REPUBLIC OF SOUTH AFRICA

CYBERCRIMES AND CYBERSECURITY BILL

DRAFT FOR PUBLIC COMMENT

_____

(As introduced in the National Assembly (proposed section 75); explanatory summary of Bill published in Government Gazette No. …….. of ……. 2015) (The English text is the official text of the Bill)

_____

(MINISTER OF JUSTICE AND CORRECTIONAL SERVICES)

[B—2015]

_____

BILL

To create offences and impose penalties which have a bearing on cybercrime; to further regulate jurisdiction of the courts; to further regulate the powers to investigate, search and access or seize; to further regulate aspects of international cooperation in respect of the investigation of cybercrime; to provide for the establishment of a 24/7 Point of Contact; to provide for the establishment of various structures to deal with cyber security; to regulate the identification and declaration of National Critical Information Infrastructures and measures to protect National Critical Information Infrastructures; to further regulate aspects relating to evidence; to impose obligations on electronic communications service providers regarding aspects which may impact on cyber security; to provide that the President may enter into agreements with foreign States to promote cyber security; to delete and amend certain provisions of certain laws; and to provide for matters connected therewith.

PARLIAMENT of the Republic of South Africa enacts as follows:—

ARRANGEMENT OF SECTIONS

CHAPTER 1

DEFINITIONS

CHAPTER 2

OFFENCES

CHAPTER 3
JURISDICTION

CHAPTER 4
POWERS TO INVESTIGATE, SEARCH AND ACCESS OR SEIZE AND INTERNATIONAL COOPERATION

CHAPTER 5

24/7 POINT OF CONTACT

CHAPTER 6

STRUCTURES TO DEAL WITH CYBER SECURITY

CHAPTER 7

NATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

CHAPTER 8
EVIDENCE

CHAPTER 9
GENERAL OBLIGATIONS OF ELECTRONIC COMMUNICATIONS SERVICE PROVIDERS AND LIABILITY

CHAPTER 10
AGREEMENTS WITH FOREIGN STATE

CHAPTER 11
GENERAL PROVISIONS

Section 66: Repeal or amendment of laws

Section 67: Regulations

Section 68: Short title and commencement

Schedule

CHAPTER 1

DEFINITIONS

Mark Heyink Comment on Definitions

This comment does not deal in great detail with the definitions as it is felt that the Bill as it stands is not capable of being rescued by ad hoc drafting. It requires a reconsideration and complete redraft with the benefit of not only the comment which has been provided on the Bill, but also proper consultation with information security experts, constitutional experts, and persons well-versed in the law and legislation governing the various criminal acts that are created in the Bill.

This having been said, the commentator has had the benefit of consulting with representatives of The Open Democracy Advice Centre ("ODAC"), the Open Web Application Security Project ("OWASP"), Professor Basie von Solms of the Centre for Cybersecurity at the University of Johannesburg and numerous other lawyers, including the Criminal Law Committee of the Law Society of South Africa. Against this background the submissions of ODAC, OWASP and Professor von Solms are expressly endorsed by the commentator.

The failure to deal with the definitions in comment should not be viewed as an acceptance that the definitions are either accurate or practically sound in the context of the Bill as it stands. Quite on the contrary, failure to comprehend some of the practical implications of the Bill or recognise the definitions of certain concepts which have been provided to us in Model Laws and Conventions is not only regrettable but renders certain sections of the Bill simply nonsensical in a democratic society.

An example of this is afforded by the definition of "electronic communications service provider" which, by virtue of the provisions in section (c), renders almost every citizen in South Africa an electronic communications service provider. This in turn allows for the Minister of State Security to declare data and computer infrastructure National Critical Information Infrastructure. This in turn results in the Minister quite legitimately being able to access information, including personal information, processed by every citizen in the country. This completely defeats the protections afforded by the Protection of Personal Information Act which provides the necessary framework for the effective protection of privacy afforded by the Constitution.

This type of drafting is simply not acceptable and for government to say that it would not abuse its powers in this regard is equally unacceptable. The legislation itself must provide appropriate protections against abuse by all parties, including government agencies.

Definitions and interpretation

1. In this Act, unless the context indicates otherwise—

"**24/7 contact point**" means a designated point of contact, established in terms of section 49;

"**computer data storage medium**" means any article, device or location from which data is capable of being reproduced or on which data is capable of being stored, by a computer device, irrespective of whether the article or device is physically attached to or connected with the computer device;

"**computer device**" means any electronic programmable device used, whether by itself or as part of a computer network, a database, a critical database, an electronic communications network or a National Critical Information Infrastructure or any other device or equipment or any part thereof, to perform predetermined arithmetic, logical, routing or storage operations in accordance with set instructions and includes all—

(a) input devices;

(*b*) output devices;

(*c*) processing devices;

(*d*) computer data storage mediums;

(*e*) programs; and

(*f*) other equipment and devices,

that are related to, connected with or used with such a device or any part thereof;

"**computer network**" means two or more inter-connected or related computer devices, which allows these inter-connected or related computer devices to—

(*a*) exchange data or any other function with each other;

(*b*) exchange data or any other function with another computer network; or

(*c*) connect to an electronic communications network;

“**computer program**” means a sequence of instructions which enables a computer device to perform a specified function;

"**critical data**" means data that is of importance for the protection of—

(*a*) the security, defence or international relations of the Republic;

(*b*) the existence or identity of a confidential source of information relating to the enforcement of a criminal law of the Republic or of a State;

(*c*) the enforcement of a law of the Republic or of a State;

(*d*) the protection of public safety;

(*e*) trade secrets;

(*f*) records of a financial institution; or

(*g*) commercial information, the disclosure of which could cause undue advantage or disadvantage to any person,

and includes data relating to aspects referred to in section 58(2)*(a)* to *(f)* of this Act or any other data which is in possession of or under the control of a National Critical Information Infrastructure;

"**critical database**" means a computer data storage medium or any part thereof which contains critical data;

“**data**” means any representation of facts, information, concepts, elements, or instructions in a form suitable for communications, interpretation, or processing in a computer device, a computer network, a database, an electronic communications network or their accessories or components or any part thereof and includes a computer program and traffic data;

"**database**" means a collection of data in a computer data storage medium;

"**data message**" means data in an intelligible form, in whatever form generated, sent, received, communicated, presented, tendered or stored by electronic means;

"**electronic communications network**" means electronic communications infrastructures and facilities used for the conveyance of data;

"**electronic communications service provider"** means any—

(*a*) person who provides an electronic communications service under and in accordance with an electronic communications service licence issued to such person under Chapter 3 of the Electronic Communications Act, 2005 (Act No. 36 of 2005), or who is deemed to be licensed or exempted from being licensed as such in terms of the Electronic Communications Act, 2005;

(*b*) 'financial institution' as defined in section 1 of the Financial Services Board Act, 1990 (Act No. 97 of 1990); or

(*c*) person or entity who or which transmits, receives, processes or stores data—

(i) on behalf of the person contemplated in paragraph (*a*) or (*b*) or the clients of such a person; or

(ii) of any other person;

"foreign State" means any State outside the Republic and includes any territory under the sovereignty or control of such State;

"**National Critical Information Infrastructure**" means means any data, computer data storage medium, computer device, database, computer network, electronic communications network, electronic communications infrastructure or any part thereof or any building, structure, facility, system or equipment associated therewith or part or portion thereof or incidental thereto—

(*a*) which is specifically declared a National Critical Information Infrastructure in terms of section 58(2) of this Act; or

(*b*) which, for purposes of Chapters 2 and 4 of this Act, are in possession of or under the control of—

(i) any department of State or administration in the national, provincial or local sphere of government; and

(ii) any other functionary or institution exercising a public power or performing a public function in terms of any legislation,

irrespective whether or not it is declared a National Critical Information Infrastructure as contemplated in paragraph (a);

"**National Commissioner**" means the National Commissioner of the South African Police Service, appointed by the President under section 207(1) of the Constitution of the Republic of South Africa, 1996;

"**person**" means a natural or a juristic person;

"**Service**" means the South African Police Service established by section 5(1) of the South African Police Service Act, 1995 (Act No. 68 of 1995); and

"**traffic data**" means data relating to a communication indicating the communication's origin, destination, route, format, time, date, size, duration or type of the underlying service.

Mark Heyink Comment on Section 1

It is believed that once the issues of principle provided in this comment have been determined that it will be advisable to revisit, and if necessary revise, the definitions provided. These definitions should, unless inappropriate, take into consideration in their possible revision similar definitions in existing legislation and efforts at ensuring consistency be strived for.

It is noted that definitions are provided as part of sections dealing with specific issues to which the definitions relate. It is suggested that for the ease of reading the words and terms used be defined at the beginning of the section to which they apply and not at the end of the section, as is currently the case.

CHAPTER 2

OFFENCES

Definitions and interpretation

2. (1) In this Chapter, unless the context indicates otherwise **"computer related"** means the use of data, a computer device, a computer network, a database or an electronic communications network to commit a prohibited act provided for in sections 11, 12, 13, 14, 15 or 16.

(2) Any act which constitutes an offence in terms of section 3(1), (2) or (3) (in so far as it relates to the acquiring, provision or use of personal information or financial information), 4(1), 5(1), 6(2)(*a*), 7(1), 8(1), 9(1) (in so far as it relates to the use of malware) or 10(1) (in so far as it relates to the acquiring, provision or use of an access code, password or similar data or devices), which is performed on request of a person who has the lawful authority to consent to such act in order to perform a security audit on data, a computer device, a computer network, a database, a critical database, an electronic communications network or a National Critical Information Infrastructure —

(*a*) may not be regarded as unlawful if it falls within the written authority which was granted by the person who has the lawfully authority to consent to such act; and

(*b*) must be regarded as unlawful if it exceeds the written authority which was granted by the person who has the lawful authority to consent to such act.

Mark Heyink Comment on Section 2

From a practical perspective in information security practice, authority may derive from policy and even, quite appropriately, inferred in determining the authority of a particular person to perform an act. It is also true that in the vast majority of instances in South Africa that documented policies or authorities to perform certain acts are, contrary to good information security practice, not in writing. The problem that this creates for the wording of the section as it stands is that it has the potential to criminalise perfectly lawful acts simply on the basis that the owner of information and communications technologies has not fulfilled its duty to provide properly documented information security practices. The fault for this lies in the hands of the owners of information and communications technologies and not necessarily in the hands of the users but it could nonetheless have the unintended consequence that by failing to deal with information security properly the owner of ICT may be able to hold users accountable and possibly criminally liable despite their own shortcomings.

It is suggested that the word “written” in both sub-paragraphs 2(a) and (b) should be deleted. Alternatively that a clause be provided that in the absence of written policies or agreements that the onus of proving that the party accused of a crime acted outside of his authority remains with the accuser, as is currently the case in our criminal law.

Personal information and financial information related offences

3. (1) Any person who unlawfully and intentionally—

(*a*) acquires by any means;

(*b*) possesses; or

(*c*) provides to another person,

the personal information of another person for purposes of committing an offence under this Act is guilty of an offence.

(2) Any person who unlawfully and intentionally—

(*a*) acquires by any means;

(*b*) possesses; or

(*c*) provides to another person,

the financial information of another person for purposes of committing an offence under this Act is guilty of an offence.

(3) Any person who unlawfully and intentionally uses the personal information or financial information of another person to commit an offence under this Act is guilty of an offence.

(4) Any person who is found in possession of personal information or financial information of another person in regard to which there is a reasonable suspicion that such personal information or financial information—

(*a*) was acquired, is possessed, or is to be provided to another person for purposes of committing an offence under this Act; or

(*b*) was used or may be used to commit an offence under this Act,

and who is unable to give a satisfactory exculpatory account of such possession, is guilty of an offence.

(5) Any person who contravenes the provisions of subsection (1), (2) or (4) is liable, on conviction to a fine not exceeding R5 million or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment.

(6) Any person who contravenes the provisions of subsection (3) is liable, on conviction to a fine not exceeding R10 million or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment.

(7) For purposes of this section—

(*a*) "**personal information**" means any 'personal information' as defined in section 1 of the Protection of Personal Information Act, 2013 (Act No. 4 of 2013); and

(*b*) "**financial information**" means any information or data which can be used to facilitate a financial transaction.

Mark Heyink Comment on Section 3

General lack of understanding of the constitutional right of privacy.

Previous comment provided to the Department of Justice and Constitutional Development (DOJ) indicated that the provisions as drafted lack an understanding of the primary purpose of the constitutional right of privacy and the protection facilitated by the Protection of Personal Information Act. The amendments made by the drafters to these provisions do not remedy this misunderstanding. Alternatively, the insistence on the wording provided in this Act betrays a complete disregard (from the JCPS Cluster) for the issue of privacy and its importance from both a national and international context. This is an issue which will be dealt with in greater detail in later comment.

It should be remembered that in paragraph 3.1 of the National Cybersecurity Policy Framework (NCPF) it is expressly stated:

> *"3.1 The purpose of the NCPF is to create a secure, dependable, reliable and trustworthy cyber environment that facilitates the protection of critical information infrastructure whilst strengthening shared human values and understanding of Cybersecurity in support of national security imperatives and the economy. This will enable the development of an information society which takes into account the fundamental rights of every South African citizen to privacy, security, dignity, access to information, the right to communication and freedom of expression."*
>
> Emphasis added by the author

While it is to be welcomed that the definition of "personal information" has been amended from a prior draft to adopt the definition of the Protection of Personal Information Act and require that the Bill is interpreted in terms of that section, the definition of "financial information of another person" is incongruent. The Protection of Personal Information Act includes financial information in its definition. Therefore the distinction between personal information and financial information should be irrelevant in this context. Attention is drawn to paragraphs 3(2), 3(3) and 3(7) as well as the definition of "personal information" in the Protection of Personal Information Act in consideration of the wording as it stands.

Against this background it is strongly recommended that instead of creating unnecessary conflicts in interpretation that may, and probably will arise from the current drafting of this provision (allowing criminals potential loopholes and defences), that the correct approach would be to simply legislate an increase of the penalties for offences stipulated in the Protection of Personal Information Act and retain the mechanisms for criminal prosecution that have been established in that Act.

Further, the provisions in the Bill do not take into consideration the powers and duties of the Regulator, established in the Protection of Personal Information Act, and the fact that responsible parties (as defined in the Protection of Personal Information Act) are subject to the Regulator's oversight. This is a critical element of the Act and the attempts to amend the provisions in the Act will do injury to the Act and the necessity that it be found by trading partners who may wish to allow personal information to be transferred to South Africa to be adequate. The failure to meet the requirements of adequacy of privacy legislation as required in many jurisdictions already has and will continue to have an adverse effect on South Africa's information economy.

It is further submitted that the drafters have not fully appreciated the extremely wide parameters that need to be covered in dealing with personal information. The principles for the processing of personal information which are statutorily recognised in the 8 conditions governing the processing of personal information in the Act, are absent from the Bill. This will have the effect that even in the innocent processing of personal information, in certain circumstances the processor will effectively be summarily guilty of an offence unless a satisfactory exculpatory account is given. This is a serious divergence from the principle of innocent until proven guilty and has the potential for malicious abuse which was so vehemently opposed in the Protection of State Information Bill (The Secrecy Bill").

There is little doubt that the provisions as they stand, in the absence of the context and protections provided by the Protection of Personal Information Act do not pass constitutional muster.

If the powers that be cannot be persuaded that dealing with personal information as has been proposed as opposed to the way that that it is drafted is the correct course of action, regard must be had to proper alignment of these provisions with the Protection of Personal Information Act. Mr Robbertse (the drafter of these provisions) indicated that Section 105 of the Protection of Personal Information Act had been considered in drafting this section. However, the ambit of this Section 3 is far broader than that contemplated in Section 105 of POPI. As such there are unintended consequences which will flow from this provision and go well beyond what was intended in POPI. Not only is Section 105 confined to unlawful acts of a responsible party but it is also restricted by the information relating to an account number. These issues do not appear to have been taken into account in the drafting of this section and if they have, they have perverted the intention of the legislature in the unanimous enactment of POPI by the House of Assembly in 2013.

Unlawful access

4. (1) Any person who unlawfully and intentionally accesses the whole or any part of —

(*a*) data;

(*b*) a computer device;

(*c*) a computer network;

(*d*) a database;

(*e*) a critical database;

(*f*) an electronic communications network; or

(*g*) a National Critical Information Infrastructure,

is guilty of an offence.

(2) Any person who contravenes the provisions of subsection (1) is liable, on conviction—

(*a*) in the case of a contravention of the provisions of subsection (1)(*a*), (*b*), (*c*), (*d*) or (*f*), to a fine not exceeding R5 million or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment; or

(*b*) in the case of a contravention of the provisions of subsection (1)(*e*) or (*g*) to a fine not exceeding R10 million or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment.

(3) For purposes of this section "**access**" includes, without limitation, to make use of, to gain entry to, to view, display, instruct, or communicate with, to store data in or retrieve data from, to copy, move, add, change, or remove data or otherwise to make use of, configure or reconfigure any resources of a computer device, a computer network, a database, a critical database, an electronic communications network or a National Critical Information Infrastructure, whether in whole or in part, including their logical, arithmetical, memory, transmission, data storage, processor, or memory functions, whether by physical, virtual, direct, or indirect means or by electronic, magnetic, audio, optical, or any other means.

(4) For purposes of this section, the actions of a person, to the extent that they exceed his or her lawful authority to access data, a computer device, a computer network, a database, a critical database, an electronic communications network or a National Critical Information Infrastructure, must be regarded as unlawful.

Mark Heyink Comment on Section 4

Unlike the position with the Protection of Personal Information Act where the Act itself provides significant context, the repeal of relevant sections in the Electronic Communications and Transactions Act and the replacement in this Act seems appropriate.

This having been said, with great respect the provisions of Section 86 of the Electronic Communications and Transactions Act relating to unauthorised access to, reception of or interference with data is significantly easier to read and evidence more clarity of thought than the equivalent provisions provided for in this draft Bill.

Leave aside the difficulties with definitions and their deviation from accepted definitions, Section 4(3), in defining “access”, while far ranging, could have unintended consequences, particularly when read with Section 4, which imperatively stipulates that needing lawful authority to access data must be regarded as unlawful. It is submitted that this significantly shifts the burden of proof required in criminal matters and appears to negate the issue of intent even though this is clearly stated in Section 4(1) to be an element of the offence.

This may be cured to some extent by including in paragraph 4(4) the words “knowingly or intentionally” before the word “exceed”. In all of the discussions that I have had with various parties in this matter, whether they be technologists, lawyers or parties interested from a business perspective, the disquiet in the shift of the onus of proof has been a prevailing theme.

Among the comment that has been received is that a person cannot be guilty purely in the absence of a good excuse. Normal criminal due process requiring that a person is found guilty without reasonable doubt should be applied and a finding of guilt should be based on a person being guilty, not on the basis that they were unable to provide a satisfactory explanation.

