2008 www.theregister.co.uk/ Although the *Police and Justice Act* 2006 deals mostly with policing reform, it also contains amendments to the *Computer Misuse Act* 1990. Also see Fafinski 2008 *Journal of Criminal Law* 53-66. The article looks at the rationale behind the amendments and examines the implications for cyber law. It is noted that the particular problem of computer misuse presents difficulties for criminal law. Therefore, it is suggested that this issue be further explored to achieve alternative government mechanisms to address the problem.

49 The new wording prohibits unauthorised acts relating to computers.

50 See further, Fafinski (n 48) 59.

51 This makes the offense serious enough that an extradition request can now be filed.

52 See Fafinski (n 48) 53-66. However, the advent of the initiative called the National Hi-Tech Crime Unit, which brings the police, private sector and academics together to combat cybercrime is lauded. See Brenner and Clarke (n 3) 682.

53 This is designed to stop child sex-offenders using social networking websites. Registered child sex-offenders will now have to provide their e-mail addresses to the police or face five years in prison. The first UK Social Networking Guidance has also been published, which provides advice on how to stay safe online. See Anon *The Peninsula* 9.

In the United Kingdom, the jurisdiction of the English courts was considered *inter alia* in *R v Smith (Wallace) No 4*.[54] The Court of Appeal had to consider the following facts: the physical presence of the defendant within England, the fact that substantial criminal activities took place in England, and whether or not it was necessary for the "last act" to be committed within its jurisdiction. The court found that the question of whether the English courts have jurisdiction or not depends on where the last act took place,[55] and it was established that a substantial part of the offence took place in England and Wales. Thus, it appears that if the offender is within the jurisdiction of the United Kingdom then the English courts have jurisdiction to try the offender. There is little judicial support for the approach in England and Wales that allows prosecution in cases where an element of the offence occurred within the court's jurisdiction. However, the statement that the terminatory approach has universal support is criticised.[56]

The UK experience demonstrates that the UK is trying its best to keep cyber criminals at bay: the increase in the penalty for unauthorised access to a computer (from six months to two years) and the criminalisation of denial of service attacks illustrate a tougher stance on cybercrime. Innovative proposals aimed at child sex offenders have been introduced by the Home Office. The advent of the National Hi-Tech Crime Unit is also lauded. This initiative, which brings the police, the private sector and academics together to combat cybercrime, ensures the participation of all of the key parties in the fight against cybercrime.

3.3 Australia

In the Australian context, cybercrime has been defined as "any unauthorised activity which involves or uses computers, digital technology, the Internet,

54 [2004] EWCA Crim 631. It should be noted that s 4 and s 5 of the CMA also provide that the UK has jurisdiction to try the offender if the offence is 'significantly linked' to the UK.

55 This is the termination theory which is supported by much case law. See further, Ormerod 2004 *Crim LR* 953.

56 *Ibid*.

communication systems or networks".[57] This definition may encompass a number of financially devastating attacks such as computer worms and viruses, Trojan programmes designed to capture personal information, large-scale phishing scams, and other means of identity theft.[58] The inadequacy of the existing criminal laws to address computer misuse and computer offences has led to calls for distinct statutory laws for computer offences in order to keep up with modern technology.

The multi-jurisdictional dimension of the Internet has led to the enactment of special extra-territorial jurisdiction for computer-related offences. The *Model Criminal Code* and *Cybercrime Act* 2001 (Cth) addresses computer-related crimes.[59] The aim of the Cth is to protect the commercial integrity of systems that process and store information rather than the information itself.[60] Jurisdiction in Australia is governed by a combination of judicial development of the common law and legislative reform. Australian criminal law assumes that "all crime is local" and this idea of territoriality has been criticised for failing to consider the extra-territorial effect of offences.[61] The modern legislative trend is to extend the extra-territorial reach of offences. Consequently, the Cth extends jurisdiction extra-territorially and identifies the alleged offender's national status as the basis for conferring jurisdiction. Thus Australian citizens who commit

57 See Bronitt and Gani 2003 *Crim LJ* 304. The authors review the evolution of and the changing rationale for computer-related offences in Australia in their article.

58 Wilson (n 7) 694.

59 It should be noted that s 15(1)(a)(c) of the *Australian Criminal Code* 1995 provides that if the conduct occurred wholly outside Australia but the perpetrator is an Australian citizen, either the individual or corporation is subject to jurisdiction. The *Cybercrime Act* 2001 (Cth) which has been influenced by the COECC, has also improved evidence-gathering by introducing expanded search warrant powers to conduct covert surveillance. According to Janine Wilson, computer viruses and denial of service attacks are new computer offences which have arisen as a result of changing technology and the pervasiveness of the Internet. These offences cannot be effectively prosecuted under traditional criminal laws. Both the Cth and the amendments to the Criminal Code have attempted to fill this void by regulating unauthorised computer access and misuse. *Id* 699. It should be noted that New Zealand has also adopted criminal codes to address both the interception of digital communications and unauthorised access, namely the *Crimes Act* 1961. See Allan (n 11) 159.

60 Bronitt and Gani (n 57) 309.

61 The termination theory, which has been regarded as the basis for criminal jurisdiction under the common law in the Australian Capital Territory, New South Wales, South Australia and Victoria, has been criticised for its incompatibility with cybercrimes and legal entities. *Id* 310.

computer offences in countries that have no real or important links to their home jurisdiction can now be prosecuted in terms of the Cth. To illustrate this, in *Director of Public Prosecution v Sutcliffe*[62] an Australian citizen, Brian Sutcliffe, was accused of stalking a Canadian actress who lived in Toronto. The charges were based on Sutcliffe's having telephoned the victim and written to her repeatedly over several years. The Australian prosecutor charged Sutcliffe with stalking but the magistrate dismissed the charges. The magistrate found that she lacked jurisdiction to adjudicate the matter because the crime of stalking occurred in Canada, where the victim was located. However, the Supreme Court of Victoria reversed the decision. The Court found that Sutcliffe was a resident of Australia and had committed all of the ingredients of the crime "save for the harmful effect" in Australia. Therefore, it was held that his conduct and presence in Australia established a "sufficient connection" to allow the court to exercise jurisdiction over the proceedings.

It has been suggested that laws allowing the police to rapidly secure evidence stored on computers and to obtain real-time access to network traffic may be needed for Australia to join a global treaty aimed at fighting fraud and electronic crime.[63] According to the Federal Attorney General's Department project director, Steven Stroud,

> a review is being carried out to establish what legislative changes would be needed if the Australian government were to join the COECC.[64]

Some academic writers advocate the participation of private actors and stakeholders such as credit card companies and corporations in the fight

62 [2001] VSC 43 (Victoria, Australia).

63 See Dearne *Australian It News Limited* 2009 http://www.australianit.news.com.au/story [accessed on 21 May 2009).

64 The Convention, which provides a standard framework for investigating and prosecuting crimes involving computers across national borders, has already been adopted by more than 45 countries. The Convention provides for data retention by service carriers, and for the expedited collection of evidence stored on computers. However, Australia doesn't have laws to this effect. Therefore it is advocated that the current legislation needs to be amended to reflect these provisions. *Ibid*.

against cybercrime, because these stakeholders have a vested interest.[65] Janine Wilson also calls for effective partnerships with the private sector and international entities in order to effectively manage and combat cybercrime.[66] The involvement of the private sector will help to improve the ability of law enforcement (the police) to effectively perform its role of combating cybercrime, and will also assist the private sector to address cyber-threats. This will also help to minimise financial damage.[67] In Australia, the role of the financial services industry in targeting cybercrime developed as a result of its being targeted by cybercriminals, and in this regard the Australian Bankers Association has undertaken a number of projects addressing the problem of rising levels of cybercrime.[68]

The extension of jurisdiction extra-territorially in the Cth adheres to the modern legislative trend. This is commendable. Although Australia has not joined the COECC, it is taking positive steps to review its current legislation to bring it in line with the COECC. The role of the Australian Banking Association in addressing the rising level of cybercrime is praiseworthy. One needs to foster co-operation and collaboration between the state and the private sector to effectively combat cybercrime.