Unlawful interception of data

5. (1) Any person who unlawfully and intentionally intercepts data to, from or within—

(*a*) a computer device;

(*b*) a computer network;

(*c*) a database;

(*d*) a critical database;

(*e*) an electronic communications network; or

(*f*) a National Critical Information Infrastructure,

or any part thereof, is guilty of an offence.

(2) Any person who contravenes the provisions of subsection (1) is liable, on conviction—

(*a*) in the case of a contravention of the provisions of subsection (1)(*a*), (*b*), (*c*), or (*e*), to a fine not exceeding R5 million or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment; or

(*b*) in the case of a contravention of the provisions of subsection (1)(*d*) or (*f*) to a fine not exceeding R10 million or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment.

(3) For purposes of this section **"interception of data**" means the acquisition, viewing, capturing or copying of data through the use of a hardware or software tool contemplated in section 6(5) or any other means, so as to make some or all of the data available to a person other than the lawful owner or holder of the data, the sender or the recipient or the intended recipient of that data and includes the—

(*a*) examination or inspection of the contents of the data; and

(*b*) diversion of the data or any part thereof from its intended destination to any other destination.

Mark Heyink Comment on Section 5

In Section 86 of the ECT Act, which this provision appears to seek to replace, interception is subject to the Interception and Monitoring Prohibition Act (now replaced by RICA). Is there any reason why this has been done away with in the Bill? While RICA is not a model of clarity, it is believed that if only for the purpose of reference by persons who have no legal background, reference to the primary legislation dealing with interception of data is not only desirable but essential.

Unlawful acts in respect of software or hardware tools

6. (1) Any person who unlawfully and intentionally manufactures, assembles, obtains, sells, purchases, makes available or advertises any software or hardware tool for the purposes of contravening the provisions of section 3(1)(*a*) or (2)(*a*), 4(1), 5(1), 7(1), 8(1), 10(1), 11(1), 12(1) or (2) or 13(1), is guilty of an offence.

(2) Any person who unlawfully and intentionally—

(*a*) uses; or

(*b*) possesses,

any software or hardware tool for purposes of contravening the provisions of section 3(1)(*a*) or (2)(*a*), 4(1), 5(1), 7(1), 8(1), 10(1), 11(1), 12(1) or (2) or 13(1), is guilty of an offence.

(3) Any person who is found in possession of a software or hardware tool in regard to which there is a reasonable suspicion that such software or hardware tool is possessed for the purposes of contravening the provisions of section 3(1)(*a*) or (*c*) or (2)(*a*) or (*c*), 4(1), 5(1), 7(1), 8(1), 10(1), 11(1), 12(1) or (2) or 13(1), and who is unable to give a satisfactory exculpatory account of such possession, is guilty of an offence.

(4) Any person who contravenes the provisions of subsections (1), (2) or (3) is liable, on conviction to a fine not exceeding R5 million or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment.

(5) For purposes of this section " **software or hardware tools**" means any data, electronic, mechanical or other instrument, device, equipment, or apparatus, which is used or can be used, whether by itself or in combination with any other data, instrument, device, equipment or apparatus, in order to—

(*a*) acquire, make available or to provide personal information or financial information as contemplated in section 3(1)(a) or (*c*), or (2)(*a*) or (*c*);

(*b*) access as contemplated in section 4(3);

(*c*) intercept data as contemplated in section 5(3);

(*d*) interfere with data as contemplated in section 7(3);

(*e*) interfere with a computer device, computer network, database, critical database, electronic communications network or National Critical Information Infrastructure as contemplated in section 8(3); or

(*f*) acquire, modify, provide, make available, copy or clone a password, access code or similar data and devices as defined in section 10(4).

Mark Heyink Comment on Section 6

This provision does provide some difficulty and has been grappled with in jurisdictions globally. The problem lies in the fact that hardware and software and neutral by nature. There are enumerable hardware and software tools which can be used for both good and bad purposes. Against this background the issue of intent is a critical issue, and particularly where it may be being determined by law enforcement officials who have not been trained in these spheres and to date have shown a lack of acumen in dealing with issues of this nature, this becomes an extremely dangerous provision. Unless it is understood who informs the "reasonable suspicion" in 5(3) just about anybody using any form of technology or mobile device may be unfairly prosecuted under these provisions.

This comment was previously made in a prior draft. However, the amendments which have been made to this provision do not address the problem. The issue of what and who informs the "reasonable suspicion" provided for in 5(3), or what a satisfactory "exculpatory account" may constitute are so wide and ill-defined that the section simply lends itself to abuse by law enforcement and national security agencies. In addition it has the effect of negating the presumption of innocence and placing the burden of proof on an accused.

The vagueness of these provisions threatens to achieve precisely the objectives that led to vehement opposition to the Protection of State Information Bill (the Secrecy Bill).

Another aspect of this is highlighted by the comments made by technologists. The fact is that if a lawyer with some background in this regard tasked with drafting the Bill is unable to define the crimes dealt with in the Bill properly, what chance do policemen and prosecutors who do not have the advantage of the drafters background have of determining what a reasonable suspicion may be. As the technologists have pointed out, the wide drafting of the definitions allow misinformed suspicions to be formed which could lead to significant injustice. Further, it also allows informed persons to make malicious decisions relating to suspicion of a particular crime and to do so with impunity. This should not be allowed in our law.

Unlawful interference with data

7. (1) Any person who unlawfully and intentionally interferes with—

(*a*) data; or

(*b*) critical data,

is guilty of an offence.

(2) Any person who contravenes the provisions of subsection (1) is liable, on conviction—

(*a*) in the case of a contravention of the provisions of subsection (1)(*a*), to a fine not exceeding R 5 million or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment; or

(*b*) in the case of a contravention of the provisions of subsection (1)(*b*), to a fine not exceeding R10 million or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment.

(3) For purposes of this section **"interference with data"** means to—

(*a*) alter data;

(*b*) hinder, block, impede, interrupt or impair the processing of, functioning of, access to, the confidentiality of, the integrity of, or the availability of data; or

(*c*) make vulnerable, suppress, corrupt, damage, delete or deteriorate data.

Mark Heyink Comment on Section 7

The question arises why there should be a distinction between the intentional and unlawful interference with “data” as opposed to “critical data”. While not necessarily agreeing with the definitions provided, if “data” includes by definition commercial information, disclosure of which could cause “undue advantage or disadvantage to any person”, it would appear that this unnecessarily places a different burden on the state in proving the offence and in fact weakens the existing provisions as formulated in the ECT Act.

It is submitted that this also does not take account of the position of personal information that may not fall within the definition of “critical data” but may suffer severe consequences as a result of the interference with his or her personal information. This issue is not dealt with in Section 3 dealing with personal information-related offences. In the circumstances the distinction in this provision seems artificial and not well thought

through. It is suggested that the unlawful interference with both data and critical data should be the subject of the greater penalty contemplated.

In any event this provision has the effect of limiting the penalties provided for in Section 107 of the Protection of Personal Information Act in certain instances. No maximum limit to a fine is indicated in that section. On the other hand, the penalties contemplated in 107(b) in the Protection of Personal Information Act should be increased to be aligned with Section 6(2) of the proposed Bill. Failure to do so would cause unnecessary confusion and the increased penalties in those instances seem to be more appropriate than when these provisions were last considered about 3 or 4 years ago.

It is further submitted that the South African Police Services and the National Prosecuting Authority must consider this provision carefully in light of any experience that there may be relating to Section 86(2) of the ECT Act. There is clearly a worrying lack of capacity relating to the issue of investigation and prosecution of crimes of this nature. This should be taken into consideration in determining the establishment of appropriate training and infrastructure needed to properly investigate and prosecute this crime and others contemplated in the proposed Bill. This is an issue which has regrettably long been neglected by both the SAPS and the NPA. It is also an issue which requires to be addressed in legal training at universities and should become part of the required curriculum for attorneys and advocates. Education is dealt with in greater detail in addressing further sections of this Bill.

Unlawful interference with computer device, computer network, database, critical database, electronic communications network or National Critical Information Infrastructure

8. (1) Any person who unlawfully and intentionally interferes with the use of —

(*a*) a computer device;

(*b*) a computer network;

(*c*) a database;

(*d*) a critical database;

(*e*) an electronic communications network; or

(*f*) a National Critical Information Infrastructure,

is guilty of an offence.

(2) Any person who contravenes the provisions of subsection (1) is liable, on conviction—

(*a*) in the case of a contravention of the provisions of subsection (1)(*a*), (*b*), (*c*), or (*e*), to a fine not exceeding R5 million or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment; or

(*b*) in the case of a contravention of the provisions of subsection (1)(*d*) or (*f*) to a fine not exceeding R10 million or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment.

(3) For purposes of this section "**interference with computer device, computer network, database, critical database, electronic communications network or National Critical Information Infrastructure"** means to hinder, block, impede, interrupt, alter or impair the functioning of, access to, the confidentiality of, the integrity of, or the availability of a computer device, computer network, database, critical database, electronic communications network or National Critical Information Infrastructure.

Mark Heyink Comment on Section 8

This provision betrays a lack of understanding of how security compromises may occur. Why should there be a greater penalty for interference with databases or national critical information infrastructure than for the other offences contemplated? It is easily conceivable that interference with a computer network or an electronic communications network (subject to the lower penalty) would result in an inability to use a database or national critical information infrastructure. It was strongly advised that before provisions of this nature are placed before Parliament and published for public comment that experts in information security be properly consulted relating to the realities of how computers and supporting infrastructure need to be protected and the appropriate safeguards that should be considered. This advice has gone unheeded.

As is indicated in many writings on this subject, the best approach to cybersecurity management is a collaborative partnership which includes, among others, lawyers, technology experts and information security experts. By moving outside of the safe harbour of the Model Laws around the world, which are relied on for the development of appropriate and consistent legislation have adopted this multidisciplinary approach. An example of how disregarding a multidisciplinary approach has impacted on our law lies in the ECT Act. Drafted only by lawyers without a proper understanding of the practicalities of electronic communications and transactions, for the most part the drafters stuck within the safe harbour of the Model Laws. Those provisions remain good law. However, in dealing with electronic signatures, because of their lack of understanding of how electronic signatures and public key infrastructures work, there

were several mistakes in drafting these provisions which have hampered the adoption and facilitation of reliable signatures in South Africa for the past 13 years. These same problems occur in dealing with electronic signatures in the National Credit Act. In dealing with electronic signatures the drafters sought to protect vested interests rather than protect the legal rights of citizens. These provisions in the National Credit Act are an ugly blight on our legislative landscape.

A further example in this regard is the provisions relating to electronic signatures and advanced electronic signatures in the Electronic Communications and Transactions Act. Despite the warnings provided to Parliament and the drafters relating to the deficiencies in Section 13 of the ECT Act, the Act was passed essentially as drafted by lawyers, with the acceptance of inexpert and the self-serving interests of the South African Post Office (no doubt resulting from its incestuous relationship with the Department of Communications) which instead of facilitating electronic commerce as the ECT Act intended, created a barrier to electronic signatures to the detriment of the country's electronic commercial aspirations. It took more than 5 years for accreditation regulations to be drafted by the Department of Communications and nearly 10 years before the accreditation of the first provider of advanced electronic signatures in South Africa.

These very expensive and potentially injurious misadventures can be avoided, or at least limited, if appropriate expert knowledge is sought and incorporated in the drafting of legislation designed to govern our information society and the security safeguards (information security already being a mature discipline) that have to be developed for its future advancement.

Unlawful acts in respect of malware

9. (1) Any person who assembles, obtains, sells, purchases, possesses, makes available, advertises or uses malware for the purposes of unlawfully and intentionally causing damage to—

(*a*) data;

(*b*) a computer device;

(*c*) a computer network;

(*d*) a database;

(*e*) a critical database;

(*f*) an electronic communications network; or

(*g*) a National Critical Information Infrastructure,

is guilty of an offence.

(2) Any person who is found in possession of malware in regard to which there is a reasonable suspicion that such malware is possessed for the purposes of unlawfully and intentionally causing damage to—

(*a*) data;

(*b*) a computer device;

(*c*) a computer network;

(*d*) a database;

(*e*) a critical database;

(*f*) an electronic communications network; or

(g) a National Critical Information Infrastructure,

and who is unable to give a satisfactory exculpatory account of such possession, is guilty of an offence.

(3) Any person who contravenes the provisions of subsection (1) or (2) is liable, on conviction—

(*a*) in the case of a contravention of the provisions of subsection (1)(*a*), (*b*), (*c*), (*d*) or (*f*) or (2), to a fine not exceeding R5 million or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment; or

(*b*) in the case of a contravention of the provisions of subsection (1)(*e*) or (*g*) to a fine not exceeding R10 million or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment.

(4) For purposes of this section "**malware**" means any data, electronic, mechanical or other instrument, device, equipment, or apparatus that is designed specifically to—

(*a*) create a vulnerability in respect of;

(*b*) modify or impair;

(*c*) compromise the confidentiality, integrity or availability of; or

(*d*) interfere with the ordinary functioning or usage of,

data, a computer device, a computer network, a database, a critical database, an electronic communications network, or a National Critical Information Infrastructure.

Mark Heyink Comment on Section 9

With regard to paragraph 9.1 an important element of the offence is intent. However, technology is neutral, it is how it is used and the intent behind the use that may be perfectly acceptable and proper or alternatively result in nefarious activity. For example, software designed for protecting vulnerabilities and anomalous activity in the normal course of facilitating information security would be "goodware". Exactly the same technology used by a third party for exactly the same purposes but with the intent of exploiting the vulnerabilities would be "malware". Therefore a person may be selling software that can be used for both good or bad purposes. Then the element of intent becomes very important. In our law the criminal concept of *dolus eventualis* applies and this would mean that anyone assembling, obtaining, selling, possessing, making available, advertising this software would be guilty of an offence if they could reasonably have foreseen that the software may be used for malicious as opposed to good purposes. This begs the question of what legal duty a person selling software has in establishing the purpose for which it should be used? Given the demonstrable incapacity of both the South African Police Services and the National Prosecuting Authority in this regard, this section becomes a very dangerous tool in the hands of uninformed or unscrupulous persons charged with investigation or prosecution of the proposed crime.

It is recommended that this provision is reconsidered and that its wording is redrafted to avoid this eventuality.

The comments provided above relating to "intent" apply equally to the possession of malware contemplated in Section 8(2).

This very draconian formulation loses sight of the fact that this is dependent on a subjective view may render it either "goodware" or "malware". As currently worded the mere possession allows somebody to be charged with an offence on the basis of a reasonable suspicion and they having to account for the subjective purpose for which they may have used the software. This simply runs counter to the constitutional right of innocence until proved guilty, is unconstitutional as it does not take into account any background upon which the reasonable suspicion may be grounded, or the intent with which the software may be used, save for the subjective thoughts of (at this stage on the current drafting) the person who may hold the suspicion. It should also be noted that the current lack of expertise, both in the SAPS and NPA, makes this section a very dangerous tool in the hands of unscrupulous investigators or prosecutors.

What must not be lost sight of in drafting this legislation are the revelations of Edward Snowden relating to the National Security Agency and other law enforcement elements in the USA. It has become clear that the NSA and law enforcement within the

government of the United States of America overreached their mandates, particularly with regard to the mass surveillance that has occurred. That similar overreaching of mandates occurs in other countries is also obvious. However, as a result of these revelations governments around the world are reassessing the powers afforded to national security and law enforcement agencies, particularly relating to the clear abuse of mass surveillance and disregard for privacy that has resulted. The importance of striking a balance between the reasonable requirements of national security and law enforcement against the privacy of individual citizens is receiving considerable attention. Despite this the drafters of the Bill have chosen to ignore these developments almost entirely. The attention of the drafters is drawn to the fact that their duty is to ensure that the constitutional principles on which all of our law is based are upheld. History tells us that there is simply no guarantee that governments will not abuse powers afforded to them, particularly in this sphere, in the absence of clear law and proper oversight. There can be little doubt that trust in current government has been eroded as a result of allegations and counter-allegations among its own senior members of impropriety in the National Prosecuting Authority and governance of the South African Police Services. These go far beyond political rhetoric as is evidenced by the numerous legal applications and actions which have ensued as a result of the mistrust that appears to be evident between certain executive branches and administrative branches of government. I hasten to add that I doubt that this would be any different if any of the opposition parties were in power. Against this background it would be naïve of the drafters to rely on "good faith" within government to ensure that the law is applied in accordance with the Constitution. Therefore, particularly in light of global developments, the necessary checks and balances need to be prescribed clearly and be capable of implementation and parliamentary oversight.

For the reasons offered above these provisions need to be reviewed in their entirety and redrafted with proper consideration to the constitutional rights of South African citizens.

Mark Heyink Comment on Section 9.4 (Definition of "Malware")

As previously stated technology is neutral and while it is all good and well to define malware, often identical technology can be used for good or bad purposes. Therefore the definition indicating that it is "designed specifically" immediately creates difficulties. It is not the intent at the time of the design of the software that may be of importance, it may have been designed for perfectly legitimate purposes, but the intent at the time of the use of the technology (which may be either good or bad) which is of importance from a criminal perspective.

Simply criminalising the possession of these tools places the possessor in a position where the presumption of innocence is subverted and the onus of proof unnecessarily shifted. It is believed that this runs counter to the provisions of the Constitution.

Unlawful acquisition, possession, provision, receipt or use of passwords, access codes or similar data or devices

10. (1) Any person who unlawfully and intentionally—

(*a*) acquires by any means;

(*b*) possesses;

(*c*) provides to another person; or

(*d*) uses,

an access code, password or similar data or device for purposes of contravening the provisions of section 3(1)(*a*) or (*c*) or (2)(*a*) or (*c*), 4(1), 5(1), 7(1), 8(1), 11(1), 12(1) or (2) or 13(1), is guilty of an offence.

(2) Any person who is found in possession of an access code, password or similar data or device in regard to which there is a reasonable suspicion that such access code, password or similar data or device was acquired, is possessed, or is to be provided to another person or was used or may be used for purposes of contravening the provisions of section 3(1)(*a*) or (*c*) or (2)(*a*) or (*c*), 4(1), 5(1), 7(1), 8(1), 11(1), 12(1) or (2) or 13(1), and who is unable to give a satisfactory exculpatory account of such possession, is guilty of an offence.

(3) Any person who contravenes the provisions of subsection (1) or (2), is liable, on conviction to a fine not exceeding R 5 million or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment.

(4) For purposes of this section **"passwords, access codes or similar data and devices"** means without limitation—

(*a*) a secret code or pin;

(*b*) an image;

(*c*) a security token;

(*d*) an access card or device;

(*e*) a biometric image;

(*f*) a word or a string of characters or numbers; or

(*g*) a password,

used for electronic transactions or user authentication in order to access data, a computer device, a computer network, a database, a critical database, an electronic communications network, or a National Critical Information Infrastructure or any other device or information.

Mark Heyink Comment on Section 10

It is submitted that these provisions do not take into account the realities of passwords, why we use them and their retention.

The relative strength of passwords should be commensurate with the value or sensitivity of information that is protected using the passwords. It is also determined to some degree by other security factors which may be used collaboratively with passwords. For instance credit cards and pins. A password is merely one of the factors of authentication. It is also important to recognise that the compromise of password information will in many instances not occur at the level of the owner or creator of the password. The compromise will occur with the party providing the system or information which is accessed using the password. No consideration is given to failures on the part of hosts of passwords to ensure that they remain confidential and that even if they are accessed they cannot be used by third parties. While it may be argued that this is protected in the context of the Protection of Personal Information Act requiring appropriate security, that Act does not criminalise the failure to do so, save for the extent that enforcement notices provided by the Regulator are ignored.

It is not clear what the wording “similar data or devices” means. “Computer device” is defined and is sufficient to cover for instance smartcards, tokens, USB drives and other mobile devices on which digital certificates or other forms of authorisation may be incorporated. Is it intended that a “computer device” as defined should be used in this provision. If not, what does “devices” mean? It is also submitted that similar data would be better defined to deal with data use as a factor of authentication in ensuring access to a computer device, a network, database, application, that may be contemplated in the Act and it is suggested that the redrafting of this provision be considered.

In view of the fact that the defence to this offence will often be that a person has been authorised to use the access code or password by the owner, it is suggested that consideration be given to expanding the meaning of “unlawfully” (not defined in the proposed Bill nor in the Interpretations Act) to expressly include “without authorisation of the owner”. As indicated previously, the wording in the ECT Act which deals with authorisation is in fact the wording that is favoured in information security writings. In the absence of any explanatory framework to the Bill, why the drafters have chosen to deviate from this formulation is not clear.

The question is then posed as to why the penalties for the unlawful acquisition etc. of passwords and access codes are limited. In light of the fact that the protection of access is such a critical element of information security and is probably one of the mechanisms most widely used in hacking (the commission of crimes using computers) and fraud, one would expect that the higher penalty would apply. Certainly, while in many instances it would appear that the higher penalties apply to government owned or critical information infrastructures, as there is no distinction in this provision in that regard and in light of the importance of access in information security and therefore cybersecurity, that the higher penalties would be more appropriate.

Computer related fraud

11. (1) Any person who unlawfully and intentionally, by means of data or a data message, makes a misrepresentation which—

(*a*) causes actual prejudice; or

(*b*) which is potentially prejudicial,

to another person is guilty of the offence of computer related fraud.

(2) (*a*) A court which convicts a person of an offence in terms of this section, may impose any sentence, as provided for in section 276 of the Criminal Procedure Act, 1977 (Act No. 51 of 1977), which that court considers appropriate and which is within that court's penal jurisdiction.

(*b*) A court which imposes any sentence in terms of this section must, without excluding other relevant factors, consider as aggravating factors—

(i) the fact that the offence was committed by electronic means;

(ii) the extent of the prejudice and loss suffered by the complainant as a result of the commission of such an offence; and

(iii) the extent to which the person gained financially, or received any favour, benefit, reward, compensation or any other advantage from the commission of the offence.

Mark Heyink Comment on Section 11

I am not an expert on fraud and suggest that it is important that this provision be considered by experts in this area of the law.

Paragraph 10(1)(b), in dealing with “potentially prejudicial”, appears to be unnecessarily wide. Against my limited experience in criminal law I am not certain whether “potential prejudice” is sufficient to sustain a conviction of fraud and I leave this to persons better qualified than I to consider.

Computer related forgery and uttering

12. (1) Any person who unlawfully and intentionally makes a false data document to the actual or potential prejudice of another person is guilty of the offence of computer related forgery.

(2) Any person who unlawfully and intentionally passes off a false data document to the actual or potential prejudice of another person is guilty of the offence of computer related uttering.

(3) (*a*) A court which convicts a person of an offence in terms of this section, may impose any sentence, as provided for in section 276 of the Criminal Procedure Act, 1977 (Act No. 51 of 1977), which that court considers appropriate and which is within that court’s penal jurisdiction.

(*b*) A court which imposes any sentence in terms of this section must, without excluding other relevant factors, consider as aggravating factors—

(i) the fact that the offence was committed by electronic means;

(ii) the extent of the prejudice and loss suffered by the complainant as a result of the commission of such an offence; and

(iii) the extent to which the person gained financially, or received any favour, benefit, reward, compensation or any other advantage from the commission of the offence.

(4) For purposes of this section "**data document**" means a data message containing the depiction of a document which portrays information.

Mark Heyink Comment on Section 12

My comments relating to my lack of expertise on fraud apply also to forgery and uttering.

With regard to the use of a false data document, this betrays the drafter's lack of understanding of the underlying meanings of "data message" (see prior comments relating to the definition of "data message").

There seems no reason why data message should be defined differently from in the ECT Act, particularly when it is the definition recommended in the Uncitral Model Laws on eCommerce and Signature. With regard to use of the words "data document", which is defined specifically for Section 11 in the definitions, this betrays a misunderstanding of "document" and "electronic record". A document is something that we consider to be typically in paper form. It is a printout of a data message or part of a data message. There is therefore no reason to define something as a "data document".

With the greatest respect, there appears to be no good reason why this distinction should be made, it is not supported in any writings that I know of dealing with the nature of data messages (which incorporate both the notion of communication and records) as defined in the Uncitral Model Law on which the ECT Act is founded, and serves only to create unnecessary confusion in interpretation.

It is strongly suggested that this provision is properly re-worded and that the definitions provided are considered in light of our current law and the sources from which this law is derived.

Computer related appropriation

13. (1) Any person who unlawfully and intentionally appropriates, in any manner—

(*a*) ownership in property, which ownership is vested in another person with the intention to—

(i) permanently; or

(ii) temporarily,

deprive the other person of the ownership in the property to the actual or potential prejudice of the owner of the property; or

(*b*) any other right in property, which right is vested in another person, with the intention to—

(i) permanently; or

(ii) temporarily,

deprive the other person of the right in the property to the actual or potential prejudice of the person in whom the right is vested,

is guilty of the offence of computer related appropriation.

(2) (*a*) A court which convicts a person of an offence in terms of subsection (1), may impose any sentence, as provided for in section 276 of the Criminal Procedure Act, 1977 (Act No. 51 of 1977), which that court considers appropriate and which is within that court's penal jurisdiction.

(*b*) A court which imposes any sentence in terms of this section must, without excluding other relevant factors, consider as aggravating factors—

(i) the fact that the offence was committed by electronic means;

(ii) the extent of the prejudice and loss suffered by the complainant as a result of the commission of such an offence; and

(iii) the extent to which the person gained financially, or received any favour, benefit, reward, compensation or any other advantage from the commission of the offence.

(3) For purposes of this section—

(*a*) "**property**" means—

(i) money;

(ii) credit; or

(iii) any other movable, immovable, corporeal or incorporeal thing which has a commercial value but excludes any registered patents as defined in the Patents Act, 1978 (Act No. 57 of 1978), any copyright works as defined in the Copyright Act, 1978 (Act No. 98 of 1978), or plant breeders' rights or designs as defined in the Designs Act, 1995 (Act No. 195 of 1993), or trademarks as defined in the Trademark Act, 1993 (Act 194 of 1993); and

(*b*) "**right in property**" means any right, privilege, claim or security in property and any interest therein and all proceeds thereof, and includes any of the foregoing involving any registered patents as defined in the Patents Act, 1978 (Act No. 57 of 1978), any copyright works as defined in the Copyright Act, 1978 (Act No. 98 of

1978), or plant breeders' rights or designs as defined in the Designs Act, 1995 (Act No. 195 of 1993), or trademarks as defined in the Trademark Act, 1993 (Act 194 of 1993).

Mark Heyink Comment on Section 13

The wording of Section 13(1) is not a model of clarity. It is certainly not clear what the intention of the provision is purely from its wording. However, at the meeting of the 18th February introducing the draft Bill, the indication was given that this applies to the appropriation of physical property or rights in property by providing fraudulent information which will result in records being altered that evidence the true owner of the property or rights and title in the property. It is submitted that on the basis of the confusion which was clear at the meeting that this provision should be reworded in far more specific terms than is currently the case.

It is not clear why the fact that the offences committed using electronic means should be an aggravating circumstance. Aside from anything else, while there may be limited circumstances (possibly the Commissioner for Intellectual Property and Companies) where information may be provided online, this is not the case with many government institutions which are currently paper-based. For instance, the Deeds Office, Master of the High Court etc. However, the records held in these offices may be subverted by changes in electronic records held elsewhere.

While it is appreciated that the Bill may be contemplating interaction with those institutions which are the repositories of records relating to rights in property and are to be welcomed in that regard, those institutions are equally responsible for ensuring the appropriate information security in processing information and documentation. Thus, this Bill should also impose an obligation on these institutions to institute appropriate information security when they are dealing with the rights of citizens and ensure not only the internal expertise to facilitate the security, but also that the processes are understood by parties interacting with it. Failure to do so should be a criminal offence on the part of those government institutions or the accounting officers responsible for the internal controls of those institutions.

It is an unfortunate truth that currently some (certainly not all) of the frauds which have resulted in this type of crime could have been avoided if proper authentication measures (both of the identity of originators of electronic and other communications and the integrity of the documentation) had been properly implemented and unauthorised access safeguarded against. This is the essence of cybersecurity, which is also part of this Bill. Those parties who do not develop and implement appropriate safety measures when dealing with electronic communications and records are accomplices to the crime (or at least negligent and possibly liable to the victims of the crime) and should be subject to criminal sanction. An answer to this statement may be that it is this Bill that will create the framework on which cybersecurity measures appropriate within

government are to be determined. That argument is disagreed with as those obligations already exist and there appears to be no reason why government departments who fail in their obligation of providing safeguards against the clear and present threats of using information and communications technologies in their processing of information should escape liability. On the contrary they should be models against which information and cybersecurity is gauged.

Computer related extortion

14. (1) Any person who unlawfully and intentionally—

(*a*) threatens to commit any offence under this Act; or

(*b*) commits any offence under this Act,

for the purposes of obtaining any advantage from another person, is guilty of the offence of computer related extortion.

(2) A person who contravenes the provisions of subsection (1) is liable on conviction to a fine not exceeding R10 million or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment.

Mark Heyink Comment on Section 14

This section is a slightly different formulation of Section 87 of the ECT Act. Section 87 of the ECT Act is expressly repealed in this Bill. Despite the rewording I believe that what this section achieves is materially identical to Section 87 of the ECT Act.

Examples of the SAPS and NPA's failure to create the appropriate capacity to deal with cybercrime are well documented and will be provided in oral public comment, as and when this opportunity is afforded.

Computer related terrorist activity and related offences

15. (1) Any person who unlawfully and intentionally engages in a computer related terrorist activity is guilty of an offence.

(2) Any person who unlawfully and intentionally does anything which will, or is likely to, enhance the ability of any person, entity or organisation to engage in a computer related terrorist activity, including—

(*a*) the provision of, or offering to provide, a skill or expertise;

(*b*) entering into any country or remaining therein; or

(*c*) making himself or herself available,

for the benefit of, at the direction of, or in association with any person, entity or organisation engaging in a computer related terrorist activity, and who knows or ought reasonably to have known or suspected, that such act was done for the purpose of enhancing the ability of such person, entity or organisation to engage in a computer related terrorist activity, is guilty of the offence of association with a computer related terrorist activity.

(3) Any person, entity or organisation who unlawfully and intentionally—

(*a*) provides or offers to provide data, any software or hardware tool as contemplated in section 6(5), malware as contemplated in section 9(4), a password, access code or similar data or device as contemplated in section 10(4), a computer device, a computer network, a database, an electronic communications network or any other device or equipment or any part thereof, to any other person for use by or for the benefit of a person, entity or organisation;

(*b*) solicits support for or gives support to a person, entity or organisation;

(*c*) provides, receives or participates in training or instruction, or recruits a person, entity or an organisation to receive training or instruction;

(*d*) recruits any person, entity or organisation; or

(*e*) possesses, receives or makes available data, any software or hardware tool as contemplated in section 6(5), malware as contemplated in section 9(4), a password, access code or similar data and device as contemplated in section 10(4) or a computer device, computer network, a database, an electronic communications network or any other device or equipment or any part thereof,

connected with the engagement in a computer related terrorist activity, and who knows or ought reasonably to have known or suspected that the actions referred to in paragraphs (*a*) to (*e*), are so connected, is guilty of the offence of facilitating a computer-related terrorist activity.

(4) Any person who contravenes the provisions of subsections (1), (2) or (3)) is liable on conviction to imprisonment for a period not exceeding 25 years.

(5) For purposes of this section "**computer related terrorist activity"** means any prohibited act contemplated in section 7(1), 8(1), 9(1) (in so far as it relates to the use of malware) or 14(1) —

(*a*) which—

(i) endangers the life, or violates the physical integrity or physical freedom of, or causes serious bodily injury to or the death of, any person, or any number of persons;

(ii) causes serious risk to the health or safety of the public or any segment of the public;

(iii) causes the destruction of or substantial damage to critical data, a critical database, an electronic communications network or a National Critical Information Infrastructure, whether public or private;

(iv) is designed or calculated to cause serious interference with or serious disruption of an essential service, critical data, a critical database, an electronic communications network or a National Critical Information Infrastructure;

(v) causes any major economic loss or extensive destabilisation of an economic system or substantial devastation of the national economy of a country; or

(vi) creates a serious public emergency situation or a general insurrection in the Republic,

irrespective whether the harm contemplated in paragraphs (*a*) (i) to (vi) is or may be suffered in or outside the Republic; and

Mark Heyink Comment on Section 15(5). Commentators and persons with whom I have had discussions have also indicated that the very wide definition of "general insurrection" can easily be used to censor free speech. This provision needs reconsideration.

(*b*) which is intended, or by its nature and context, can reasonably be regarded as being intended, in whole or in part, directly or indirectly, to—

(i) threaten the unity and territorial integrity of the Republic;

(ii) intimidate, or to induce or cause feelings of insecurity among members of the public, or a segment of the public, with regard to its security, including its economic security, or to induce, cause or spread feelings of terror, fear or panic in a civilian population; or

(iii) unduly compel, intimidate, force, coerce, induce or cause a person, a government, the general public or a segment of the public, or a domestic or an international organisation or body or intergovernmental organisation or body, to do or to abstain or refrain from doing any act, or to adopt or abandon a particular standpoint, or to act in accordance with certain principles,

Mark Heyink Comment on Section 15(5)(b)(iii)

A commentator who wishes to remain anonymous sets out:

"The words "coerce" and "induce" should not be in here, because if they stay in here, it will prevent political parties from launching online campaigns, the very nature of which is to coerce or induce people to abandon a specific standpoint and act in accordance with another."

whether the public or the person, government, body, or organisation or institution referred to in subparagraphs (ii) or (iii), as the case may be, is inside or outside the Republic.

Mark Heyink Comment on Section 15

I immediately confess my lack of background relating to terrorism-related legislation.

It seems that the crux of these provisions lie in the definition of computer-related terrorist activity. I am not certain why the definition confines a terrorist-related activity to only certain provisions contained in this chapter. A number of the crimes which are expressly contained in this chapter and that have been excluded from computer-related terrorist activity in terms of the definition could be a precursor to or, alternatively, part of a terrorist activity. The issue is one of intent. For instance, it is a well-known fact that person who wish to interfere with information and communications technologies will use

"zero day" vulnerabilities to achieve this. The Stuxnet Virus used by the USA and Israel against Iran nuclear installations used four different zero day vulnerabilities. By excluding the provisions of 9(2) an actor in possession of information relating to zero day vulnerabilities would, on the basis of the current definition, not necessarily be guilty of an offence of terrorism regardless of the intent of that person. Thus, if the possession of information relating to zero day vulnerabilities and the malware that would be inserted into information and communications technology infrastructures to perform the terrorist deed are in the possession of a terrorist, this would currently not be susceptible to prosecution in terms of this particular provision.

It is also not clear to me why the provisions of Sections 2, 3, 4, 5, 9, 10, 11 and 12 are omitted. It would appear to me that to a greater or lesser degree the contravention of any of those provisions where the intention is a terrorist activity should be subject to this provision. For instance, the compromise of personal information contained in all manner of records may be designed to create confusion as to a person's citizen status from a health perspective, from a criminal perspective as to offices they hold etc. All these actions are designed to create confusion and terror and depending on the success of the action may quite clearly constitute a terrorist attack. With regard to Sections 2 and 9 it is well known that identity theft and acquisition of passwords is one of the mechanisms used by terrorist organisations to commit the frauds that fund their organisations.

While again stressing my lack of background to terrorist-related legislation, I feel nonetheless that the provisions as they stand evidence a lack of appreciation of how terrorist organisations are actually conducting their activities in cyberspace.

With regard to the concept and nature of legislation relating to terrorism, what is concerning about these provisions is the vague and extremely wide wording that is used. The argument will immediately be raised that security and law enforcement need wide powers to combat terrorism but there seems to be no regard whatever for the balance and perspective of civil liberties, which is by its very nature part of an open democracy. At the moment the vagueness and wideness of the provisions simply allows agents of the state in law enforcement and national security far too wide a latitude in their actions. At a time in South Africa's history where there is an open turf-war between senior members of the executive, widespread allegations of interference with policing and prosecution, and legal claims and counterclaims being entertained by our courts relating to the structures and protections in our Constitution, the ability to use the vagueness and wide ambit of the legislation as it is drafted can only lead to repression of the freedom of expression and other civil liberties which are fundamental to the protections of the Constitution and ensuring the openness of our democracy.

The dangers of the abuse of these provisions, particularly in light of the fact of the drafters own deficiencies in understanding electronic communications and records, information security and how that security may be circumvented, allied to a

demonstrable lack of capacity in understanding these issues within law enforcement and state security, demands a rewording of these provisions. On the current wording there are very few citizens from the President across the spectrum of South African citizens who would not find themselves unwittingly branded a terrorist.

From a slightly different perspective it must also be appreciated that in determining intent one of the difficulties that we face with electronic communications is that it is very often difficult (if not impossible) to establish the context of communications. There are numerous instances of innocent communications, which taken out of context and without an appreciation of the tone of the communication, have led to unwarranted arrest, detention and court action. The vagueness of these provisions would only serve to allow this to happen or for law enforcement and state security to abuse their powers in this regard.

Computer related espionage and unlawful access to restricted data

16. (1) (*a*) Any person who unlawfully and intentionally performs or authorises, procures or allows another person to perform a prohibited act contemplated in section 3(1) or (3), in so far as it relates to the use of personal information, 4(1), 5(1), 6(1) or (2), 7(1), 8(1), 9(1) or 10(1), in order to—

(i) gain access, as contemplated in section 4(3), to critical data, a critical database or a National Critical Information Infrastructure; or

(ii) intercept data, as contemplated in section 5(3), to, from or within a critical database or a National Critical Information Infrastructure,

with the intention of directly or indirectly benefiting a foreign state or any person engaged in a terrorist activity against the Republic, is guilty of an offence.