3.4 India

In India, cybercrime has to be voluntary and willful, an act that adversely affects a person or his property. The *Cybercrimes and Information Technology Act (IT)*, 2000 (the IT Act 2000) was introduced to amend outdated laws and to adequately address cybercrime. Although the primary objective of the Act was

65 These multinational corporations also have powers to prevent and detect crime that transcends national borders. Bronitt and Gani (n 57) 313, 317.

66 Wilson (n 7) 694. The article considers *inter alia*, the nature and scale of cybercrime in the private sector and the financial services industry, and the need for effective public and private partnerships to stem the tide of increasing instances of cybercrime, to obtain recovery of lost funds, and to pursue the perpetrators of cybercrime.

67 *Id* 700-701.

68 The increase in cybercrime has placed an enormous financial burden on the financial services industry, for which its members already absorb much of the costs. Nevertheless, the partnership between the financial service industry and the police is said to be a successful one. It is advocated that a similar partnership should be extended to the private sector to counteract cybercrimes. *Id* 702.

to create an enabling environment for commercial use of IT, it also aims to provide a legal framework for the protection of all electronic records and other activities carried out by electronic means.[69] The Act also prescribes remedies for corporations where their computer systems are tampered with.[70] The IT Act 2000 provides legal recognition of digital signatures and a legal framework for E-governance, offences, penalties, adjudication and investigation of cybercrime. Although the Act was welcomed it had shortcomings: it did not effectively address cyberstalking and cyber harassment; it contained ambiguous definitions; there was a lack of awareness by netizens about their rights; the question of jurisdiction was not addressed in the Act, and there were problems with extra-territorial jurisdiction.[71]

Although cybercrime is on the increase it is not adequately reported to avoid harassment of offenders by the police, and companies also want to avoid bad publicity in the media.[72] However, the increase in ATM frauds and cybercrime led to calls to amend the IT Act 2000 and this resulted in the Cybercrime Bill being passed in Parliament during December 2008. It is called the Information Technology (Amendment) Bill.[73] It prescribes punishment which could extend to life imprisonment for cyber terrorism and imprisonment of five years, and a fine of Rs10 lakh for publishing obscene material or transmitting obscene material in electronic form. A severe punishment is also prescribed for offences relating to the misuse of computers and communication equipment.[74]

---

69 Ch IX refers to penalties for damage to a computer and computer systems. Damages are fixed at Rs 1000 000 (Rupees) for affected persons. It also requires the adjudicating officer not below the rank of Director to adjudicate contraventions of the Act. Ch X refers to a Cyber Regulations Appellate Tribunal, which hears appeals against the decision of the adjudicating officer. Ch XI prescribes various offences such as tampering with computer documents, publishing obscene information and hacking. These offences will be investigated by a police officer not below the rank of a Deputy Superintendent of the Police.

70 See further, DIT 2009 dit.mp.gov.in/

71 See Dadhich and Shukla (2007) "Cybercrimes" 414-425.

72 The role of the police in combating cybercrime has been criticised because of the poor rate of conviction. However, the police in India are now becoming cybercrime aware and hiring trained people, and cyber police stations are functioning in major cities throughout the country. See Singh 2009 www.ind.ii.org/

73 This bill amends the *Cyber Crimes and Information Technology Act* 2000. See further Special Correspondent 2008 www.thehindu.com/

74 The Bill also includes a proposal to introduce a Cyber Appellate Tribunal to hear appeals.

The Indian Government introduced the Amendment Bill to overcome shortcomings in the current law. The imposition of stringent punishment for cyber terrorism demonstrates the government's intention to prevent terrorists from using the Internet to perpetrate crime. The Cyber Appellate Tribunal is a specialised tribunal which hears appeals in cyber cases. Specialised tribunals are important because they prioritise and expedite cyber cases.

3.5 Gulf states

Pirated software causes heavy losses for software companies worldwide.[75] The Gulf Cooperation Council (the GCC) recommended during June 2007 that members adopt a treaty on cybercrimes among the Gulf States.[76]

3.5.1 United Arab Emirates

The United Arab Emirates (the UAE) was the first country to enact a comprehensive cyber law among the Gulf States. The *Cybercrimes Act*, Law No 2 of 2006, contains 29 articles, and it contains prohibitions *inter alia* against hacking, credit-card fraud, human trafficking, and abuse of any Islamic holy shrine or ritual.[77] The Act prescribes punishment ranging from imprisonment to a fine or both. The terms of imprisonment range from one year to seven years and the fines range from Dh 20, 000 to Dh 50,000 (Dhirams) depending on the type of offence committed. The Act has been effective in addressing cybercrime in the country. The GCC countries were urged to follow the example of the UAE by enacting comprehensive cyber legislation.

---

75 To illustrate this, in 2006 alone, member companies of BSA lost around $40 billion (about Dh 146,9 million). Anon 2006b archive.gulfnews.com/

76 It should be noted that the GCC members are Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the UAE. For further discussion, see Howe 2007 archive.gulfnews.com/; Roberts archive.gulfnews.com/

77 The UAE has also enacted an effective copyright law which takes tough action against piracy. Anon 2006a archive.gulfnews.com/ For further discussion of the UAE *Cybercrime Act* see also Van der Merwe *et al ICT Law* 101.

3.5.2 Saudi Arabia

Saudi Arabia passed laws governing cybercrime during October 2006.[78] The Shoura Council, which is responsible for enacting laws in Saudi Arabia, passed the Kingdom's first legislation to address the rise in electronic crime. The Council enacted provisions *inter alia* in illegal access and data interference. The legislation addresses offences such as hacking, defamation, and the spread of terrorism. It is aimed at protecting individuals, companies and organisations from being defamed or harmed via the Internet. The maximum punishment under the new legislation is a prison sentence of ten years and a fine of $1,3 million. It can be imposed on anyone found guilty of hacking into government networks to steal information related to national security or using the Internet to support terrorism.

3.5.3 Qatar

There are no specific laws addressing internet crime in Qatar. However, internet crimes are regulated by the *Penal Code Act* 11 of 2004. Currently, law enforcement authorities are unable to effectively prosecute cyber criminals, such as hackers, who steal personal data from computers and place malicious programmes on PCs undetected so as to gather information such as passwords and credit card numbers. Some hackers have been arrested and prosecuted in the past in terms of the country's telecommunications and criminal laws.[79] However, there have been increasing calls for stringent legal steps to fight cybercrime.[80] Difficulties are encountered with finding sufficient evidence for prosecution, as the perpetrators are often very intelligent and expert at covering their tracks. Victims are also hesitant to come forward and report crimes because of embarrassment. According to the ICTQATAR Regulatory Authority's legal and regulatory manager, Meegan Webb, there are no specific laws addressing cyber criminal activity in Qatar.[81] A need also arises to extend current laws to cover businesses operating outside Qatar, but

78 Also see Bowman 2006 www.itp.net/
79 See Anon 2006b archive.gulfnews.com/
80 Townson 2008 www.gulf-times.com/
81 ICTQATAR had been involved with drafting the telecommunications law, as well as the draft e-commerce law which is expected to be passed in the near future. *Ibid*.

which are conducting business within the country. Qatar is said to account for 4,3% of infected computers in the Middle East, and data-stealing hardware which infiltrates the most secure enterprises is said to be on the increase.[82] Thus, a need exists for the formulation of adequate cybercrime legislation to combat cybercrime in Qatar.[83]

The Gulf states have recognised their vulnerability to cybercrime. They have taken steps to address this problem by introducing specialised legislation to address cybercrime. Qatar is also taking steps to enact adequate cybercrime legislation. It is submitted that the existence of adequate laws outlawing cyber criminal activities facilitates the prosecution of cyber criminals by law enforcement officials (the police). However, countries which introduce computer-specific criminal statutes should also adapt their rules of evidence to computer crimes to facilitate prosecution of cyber criminals.

4 South African law

4.1 Position before the inception of the Electronic Communications and Transactions Act 25 of 2002

Most of the so-called traditional crimes such as murder, rape, theft, malicious injury to property and housebreaking originate from the South African common law, namely Roman-Dutch law. These traditional crimes deal only with tangibles whereas IT crime or cybercrime deals with intangibles. The perception has thus arisen that the common law cannot effectively deal with IT crime.[84]

82 See Anon 2009 www.zawya.com. It should be noted that Trend Micro, an international company specialising in internet content security, is educating regional organisations and individuals about cybercrime.

83 Townson (n 80).

84 To illustrate this, the common-law crime of theft is not adequate for combating IT crime in South Africa. So too the common-law crime of fraud. For further discussion about the inability of the common law to address IT crime, see Anon 2005 *Cyber Law* 121, par 346-349. Also see Burchell 2002 *SALJ* 585, where Professor Burchell states that the common law is not suited to punish conduct such as unauthorised access to computer systems and altering computer data. However, he maintains that conduct committed using a computer

Before the commencement of the *Electronic Communications and Transactions Act* 25 of 2002 (hereinafter, the ECT), the common law and statutory law applied to online forms of offences such as indecency (child pornography), fraud (cyber fraud) and *crimen injuria* (cyber-smearing).[85] However, the common law was ineffective in addressing crimes such as theft, extortion, spamming and phishing.

The case of *S v Mashiyi*[86] considered the question of admissibility of computer-generated documents. The court held that documents which contain information that has been processed and generated by a computer are not admissible as evidence in a criminal trial. On the other hand, the court found that where documents have been scanned to produce an electronic image of the original, then such an image is regarded as an exact image and is therefore admissible. However, in terms of the "prevailing law" the court could not admit into evidence the disputed documents which contained information that has been processed and generated by a computer.[87]

4.2 The ECT and its effect[88]

The aim of the ECT is *inter alia* "to provide for the facilitation and regulation of electronic communications and transactions; to provide for the development of a national e-strategy for the Republic; to promote universal access for

---

as an instrument is generally covered by existing common-law crimes such as theft, fraud, invasion of privacy and murder.

85 Prior to the inception of the ECT, crimes such as the possession and distribution of child pornography could be prosecuted in terms of s 27(1) and s 28 of the *Films and Publications Act* 65 of 1996.

86 2002 (2) SACR 387. It should be noted that this case was decided before the inception of the ECT. The court in *Mashiyi* referred to *Narlis v South African Bank of Athens* 1976 (2) SA 573 (A), which held that a computer print-out cannot be received as evidence in terms of s 34 of the *Civil Proceedings Evidence Act* 25 of 1965. The reason for the rejection of a computer print-out as admissible evidence in the above case was that a computer is not a person and therefore a computer print-out is not a statement made by a person. The court also referred to *S v Harper* 1981 (1) SA 88 (D) which found that computer-generated documents were admissible under the section only if the computer merely stored or recorded the information.

87 *S v Mashiyi* 393 C-D. For further discussion about case law addressing IT crime before the inception of the ECT, see Van der Merwe *et al* (n 77) 70-74.

88 It should be noted that this discussion deals only with certain provisions of the ECT. A detailed discussion of the provisions of the ECT is beyond the scope of this article.

electronic communications, transactions and the use of electronic transactions by SMMEs; to prevent abuse of information systems and to encourage the use of e-government services". Indeed, the focus of the ECT is on protecting 'data' or data messages. The ECT deals comprehensively with cybercrime in Chapter X111. The following offences are punishable offences in the ECT, namely sections 86(4) and 86(3) address new forms of crimes, the law being called anti-cracking (anti-thwarting) and hacking law, which prohibits the selling, designing or producing of anti-security circumventing technology; e-mail bombing and spamming is addressed in terms of sections 86(5) and 45 of the ECT respectively; whereas the crimes of extortion, fraud and forgery are addressed in terms of section 87.[89] Section 3 of the ECT provides that in instances where the ECT has not made any specific provisions for criminal sanctions, then the common law will prevail. However, other statutory remedies prevail in the prosecution of other cybercrime. For example, money laundering and other financially related crimes are addressed in terms of the *Prevention of Organised Crime Second Amendment Act* 38 of 1999 (POCAA) and *Financial Intelligence Centre Act* 2001 (FICA).[90]

The traditional requirement for documentary evidence was that it must be relevant and admissible, its authenticity must be proved and the original document must be produced.[91] This has now changed as a result of the ECT. Section 15 of the ECT provides that the rules of evidence must not be used to

89 Therefore, s 86 prevents unauthorised access to or interception of or interference with data; s 87 refers to computer-related extortion, fraud and forgery whilst s 88 refers to aiding and abetting. Regarding anti-pirating software and the protection of security software, see s 86(4) of the ECT and s 27 of the *Copyright Act* 98 of 1978 respectively. The creation of law that addresses new crimes such as hacking is considered to be one of the greatest contributions by the ECT. It is submitted that any measure that protects the integrity of data is welcome, as this is fundamental to successful electronic commerce. Also see Mndzima and Snail 2009 www.hg.org/; Van der Merwe 2003 *JCRDL* 43-44 and Van der Merwe 2007 (n 1) 313 for further discussion on these provisions.

90 It should be noted that POCAA targets organised crime, money laundering and criminal gang activities both nationally and internationally, whilst FICA outlaws money laundering and other unlawful actions.

91 See *inter alia*, *Seccombe v AG* 1919 TPD 270 at 277; *S v Mpumlo* 1986 (3) SA 485 (E) at 489. However, there are exceptions to the general rule where the original document is destroyed, it cannot be located, or its production is illegal. Secondary evidence is admissible in these circumstances. See *inter alia*, *Ex parte Ntuli* 1970 (2) SA 278 (W). It should be noted that South African e-discovery obligations arise from the ECT read together with the Uniform Rules of Court (which were promulgated during 1965).

deny admissibility of data messages on the ground that they are not in their original form.[92] The ECT thus creates a rebuttable presumption that data messages and or printouts are admissible in evidence.[93] It is submitted that this facilitates the admission of information in electronic format. This is commendable.

The Act has also created 'cyber-inspectors' who are authorised to enter premises or access information regarding cybercrime.[94] Cyber inspectors are empowered in terms of the Act to enter any premises and access information that may impact on an investigation into cybercrime. However, the provision in respect of search and seizure (section 82) may infringe section 14 of the *Constitution of the Republic of South Africa* 1996 (the right to privacy).[95]

---

92 S 15 deals with the admissibility and evidential weight of data messages. Regarding the definition of a data message, see s 1 of the ECT. It should be noted that Hofman disagrees with Collier that the definition of a data message in s 1 is broad enough to include hearsay evidence. Hofman maintains that the definition of data refers to the form in which information is kept and not the content of the message. Hofman adds that a data message should be treated the same way as a document in that it is admissible only if the author of the data message testifies about the contents of the message. For further discussion about whether a data message constitutes hearsay, see Hofman 2006 *SACJ* 264; Collier 2005 *Juta's Business Law* 6-9. Regarding documentary evidence, see s 17 (production of evidence); s 14 (production of original evidence) and s 15(b)(exceptions) of the ECT respectively.