(*b*) Any person who unlawfully and intentionally—

(i) possesses;

(ii) communicates, delivers or makes available; or

(iii) receives,

data contemplated in subsection (1)(*a*)(ii) or critical data with the intention of directly or indirectly benefiting a foreign state or any person engaged in a terrorist activity against the Republic, is guilty of an offence.

(2) (*a*) Any person who unlawfully and intentionally performs or authorises, procures or allows another person to perform a prohibited act contemplated in section 3(1) or (3), in sofar as it relates to the use of personal information, 4(1), 5(1), 6(1) or (2), 7(1), 8(1), 9(1) or 10(1), in order to gain access, as contemplated in section 4(3), to, or intercept data, as contemplated in section 5(3), which is in the possession of the State and which is classified as confidential, with the intention of directly or indirectly benefiting a foreign state or any person engaged in a terrorist activity against the Republic, is guilty of an offence.

(*b*) Any person who unlawfully and intentionally—

(i) possesses;

(ii) communicates, delivers or makes available; or

(iii) receives,

data which is in the possession of the State and which is classified as confidential, with the intention of directly or indirectly benefiting a foreign state or any person engaged in a terrorist activity against the Republic, is guilty of an offence.

(3) (*a*) Any person who unlawfully and intentionally performs or authorises, procures or allows another person to perform a prohibited act contemplated in section 3(1) or (3), in sofar as it relates to the use of personal information, 4(1), 5(1), 6(1) or (2), 7(1), 8(1), 9(1) or 10(1), in order to gain access, as contemplated in section 4(3), to or intercept data, as contemplated in section 5(3), which is in the possession of the State and which is classified as secret, with the intention of directly or indirectly benefiting a foreign state or any person engaged in a terrorist activity against the Republic, is guilty of an offence.

(*b*) Any person who unlawfully and intentionally—

(i) possesses;

(ii) communicates, delivers or makes available; or

(iii) receives,

data which is in the possession of the State and which is classified as secret, with the intention of directly or indirectly benefiting a foreign state or any person engaged in a terrorist activity against the Republic, is guilty of an offence.

(4) (*a*) Any person who unlawfully and intentionally performs or authorises, procures or allows another person to perform a prohibited act contemplated in section 3(1) or (3), in sofar as it relates to the use of personal information, 4(1), 5(1), 6(1) or (2), 7(1), 8(1), 9(1) or 10(1), in order to gain access, as contemplated in section 4(3), to or intercept data, as contemplated in section 5(3), which is in the possession of the State and which is classified as top secret, with the intention of directly or indirectly benefiting a foreign state or any person engaged in a terrorist activity against the Republic, is guilty of an offence.

(*b*) Any person who unlawfully and intentionally—

(i) possesses;

(ii) communicates, delivers or makes available; or

(iii) receives,

data which is in the possession of the State and which is classified as top secret, with the intention of directly or indirectly benefiting a foreign state or any person engaged in a terrorist activity against the Republic, is guilty of an offence.

(5) (*a*) Any person who unlawfully and intentionally performs or authorises, procures or allows another person to perform a prohibited act contemplated in section 3(1) or (3), in sofar as it relates to the use of personal information, 4(1), 5(1), 6(1) or (2), 7(1), 8(1), 9(1) or 10(1), in order to gain access, as contemplated in section 4(3), to, or intercept data, as contemplated in section 5(3), which is in the possession of the State and which is classified as confidential, is guilty of an offence.

(*b*) Any person who unlawfully and intentionally—

(i) possesses;

(ii) communicates, delivers or makes available; or

(iii) receives,

data which is in the possession of the State and which is classified as confidential, is guilty of an offence.

(6) (*a*) Any person who unlawfully and intentionally performs or authorises, procures or allows another person to perform a prohibited act contemplated in section 3(1) or (3), in sofar as it relates to the use of personal information, 4(1), 5(1), 6(1) or (2), 7(1), 8(1), 9(1) or 10(1), in order to gain access, as contemplated in section 4(3), to or intercept data which is in the possession of the State and which is classified as secret, is guilty of an offence.

(*b*) Any person who unlawfully and intentionally—

(i) possesses;

(ii) communicates, delivers or makes available; or

(iii) receives,

data which is in the possession of the State and which is classified as secret, is guilty of an offence.

(7) (*a*) Any person who unlawfully and intentionally performs or authorises, procures or allows another person to perform a prohibited act contemplated in section 3(1) or (3), in sofar as it relates to the use of personal information, 4(1), 5(1), 6(1) or (2), 7(1), 8(1), 9(1) or 10(1), in order to gain access to or intercept data which is in the possession of the State and which is classified as top secret, is guilty of an offence.

(*b*) Any person who unlawfully and intentionally—

(i) possesses;

(ii) communicates, delivers or makes available; or

(iii) receives,

data which is in the possession of the State and which is classified as top secret, is guilty of an offence.

(8) Any person who contravenes the provisions of —

(*a*) subsection (1) is liable on conviction to imprisonment for a period not exceeding 20 years;

(*b*) subsection (2) is liable on conviction to imprisonment for a period not exceeding 10 years;

(*c*) subsection (3), is liable on conviction to imprisonment for a period not exceeding 15 years;

(*d*) subsection (4) is liable on conviction to imprisonment for a period not exceeding 25 years;

(*e*) subsection (5) is liable on conviction to imprisonment for a period not exceeding 5 years;

(*f*) subsection (6) is liable on conviction to imprisonment for a period not exceeding 10 years; or

(*g*) subsection (7) is liable on conviction to imprisonment for a period not exceeding 15 years.

(8) For purposes of this section "**terrorist activity**" means—

(*a*) a computer related terrorist activity referred to in section 15 of this Act; or

(*b*) any offence referred to in the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004 (Act 33 of 2004).

Mark Heyink Comment on Section 16

The comments on each of these subsections are described by the letters (a) to (g) below:

(a) It appears that any act intended to gain access to a critical database or national critical information infrastructure with the intent of benefiting a foreign state is an offence, the conviction of which is subject to imprisonment of 20 years.

In considering this it must be remembered that a critical database may not necessarily be state-owned infrastructure, nor may critical data be information processed that is owned or controlled by the state. Therefore the issue of industrial espionage (not necessarily benefiting a foreign state) is not addressed.

A foreign state or territory is defined as "a state or territory other than the Republic". A terrorist group may be neither a territory nor a state. This issue applies to all of the different offences defined in this section. This would defeat the apparent purpose for this offence and needs to be reconsidered and properly addressed.

(b) With regard to the issue of classified information, the same objections that have been raised in connection with the Protection of State Information Bill (the Secrecy Act) apply in principle. In its current form, because of the extremely wide wording and the issues relating to classification of information, this provision seeks to circumvent the criticism that has been made relating to the protection of State Information Bill and is, in my view, unconstitutional.

(c)-(g) These provisions are subject to the same comment as provided above.

Prohibition on dissemination of data message which advocates, promotes or incites hate, discrimination or violence

17. (1) Any person who unlawfully and intentionally—

(*a*) makes available, broadcasts or distributes;

(*b*) causes to be made available, broadcast or distributed; or

(*c*) assists in making available, broadcasts or distributes,

through a computer network or an electronic communications network, to a specific person or the general public, a data message which advocates, promotes or incites hate, discrimination or violence against a person or a group of persons, is guilty of an offence.

(2) Any person who contravenes the provisions of subsection (1) is liable, on conviction to a fine or imprisonment not exceeding 2 years.

(3) For purposes of this section "**data message which advocates, promotes or incites hate, discrimination or violence**" means any data message representing ideas or theories, which advocate, promote or incite hatred, discrimination or violence, against a person or a group of persons, based on—

(*a*) national or social origin;

(*b*) race;

(*c*) colour;

(*d*) ethnicity;

(*e*) religious beliefs;

(*f*) gender;

(*g*) gender identity;

(*h*) sexual orientation;

(*i*) caste; or

(*j*) mental or physical disability.

Mark Heyink Comment on Section 17

The definition of "racist and xenophobic material" is to a large degree taken from the wording of our Constitution and in particular Section 16(2) of the Constitution. The one issue which is not covered is propaganda for war. Perhaps this should be considered to be inserted in Section 17 to ensure that the provisions contemplated in the Constitution are fully covered.

This having been said, the wide ambit of the definition of "racist and xenophobic material" is not qualified by the words "a data message which is reasonably …" as is the case with the prohibition against the incitement of violence.

Against this background it seems to the author that the "distribution" as opposed to "broadcast" of what might be defined as racist or xenophobic material by one person to another (who is not a target of the alleged racism or xenophobia) probably impinges on the constitutional right of freedom of expression. As an example, a communication by one spouse to another of information defined as racist or xenophobic and so limited in its publication that it will cause no harm, becomes an offence. If the same communication occurred verbally it is likely that it would never be discovered, however merely because that communication is made on a computer network or electronic communications network it is immediately deemed to be racist. This, in my view, aside from the subjectivity of the interpretation of racism and xenophobia, ignores context and tone and therefore endangers freedom of expression.

Prohibition on incitement of violence and damage to property

18. (1) Any person who unlawfully and intentionally—

(*a*) makes available, broadcasts or distributes;

(*b*) causes to be made available, broadcast or distributed;

(*c*) assists in making available, broadcasts or distributes,

to a specific person or the general public, through a computer network or an electronic communications network, a data message which is reasonably likely to incite—

A commentator who wishes to remain anonymous has indicated, with regard to the wording in 18(1) at "likely to incite":

"Once again we need to move away from such language, because it impedes on the constitutional right to free speech and how can something that is just likely to incite damage, without actually inciting damage an offence?"

(i) violence against; or

(ii) damage to the property belonging to,

a person or a group of persons, is guilty of an offence.

(2) Any person who contravenes the provisions of subsection (1) is liable, on conviction to a fine or imprisonment not exceeding 2 years or to both such fine and imprisonment.

Mark Heyink Comment on Section 18

The distinction between "broadcasts" or "distributes" is problematical. "Broadcasts" is not defined in the Act but it does have a clear and accepted meaning in terms of other law. "Distributes" on the other hand is not as clearly defined in our law and the wide interpretation that can be attributed to it creates unacceptable problems. These provisions need to be reconsidered.

The qualification that a data message must be "reasonably likely to incite violence" softens the potential danger of this provision. However, as with many communications, unless they are placed in proper context and the tone understood, this determination may be difficult. It is suggested that it is specifically legislated that persons who may adjudicate on these issues take into account the context, including who the audience or intended audience of the electronic communication is, the tone, was it intended lightly or was it intended seriously to incite violence, and other relevant factors.

Prohibited financial transactions

19. (1) Any person who unlawfully and intentionally participates in, processes or facilitates a financial transaction through a computer network or an electronic communications network—

(*a*) in order to promote an unlawful activity; or

(*b*) which involves the proceeds of any unlawful activity,

is guilty of the offence of committing a prohibited financial transaction.

(2) Any person who contravenes the provisions of subsection (1) is liable, on conviction to a fine not exceeding R5 million or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment.

(3) For purposes of this section "**unlawful activity**" means any conduct which contravenes any law of the Republic.

Mark Heyink Comment on Section 19

I have not made comment on this provision as I believe that comment should be forthcoming from the financial sectors that have a greater insight into dealing with financial transactions. This having been said, given the very wide scope of different financial transactions, I instinctively believe that the provision as it stands may be an over simplification and requires thought from appropriate experts.

Infringement of copyright

A commentator who wishes to remain anonymous has indicated in respect of Section 20:

"Is this necessary? The copyright act already provides this protection."

20. (1) Any person who unlawfully and intentionally, at a time when copyright exists in respect of any work, without the authority of the owner of the copyright, by means of a computer network or an electronic communications network—

(*a*) sells;

(*b*) offers for download;

(*c*) distributes; or

(*d*) otherwise makes available,

any work, which the person knows is subject to copyright and that the actions contemplated in paragraphs (*a*), (*b*), (*c*) or (*d*) will be prejudicial to the owner of the copyright, is guilty of an offence.

(2) Any person who contravenes the provisions of subsection (1), is liable on conviction to a fine or imprisonment not exceeding three years or to both such fine and imprisonment.

(3) For purposes of this section "**work**" means any—

(*a*) literary work;

(*b*) musical work;

(*c*) artistic work;

(*d*) cinematograph film;

(*e*) sound recording;

(*f*) broadcast;

(*g*) programme-carrying signal;

(*h*) published edition; or

(*i*) computer program,

which is eligible for copyright in terms of section 2 of the Copyrights Act, 1978 (Act No. 98 of 1978), or similar legislation of any State designated by the Minister by notice in the *Gazette*.

Mark Heyink Comment on Section 20

While I have had exposure to areas of intellectual property law I do not profess expertise in the subject. My simple understanding of copyright is that it is intended to protect the originality of work that can be attributed to the author or (where the author acts within the scope of his employment), the employer.

My understanding is that copyright vests automatically in a work, there is no necessity for any form of registration or even for the mark © to be associated with the work protected for the protection to occur. Further, that no “guilty knowledge” on the part of a person distributing works protected by copyright is necessary for an infringement to occur.

Against this background a simple letter which is original and which may be communicated electronically is subject to copyright. Any further passing on of this letter will immediately constitute an infringement and it appears would be subject to criminalisation in terms of this provision. I am not certain whether the drafters intended this as a possible consequence of this section and it is strongly recommended that experts in the area of intellectual property be consulted and provide comment as to whether this provision is properly aligned with our existing intellectual property law and whether it is harmonised with global developments relating to the protection of copyright.

Harbouring or concealing person who commits offence

21. (1) Any person who unlawfully and intentionally harbours or conceals a person whom he or she knows, or has reasonable grounds to believe or suspect, has committed, or is about to commit, an offence contemplated in—

(*a*) section 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 17, 18, 19 or 20; or

(*b*) any offence contemplated in section 15 or 16,

is guilty of an offence.

(2) Any person who contravenes the provisions of—

(*a*) subsection (1)(*a*), is liable, on conviction to a fine or imprisonment not exceeding two years or to both such fine and imprisonment; and

(*b*) subsection (1)(*b*), is liable, on conviction to imprisonment for a period of 10 years.

Mark Heyink Comment on Section 21

With great respect this provision is incredibly wide and has far reaching consequences which appear on the face of it to be unconstitutional and allows law enforcement powers which seem to go far further than the provisions of the Corruption Act which, as indicated, they are intended to mirror. The sheer extent of the provisions (based on "reasonable grounds to believe or suspect") is simply laying the type of foundation for a securocratic or police state that our Constitution protects against.

Attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding, or procuring to commit offence

22. Any person who unlawfully and intentionally—

(*a*) attempts;

(*b*) conspires with any other person; or

(*c*) aids, abets, induces, incites, instigates, instructs, commands, or procures another person,

to commit an offence in terms of this Chapter, is guilty of an offence and is liable on conviction to the punishment to which a person convicted of actually committing that offence would be liable.

Aggravating circumstances

23. (1) If a person is convicted of any offence in terms of this Chapter, a court which imposes any sentence in terms of this Chapter must, without excluding other relevant factors, consider as an aggravating factor the fact that the offence was committed in concert with one or more persons.

(2) If a person is convicted of any offence provided for in section 3, 4, 5, 7, 8 or 10, a court which imposes any sentence in terms of those sections must, without excluding other relevant factors, consider as an aggravating factor the fact that the offence was committed by a person, or with the collusion or assistance of that person, who as part of his or her duties, functions or lawful authority—

(*a*) is responsible for the processing of personal information or financial information, which personal information or financial information was involved in any offence provided for in section 3;

(*b*) is in charge of, in control of, or has access to data, a computer device, a computer network, a database, a critical database, an electronic communications network, or a National Critical Information Infrastructure or any part thereof which was involved in any offence provided for in section 4, 5, 7 and 8; or

(*c*) is the holder of a password, access code or similar data or device which was used to commit any offence provided for in section 10.

(3) If a person contemplated in subsection (2) is convicted of the offence in question, a court must, unless substantial and compelling circumstances exist which justify the imposition of another sentence as prescribed in paragraphs (*a*) or (*b*) of this subsection, impose, with or without a fine, in the case of—

(*a*) a first contravention of section 3, 4, 5, 7, 8 or 10, a period of direct imprisonment of no less than half of the period of imprisonment prescribed by the section which is contravened; and

(*b*) any second or subsequent contravention of section 3, 4, 5, 7, 8 or 10, the maximum period of imprisonment prescribed by the section which is contravened.

Savings

24. The provisions of this Chapter do not affect criminal liability in terms of the common law or any other legislation.

CHAPTER 3

JURISDICTION

Mark Heyink Comment on Chapter 3

In our information society one of the burning issues relating to the prosecution of cybercrime is that of jurisdiction. Against this background the issue of international cooperation, dealt with in Chapter 4 below, is of critical importance, as are the conventions that apply relating to jurisdiction. For instance in the field of intellectual property, several conventions have been developed and parties to the conventions will uphold within their jurisdictions the rights of owners of intellectual property in other jurisdictions (eg. the Rome Convention and Madrid Convention). In the context of cybercrime, the Budapest Convention (Council of Europe Convention on Cybercrime) and the African Union Convention on Cybersecurity and Personal Data Protection are both important instruments in this regard. It should remembered that South Africa was a signatory to the Budapest Convention on Cybercrime in 2002 and it is only 13 years later that through this draft legislation it is beginning to place itself in a position to properly take advantage of international cooperation in this regard.

While the African Union Convention is of far more recent vintage, it appears to have prompted the Department of Justice and shaken government from the state of lethargy in regard to cybercrime, which has been evident for many years. It is hoped that taking the African Union Convention seriously will also promote other areas of law, including the protection of personal information which has suffered inordinate delays at the hands of the Department of Justice, and necessary capacity building within the Department of Justice to deal with electronic communications and transactions in terms of the provisions of the ECT Act properly and in line with its duty to provide these services to South Africa in the 21st century.

Equally, it is hoped that as jurisdiction is a “two way street”, that the necessary diplomatic effort will be initiated in this regard. This is not clear from the draft Bill itself and in the absence of a clear framework or policy in this regard from the Department of Justice, these are issues which the Department of Justice should address and provide appropriate assurances as to how it will deal with these issues, failing which, as is so often the case, we will end up with strong legislative frameworks but a lack of capacity and often a lack of appropriate political will, required to fulfil the purposes of the legislation.

Jurisdiction

25. (1) A court in the Republic trying an offence in terms of this Act has jurisdiction where—

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

(*b*) any act or omission in preparation for the offence or any part of the offence was committed in the Republic, or where any result of the offence has had an effect in the Republic;

(*c*) the offence was committed in the Republic or outside the Republic by a South African citizen or a person with permanent residence in the Republic or by a person carrying on business in the Republic; or

(*d*) the offence was committed on board any ship or aircraft registered in the Republic or on a voyage or flight to or from the Republic at the time that the offence was committed.