93 Also see Hofman (n 92) 262, where it is stated that the ordinary South African law on the admissibility of evidence will apply to data messages except where the ECT changes it. See *inter alia*, *SB Jafta v Ezemvelo KZN Wildlife* (Case D204/07) where an e-mail which was used to accept an employment contract was regarded as conclusive proof that the said employment had been accepted. Also see *S v Motata* (Case number 63/968/07) where electronic information, that is data in the form of images and sound from a cell phone, was admitted into evidence at the conclusion of a trial within a trial. In this case, Judge Motata allegedly drove into a wall of a private home whilst being under the influence of liquor. The owner of the home made an audio recording of the accident on his cellphone. The judge had challenged the admissibility of five cellphone recordings in his trial for driving under the influence. The recording was copied onto a computer and the issue arose whether this constituted real or documentary evidence. The judge was found guilty of drunken driving by the Johannesburg magistrate's court on 2 September 2009. However, he was acquitted of the other charges of obstructing the ends of justice and an alternative charge for resisting arrest. The judge was sentenced to a R20 000 fine or 12 months' imprisonment for drunken driving in the Johannesburg magistrate's court on 9 September 2009. His defence has indicated that the judge will apply for leave to appeal. The state has indicated that it would oppose the application. See further, Anon 2009 www.legalbrief.co.za/, Anon 2009a www.mg.co.za/ and Anon 2009b www.mg.co.za/ Also see *Motata v Nair* 2009 (1) SACR 263 (T); 2009 (2) SA 575 (T); (7023/2008) [2008] ZAFSHC 53 (11 June 2008) regarding the admissibility of playing the recordings during the course of a trial-within-a-trial.

94 See s 82(1) of the ECT. The actions of the cyber inspectors are regulated by s 80-84.

95 S 14 provides that everyone has a right to privacy, which includes the right not to have their person or home searched, their property searched, their possessions seized, or the

The criminal sanctions in the ECT have been criticised for not being severe enough![96] To illustrate this, section 89(1) provides a maximum period of one year's imprisonment for most crimes prohibited by section 86, whilst the crimes prohibited in sections 86(4) and (5) (matters such as denial of service-attacks) and crimes prohibited in section 87 (extortion, fraud and forgery) prescribe a fine or imprisonment not exceeding five years. However, the *Regulation of Interception of Communications and Provision of Communications-Related Information Act* 70 of 2002 (the RICA) prescribes harsher measures.[97] Thus, the criminal sanctions in the ECT appear to be inadequate when compared with the RICA. It is submitted that more stringent penalties are required to deter cyber criminals.

Jurisdictional issues are regulated by section 90 of the ECT.[98] To illustrate this, section 90 of the ECT provides that a court in the Republic (SA) trying an offence in terms of this act committed elsewhere will have jurisdiction in the following instances:

(a) where the offence was committed in the Republic;

---

privacy of their communications infringed. However, this may be limited in terms of s 36 of the Constitution (limitation clause).

96 Van der Merwe *et al* (n 77) 78.

97 S 51 of the RICA prescribes fines not exceeding R 2 000 000 or imprisonment not exceeding ten years. Regarding juristic persons, fines may increase to a maximum of R 5 000 000. For further evaluation of the criminal provisions of the ECT, see Van der Merwe *et al* (n 77) 75-78.

98 Jurisdiction refers to the competence of a court to hear a matter. Usually the courts will exercise jurisdiction regarding offences committed on South African territory only. See *inter alia*, *S v Maseki* 1981 (4) SA 374 (T). The general rule regarding jurisdiction was that when a crime was committed outside the borders of SA, a South African court will not have jurisdiction to adjudicate on the case. However, there are exceptions, namely high treason, theft committed in a foreign country, and offences committed on board ships or on aircrafts. For further information see Bekker *et al* "The criminal courts" 37-38. Also see *Bid Industrial Holdings (Pty) Ltd v Strang* 2007 SCA 144 (RSA), where the Supreme Court of Appeal had to consider the constitutionality of jurisdictional arrest of a foreigner and whether it was aimed at founding or confirming arrest. The Court found legally competent alternatives to requiring arrest as a jurisdictional prerequisite where attachment is not possible, such as serving the defendant with summons whilst he was in SA, or establishing a connection between the suit and the area of jurisdiction, for example by the cause of action arising within the court's area of jurisdiction.

(b) where part of the offence was committed in the Republic or the result of the offence had an effect in the Republic;
(c) where the offence was committed by a South African citizen or a person with permanent residence in the Republic or a person carrying on business in the Republic;
(d) or the offence was committed on board any ship or aircraft registered in the Republic or on a voyage or flight from the Republic at the time that the offence was committed.[99]

Section 90(b) is helpful because it facilitates the prosecution of perpetrators who create and disseminate viruses overseas, because these viruses may damage our computer networks. Similarly, it facilitates the prosecution of overseas -based hackers who may damage our computer systems. A South African court will thus be vested with jurisdiction because the above-mentioned crimes "had an effect in the Republic". A South African court will also have jurisdiction if a South African national commits a cybercrime abroad based solely on the nationality of the perpetrator.[100] However, the jurisdictional provisions of the ECT are not without criticism.[101]

---

99 It is submitted that s 90 is more comprehensive than a 22 of the COECC. Art 22 provides that a country has jurisdiction when an offence is committed in:
(a) its territory;
(b) on board a ship flying a flag of that party;
(c) on board an aircraft registered in that country;
(d) by one of its nationals if the offence is punishable under criminal law where it was committed or if the offence was committed outside the territorial jurisdiction of any state.
The application of s 90 is, however, limited to crimes that can be committed under the ECT.

100 S 90(c) is regarded as being "too broad". It appears that where no country has jurisdiction in respect of the offence, then the nationality of the perpetrator should play an important role in deciding where he should be prosecuted. This conforms with art 22 of the COECC.

101 S 90(d) is also said to be problematic, because it differs from s 28(1)(d) of the *Magistrate's Courts Act* 32 of 1944, which requires the "whole cause of action" to take place within a particular court or district (territorial borders), whilst s 90(d) provides for jurisdiction in terms of nationality rather than because the offence was committed within its territorial borders. It is also problematic if the cybercrime is committed beyond our borders but the offender is prosecuted in South Africa. Then the question arises as to which regional court or district court has jurisdiction to hear the matter. The ECT has also been criticised for "missing the opportunity to address some of the jurisdictional problems, particularly the regulation of jurisdictional connecting factors in e-contracts". In this regard, see Sibanda "Choice of law" 264. S 90 is also criticised for failing to address sexual crimes. See Van Zyl 2008 *JCRDL* 235 in this regard.

4.3 Recent case law addressing cybercrime

In *Ndlovu v Minister of Correctional Services*,[102] the court had to consider *inter alia* whether a computer print-out which was a copy, complied with the best evidence rule or could not be admitted into evidence unless properly proved. The court found that firstly, the plaintiff's failure to object to the evidence during the trial precluded him from relying on the best evidence rule only during argument. The plaintiff had also referred extensively to the print-out during evidence without objecting, with the result that it amounted to a tacit waiver of the best evidence principle. Secondly, the court found that as the print-out was generated by a computer, it was governed by the ECT. Thus, it examined section 15 of the ECT and found that section 15(1)(a) prohibits the exclusion from evidence of a data message on the mere grounds that it was generated by a computer and not by a natural person, and section 15(1)(b) on the mere grounds that it is not in its original form. However, the court found that the print-out was admissible into evidence not in terms of section 15 of the ECT but in terms of the court's statutory discretion to admit hearsay evidence in terms of the *Law of Evidence Amendment Act* 45 of 1988. This decision has been criticised for not providing clarity on the effect of section 15 of the ECT on the authenticity rule and the hearsay rule.[103]

In *S v Ndiki*[104] the state sought to introduce certain documentary evidence consisting of computer-generated print-outs, designated as exhibits D1-D9, during the course of a criminal trial. The accused objected to the admission of these exhibits as a result of which the court conducted a trial-within-a trial to determine the true nature of the print-outs, the class of document into which

102 2006 (4) All SA 165 (W). The plaintiff sued the defendants for damages as a result of an alleged wrongful imprisonment and wrongful deprivation of privileges as an awaiting-trial detainee. The documents before the court comprised print-outs reflecting the monitoring of the plaintiff from the date of his release on parole.

103 For a critical analysis about the case, see Collier 2005 *Juta's Business Law* 6-9.

104 2008 (2) SACR 252. The accused was charged with a number of counts of fraud and theft in connection with the delivery of medical supplies to the Department of Health and Welfare in the Eastern Cape. The problem arose when the state relied on the evidence of computer printouts which constituted necessary evidence to prove the fraudulent actions. The accused objected to the admissibility of such print-outs as the ECT had not come into operation at the time of the commission of the offence. The court found that since the documents in question were admissible in terms of the existing law, it was unnecessary to make a finding on the retrospective application of the ECT.

they fell and whether their admission was sanctioned by the provisions of any legislation dealing with the admission of documentary evidence. The court held that if a computer print-out contained a statement of which an individual had personal knowledge and which was stored in the computer's memory, then its use in evidence would depend on the credibility of an identifiable individual and would therefore constitute hearsay. On the other hand, where the probative value of a statement in a print-out depended on the 'credibility' of the computer, then section 3 of the *Law of Evidence Amendment Act* 45 of 1988 would not apply.[105] The court found that because certain individuals had signed exhibits D1 to D4, the computer had been used as a tool to create the relevant documentation. Therefore, these documents constituted hearsay. Exhibits D5 to D9 had been created without human intervention and such evidence constituted real evidence. Therefore, the admissibility of this evidence depended on the reliability and accuracy of the computer and its operating systems and processes. The duty to prove such accuracy and reliability lay with the state.[106] However, exhibits D1-D9 were found to have complied with section 221 of the *Criminal Procedure Act* 51 of 1977, and they were therefore provisionally admitted into evidence.[107] The court's progressive approach in regarding part of the computer-based evidence as real evidence has been lauded.[108]

The above discussion demonstrates that our courts are adopting a cautious approach in cybercrime cases. Although the *Ndiki* decision is encouraging, it is

105 It should be noted that s 3 gives the court a discretion to admit hearsay evidence if it is in the interests of justice.

106 S 34 requires documents to be made by a person (in terms of *Civil Proceedings Evidence Act* 25 of 1965). It was clear from the evidence that the computer was used as a tool with respect to exhibits D1 to D4. Although printed on a computer, the exhibits were signed by a functionary as envisaged by s 34(4). Therefore, this was 'made' by a functionary as envisaged by s 34(1). The court held that exhibits D5-D9 did not comply with the requirements of s 34 as these exhibits were not 'made' by a functionary.

107 It should be noted that s 221 deals with the admissibility of certain trade or business records provided that certain conditions are met. The court found that the print-outs were documents and they fell within the category of a record relating to a trade or business. The statements the state sought to introduce in exhibits D1-D4 had been obtained from persons who had personal knowledge of their contents, whilst the information in these statements had been sorted out and collated by a computer to produce exhibits D5-D9.

108 For further discussion about the case see Van der Merwe *et al* (n 77) 121-123, where Professor Van der Merwe lauds the court's progressive approach. Van der Merwe's comments are supported.

submitted that more clear and concise judicial guidance on the admissibility and evidential weight of electronic evidence is needed in future cases.

4.4 The South African banking sector

South African banks are also vulnerable to cybercrime.[109] Banks have expressed concern about the increase in phishing schemes.[110] Cybercrime is said to be increasing rapidly in South Africa. Many companies are said to underestimate the threat from phishing, data loss, identity theft, information leakage and other cyber activities. It is also acknowledged that many of the phishing operators are part of the Nigerian 419 scam.[111] The recent bank SMS scam case has also raised serious questions about the security of online banking.[112] However, the establishment of organisations such as SABRIC to combat cybercrime in the banking industry is lauded. SABRIC provides the banking industry with crime risk information management services and facilitates inter-bank initiatives to reduce the risk of organised bank-related crime through effective public private partnerships.[113] It is submitted that the private sector has a vested interest in addressing bank-related crime.

4.5 Way forward

South Africa has adopted the COECC but not ratified it. The treaty contains important provisions to assist law enforcement (the police) in their fight against transborder cybercrime. Therefore, South Africa needs to ratify the cybercrime

109 See *inter alia* Anon 2007 www.crime-research.org/ and Herselman and Warren 2004 www.dealin.edu.au/ It is advocated in the latter article that South Africa should learn from and apply the Organisation for Economic Co-operation and Development (OECD) guidelines (2002) to safeguard businesses against cybercrime.

110 The major banks such as Absa, Standard Bank and First National Bank have confirmed breach of their clients' accounts by phishing schemes during 2007. See Anon 2007 www.iol.co.za/ Also see Van der Merwe *et al* (n 77) 66-67 for further discussion about the vulnerability of South African banks.

111 The so-called '419' swindle is named after the article in the Nigerian penal code which outlaws it.

112 It involved a Vodacom employee who was working with a syndicate to intercept SMS notifications from banks to their customers. It has been reported that about R 7-million was siphoned off from customers' accounts as result of this scam. See Chelemu 2009 *The Times* 6.

113 SABRIC was established in 2002 as a wholly-owned subsidiary of the Banking Association. Its key stakeholders are the four major South African banks, namely, Standard Bank, Nedbank, Absa and First National Bank. For further information, see SABRIC 2009 www.sabric.co.za.

treaty to avoid becoming an easy target for international cybercrime. The South African government seems to be presently focused on basic service delivery and more traditional crimes, given the current situation in the country where crime and poverty are rife. However, the establishment of the Computer Security Incident Response Team (CSIRT) indicates that the aim to tackle cybercrime is gathering momentum.[114] The South African Law Reform Commission (SALRC) has also recommended the introduction of legislation on the protection of personal information (so-called "information protection legislation or information privacy legislation").[115] It is submitted that the promulgation of information protection legislation in South Africa will impact on *inter alia* the *Promotion of Access to Information Act* 2 of 2000 (the PAIA) and the ECT as far as information privacy is concerned.

It is submitted that South Africa can learn from the approaches followed in other countries. We can take note of the UK model (as in the CMA) by introducing stricter penalties in the ECT. We need to prescribe harsher penalties to deter cyber criminals. We can also examine the feasibility of introducing collaborative initiatives involving the police, the private sector and academics to combat cybercrime (as in the US and the UK). It is important to involve all role players in the struggle against cybercrime. The role of the Australian Banking Association in combating rising levels of cybercrime in the banking industry can be favourably compared to the role of SABRIC. It is important to enlist the aid of the private sector to combat cybercrime. The introduction of a Cyber Appellate Tribunal similar to that in India will also ensure that cyber cases are given priority. It will also lessen the case load on our already over-burdened courts. Indeed, our police and judiciary should also become more cybercrime savvy, like their Indian counterparts. Last but not least, we should follow the US in

114 See Anon 2007 it-online.co.za/; Anon 2009 www.ib.com/ The latter article commends the actions of the SA government in reducing software piracy.