(2) If the act or omission alleged to constitute an offence under this Act occurred outside the Republic, a court of the Republic, regardless of whether or not the act or omission constitutes an offence at the place of its commission, has jurisdiction in respect of that offence if the person to be charged—

(*a*) is a citizen of the Republic;

(*b*) is ordinarily resident in the Republic;

(*c*) was arrested in the territory of the Republic, or in its territorial waters or on board a ship or aircraft registered or required to be registered in the Republic at the time the offence was committed;

(*d*) is a company, incorporated or registered as such under any law, in the Republic; or

(*e*) any body of persons, corporate or unincorporated, in the Republic.

(3) Any act or omission alleged to constitute an offence under this Act and which is committed outside the Republic by a person, other than a person contemplated in subsection (2), is, regardless of whether or not the act or omission constitutes an offence or not at the place of its commission, deemed to have also been committed in the Republic if that—

(*a*) act or omission affects or is intended to affect a public body, a business or any other person in the Republic;

(*b*) person is found to be in South Africa; and

(*c*) person is for one or other reason not extradited by South Africa or if there is no application to extradite that person.

(4) Where a person is charged with attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring to commit an offence or as an accessory after the offence, the offence is deemed to have been committed not only at the place where the act was committed, but also at every place where the person acted or, in case of an omission, should have acted.

CHAPTER 4

POWERS TO INVESTIGATE, SEARCH AND ACCESS OR SEIZE AND INTERNATIONAL COOPERATION

Mark Heyink Comment on Chapter 4

From Chapter 4 onwards in the Bill the emphasis is not on cybercrime but on cybersecurity and the measures necessary to deal with cybersecurity. The necessity to provide powers to investigate, search and access or seize, specifically relating to cybercrime, are essential elements of a modern society and are long overdue. The provisions as they are currently drafted and the mechanisms for combatting cybercrime that they facilitate are not commented on by me in any detail as I am not an expert on criminal procedure. However, this having been said, the powers that are granted in

terms of the proposed draft Bill, emanating as they do from the JCPS Cluster, are heavily biased in favour of law enforcement and impact significantly on the civil liberties of citizens.

The NCPF mentions the issue of privacy, but in the drafting of this Bill it is virtually ignored. This is despite international frameworks globally highlighting the importance of the balance that must be struck between law enforcement and national security on the one hand and the right of privacy on the other.

This not a trivial issue. Events over the past year relating to the revelation by Edward Snowden (and others) of the disregard for privacy in fulfilling national security obligations by governments has led to a sea change in how powers are granted to law enforcement and national security agencies are to be exercised. Further, what controls must be in place to prevent the erosion of civil liberties and in particular the right of privacy, which is a constitutional right in South Africa. The impact of the overreaching of powers by national security and law enforcement agencies has been emphasised recently by the European Court of Justice declaring the safe harbour protections governing the flow of information between the United States and European Union countries to be invalid. This has very severe economic consequences in our information society where not only are our economies dependent on information and communications technologies, but a significant part of our economy lies in the processing of information (much of which is personal information).

It is submitted that the drafters have failed to take this into account in drafting these sections of the Bill and that they require significant research and debate by taking into account what has occurred globally and ensuring that the Bill is properly aligned with international developments. Unless and until the measures contemplated in the Protection of Personal Information Act have been properly implemented in South Africa (the delays being entirely in the hands of government at this time) it will be impossible to align our legislation with international developments.

With regard to international cooperation, while recognition is made of its importance in the NCPF and South Africa is a party to conventions dealing with cybersecurity and requiring international cooperation, little has been done by the powers that be to properly establish a cooperative effort and there is no evidence in the drafting of these provisions that any effort has been made to work with parties to the international instruments in determining their appropriateness in this regard.

It is also noted that consultation process embarked upon by the Department in coming to this point in drafting the Bill is seriously flawed. In essence it strongly reflects the views of the JDPS Cluster without consideration for the views of other interested parties. Without putting too fine a point on it, the process to date has been a “show consultation” in the same manner as some governments have “show” trials”.

It is fully appreciated that national security and law enforcement have elements which do not fall within the public domain. It is noted that the NCPF Framework which has been published has been published as the “public version”. This having been said, the development of that framework has been made largely in the absence of public/private partnerships, and engagements on cybersecurity requirements that are foundational elements in all credible cybersecurity frameworks. The lack of engagement with industry, civil society and academia to date is in stark contrast to the stated principles of the NCPF, which are to foster cooperation and coordination between the public sector, private sector and civil society.

Definitions and interpretation

26. For purposes of this Chapter, unless the context indicates otherwise—

"**access**" means to make use of, to gain entry to, to view, display, to retrieve, to copy data, or otherwise make use of a computer device, a computer network, a database, a critical database, an electronic communications network or a National Critical Information Infrastructure or their accessories or components or any part thereof;

"**article**" means any data, a computer device, a computer network, a database, a critical database, an electronic communications network or a National Critical Information Infrastructure or any part thereof or any other information, instrument, device or equipment which—

(*a*) is concerned in, connected with or is, on reasonable grounds, believed to be concerned in or connected with the commission or suspected commission;

(*b*) may afford evidence of the commission or suspected commission; or

(*c*) is intended to be used or is, on reasonable grounds, believed to be intended to be used in the commission,

of an offence in terms of this Act or any other offence which may be committed by means of or facilitated through, the use of an article, whether within the Republic or elsewhere;

"**investigator**" means an appropriately qualified, fit and proper person, who is not a member of a law enforcement agency, and who is appointed by the National Commissioner or the Director-General: State Security, on the strength of his or her expertise in order to, subject to the control and directions of a member of a law

enforcement agency, assist a law enforcement agency in an investigation in terms of this Act;

Comment on Definition of "investigator"

While this provision has been amended from the initial draft, the provision that a person be appointed "on the strength of his or her expertise" needs to be further qualified. It is suggested that it be dealt with by way of regulation and that some benchmark for the expertise established. An appropriate amendment is indicated.

"**designated judge**" means a designated judge as defined in section 1 of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act No. 70 of 2002);

"law enforcement agency" means—

(*a*) the South African Police Service referred to in section 5 of the South African Police Service Act, 1995 (Act No. 68 of 1995); and

(b) the State Security Agency referred to in section 3(1) of the Intelligence Services Act, 2002 (Act No. 65 of 2002);

"magistrate" includes a regional court magistrate;

"**public available data**" means data which is accessible in the public domain without restriction; and

"specifically designated member of a law enforcement agency" means—

(*a*) a commissioned officer referred to in section 33 of the South African Police Service Act, 1995 (Act No. 68 of 1995), who has been designated in writing by the National Commissioner; or

(*b*) a member as defined in section 1 of the Intelligence Services Act, 2002 (Act No. 65 of 2002), who has has been designated in writing by the Director-General: State Security;

to—

(i) make oral applications for a search warrant or an amendment of a warrant contemplated in section 30;

(ii) issue expedited preservation of data directions contemplated in section 40; or

(iii) serve a disclosure of data direction from the designated judge on a person or electronic communications service provider contemplated in section 41(7).

Comment on Definition of "specifically designated member of a law enforcement agency"

In what manner will a person evidence the authority required in terms of this section, to make an oral application for a search warrant, issue expedited preservation of data directions or serve disclosure of data direction? While this may well be dealt with in regulations, this also needs to be considered in the Bill. In the absence of any background or framework in this regard, it is difficult to make cogent comment. It is also noted that they are not restricted by any existing legislation but are, in terms of Section 27 in addition to the provisions of that legislation. Therefore, to the extent that they are more extensive than the existing legislation, the necessary checks and balances on the exercise of these powers is a critical element of this Bill.

Application of provisions in this Chapter

27. The provisions of this Chapter apply in addition to—

(*a*) Chapter 2 of the Criminal Procedure Act, 1977 (Act No. 51 of 1977), or any other applicable law which regulates the search and accessing or seizure of articles connected with offences; and

(*b*) Chapter 2 of the International Co-operation in Criminal Matters Act, 1996 (Act No. 75 of 1996), which regulates the mutual provision of evidence in criminal matters.

Search for and access to or seizure of, certain articles

28. Any member of a law enforcement agency or an investigator accompanied by a member of a law enforcement agency may, in accordance with the provisions of this Chapter, access or seize any article, whether within the Republic or elsewhere.

Mark Heyink Comment on Section 28

I have grave concerns relating to the failure to balance the rights of privacy (including issues relating to decryption which are being hotly debated globally) with the provisions

as they stand. With respect, it appears from the drafting of this Bill, little attention has been paid to the issues of privacy in terms of the Protection of Personal Information Act or the frameworks of the European Union or African Union in this regard.

Against the failure of the drafters to provide any form of background research, justification or comment and the stubborn insistence by the JCPS Security Cluster to deal with issues of cybersecurity in the covert manner that it has done as opposed to the transparency that is required in our Constitution, cogent comment is made difficult, if not impossible.

In view of the damage that can result from unlawful seizure of information and communications technologies, particularly where what is required is information hosted on hardware supporting those technologies, it would be wise for consideration to be given to the cautionary rules that have been developed by our courts in connection with Anton Piller Orders. While appreciating that these are apply by their nature to civil proceedings, recognition of appropriate mechanisms of search and seizure to avoid legitimate processing of information that may be interrupted by search and seizure should be taken into account. See further comment on the comment provided to Section 30.

Article to be accessed or seized under search warrant

29. (1) Subject to the provisions of sections 31, an article referred to in section 28 can only be accessed or seized by virtue of a search warrant issued—

(*a*) by a magistrate or judge of the High Court, on written application by a member of a law enforcement agency, if it appears to the magistrate or judge, from information on oath or by way of affirmation that there are reasonable grounds for believing that an article is—

(i) within his or her area of jurisdiction; or

(ii) being used or is involved in the commission of an offence—

(*aa*) within his or her area of jurisdiction; or

(*bb*) within the Republic, if it is unsure within which area of jurisdiction the article is being used or is involved in the commission of an offence; or

(*b*) by a magistrate or judge presiding at criminal proceedings, if it appears to such magistrate or judge that an article is required in evidence at such proceedings.

(2) A search warrant issued under subsection (1) must require a member of a law enforcement agency or an investigator who is accompanied by a member of a law enforcement agency to access or seize the article in question and, to that end, must authorize the member of a law enforcement agency or an investigator who is accompanied by a member of the law enforcement agency to—

(*a*) search any person identified in the warrant;

(*b*) enter and search any container, premises, vehicle, facility, ship or aircraft identified in the warrant;

(*c*) search any person who is believed, on reasonable grounds, to be able to furnish any information of material importance concerning the matter under investigation and who is found near such container, on or at such premises, vehicle, facility, ship or aircraft;

(*d*) search any person who is believed, on reasonable grounds, to be able to furnish any information of material importance concerning the matter under investigation and who—

(i) is nearby;

(ii) uses; or

(ii) is in possession of or in direct control of,

any data, computer device, computer network, database, critical database, electronic communications network or National Critical Information Infrastructure identified in the warrant to the extent as is set out in the warrant;

(*e*) access and search any data, computer device, computer network, database, critical database, electronic communications network or National Critical Information Infrastructure identified in the warrant to the extent as is set out in the warrant;

(*f*) obtain and use any instrument, device, equipment, password, decryption key, data or other information that is believed, on reasonable grounds, to be

necessary to access or use any part of any data, computer device, computer network, database, critical database, electronic communications network or National Critical Information Infrastructure identified in the warrant to the extent as is set out in the warrant;

(*g*) copy any data or other information to the extent as is set out in the warrant; or

(*h*) seize an article identified in the warrant to the extent as is set out in the warrant.

(3) For purposes of subsection (2), whenever a search warrant issued under subsection (1), authorises an investigator who is accompanied by a member of the law enforcement agency to search any person, the search of such a person must, subject to section 35(2), be carried out by a member of the law enforcement agency accompanying the investigator.

(4) (*a*) A search warrant may be executed at any time, unless the person issuing the warrant in writing specifies otherwise.

(*b*) A search warrant may be issued on any day and is of force until it is executed or is cancelled by the person who issued it or, if such person is not available, by a person with like authority.

(5) A member of a law enforcement agency or an investigator who is accompanied by a member of a law enforcement agency who executes a warrant under this section must, upon demand by any person whose rights in respect of any search or article accessed or seized under the warrant have been affected, hand to him or her a copy of the warrant.

Oral application for search warrant or amendment of warrant

30. (1) An application referred to in section 29(1)(*a*), or an application for the amendment of a warrant issued in terms of section 29(1)(*a*), may be made orally by a specifically designated member of a law enforcement agency, if it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written application.

(2) An oral application referred to in subsection (1) must—

(*a*) indicate the particulars of the urgency of the case or the other exceptional circumstances which, in the opinion of the member of the law enforcement agency, justify the making of an oral application; and

(*b*) comply with any supplementary directives relating to oral applications issued by the Judges President of the respective Divisions of the High Court.

(3) A magistrate or judge of the High Court may, upon an oral application made to him or her in terms of subsection (1) and subject to subsection (4), issue a warrant.

(4) A warrant may only be issued under subsection (3)—

(*a*) if the magistrate or judge of the High Court concerned is satisfied, on the facts alleged in the oral application concerned, that—

(i) there are reasonable grounds to believe that a warrant applied for could be issued;

(ii) a warrant is necessary immediately in order to access or seize or search for an article within his or her area of jurisdiction or an article which is being used or is involved in the commission of an offence—

(*aa*) within his or her area of jurisdiction; or

(*bb*) within the Republic, if it is unsure within which area of jurisdiction the article is being used or is involved in the commission of an offence; and

(iii) it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written application for the issuing of a warrant; and

(*b*) on condition that the member of the law enforcement agency concerned must submit a written application to the magistrate or judge of the High Court concerned within 48 hours after the issuing of the warrant under subsection (3).

(5) A warrant issued under subsection (3) must be in writing and must be transmitted electronically to the member of the law enforcement agency.

(6) A magistrate or judge of the High Court who has issued a warrant under subsection (3) or, if he or she is not available, any other magistrate or judge of the High Court must, upon receipt of a written application submitted to him or her in terms of subsection (4)(*b*), reconsider that application whereupon he or she may confirm, amend or cancel that warrant.

Mark Heyink Comment on Section 30

These provisions are, with respect, defective in light of the comment made on the definition of "specifically designated member of a law enforcement agency". No provision is made for a magistrate to properly identify the person seeking a warrant.

In addition the whole issue of the urgency of warrants, while understandable in certain circumstances, needs to ensure that there are proper checks and balances and facilitates the ability of a person or organisation which is subject to the warrant to be properly protected, particularly in relation to computers and information that may be seized. In this regard, particularly in relation to information, there should be specific provisions relating to the copying of information at a particular time without necessarily preventing the use of the information or computers processing the information. As computers and the processing of information in many cases are essential elements of business which may be conducted by an individual or an organisation, the prevention of the continuance of business by virtue of searches and seizures is, with respect, not adequately dealt with.

What is also not dealt with is that while specifically designated members of law enforcement agencies will deal with on what grounds an authority be obtained, nothing is said of the expertise that is needed to perform searches and seizures appropriately, secure electronic information properly, and ensure that no harm is done which will unnecessarily hamper the lawful use of the information or computers which may be subject to the search.

While assurances may be granted by law enforcement that the capability exists in this regard, and may indeed be in place to a very limited degree, for the most part this capability does not exist and there has been a failure on the part of government to address this incapacity, at least since promulgation of the Electronic Communications and Transactions Act. From my own experience and from reliable sources who provided me with information in this regard, this problem is real and while it may be claimed is dealt with in this legislation, it is mentioned peripherally without any substantive background information as to how this issue is to be addressed.

Search and access or seizure without search warrant

31. Any member of a law enforcement agency or an investigator who is accompanied by a member of a law enforcement agency may, without a search warrant, execute the powers referred to in section 29(2) of this Act, subject to any other law if the person who has the lawful authority to consent to the—

(*a*) search for and access to or seizure of the article in question; or

(*b*) search of a container, premises, vehicle, facility, ship, aircraft, data, computer device, computer network, database, critical database, electronic communications network or a National Critical Information Infrastructure,

consents, in writing, to such search and access to or seizure of the article in question.

Mark Heyink Comment on Section 31

This provision is very glibly phrased. No consideration is given as to whether the consent is informed or that the consent must be provided prior to the search, access or seizure. It simply, as is the case with so many sections of the Bill, provides law enforcement with powers which go beyond what is reasonable, particularly in light of the failures to consider the nature of electronic information as opposed to physical artefacts and provide appropriate checks and balances with the exercise of these powers.

Search and seizure for and access to article on arrest of person

32. (1) On the arrest of any person on suspicion that he or she has committed—

(*a*) an offence under this Act; or

(*b*) any other offence,

a member of a law enforcement agency may search the arrested person and seize any article referred to in section 28 which is in the possession of, in the custody of or under the direct control of, the arrested person.

(2) A member of a law enforcement agency or an investigator who is accompanied by a member of a law enforcement agency may access and search any article referred to in subsection (1).

Assisting member of law enforcement agency or investigator

33. (1) An electronic communications service provider or person, other than the person who is suspected of having committed an offence under this Act, who is in control of any container, premises, vehicle, facility, ship, aircraft, data, computer device, computer network, database, critical database, electronic communications network or National Critical Information Infrastructure or any other information, instrument, device or equipment that is subject to a search authorised in terms of section 29(1) or 30(3) or which takes place in terms of section 31 must, if required, provide—

(*a*) technical assistance; and

(*b*) such other assistance as may be necessary,

to the member of the law enforcement agency or investigator who is accompanied by a member of a law enforcement agency in order to—

(i) access or use any data, computer device, computer network, database, critical database, electronic communications network or National Critical Information Infrastructure or any other information, instrument, device or equipment;

(ii) copy data or other information;

(iii) obtain an intelligible output of data; or

(iv) remove a computer device, any part of a computer network, database, critical database, electronic communications network or National Critical Information Infrastructure.

(2) An electronic communications service provider or person who fails to comply with the provisions of subsection (1) is guilty of an offence and is liable on conviction to a fine not exceeding R5 million or imprisonment not exceeding 5 years or to both such fine and imprisonment.

Obstructing or hindering member of law enforcement agency or investigator who is accompanied by member of law enforcement agency and authority to overcome resistance

34. (1) Any person who obstructs or hinders a member of a law enforcement agency or an investigator who is accompanied by a member of a law enforcement agency in the exercise of his or her powers or the performance of his or her duties or functions in terms of this Chapter or who refuses or fails to comply with a search warrant issued in terms of section 29(1), section 30(3) or which takes place in terms of section 31, is guilty of an offence and is liable on conviction to a fine not exceeding R5 million or imprisonment not exceeding 5 years or to both such fine and imprisonment.

(2) (*a*) A member of a law enforcement agency or a member of a law enforcement agency who accompanies an investigator who may lawfully execute any power conferred upon him or her in terms of section 29(2) of this Act, may use such force as may be reasonably necessary, proportional to all the circumstances relating to the execution of such powers.