115 See SALRC Discussion Paper 109. It should be noted that information protection relates to the protection of a person's right to privacy. The right to privacy is protected in terms of s 14 of the Constitution. The Protection of Personal Information Bill is regarded as a mechanism for the protection of the right to information protection and will be enacted at some time during 2009.

ratifying the COECC, as the treaty offers a global approach to the global problem of cybercrime.

4.6 Africa perspective

African countries have been criticised for dealing inadequately with cybercrime as their law enforcement agencies are inadequately equipped in terms of personnel, intelligence and infrastructure, and the private sector is also lagging behind in curbing cybercrime. African countries are pre-occupied with attending to pressing issues such as poverty, the Aids crisis, the fuel crisis, political instability, ethnic instability and traditional crimes such as murder, rape and theft, with the result that the fight against cybercrime is lagging behind. It is submitted that international mutual legal and technical assistance should be rendered to African countries by corporate and individual entities to effectively combat cybercrime in Africa. African countries need to build partnerships to combat internet crime and corruption. Nevertheless, it is laudable that other African countries (besides South Africa) are making attempts to address cybercrime. Kenya has enacted cyber legislation to combat cyber crimes.[116] Botswana has presented a Bill on Cybercrime and Computer-Related Crimes to the National Assembly, which will go for a third reading before it is signed into law.[117] The Economic Community of West African States (ECOWAS) has also met to discuss *inter alia* the implementation of ICT policy and legislation, access and interconnection regulation, the granting of universal access and the provision of guidelines for gradual transition to open markets.[118] There is a growing recognition that cybercrime is thriving on the African continent because of a lack of IT knowledge by the public and the absence of suitable legal frameworks to deal with cybercrime at national and regional levels. Attempts are therefore being made to address cybercrime.

---

116 The Kenyan *Communications Act* was passed by the Kenyan Parliament and signed by the President during January 2009. The Act includes legislation on cybercrime in s 83 W-Z and s 84 A-F on *inter alia* unauthorised access to computer data, access with intent to commit offences, unauthorised access to and interception of computer services, damaging or denying access to computer systems, unlawful possession of devices and data, electronic fraud, tampering with computer source documents and publishing obscene material in electronic form. See further, Cybercrime Law 2009 www.cybercrimelaw.net/

117 *Ibid*.

118 See Ogundeji 2008 www.thestandard.com/

5 Conclusion

The global nature of computer technology presents a challenge to nations to address cybercrime.[119] Domestic solutions are inadequate because cyberspace has no geographic or political boundaries, and many computer systems can be easily accessed from anywhere in the world. It is also difficult to obtain accurate cybercrime statistics because an unknown number of crimes go undetected and unreported. It is also costly to develop and maintain security and other preventative measures. International financial organisations are also common targets for computer fraud and embezzlement schemes.[120] Organised crime and terrorist groups are also using sophisticated computer technology to bypass government detection and carry out destructive acts of violence.[121] It is thus a continuous uphill battle to develop computer crime legislation that applies to both domestic and international audiences.[122]

The efforts of professional organisations such as the International Criminal Police Organisation (Interpol) are necessary to combat cybercrime. To this end, Interpol has provided technical guidance in cybercrime detection, investigation and evidence collection.[123] The role of multi-national organisations such as the

119 The following reasons illustrate the difficulty in addressing cybercrime: the lack of tools for the use of police to tackle the problem; the fact that the 'old' laws do not fit the 'new' crimes being committed; the fact that the new laws have not adjusted to the reality on the ground; that there are few precedents to be used for guidance; that there are debates over privacy issues which hamper the ability of enforcement agents to gather evidence needed to prosecute new cases; and that the distrust between police and computer professionals hampers close co-operation between the two parties to effectively address the cybercrime problem and make the Internet a safe place. See Singh (n 72) 1.

120 See Bazelon *et al* (n 1) 306.

121 The case of Rami Yousef who orchestrated the 1993 World Trade Center bombing by using encryption to store details of his scheme on his laptop computer is a case in point. *Ibid*.

122 Regarding the practical impediments to international investigation and enforcement, see Miquelan-Weissmann (n 3) 335-336.

123 Interpol is co-operating with credit card companies to combat payment fraud by building a database on Interpol's web site. Interpol is also making efforts to establish a network for collating information relating to illegal activities on the Internet. Regional efforts have also been made to combat cybercrime by bodies such as the Asia-Pacific Economic Co-operation (APEC), the Council of Europe (the COE), the European Union and the

Commonwealth of Nations, the Group of 8 (the G8) and the Organisation for Economic Co-operation and Development (the OECD) is important because their work encompasses a broader territorial environment.[124] The COECC's role is also lauded as it attempts to establish consistency in the cybercrime laws of various countries. However, many states still have to sign, let alone ratify, the Convention to serve as a deterrent.[125] The unanimous participation of all nations is required in order to achieve meaningful prosecution.

Although technology advancement is welcomed, it has created numerous challenges. There is a need for security-related features on the internet to respond to these challenges. Countries should strive to strike a balance between protecting the safety and security of individuals and guaranteeing the free dissemination of information and opinion.[126] H Jahankhani calls for a global digital community to take steps to evaluate and safeguard cyber legislation to achieve efficient and socially responsible use of the Internet, because the global community is responsible for evaluating such legislation.[127] An effective fight against cybercrime requires increased, rapid and efficient international co-operation in criminal matters. Regarding the problem with jurisdiction, Brenner suggests that a country should expand the "territorial notion" of jurisdiction to prosecute so that it allows a country to prosecute regardless of whether the offender's conduct occurred in whole or in part in the prosecuting country's territory.[128] Brenner also suggests that countries should evaluate their procedural law governing collection and analysis of evidence to include intangible evidence derived from cybercrimes as opposed to traditional crimes

---

Organisation of American States (the OAS). However, these regional efforts are limited to specific states. See Xingan (n 15) 3-4.

124 International organisations examine the promotion of security awareness at both the international and national levels, the harmonisation of national legislation, coordination and co-operation in law enforcement and they direct anti-cybercrime actions.

125 International co-operation is required to punish cybercrime offenders. Thus, international co-operation is limited to the particular participants and treaty signatories who have enacted domestic cybercrime legislation.

126 The efforts by the UK Home Office to censure sex offencers on the Internet are lauded. See Anon (n 53) 9.

127 See Jahankhani (n 26) 10.

128 She also suggests that countries should impose their own criminal laws on their citizens when the citizens are abroad, which would facilitate prosecution when a crime was committed abroad. The 'love bug' virus has demonstrated that cybercriminals can exploit gaps in a country's penal and procedural laws to evade prosecution. Brenner (n 5) 14.

which generate tangible evidence.[129] The courts also need to understand the technical characteristics of the Internet and develop well-settled precedents to address the question of jurisdiction in an intelligent and logical manner. Indeed the judicious use of criminal sanctions and administrative regulation is mooted as an effective way to prevent cybercrime.[130]

It is submitted that the advent of the ECT goes a long way towards addressing cybercrime in South Africa. However, there is room for improvement.[131] As stated earlier, South Africa needs to ratify the COECC to avoid becoming vulnerable to international cybercrime. A need also arises for the introduction of more specialised prosecutors and specialised procedures to facilitate the prosecution of cybercrime cases on a priority basis. Internet users should also be encouraged to share the burden of securing informational privacy where feasible.[132] Computer ethics education should also be taught to children in schools to educate them about the negative consequences of committing cybercrime. The possibility exists that new forms of cybercrime will emerge with evolving technology. New cyber laws should therefore be introduced to respond to these rapid changes. There should also be continuous research and training of IT security personnel, finance services sector personnel, police officers, prosecutors and the judiciary to keep them abreast of advancing computer technology. At the end of the day, a balanced approach that considers the protection of fundamental human rights and the need for the effective prosecution of cybercrimes is the way forward.