(*b*) No member of a law enforcement agency may enter upon or search any premises, vehicle, facility, ship or aircraft unless he or she has audibly demanded admission to the premises, vehicle, facility, ship or aircraft and has notified the purpose of his or her entry.

(*c*) The provisions of paragraph (*b*) do not apply where the member of a law enforcement agency is, on reasonable grounds, of the opinion that an article which is the subject of the search may be destroyed, disposed of or tampered with if the provisions of paragraph (*b*) are complied with.

Powers conferred upon member of law enforcement agency or investigator who is accompanied by member of law enforcement agency to be conducted in decent and orderly manner with due regard to rights of other persons

35. (1) The powers conferred upon member of a law enforcement agency or an investigator who is accompanied by a member of a law enforcement agency in terms of section 29(2) of this Act, must be conducted —

(*a*) with strict regard to decency and order; and

(*b*) with due regard to the the rights, responsibilities and legitimate interests of other persons in proportion to the severity of the offence.

(2) If a female needs to be searched physically in terms of section 29(2)(*a*), (*c*) or (*d*) or section 32 of this Act, such search must be carried out by a member of a law enforcement agency who is also a female: Provided that if no female member of a law enforcement agency is available, the search must be carried out by any female designated for that purpose by a member of a law enforcement agency.

Wrongful search and access or seizure and restriction on use of instrument, device, password or decryption key or information to gain access

36. (1) A member of a law enforcement agency or an investigator—

(*a*) who acts contrary to the authority of a search warrant issued under section 29(1) or section 30(3); or

(*b*) who, without being authorized thereto under this Chapter or the provision of any other law which affords similar powers to a member of a law enforcement agency or investigator—

(i) accesses, searches, copies or seizes data, a computer device, any part of a computer network, a database, a critical database, an electronic communications network or a National Critical Information Infrastructure or any other information, instrument, device or equipment; or

(ii) obtains any instrument, device, password, decryption key or other information that is necessary to access or uses data, a computer device, any part of a computer network, a database, a critical database, an

electronic communications network or a National Critical Information Infrastructure,

is guilty of an offence and is liable on conviction to a fine not exceeding R300 000 or imprisonment for a period not exceeding 3 years or to both such fine and imprisonment.

(2) A member of a law enforcement agency or an investigator who obtains or uses any instrument, device, equipment, password, decryption key, data or other information contemplated in section 29(2)(*f*)—

(*a*) must use the instrument, device, equipment, password, decryption key, data or information only in respect of and to the extent specified in the warrant to gain access to or use data, a program, a computer data storage medium, a computer device, any part of a computer network, a database, any part of an electronic communications network or any part of an electronic communications infrastructure in the manner and for the purposes, specified in the search warrant concerned; and

(*b*) must destroy all information if—

(i) it will not be required for purposes of any criminal or civil proceedings contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act or for purposes of evidence or for purposes of an order of court; or

(ii) no criminal proceedings or civil proceedings as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act, are to be instituted in connection with such information.

(3) The provisions of subsection (2) apply with the necessary changes required by the context to a search and access or seizure without a search warrant contemplated in section 31 or access to and search of an article contemplated in section 32(2).

(4) A member of a law enforcement agency or an investigator who fails to comply with subsections (2) or (3), is guilty of an offence and is liable on conviction to a fine not exceeding R300 000 or imprisonment for a period not exceeding 3 years or to both such fine and imprisonment.

(5) Where a member of a law enforcement agency or an investigator is convicted of an offence referred to in subsection (1) or (4), the court convicting such a person, may upon application of any person who has suffered damage, or upon the application of the prosecutor acting on the instructions of that person, award compensation in respect of such damage, whereupon the provisions of section 300 of the Criminal Procedure Act, 1977 (Act No. 51 of 1977), apply with the necessary changes, with reference to such award.

Mark Heyink Comment on Section 36

The drafting of these provisions really makes no distinction between search and seizure of physical goods and of information. Given the demonstrable lack of capacity and competence within the SAPS in this regard and the fact that the seizure of information and communications technologies as opposed to the information being processed on the technologies may cause considerable harm to the owner or possessors of the information and communications technologies, this provision is far too open-ended and may be subject to the malice of complainants and overzealous enforcement by law enforcement authorities.

It must be born in mind that search warrants are obtained on the basis of only one side of the story and not allowing a party adversely affected by a search warrant to state its case is contrary to the rule of natural justice *audi alterem partem*. Thus, allowing these powers without appropriate restrictions (as has been developed in our civil courts relating to Anton Piller Orders) is, it is submitted, not only extremely dangerous but manifestly unconstitutional.

The addition of sub-section 5 in the initial draft of these provisions is to be welcomed. However, it does not appear that the objection initially raised to sub-section (4) which is, in light of the extensive powers assigned to law enforcement in terms of the provisions of Chapter 4 of this Bill and the penalties attributed to offences in terms of this Act generally, allied to the known difficulties in prosecuting improper behaviour of members of law enforcement and the security services, the penalties proposed are completely out of line with the potential consequences of improper behaviour on the part of law enforcement.

False information under oath or by way of affirmation

37. (1) Any person who gives false information under oath or by way of affirmation knowing it to be false or not knowing it to be true, with the result that a search warrant is issued, or is issued and executed, or a search contemplated in section 31 took place on the basis of such information, is guilty of an offence and is

liable on conviction to a fine or to imprisonment for a period not exceeding 2 years or to both such fine and imprisonment.

(2) Where a person is convicted of an offence referred to in subsection (1), the court convicting such a person, may upon application of any person who has suffered damage, or upon the application of the prosecutor acting on the instructions of that person, award compensation in respect of such damage, whereupon the provisions of section 300 of the Criminal Procedure Act, 1977 (Act No. 51 of 1977), apply with the necessary changes, with reference to such award.

Mark Heyink Comment on Section 37

The comment provided in Section 36 above applies equally to this provision.

The importance of this provision should not be underestimated. In my experience it has occurred on several occasions that search warrants relating to seizure of information and in some cases computer equipment on which the information is hosted, is based on speculation on the part of complainants. Unfortunately the lack of competence of investigating officers in this regard is often used as a mechanism to, either avoid prosecuting when it suits the SAPS, or maliciously harassment of owners of information and communications technologies, pressurising them into extortionate agreements. I have personal experience of both instances. It is strongly suggested that the provisions of this section should be carefully considered to address the specifics of this type of behaviour on the part of a complainant. It is also suggested that consequential amendments to sections relating to the issue of search warrants should also be considered.

Prohibition on disclosure of information

38. (1) No person, investigator, member of a law enforcement agency, electronic communications service provider or an employee of an electronic communications service provider may disclose any information which he, she or it has obtained in the exercise of his, her or its powers or the performance of his, her or its duties in terms of this Act, except—

(*a*) to any other person who of necessity requires it for the performance of his or her functions in terms of this Act;

(*b*) if he or she is a person who of necessity supplies such information in the performance of his or her functions in terms of this Act;

(*c*) if it is information which is required in terms of any law or as evidence in any court of law;

(*d*) if it constitutes information-sharing—

(i) contemplated in Chapter 6 of this Act; or

(ii) between electronic communications service providers, the South African Police Service or any other person or entity which is aimed at preventing, investigating or mitigating cybercrime or relating to aspects of cyber security:

Provided that such information-sharing may not prejudice any criminal investigation or criminal proceedings;

(*e*) to any competent authority which requires it for the institution of criminal proceedings or an investigation with a view to instituting criminal proceedings.

(2) A person, investigator, member of a law enforcement agency, electronic communications service provider or an employee of an electronic communications service provider who contravenes the provisions of subsection (1) is guilty of an offence and is liable on conviction to a fine not exceeding R5 million or imprisonment not exceeding 5 years or to both such fine and imprisonment.

Interception of data

39. (1) The interception of data which is an indirect communication as defined in section 1 of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act No. 70 of 2002), must take place in terms of an interception direction issued in terms of section 16 of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act No. 70 of 2002), and must, subject to subsection (3), be dealt with further in the manner provided for in that Act.

(2) If no interception direction has been issued, the interception of data on an ongoing basis, which is real-time communication-related information as defined in section 1 of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act No. 70 of 2002), must take place in terms of a real-time communication-related direction issued in terms of section 17 of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act No. 70 of 2002), and must, subject to subsection (3), be dealt with further in the manner provided for in that Act.

(3) Data referred to in subsection (1) or (2), which is intercepted at the request of an authority, court or tribunal exercising jurisdiction in a foreign State must, after the interception, be dealt with in the manner provided in an order referred to in section 46(6), which is issued by the designated judge.

Expedited preservation of data direction

40. (1) A specifically designated member of a law enforcement agency may, if he or she on reasonable grounds believes that any person or an electronic communications service provider, which is not required to provide an electronic communications service which has the capability to be intercepted or to store communication-related information, as contemplated in section 30 of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act No. 70 of 2002), may receive, is in possession of, or is in control of data—

(*a*) which is relevant to;

(*b*) which was used or may be used in;

(*c*) for the purposes of or in connection with;

(*d*) which has facilitated or may facilitate; or

(*e*) which may afford evidence of,

the commission or intended commission of—

(i) an offence under Chapter 2 of this Act;

(ii) any other offence in terms of the laws of the Republic which is or was committed by means of, or facilitated by, the use of an article; or

(iii) an offence—

(*aa*) similar to those contemplated in Chapter 2 of this Act; or

(*bb*) substantially similar to an offence recognised in the Republic which is or was committed by means of, or facilitated by the use of an article,

in a foreign State,

issue an expedited preservation of data direction to such a person or electronic communications service provider.

(2) An expedited preservation of data direction must be in the prescribed form and must be served on the person or electronic communications service provider affected thereby, in the prescribed manner by a member of a law enforcement agency.

(3) An expedited preservation of data direction must direct the person or electronic communications service provider affected thereby, from the time of service of the direction, and for a period of 120 days—

(*a*) to preserve the current status of;

(*b*) not to deal in any manner with; or

(*c*) to deal in a certain manner with,

the data referred to in the direction in order to preserve the availability and integrity of the data.

(4) No data may be disclosed to a law enforcement agency on the strength of an expedited preservation of data direction unless it is authorised in terms of section 41.

(5) The 120 day period referred to in subsection (3), may only be extended by way of a preservation of evidence direction contemplated in section 42 of this Act.

(6) A person or electronic communications service provider to whom an expedited preservation of data direction referred to in subsection (1) is addressed, may, in writing, apply to a magistrate in whose area of jurisdiction the person or electronic communications service provider is situated, for an amendment or the cancellation of the direction concerned on the ground that he, she or it cannot timeously or in a reasonable fashion, comply with the direction.

(7) The magistrate to whom an application is made in terms of subsection (6) must, as soon as possible after receipt thereof—

(*a*) consider the application and may for this purpose, order oral or written evidence to be adduced regarding any fact alleged in the application;

(*b*) give a decision in respect of the application; and

(*c*) inform the applicant and member of the law enforcement agency referred to in subsection (1) of the outcome of the application.

(8) A person or an electronic communications service provider referred to in subsection (1) who—

(*a*) fails to comply with an expedited preservation of data direction or contravenes the provisions of subsection (4); or

(*b*) makes a false statement in an application referred to in subsection (6),

is guilty of an offence and is liable on conviction to a fine not exceeding R5 million or imprisonment not exceeding 5 years or to both such fine and imprisonment.

Disclosure of data direction

41. (1) Subject to sections 15(2), 16 and 17 of the Regulation of Interception of Communications and Provision of Communication-related information Act, 2002 (Act No. 70 of 2002), and subsection (4), a magistrate or judge of the High Court, may on written application by a member of a law enforcement agency, if it appears to the magistrate or judge, from information on oath or by way of affirmation that there are reasonable grounds for believing that a person or electronic

communications service provider may receive, is in possession of, or is in control of data which is relevant to or which may afford evidence of, the commission or intended commission of—

(*a*) an offence under Chapter 2 of this Act; or

(*b*) any other offence in terms of the laws of the Republic which is or was committed by means of, or facilitated by the use of an article,

issue a disclosure of data direction.

(2) An application contemplated in subsection (1) must—

(*a*) contain the identity of the member of the law enforcement agency who applies for the disclosure of data direction;

(*b*) identify the customer, if known, or the service or communication in respect of whom data is to be provided;

(*c*) identify the person or electronic communications service provider to whom the disclosure of data direction must be addressed;

(*d*) contain a description of the data which must be provided;

(*e*) contain a description of the offence which has been or is being or will probably be committed; and

(*f*) comply with any supplementary directives relating to applications for expedited disclosure of data issued by the Judges President of the respective Divisions of the High Court.

(3) Upon receipt of an application in terms of subsection (1), a magistrate or judge, must satisfy himself or herself—

(*a*) that there are reasonable grounds for believing that—

(i) an offence in terms of Chapter 2 of this Act; or

(ii) any other offence in terms of the laws of the Republic which is or was committed by means of, or facilitated by the use of an article,

has been, is being or will probably be committed or that it is necessary to determine whether such an offence has been so committed; and

(*b*) that it will be in the interests of justice if a disclosure of data direction is issued.

(4) (*a*) The designated judge, may on request of an authority, court or tribunal of a foreign State, if it appears to the designated judge, from information on oath or by way of affirmation that there are reasonable grounds for believing that any person or electronic communications service provider in the Republic may receive, is in possession of, or is in control of data which is relevant to, or which may afford evidence of, the commission or intended commission of an offence—

(i) similar to those contemplated in Chapter 2 of this Act; or

(ii) any other offence substantially similar to an offence recognised in the Republic which is or was committed by means of, or facilitated by the use of an article,

in a foreign State, issue, subject to paragraph (*b*), a disclosure of data direction.

(*b*) The designated judge must, before a disclosure of data direction as contemplated in paragraph (*a*) is issued, inform the Cabinet member responsible for the administration of justice, in writing of the—

(i) fact that he or she intends to issue a disclosure of data direction; and

(ii) reasons for such decision.

(5) A request contemplated in subsection (4) must—

(*a*) identify the customer, if known, or the service or communication in respect of whom data is to be provided;

(*b*) identify the person or electronic communications service provider to whom the disclosure of data direction must be addressed;

(*c*) contain a description of the data which must be provided;

(*d*) contain a description of the offence which has been or is being or will probably be committed; and

(*e*) comply with any supplementary directives relating to applications for disclosure of data issued by the designated judge.

(6) Upon receipt of a request in terms of subsections (4), the designated judge must satisfy himself or herself—

(*a*) that there are reasonable grounds for believing that an offence—

(i) similar to those contemplated in Chapter 2 of this Act; or

(ii) substantially similar to an offence recognised in the Republic which is or was committed by means of, or facilitated by the use of an article,

in the requesting foreign State, has been committed or that it is necessary to determine whether such an offence has been so committed and that an investigation in respect thereof is being conducted in the requesting foreign State;

(*b*) that the request, where applicable, is in accordance with—

(i) any treaty, convention or other international agreement to which that foreign state and the Republic are parties; or

(ii) any agreement with any foreign State entered into in terms of section 65 of this Act; and

(*c*) that it will be in the interests of justice if a disclosure of data direction is issued.

(7) A disclosure of data direction must be in the prescribed form and must be served on the person or electronic communications service provider affected thereby, in the prescribed manner by a member of a law enforcement agency or in the case of subsection (4), a specifically designated member of a law enforcement agency.

(8) The disclosure of data direction—

(*a*) must direct the person or electronic communications service provider to provide data identified in the direction to the extent as is set out in the direction to an identified member of the law enforcement agency;

(*b*) must set out the period within which the data identified in paragraph (*a*) must be provided; and

(*c*) may specify conditions or restrictions relating to the provision of data authorised therein.

(9) A person or electronic communications service provider to whom a disclosure of data direction referred to in subsection (7) is addressed, may in writing apply to the magistrate or judge or the designated judge for an amendment or the cancellation of the direction concerned on the ground that he, she or it cannot timeously or in a reasonable fashion, comply with the direction.

(10) The magistrate or judge or the designated judge to whom an application is made in terms of subsection (9) must, as soon as possible after receipt thereof—

(*a*) consider the application and may, for this purpose, order oral or written evidence to be adduced regarding any fact alleged in the application;

(*b*) give a decision in respect of the application; and

(*c*) if the application is successful, inform the law enforcement agency or authority, court or tribunal of a foreign State, of the outcome of the application.

(11) A person or an electronic communications service provider who—

(*a*) fails to comply with a disclosure of data direction; or

(*b*) makes a false statement in an application referred to in subsection (9),

is guilty of an offence and is liable on conviction to a fine not exceeding R5 million or imprisonment not exceeding 5 years or to both such fine and imprisonment.

Preservation of evidence direction

42. (1) A magistrate or judge of the High Court, may on written application by a member of a law enforcement agency, if it appears to the magistrate or judge, from information on oath or by way of affirmation that there are reasonable grounds for believing that any person or electronic communications service provider may receive, is in possession of, or is in control of an article—

(*a*) relevant to;

(*b*) which was used or may be used in;

(*c*) for the purpose of or in connection with;

(*d*) which has facilitated or may facilitate; or

(*e*) may afford evidence of,

the commission or intended commission of—

(i) an offence under Chapter 2 of this Act;

(ii) any other offence in terms of the laws of the Republic which is or was committed by means of, or facilitated by the use of an article; or

(iii) an offence—

(*aa*) similar to those contemplated in Chapter 2 of this Act; or

(*bb*) any other offence substantially similar to an offence recognised in the Republic which is or was committed by means of, or facilitated by the use of an article,

in a foreign State,

issue a preservation of evidence direction.

(2) A preservation of evidence direction must be in the prescribed form and must be served on the person or electronic communications service provider affected thereby, in the prescribed manner by a member of a law enforcement agency.

(3) The preservation of evidence direction must direct the person or electronic communications service provider, from the time of service of the direction, and for the time period specified in the direction, immediately—

(*a*) to preserve the current status of;

(*b*) not to deal in any manner with; or

(*c*) to deal in a certain manner with,

an article in order to preserve the integrity of the evidence.

(4) Any person or electronic communications service provider who fails to comply with a preservation of evidence direction is guilty of an offence and is liable on conviction to a fine not exceeding R5 million or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment.

(5) A person or electronic communications service provider to whom a preservation of evidence direction referred to in subsection (1) is addressed, may in writing apply to a magistrate or judge of the High Court in whose area of jurisdiction the person or electronic communications service provider is situated for an amendment or the cancellation of the direction concerned on the ground that he, she or it cannot timeously or in a reasonable fashion, comply with the order.

(6) The magistrate or judge of the High Court to whom an application is made in terms of subsection (5) must, as soon as possible after receipt thereof—

(*a*) consider the application and may, for this purpose, order oral or written evidence to be adduced regarding any fact alleged in the application;

(*b*) give a decision in respect of the application; and

(*c*) inform the applicant and law enforcement agency of the outcome of the application.