129 *Id*.
130 Brenner and Clarke (n 3) 709.
131 The ECT is criticised for not having severe criminal penalties. It is recommended that the criminal jurisdictional limit and the anti-spam provision in the ECT should be amended. See Van der Merwe (n 1) 319 in this regard.
132 See Allan (n11) 149-150.

Bibliography

Allan 2005 *NZLR*

Allan G "Responding to cybercrime: A delicate blend of the orthodox and the alternative" 2005 *New Zealand Law Review* 149-178

Anon 2006 *Computer Fraud and Security*

Anonymous "US ratifies international crime treaty" 2006 (11) *Computer Fraud and Security* 2-3

Anon 2006 *Harvard LR*

Anonymous "Immunizing the Internet, or: how I learned to stop worrying and love the worm" 2006 (119) *Harvard Law Review* 2442-2463

Anon *The Peninsula*

Anonymous 'Online sex pests censured' *The Peninsula* 5 April 2008 9

Audal *et al* 2008 *ACLR*

Audal *et al* "Computer crimes" 2008 (45) *The American Criminal Law Review* 233-272

Bazelon *et al* 2006 *ACLR*

Bazelon E *et al* "Computer crimes" 2006 (43) *The American Criminal Law Review* 260-308

Bekker *et al* "The criminal courts"

Bekker PM *et al* "The criminal courts of the Republic" in Joubert JJ *et al* (eds) *Criminal Procedure Handbook* (Juta Cape Town 2007) 37-38

Berg 2007 *Michigan Bar Journal*

Berg T "The changing face of cybercrime: New Internet threats create challenges to law enforcement" 2007 (86) *Michigan Bar Journal* 18-22

Blackwell 1997 *Canadian Lawyer*

Blackwell G "A jurisdiction called cyberspace?" 1997 *Canadian Lawyer* 22-23

Brenner 2001 *Murdoch Univ EJL*

Brenner S "Cybercrime investigation and prosecution: the role of penal and procedural law" 2001 (8) *Murdoch University Electronic Journal of Law* 1-16

Brenner and Clarke 2005 *John Marshall JCIL*

Brenner SW and Clarke LL "Distributing security: Preventing cybercrime" 2005 (23) *John Marshall Journal of Computer and Information Law* 659-209

Brenner and Koops 2004 *JHTL*

Brenner S and Koops B-J "Approaches to jurisdiction" 2004 (4) *Journal of High Technology Law* 1-46

Bronitt and Gani 2003 *Crim LJ*

Bronitt S and Gani M "Shifting boundaries of cybercrime: From computer hacking to cyberterrorism" 2003 (27) *Criminal Law Journal* 303-317

Burchell 2002 *SALJ*

Burchell J "Criminal justice at the crossroads" 2002 *South African Law Journal* 579-602

Chelemu 2009 *The Times*

Chelemu K "Banks open files for police in SMS scam case" 2009 *The Times* 23 July 2009 6

Collier 2005 *Juta's Business Law*

Collier D "Evidently not so simple: producing computer print-outs in court" 2005 (13) *Juta's Business Law* 6-9

Dadhich and Shukla "Cybercrimes"

Dadhich A and Shukla G "Cybercrimes: An insight to the Indian position" in Kierkegaard SM (ed) *Cyberlaw Security and Privacy* (International Association of IT lawyers 2007) 414-425

Fafinski 2008 *Journal of Criminal Law*

Fafinski S "Computer misuse: The implications of the Police and Justice Act 2006" 2008 (72) *Journal of Criminal Law* 53-66

Finlay 1999 *TBL*

Finlay E "Litigation on the Net: personal jurisdiction in cyberspace" 1999 (62) *Texas Bar Journal* 334-341

Goodman and Brenner 2002 *IJLIT*

Goodman MD and Brenner S "The emerging consensus on criminal conduct in cyberspace" 2002 *International Journal of Law and Information Technology* 10 139-222

Hofman 2006 *SACJ*

Hofman J "Electronic evidence in criminal cases" 2006 *South African Journal of Criminal Justice* 3 257-275

Jahankhani 2007 *IJESDF*

Jahankhani H "Evaluating of cyber legislations trading in the global cyber village" 2007 (1)*International Journal of Electronic Security and Digital Forensics* 1-11

Kerr 2005/2006 *Harvard LR*

Kerr OS "Searches and seizures in a digital world" 2005/2006 119 (1-3) *Harvard Law Review* 532-585

McKenna 2004 *Infosecurity Today*

McKenna B "UK MPs call for Computer Misuse Act upgrade" 2004 *Infosecurity Today* July/August 5

Miquelan-Weissmann 2005 *John Marshall JCIL*

Miquelan-Weissmann MF "The Convention on Cybercrime: A harmonised implementation of international penal law: what prospects for procedural due process?" 2005 (23) *John Marshall Journal of Computer and Information Law* 1-28

Ormerod 2004 *Crim LR*

Ormerod DC "Case and comment" 2004 *Criminal Law Review* 951-954

SALRC Discussion Paper 109

South African Law Reform Commission Discussion Paper 109 Project 124 (October 2005)

Sibanda "Choice of law"

Sibanda OS "Choice of law, jurisdiction and recognition and enforcement of judgments in e-commerce in South Africa" in Kierkegaard SM (ed) *Cyber Security and Privacy* (International Association of IT lawyers 2007) 259-266

Snail and Madziwa 2008 *Without Prejudice*

Snail S and Madziwa S "Hacking, cracking and other unlawful online activities" 2008 *Without Prejudice* 30-31

Van der Merwe 2003 *JCRDL*

Van der Merwe DP "Computer crime- recent national and international developments" 2003 *Journal of Contemporary Roman-Dutch Law* 30-44

Van der Merwe 2007 *JCRDL*

Van der Merwe DP "Information technology crime – a new paradigm is needed" 2007 *Journal of Contemporary Roman-Dutch Law* 309-319

Van der Merwe *et al ICT Law*

Van der Merwe DP *et al Information and Communications Technology Law* (Lexis Nexis Durban 2008)

Van Zyl 2008 *JCRDL*

Van Zyl SP "Sexual offences and the Internet: Are we ready for 2010?" 2008 *Journal of Contemporary Roman-Dutch Law* 71 222-239

Wilson 2006 *Aust LJ*

Wilson J "Cybercrime in the private sector: partnerships between the private sector and law enforcement" 2006 (80) *Australian Law Journal* 694-704

Xingan 2007 *Webology*

Xingan L "International actions against cybercrime: Networking legal systems in the networked crime scene" 2007 (4) *Webology* 1-31

Register of legislation

South Africa

Constitution of the Republic of South Africa 1996

Civil Proceedings Act 25 of 1965

Criminal Procedure Act 51 of 1977

Electronic Communications and Transactions Act 25 of 2002

Films and Publications Act 65 of 1996

Financial Intelligent Centre Act 38 of 2001

Magistrate's Courts Act 32 of 1944

Prevention of Organised Crime Second Amendment Act 38 of 1999

Regulation of Interception of Communications and Provision of Communications-Related Information Act 70 of 2002

International

Australian Criminal Code 1995

Cybercrimes and Information Technology Act 2000 (India)

Cybercrimes Act Law 2 of 2006 (UAE)

Computer Misuse Act 1990 (UK)

Criminal Code and Cybercrime Act 2001 (Australia)

Electronic Communications Privacy Act of 1986 (USA)

National Information Infrastructure Protection Act 1996 (USA)

Penal Code Act 11 of 2004 (Qatar)

Patriot Act 2001 (USA)

Register of court cases

South Africa

Bid Industrial Holdings (Pty) Ltd v Strang and Others 2007 SCA 144 (RSA)

Motata v Nair NO and Another 2009 1 SACR 263 (T); 2009 2 SA 575 (T); (7023/2008) [2008] ZAFSHC 53 (11 June 2008)

SB Jafta v Ezemvelo KZN Wildlife (Case D 204/07)

S v Harper and Another 1981 (1) SA 88 (D)

Narlis v South African Bank of Athens 1976 (2) SA 573 (A)

S v Ndiki and Others 2008 (2) SACR 252

Ndlovu v Minister of Correctional Services and Another 2006 (4) All SA 165 (W)

S v Ntuli 1970 (2) SA 278 (W)

S v Maseki 1981 (4) SA 374 (T)

S v Mpumlo 1986 (3) SA 485 (E)

Secombe v AG 1919 TPD 270

International

Director of Public Prosecution v Sutcliffe [2001] VSC 43 (Victoria, Australia)

R v Gold (1988) AC 1063

R v Smith (Wallace) No 4 [2004] EWCA Crim 631

US v Councilman 385 F3d 793 (first Circuit 2005)

US v Gorshov 2001 WL 1024026

US v Judd 46 F3d 961 (California Circuit 1995)

US v Thomas 74 F3d 70 (Sixth Circuit 1996)

Register of internet resources

Anon 2009 www.ib.com/

Anonymous 2009 *South Africa has the lowest software piracy rate in Africa, while Zimbabwe has the highest in the world* www.ib/.com/internat.law-news [accessed on 1 June 2009]

Anon 2009 www.legalbrief.co.za/

Anonymous 2009 *Judge Motata guilty of drunk driving* www.legalbrief.co.za/article [accessed on 3 September 2009]

Anon 2009 www.news24.com/

Anonymous 2009 *Huge growth in cybercrime* www.news24.com/News24/SouthAfrica [accessed on 10 June 2009]

Anon 2009 www.zawya.com

Anonymous 2009 *Cybercrime increasing in Qatar* www.zawya.com [accessed on 20 May 2009]

Anon 2009a www.mg.co.za/

Anonymous 2009a *Motata found guilty of drunken driving* www.mg.co.za/article/2009-09-02 [accessed on 3 September 2009]

Anon 2009b www.mg.co.za/

Anonymous 2009b *Motata to appeal drunken-driving ruling* www.mg.co.za/article/2009-09-09 [accessed on 10 September 2009]

Anon 2007 it-online.co.za/

Anonymous 2007 *SA looks to tackle cyber crime with CSIRT* it-online.co.za/conte't/view/180306/129 [accessed on 26 November 2007]

Anon 2007 www.crime-research.org/

Anonymous 2007 *South Africa to tackle cyber crime* www.crime-research.org/news/11.07.2006/2115/ [accessed on 26 November 2007]

Anon 2007 www.iol.co.za/

Anonymous 2007 *Bank clients warned of phishing scam* www.iol.co.za/general/news [accessed on 27 May 2007]

Anon 2007 www.polity.org.za/

Anonymous 2007 *Examining the real cost of virtual crime* www.polity.org.za/article [accessed on 27 November 2007]

Anon 2006a archive.gulfnews.com/

Anonymous 2006a *E-government studies smart card to replace ID* archive.gulfnews.com/articles [accessed on 3 March 2009]

Anon 2006b archive.gulfnews.com

Anonymous 2006b *Federal law covers all areas of cyber crime* archive.gulfnews.com [accessed on 12 February 2006]

Bowman 2006 www.itp.net/

Bowman D 2006 *Saudi passes cyber crime laws* www.itp.net/index [accessed on 15 October 2006]

Cybercrime Law 2007 www.cybercrimelaw.net/

Cybercrime Law 2007 *What is cybercrime?* www.cybercrimelaw.net/content/cybercrime.html [accessed on 27 November 2007]

Cybercrime Law 2009 www.cybercrimelaw.net/

Cybercrime Law 2009 *Cybercrime Law* www.cybercrimelaw.net/ [accessed on 21 May 2009]

Dearne 2008 www.australianit.news.com.au/

Dearne K 2008 *Cyber treaty may mean new laws* www.australianit.news.com.au/story [accessed on 27 May 2008]

DIT 2009 dit.mp.gov.in/

Department of Information Technology Government of Madhya Pradesh 2009 *Cyber laws in India* dit.mp.gov.in/cyberlawt.htm [accessed on 6 May 2009]

DPA 2009 www.thepeninsulaqatar.com/

DPA 2009 *Tourists in Philippines attracted to pirated goods* www.thepeninsulaqatar.com/Display_news.asp?section=world_news&month=march2009&file=world_news200903018535.xml [accessed on 1 March 2009]

Herselman and Warren 2004 www.dealin.edu.au/

Herselman M and Warren M 2004 *Cyber crime influencing businesses in South Africa* www.dealin.edu.au/dro/view [accessed on 10 June 2009]

Howe 2007 archive.gulfnews.com/

Howe M 2007 *Gulf States to combat cybercrime* archive.gulfnews.com/articles [accessed on 19 June 2007]

Krebs 2008 blog.washingtonpost-com/

Krebs B 2008 *Senate approves bill to fight cyber-crime* blog.washingtonpost-com/security fix/2008/07 [accessed on 21 May 2009]

Leyden 2008 www.theregister.co.uk/

Leyden J 2008 *UK cyber crime overhaul finally comes into effect* www.theregister.co.uk/2008/09 [accessed on 21 May 2009]

Mndzima and Snail 2009 www.hg.org/

Mndzima S and Snail S 2009 *Cyber crime in South Africa* www.hg.org/article [accessed on 14 April 2009]

Ogundeji 2008 www.thestandard.com/

Ogundeji OA 2008 *African states to discuss cybercrime* www.thestandard.com/news/2008 [accessed on 21 May 2009]

Roberts 2007 archive.gulfnews.com/

Roberts L 2007 *Gulf States to combat cyber crime; Gulf States plan unified action on cybercrime law* archive.gulfnews.com/articles [accessed on 19 June 2007]

Singh 2009 www.ind.ii.org/

Singh T 2009 *Cyberlaw and Information Technology* www.ind.ii.org/cyberlaw.aspx [accessed on 6 May 2009]

SABRIC 2009 www.sabric.co.za

SABRIC 2009 *South African Banking Risk Information Centre* www.sabric.co.za/ [accessed on 10 December 2009]

Special Correspondent 2008 www.thehindu.com/

Special Correspondent 2008 *Parliament approves cyber crime Bill* www.thehindu.com/2008/12/24/stories/2008122456021400.htm [accessed on 21 May 2009]

Townson 2006 www.gulf-times.com

Townson P 2006 *Call for legal steps to fight cyber crimes* www.gulf-times.com [accessed on 3 March 2009]

List of abbreviations

BSA	Business Software Alliance
ch	chapter(s)
CMA	Computer Misuse Act
COECC	Council of Europe's Convention on Cybercrime

CSIRT	Computer Security Incident Response Team
ECOWAS	Economic Community of West African States
ECPA	Electronic Communications Privacy Act
ECT	Electronic Communications and Transactions Act
FICA	Financial Intelligence Centre Act
G8	Commonwealth of Nations, the Group of 8
Interpol	International Criminal Police Organisation
NIIPA	National Information Infrastructure Protection Act
OECD	Organisation for Economic Co-operation and Development
par	paragraph(s)
PAIA	Promotion of Access to Information Act
POCAA	Prevention of Organised Crime Second Amendment Act
reg	regulation(s)
RICA	Regulation of Interception of Communications and Provision of Communications-Related Information Act
s	section(s)
UAE	United Arab Emirates
SALRC	South African Law Reform Commission