Mark Heyink Comment on Section 42

Specifically in dealing with personal information, the preservation of evidence has to be carefully considered. It is recommended that the court only provide an order against not just a written application but information provided on how the preservation order may impact on personal information. The international outrage at law enforcement requiring vast tracts of information to be provided by service providers to it, revealed by Edward Snowden and now admitted to by a number of service providers, has important and far-reaching privacy ramifications. This needs to be taken into consideration in dealing with these provisions.

Oral application for preservation of evidence direction

43. (1) An application referred to in section 42(1), may be made orally by a member of a law enforcement agency, if he or she is of the opinion that it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written application.

(2) An oral application referred to in subsection (1) must—

(*a*) indicate the particulars of the urgency of the case or the other exceptional circumstances which, in the opinion of the member of the law enforcement agency, justify the making of an oral application; and

(*b*) comply with any supplementary directives relating to oral applications issued by the Judges President of the respective Divisions of the High Court.

(3) A magistrate or judge of the High Court may, upon an oral application made to him or her in terms of subsection (1), issue the preservation of evidence direction applied for.

(4) A preservation of evidence direction may only be issued under subsection (3) —

(a) if the magistrate or judge of the High Court concerned is satisfied, on the facts alleged in the oral application concerned, that—

(i) there are reasonable grounds to believe that a preservation of evidence direction applied for could be issued;

(ii) a preservation of evidence direction is necessary immediately in order to preserve the integrity of the evidence; and

(iii) it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written application for the issuing of the preservation of evidence direction applied for; and

(*b*) on condition that the member of the law enforcement agency concerned must submit a written application to the magistrate or judge of the High Court concerned within 48 hours after the issuing of the preservation of evidence direction under subsection (3).

(5) A preservation of evidence direction issued under subsection (3) must be in writing and must be transmitted electronically to the member of the law enforcement agency.

(6) A magistrate or judge of the High Court who issued a direction under subsection (3) or, if he or she is not available, any other magistrate or judge of the High Court must, upon receipt of a written application submitted to him or her in terms of subsection (4)(*b*), reconsider that application whereupon he or she may confirm, amend or cancel that preservation of evidence direction.

Mark Heyink Comment on Section 43

It is submitted that the dangers of the potential abuse of this provision, which are already commented on relating to section 30 of the Bill, become even more important in dealing with oral applications. It is submitted that the powers afforded to law enforcement in this draft provision are far too extensive and in dealing with the preservation of evidence, oral applications should not be permitted.

Access to data and receipt and forwarding of unsolicited information

44. (1) Any member of a law enforcement agency or an investigator may, without being specifically authorised thereto in terms of this Chapter—

(*a*) access public available data regardless of where the data is located geographically;

(*b*) access or receive non-public available data, regardless of where the data is located geographically, if the person who has the lawful authority to disclose the data, voluntarily—

(i) in writing, consents to such accessing of data; or

(ii) provides the data to a member of a law enforcement agency or an investigator; or

(c) access any data, regardless of where the data is located geographically, if such data is lawfully—

(i) accessible from; or

(ii) available to,

a computer device, a computer network, a database, a critical database, an electronic communications network or a National Critical Information Infrastructure which is being accessed or seized in terms of section 29, 30, 31 or 32.

(2) The head of a law enforcement agency may, after obtaining the written approval of the National Director of Public Prosecutions as contemplated in subsection (3), forward any information obtained during any investigation to a law enforcement agency of a foreign State when that head of a law enforcement agency is of the opinion that the disclosure of such information may—

(*a*) assist the foreign State in the initiation or carrying out of investigations regarding an offence committed within the jurisdiction of a foreign State; or

(*b*) lead to further cooperation with a foreign State to carry out an investigation regarding the commission or intended commission of—

(i) an offence under Chapter 2 of this Act;

(ii) any other offence in terms of the laws of the Republic which may be committed or facilitated by means of an article; or

(iii) an offence—

(*aa*) similar to those contemplated in Chapter 2 of this Act; or

(*bb*) any other offence substantially similar to an offence recognised in the Republic which is or was committed by means of, or facilitated by the use of an article,

in a foreign State.

(3) The National Director of Public Prosecutions must consider a request by a head of a law enforcement agency in terms of subsection (2) and may only grant approval referred to in subsection (2) if he or she is satisfied that the forwarding of information —

(*a*) will not affect any pending criminal proceedings or investigations adversely regarding criminal offences committed within the Republic; and

(*b*) is in accordance with any applicable law of the Republic.

(4) A law enforcement agency may receive any information from a foreign State which will—

(*a*) assist the law enforcement agency in the initiation or carrying out of investigations regarding an offence committed within the Republic; or

(*b*) lead to further cooperation with a foreign State to carry out an investigation regarding the commission or intended commission of—

(i) an offence under Chapter 2 of this Act; or

(ii) any other offence in terms of the laws of the Republic which may be committed by means of or facilitated by, an article.

Mark Heyink Comment on Section 44

In the first instance “public available data” is not defined. This does not take account of the principles relating to privacy of information in which, even where information may be publicly available, its use may be defined by the purpose of the processing of the information.

Further, the provisions of the Protection of Personal Information Act, which are studiously avoided throughout the discussion of the Cybercrimes and Cybersecurity Bill, also apply. The provisions of this section should also include the express requirement that, in the case of personal information, it is only the data subject who may consent to the provision of the information to law enforcement. In light of the lamentable failure of the Department of Justice to deal with the implementation of the Protection of Personal Information Act, issues of this nature relating to lawful authority may be confusing. In any event what is also ignored in the provisions as they stand is the office of the Regulator in terms of the Protection of Personal Information Act. In many circumstances the lawful processing of personal information, including whether it may be provided to law enforcement, will be the remit of regulations and rulings under the control of the Regulator.

As is evidenced throughout this document, the checks and balances necessary for the processing of information of whatever nature but in particular personal information, have been, by design or unwittingly, omitted from the consideration of the proposed draft legislation. This is out of line with the European Union Convention on Cybercrime, the African Union Convention on Cybersecurity (which devotes considerable guidance to this requirement) and all credible frameworks for cybersecurity and the inherent cybercrime provisions in this type of legislation.

Issuing of direction requesting foreign assistance and cooperation

45. (1) If it appears to a magistrate or judge of the High Court from information on oath or by way of affirmation that there are reasonable grounds for believing that an article necessary for the investigation or prosecution of—

(*a*) an offence under Chapter 2 of this Act; or

(*b*) any other offence in terms of the laws of the Republic which may be committed or facilitated by means of an article,

is in the possession of, under the control of or upon any person or in a container, upon or at any premises, vehicle, facility, ship, aircraft, computer device, computer network,

database or any part of an electronic communications network within the area of jurisdiction of a foreign State, the magistrate or the judge may issue a direction in the prescribed form, in which assistance from that foreign State is sought in order to—

(i) preserve an article; or

(ii) intercept or obtain and provide data,

as is stated in the direction.

(2) A direction contemplated in subsection (1) must specify that—

(*a*) there are reasonable grounds for believing that an offence contemplated in this Act has been committed in the Republic or that it is necessary to determine whether an offence has been committed;

(*b*) an investigation in respect thereof is being conducted; and

(*c*) for purposes of the investigation, it is necessary, in the interests of justice, that the article be preserved, or that data be intercepted or obtained and be provided by a person or authority in a foreign State.

(3) Subject to subsection (4), a direction must be sent to the National Director of Public Prosecutions for transmission to—

(*a*) the court or tribunal specified in the direction;

(*b*) the appropriate authority in the foreign State which is requested to provide assistance and cooperation; or

(*c*) a designated 24/7 contact point in the foreign State which is requested to provide assistance and cooperation.

(4) (*a*) In a case of urgency a direction may be transmitted directly to the court or tribunal referred to in subsection (3)(*a*), exercising jurisdiction in the place where the article is to be preserved, or the data is to be intercepted or obtained and be provided, or to the appropriate government authority referred to in subsection (3)(*b*) or designated 24/7 contact point referred to in subsection (3)(*c*).

(*b*) The National Director of Public Prosecutions must, as soon as practicable, be notified that a direction has been sent in the manner referred to in paragraph (*a*) and he or she must be furnished with a copy of such direction.

(5) The Cabinet member responsible for the administration of justice must be notified that a direction has been sent as contemplated in subsection (3) or (4) and must be furnished with a copy of such direction.

Foreign requests for assistance and cooperation

46. (1) A request by an authority, court or tribunal exercising jurisdiction in a foreign State for assistance in preserving an article or the interception or the obtaining and providing of data in the Republic for use by such foreign State must be submitted—

(*a*) to the 24/7 point of contact established in terms of section 49 of this Act, which must submit it—

(i) to the National Director of Public Prosecutions; or

(ii) in a case of urgency, to the designated judge;

(*b*) to the National Director of Public Prosecutions; or

(*c*) in a case of urgency, to the designated judge.

(2) Upon receipt of a request in terms of subsection (1)(*a*)(i) or (*b*), the National Director of Public Prosecutions must satisfy himself or herself—

(*a*) that proceedings have been instituted in a court or tribunal exercising jurisdiction in the requesting foreign State; or

(*b*) that there are reasonable grounds for believing that an offence has been committed in the requesting foreign State or that it is necessary to determine whether an offence has been so committed and that an investigation in respect thereof is being conducted in the requesting foreign State.

(3) Upon receipt of a request in terms of subsection (1)(*a*)(ii) or (*c*), the designated judge, must—

(*a*) satisfy himself or herself—

(i) that proceedings have been instituted in a court or tribunal exercising jurisdiction in the requesting foreign State; or

(ii) that there are reasonable grounds for believing that an offence has been committed in the requesting foreign State or that it is necessary to determine whether an offence has been so committed and that an investigation in respect thereof is being conducted in the requesting foreign State; and

(*b*) obtain the recommendations of the National Director of Public Prosecutions on the request.

(4) For purposes of subsection (2) and (3)(*a*), the National Director of Public Prosecutions or the designated judge may rely on a certificate purported to be issued by a competent authority in the foreign State concerned, stating the facts contemplated in the said subsections.

(5) (*a*) The National Director of Public Prosecutions must, if satisfied as contemplated in subsection (2), submit the request for assistance in preserving an article or intercepting or obtaining and providing data, together with his or her recommendations, to the Cabinet member responsible for the administration of justice, for his or her approval.

(*b*) Upon being notified of the Cabinet member's approval the National Director of Public Prosecutions must forward the request contemplated in subsection (1)(*a*) or (*b*) to the designated judge, for consideration.

(6) (*a*) Subject to subsection (7), the designated judge may on receipt of a request referred to—

(i) in subsection (1)(*a*)(ii) or (*c*), subject to paragraph (*b*); or

(ii) in subsection (5)(*b*),

issue any order which he or she deems appropriate to ensure that the requested—

(*aa*) article is preserved for a period; or

(*bb*) data is intercepted or obtained and provided,

as is specified in the request.

(*b*) The designated judge must, before any order as contemplated in paragraph (*a*) is issued, inform the Cabinet member responsible for the administration of justice, in writing of the—

(i) fact that he or she intends to issue an order; and

(ii) reasons for such decision.

(7) The designated judge may only issue an order contemplated in subsection (6)(*a*), if—

(*a*) on the facts alleged in the request, there are reasonable grounds to believe that—

(i) an offence substantially similar to the offences contemplated in Chapter 2 of this Act, has been or is being or will probably be committed; or

(ii) any other offence substantially similar to an offence recognised in the Republic was committed by means of, or facilitated through the use of an article; and

(iii) that for purposes of the investigation it is necessary in the interests of justice that an article be preserve for a period or that data be intercepted or obtained and provided;

(*b*) the request clearly identifies—

(i) the article that must be preserved;

(ii) the data which must be intercepted or obtained and be provided; and

(iii) the person, entity or electronic communications service provider—

(*aa*) who or which is in possession of the article that must be preserved;

(*bb*) from whose facilities the data must be intercepted and provided; or

(cc) from whom the data must be obtained or provided;

(*c*) the request is, where applicable, in accordance with—

(i) any treaty, convention or other international agreement to which that foreign state and the Republic are parties; or

(ii) any agreement with any foreign State entered into in terms of section 65 of this Act;

(*d*) the order contemplated in subsection (6)(*a*) is in accordance with any applicable law of the Republic; and

(*e*) that it will be in the interests of justice if the order contemplated in subsection 6(*a*) is made.

(8) An order contemplated in subsection (6)(*a*) must be executed by a member of the South African Police Service referred to in section 33 of the South African Police Service Act, 1995 (Act No. 68 of 1995), who is specifically designated in writing by the National Commissioner to execute such orders.

Complying with order of designated judge

47. (1) A person or electronic communications service provider must immediately comply with an order of the designated judge issued in terms of section 46(6).

(2) A person or electronic communications service provider to whom an order referred to in section 46(6) is addressed, may in writing apply to the designated judge for an amendment or the cancellation of the order concerned on the ground that he, she or it cannot timeously or in a reasonable fashion, comply with the order.

(3) The designated judge to whom an application is made in terms of subsection (2) must, as soon as possible after receipt thereof—

(*a*) consider the application and may, for this purpose, order oral or written evidence to be adduced regarding any fact alleged in the application;

(*b*) give a decision in respect of the application; and

(*c*) if the application is successful, inform the National Director of Public Prosecutions of the outcome of the application.

(4) A person or an electronic communications service provider who—

(*a*) fails to comply with an order referred to in section 46(6); or

(*b*) makes a false statement in an application referred to in subsection (2),

is guilty of an offence and is liable on conviction to a fine not exceeding R5 million or imprisonment not exceeding 5 years or to both such fine and imprisonment.

Informing foreign State of outcome of request for assistance and cooperation and furnishing of data to foreign State

48. (1) The National Director of Public Prosecutions must inform a foreign State of the outcome of its request for assistance and cooperation**.**

(2) Any data which is intercepted or obtained in terms of an order referred to in section 46(6) of this Act, must be—

(*a*) provided to the 24/7 Point of Contact, established in terms of section 49 of this Act, for submission to an authority, court or tribunal of a foreign State, in an industry-standard format which ensures ease of access to the information and which guarantees the authenticity, integrity and reliability of the information; and

(*b*) accompanied by—

(i) a copy of the order referred to in section 46(6); and

(ii) an affidavit in the prescribed form by the person or authorised representative of an electronic communications service provider, verifying the authenticity, integrity and reliability of the information that is furnished.

(3) A person or electronic communications service provider must keep copies of any the information which is furnished to the 24/7 Point of Contact in terms of subsection (2)(*a*), for a period of three years, in a manner which will ensure the authenticity, integrity and reliability of the information.

(4) The information referred to in subsection (2)(*a*), together with the copy of the order and affidavit referred to in subsection (2)(*b*), must be provided to the authority, court or tribunal exercising jurisdiction in a foreign State which requested the assistance in terms of section 46(1), in the manner agreed upon.

(5) A person or electronic communications service provider who—

(*a*) fails to comply with subsections (2) or (3);

(*b*) makes a false statement in an affidavit referred to in subsection (2)*(b)*(ii),

is guilty of an offence and is liable on conviction to a fine or imprisonment not exceeding 3 years or to both such fine and imprisonment.

Mark Heyink Comment on Section 48

Subject to prior comment, the wording of this section does not give rise to any difficulty. However, what is noted is that, while this section expressly provides that copies of information be maintained by electronic service providers in a manner that will ensure the authenticity, integrity and reliability of the information, nowhere in the proposed provisions is the same obligation relating to evidence obtained by law enforcement to ensure appropriate security of the information and evidence obtained. There seems to be no reason why law enforcement should not be compelled to ensure authenticity, integrity and reliability of information in the same manner as with physical artefacts it is required to ensure a credible chain of custody. The same principles apply and that is that the integrity of the evidence is to be maintained.

CHAPTER 5

24/7 POINT OF CONTACT

At a consultative meeting by the Department of Justice on the 18th February 2015, Mr Robbertse indicated that this provision has been included in the legislation to ensure compliance with the European Union Convention on Cybercrime. As more fully indicated in the comment on Chapter 6, the comment provided on this chapter must be considered against the background of the failure of the drafters to provide any framework within which this legislation is drafted, any background research and/or the failure to declassify the NCFP until halfway through the period for comment on the Bill. Against these deficiencies consideration of this Bill is conducted in a vacuum. As information pervades every area of our information society in the 21st century, not only are these deficiencies undesirable but it is submitted that they will lead to bad law.

It also needs to be stressed that the drafting of legislation as “show legislation” is merely to say that we have legislation in place, but failing to address this within an appropriate policy framework, and without consideration for the capacity required to implement, monitor and enforce the law (including an assessment of the political will to the application of appropriate resources, essential for its operation), is as disingenuous as installing a toilet bowl without the necessary plumbing.

Against the failure of the Department of Justice’s provision of information, questions as opposed to comment arise.

- Why is the 24/7 point of contact dealt with outside of the structures to deal with cybersecurity in Chapter 6?
- What is the hierarchy of authority in dealing with cybersecurity and where does the 24/7 point of contact fit in?
- Among its obligations appears to be the coordination of the activities of the 24/7 point of contact with other cybersecurity functions. Is it intended that the 24/7 point of contact also coordinates activities between those functions in their interaction with one another?
- The reporting structure of the 24/7 point of contact appears to be confined to law enforcement authorities and goes no higher than the cabinet minister responsible for policing. What are the obligations of the Minister to report to Parliament relating to the activities of the 24/7 point of contact?

Subject to answers that may be provided to these questions, the following comment is made. Currently, while conceptually the establishment of the Cybersecurity Hub has been authorised, no funds have been made available, for a considerable period of time to allow for its establishment and to perform the duties that it is supposed to perform. It seems that there are strong overlaps between the concept of the 24/7 point of contact and the cybersecurity hub. The duplication appears to be totally unnecessary and ill-advised in view of the dearth of information security skills within government and failures by government to address capacity building. The separation of duties evident in Chapter 6 and in the provisions relating to the 24/7 point of contact appear to be unnecessary and will simply result in inefficiencies and a bloated infrastructure relating to cybersecurity that the country can ill-afford.

It was also indicated at the meeting of the 18th February that a 24/7 point of contact has been established. As a person who deals with information and cybersecurity on a daily basis I have no knowledge of how the 24/7 point of contact may be used. I am fairly confident that only a minuscule fraction of the members of the public have any knowledge of this either. Had I known about this I would have taken advantage of it to deal with certain matters where it is plain that the South African Police Services are incapable of providing mechanisms to report cybercrimes.

My ignorance in this regard is also is a reflection of the failure of the Department of Justice to provide proper background information motivating some of the drafting of the Bill.

It is assumed that it is intended that this point of contact will be an online facility in the future but what is not clear is how the investigation of offences in terms of Chapter 2 of the Act are to be dealt with. Currently the position is that there is a dire lack of capacity on the part of the South African Police Services relating to the investigation of cybercrimes. This comment is not anecdotal, it is empirical. No indication is given as to

how these critical deficiencies in skills in the 21st century will be addressed to make the investigative skills available to the general public and victims of offences in Chapter 2 of the Act.

What is also not addressed is whether the 24/7 point of contact has any duties relating to offences detailed in the Protection of Personal Information Act and which may have data subjects desire to have them prosecuted, alternatively the Regulator have these offences prosecuted. While Chapter 2 deals with certain offences, it does not deal with all of the offences contemplated in the Protection of Personal Information Act. In fact, in stark contrast to other frameworks and the consideration given to the protection of personal information in the African Union Convention, the failure by the drafters to properly consider the importance of the protection of personal information, the breach of which is the largest contributor to providing information for the commission of cybercrimes contemplated in the Bill, is astounding.

It is strongly urged that the Regulator remains the primary arbiter of issues relating to personal information and consideration be given as to how the Regulator may use the provisions of this Bill to fulfil the duties set out in the Protection of Personal Information Act.

Neither the Discussion Paper of the Cybercrimes and Cybersecurity Bill nor the NCFP provide any guidance in this regard. The former simply restates the provisions in the Bill, and the latter does not address it at all.

Establishment of 24/7 Point of Contact

49. (1) The Cabinet member responsible for policing must, in consultation with the Cabinet member responsible for national financial matters—

(a) establish an office to be known as the 24/7 Point of Contact for the Republic; and

(*b*) equip, operate and maintain the 24/7 Point of Contact.

(2) The Cabinet member responsible for policing exercises final responsibility over the administration and functioning of the 24/7 Point of Contact.

(3) (*a*) The National Commissioner must appoint a member of the Service—

(i) who, on the grounds of his or her technical knowledge and experience, is a suitable and qualified person; and

(ii) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State security,

as Director of the 24/7 Point of Contact.

(*b*) The Director must exercise the powers and must perform the functions and carry out the duties conferred upon, assigned to or imposed upon him or her by the National Commissioner or under this Act, subject to the control and directions of the National Commissioner.

(*c*) Whenever the Director is for any reason temporarily unable to exercise, perform and carry out his or her powers, functions and duties, the National Commissioner must appoint a member of the Service—

(i) who on the grounds of his or her technical knowledge and experience, is a suitable and qualified person; and

(ii) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State security,

as acting Director.

(*d*) The Director must, in the exercise of the powers, performance of the functions and carrying out of the duties conferred upon, assigned to or imposed upon him or her by the National Commissioner or under this Act, be assisted, subject to his or her control and directions, by—

(i) appropriately qualified members of the Service designated to the 24/7 Point of Contact and to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State security;

(ii) a member of the National Prosecuting Authority at the rank of at least Deputy-Director of Public Prosecutions—

(*aa*) who has particular knowledge and skills in respect of any aspect dealt with in this Act;

(*bb*) who is seconded to the 24/7 Point of Contact to assist the Director; and

(*cc*) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State Security; and

(iii) any person or entity—

(*aa*) who or which has particular knowledge and skills in respect of any aspect dealt with in this Act;

(*bb*) who or which is appointed to assist the Director from time to time; and

(*cc*) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State Security.

(*e*) In order to achieve the objects of this Act, the Director must—

(i) carry out the administrative duties relating to the functioning of the 24/7 Point of Contact;

(ii) exercise control over the persons contemplated in subsection (3)(*d*);

(iii) manage and exercise administrative and technical control over the 24/7 Point of Contact;

(iv) regulate the procedure and determine the manner in which the provisions of this Act must be carried out by the 24/7 Point of Contact; and

(v) co-ordinate the activities of the 24/7 Point of Contact with those of the Cyber Security Centre, the Government Security Incident Response teams, the Cyber Crime Response Centre, the Cyber Command, the Cyber Security Hub and the Private Sector Security Incident Response Teams.

(*f*) The Director is, for the purposes of the exercising the powers, performing the functions and carrying out of the duties conferred upon, assigned to or imposed upon him or her by the National Commissioner or under this Act, accountable to the National Commissioner regarding any matter relevant to, incidental to or which may impact on the objects and functions of the 24/7 Point of Contact as set out in subsection (4).

(*g*) The Director must, on a monthly basis, or as the National Commissioner requires, submit a written report to the National Commissioner regarding any matter relevant to, incidental to or which may impact on the objects and functions of the 24/7 Point of Contact as set out in subsection (4).

(*h*) The Director must, on a quarterly basis, or as the Chairperson of the Cyber Response Committee requires, submit a written report to the Cabinet member responsible for policing and the Chairperson of the Cyber Response Committee regarding any matter relating to this Act which the Director wishes to or may want to bring to the attention of the Cyber Response Committee.

(4) (*a*) The 24/7 Point of Contact must operate on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate expedited assistance for the purpose of proceedings or investigations regarding the commission or intended commission of—

(i) an offence under Chapter 2 of this Act;

(ii) any other offence in terms of the laws of the Republic which may be committed or facilitated by means of an article; or

(iii) an offence—

(*aa*) similar to those contemplated in Chapter 2 of this Act; or

(*bb*) any other offence substantially similar to an offence recognised in the Republic which is or was committed by means of, or facilitated by the use of an article,

in a foreign State.

(*b*) The assistance contemplated in subsection (4)(*a*), includes—

(i) the provision of technical advice and assistance;

(ii) the facilitation or provision of assistance regarding anything which is authorised under Chapter 4 of this Act;

(iii) the provision of legal information;

(iv) the identification and location of an article;

(v) the identification and location of a suspect; and

(vi) cooperation with appropriate authorities of a foreign State.

(5) The Cabinet member responsible for policing may, after consultation with the Cyber Response Committee, make regulations to further—

(*a*) regulate any aspect provided for in subsection (4);

(*b*) impose additional duties on the 24/7 Point of Contact; and

(*c*) regulate any aspect which is necessary or expedient for the proper implementation of this section.

(6) (*a*) The Cabinet member responsible for policing must, at the end of each financial year, submit a report to Chairperson of the Joint Standing Committee on Intelligence established by section 2 of the Intelligence Services Control Act, 1994 (Act 40 of 1994), on the functions and activities of the 24/7 Point of Contact.

(*b*) The report contemplated in paragraph (*a*) must include—

(i) the number of matters in which technical advice and assistance were provided to a foreign State; and

(ii) the number of matters in which technical advice and assistance were received from a foreign State.

CHAPTER 6

STRUCTURES TO DEAL WITH CYBER SECURITY

As previously stated, the task of providing cogent comment is rendered extremely difficult by the Department of Justice's failure to follow any recognised processes in the development of legislation. There is a total absence of background information and with

regard to this particular chapter, the documents necessary to consider in providing comment remain classified, although a “Public Version” of the NCFP was published in mid-October (halfway through the period allowed for public comment on the Bill) it does provide limited insight into what is intended by government. The covertness within which the Department of Justice and the Department of State Security is dealing with these issues is simply quite unnecessary.

While it is acknowledged that there may be limited elements of cybersecurity which fall within the remit of law enforcement and state security and which possibly are not appropriate to be dealt with in the public domain, the vast majority of cybersecurity falls outside of those parameters. The approach, with great respect, is authoritarian in nature and diametrically opposed to the transparency that is demanded in an open democracy and enshrined in our Constitution. That aside, some of the “dictatorial” drafting of the Bill and the complete absence of important checks and balances that are part of every credible cybersecurity framework, is not only astounding but extremely concerning.

Definitions and interpretation

50. For purposes of this Chapter, unless the context indicates otherwise—

(*a*) **"Head of a Department"** means the incumbent of a post mentioned in Column 2 of Schedule 1, 2 or 3 to the Public Service Act, 1994 (Proclamation 103 of 3 June 1994), and includes any employee acting in such post; and

(*b*) "**representative Department**" means—

(i) the Department of Correctional Services;

(ii) the Department of Defence;

(iii) the Department of Home Affairs;

(iv) the Department of Justice and Constitutional Development;

(v*)* the National Prosecuting Authority;

(vi*)* the South African Police Service;

(vii) the State Security Agency;

(viii) the Department of Finance;

(ix) the Financial Intelligence Centre, established by section 2 of the Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001);

(x) the State Information Technology Agency, established in terms of section 2 of the State Information Technology Agency Act, 1998 (Act No. 88 of 1998);

(xi) the Department of Science and Technology; and

(xii) any other Department or public entity which is requested, in writing, by the Chairperson of the Cyber Response Committee to assist the Committee.

Cyber Response Committee

51. (1) The Cyber Response Committee is hereby established.

(2) The Cyber Response Committee consists of—

(*a*) a chairperson who is the Director-General: State Security;

(*b*) members who are the Heads of the representative Departments and their nominees who must be officials—

(i) at the rank of at least a chief director or equivalent, of a representative Department, who are specifically nominated by a Head of that representative Department to serve on the Cyber Response Committee; and

(ii) to whom a security clearance certificate has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994); and

(*c*) any person who has particular knowledge and skills in respect of any aspect dealt with in this Act and who is, from time to time, requested, in writing, by the Chairperson of the Cyber Response Committee to assist the Committee.

(3) The Cabinet member responsible for State security must appoint a member to act as chairperson whenever the chairperson is absent from the Republic or from duty, or for any reason, is temporarily unable to carry out the responsibilities as chairperson.

(4) The work incidental to the performance of the functions of the Cyber Response Committee must be performed by a secretariat, consisting of designated administrative personnel of the State Security Agency allocated to the Cyber Security Centre established in terms of section 52 of this Act.

(5) The chairperson of the Cyber Response Committee must determine the scheduled time and place of meetings of the Committee and make this known to the other members of the Committee.

(6) The objects and functions of the Cyber Response Committee are to—

(*a*) implement Government policy relating to cybersecurity;

(*b*) identify and prioritise areas of intervention;

(*c*) coordinate cybersecurity activities and be a central point of contact on all cybersecurity matters pertinent to national security;

(*d*) identify and prioritise areas of intervention and promote focussed attention and guidance where required regarding cybersecurity related threats and incidents;

(*e*) promote, guide and coordinate activities aimed at improving cybersecurity measures by all role players, which includes the strengthening of intelligence collection and improved State capacity to investigate, prosecute and combat cybercrime and to deal with cyber threats;

(*f*) oversee and guide the functioning of the 24/7 Point of Contact, the Cyber Security Centre, the Government Security Incident Response Teams, the Cyber Crime Response Centre, the Cyber Command, the Cyber Security Hub and the Private Sector Security Incident Response Teams established in the Republic;

(*g*) promote and provide guidance in respect of the development and implementation of—

(i) the National Critical Information Infrastructure Plan;

(ii) any situational analysis and awareness campaigns concerning the risk environment of South African cyberspace;

(iii) a cybersecurity culture and compliance with minimum security standards;

(iv) public-private partnerships and national and regional action plans in line with Government policy;

(v) appropriate technical and operational cybersecurity standards;

(vi) cybersecurity training, education, research and development and skills development programmes; and

(vii) international cooperation initiatives;

(*h*) facilitate interaction on cyber security, both nationally and internationally and to develop policy guidelines in order to give effect to such interaction;

(*i*) facilitate the establishment of sector, regional and continental Computer Security Incident Response Teams; and

(*j*) establish and promote a comprehensive legal framework governing cyber-related matters.

(7) (*a*) No person referred to in subsection (2), may disclose any confidential information or document obtained by that person in the performance of his or her functions in terms of this Act, except—

(i) to the extent to which it may be necessary for the proper administration of any provision of this Act;

(ii) to any person who of necessity requires it for the performance of any function in terms of this Act;

(iii) when required to do so by order of a court of law; or

(iv) with the written permission of the Cyber Response Committee.

(*b*) Any person who contravenes a provision of paragraph (*a*) is guilty of an offence and is liable on conviction to a fine, or to imprisonment for a period not exceeding 2 years or to both such fine and imprisonment.

(*c*) Any person referred to in subsection (2)(*c),* must, before assisting the Cyber Security Committee, make and subscribe to an affirmation of secrecy in the following form:

'I, ... solemnly declare:

(i) I have taken cognizance of the provisions of section 51(7) of the Cyber Crimes and Cybersecurity Act, ... (Act No. of .....).

(ii) I understand that I may not disclose any information or document, or the contents thereof, of whatever nature that comes to my knowledge or into my possession in consequence of my performance of any function in terms of the Cyber Crimes and Cybersecurity Act, ... (Act No. of .....), whether verbal or in writing, to any unauthorized person without the prior written approval of the Chairperson of the Cyber Security Committee.

(iii) I am fully aware of the serious consequences which may follow any breach or contravention of the above-mentioned provisions.

.....

(Signature)'.

(8) The Cabinet member responsible for State security may, in consultation with the Cabinet member responsible for national financial matters, make regulations regarding travelling, subsistence, remuneration and other expenses and allowances payable to a person referred to in subsection (2)(*c*).

(9) The Cabinet member responsible for State security must oversee and exercise control over the performance of the functions of the Cyber Response Committee.

(10) The Cabinet member responsible for State security must, at the end of each financial year, submit a report to Chairperson of the Joint Standing Committee on Intelligence established by section 2 of the Intelligence Services Control Act, 1994 (Act 40 of 1994), regarding progress that has been made towards achieving the objects and functions of the Cyber Response Committee.

Mark Heyink Comment on Section 51

The pervasive nature of electronic information in our society and the wide-reaching powers of the Cyber Response Committee, which is, in essence, a national security extension, places all information in South Africa under the control of law enforcement and state security. There is no provision relating to the oversight of this committee by

Parliament but merely by a cabinet minister. This is fundamentally at odds with provisions relating to accountability and the ongoing role of the Joint Standing Committee on Intelligence.

Cyber Security Centre

52. (1) The Cabinet member responsible for State security must, in consultation with the Cabinet member responsible for national financial matters—

(*a*) establish a Cyber Security Centre; and

(*b*) equip, operate and maintain the Cyber Security Centre.

(2) The Cabinet member responsible for State security exercises final responsibility over the administration and functioning of the Cyber Security Centre.

(3) The Cabinet member responsible for State security must enter into service level agreements with—

(*a*) the Head of a department; and

(*b*) any entity or institution,

in respect of the provision of services by the Cyber Security Centre.

(4) (*a*) The Cabinet member responsible for State security must appoint a person from the State Security Agency—

(i) who, on the grounds of his or her technical knowledge and experience, is a suitable and qualified person; and

(ii) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State security,

as Director of the Cyber Security Centre.

(*b*) The Director must exercise the powers and must perform the functions and carry out the duties conferred upon, assigned to or imposed upon him or her by the Cabinet member responsible for State security or under this Act, subject to the control and directions of the Cabinet member.

(*c*) Whenever the Director is for any reason temporarily unable to exercise, perform or carry out his or her powers, functions and duties, the Cabinet member responsible for State security must appoint a person from the State Security Agency—

(i) who, on the grounds of his or her knowledge and experience, is a suitable and qualified person; and

(ii) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State security,

as acting Director.

(*d*) The Director must, in the exercise of the powers, performance of the functions and carrying out of the duties conferred upon, assigned to or imposed upon him or her by the Cabinet member or under this Act, be assisted, subject to his or her control and directions, by—

(i) members of the State Security Agency allocated to the Cyber Security Centre to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State security;

(ii) any person or a entity—

(*aa*) who or which has particular knowledge and skills in respect of any aspect dealt with in this Act;

(*bb*) who or which is, from time to time, appointed to assist the Director; and

(*cc*) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994, to the satisfaction of the Cabinet member responsible for State Security.

(*e*) In order to achieve the objects of this Act, the Director must—

(i) carry out the administrative duties relating to the functioning of the Cyber Security Centre;

(ii) exercise control over the members of the State Security Agency allocated to the Cyber Security Centre, Government Security Incident Response Teams or persons or entities contemplated in subsection (4)(*d*)(ii);

(iii) manage, and exercise administrative and technical control over the Cyber Security Centre and Government Security Incident Response Teams;

(iv) regulate the procedure and determine the manner in which the provisions of this Act must be carried out by Cyber Security Centre and Government Security Incident Response Teams; and

(v) co-ordinate the activities of the Cyber Security Centre and Government Security Incident Response teams with those of the 24/7 Point of Contact, the National Cybercrime Centre, the Cyber Command, the Cyber Security Hub and the Private Sector Security Incident Response Teams.

(*f*) The Director is, for the purposes of exercising the powers, performing the functions and carrying out the duties conferred upon, assigned to or imposed upon him or her by the Cabinet member responsible for State Security or under this Act, accountable to the Cabinet member.

(*g*) The Director must, on a quarterly basis, or as the Chairperson of the Cyber Response Committee requires, submit a written report to the Cabinet member responsible for State security and the Chairperson of the Cyber Response Committee regarding—

(i) cyber security-related threats, any measures implemented to address such cyber security-related threats and shortcomings in addressing such cyber security related threats;

(ii) any matter relevant to, incidental to or which may impact on the objects and functions of the Cyber Security Centre as set out in subsection (5); and

(iii) any other matter relating to this Act which the Director wishes to or may want to bring to the attention of the Cyber Response Committee.

(5) The objects and functions of the Cyber Security Centre are to—

(*a*) facilitate the operational coordination of cyber security incident response activities regarding national intelligence;

(*b*) develop measures to deal with cyber security matters impacting on national security;

(*c*) facilitate the analysis of cyber security incidents, trends, vulnerabilities, information-sharing, technology exchange on national security and threats in order to improve technical response coordination;

(*d*) provide guidance to and facilitate the identification, protection and securing of National Critical Information Infrastructures;

(*e*) ensure the assessment and testing of National Critical Information Infrastructures, including vulnerability assessments, threat and risk assessments and penetration testing, on the written request of the Director-General: State Security;

(*f*) provide coordination and guidance regarding corporate security and policy development, governance, risk management and compliance, identity and security management, security information and event management and cyber forensics;

(*g*) develop response protocols in order to guide coordinated responses to cyber security incidents and interaction with the various stakeholders;

(*h*) ensure the conducting of cyber security audits, assessments and readiness exercises and provide advice on the development of national response plans;

(*i*) act as a point of contact regarding matters relating to State security; and

(*j*) provide the secretarial services required in relation to the Cyber Response Committee.

(6) The Cabinet Member responsible for State security may make regulations to further—

(*a*) regulate any aspect provided for in subsection (5);

(*b*) impose additional duties upon the Cyber Security Centre; and

(*c*) regulate any aspect which is necessary or expedient for the proper implementation of this section.

(7) The Cabinet member responsible for State security may, in consultation with the Cabinet member responsible for national financial matters, make regulations regarding travelling, subsistence, remuneration and other expenses and allowances payable to a person or entity referred to in subsection (4)(*d*)(ii).

(8) The Cabinet member responsible for State security must, at the end of each financial year, submit a report to Chairperson of the Joint Standing Committee on Intelligence established by section 2 of the Intelligence Services Control Act, 1994 (Act 40 of 1994), on the functions of the Cyber Security Centre.

Government Security Incident Response Teams

53. (1) The Cabinet member responsible for State security must, in consultation with the Cabinet member responsible for national financial matters—

(*a*) establish one or more Government Security Incident Response Teams; and

(*b*) equip, operate and maintain the Government Security Incident Response Teams.

(2) The Cabinet member responsible for State security exercises final responsibility over the administration and functioning of the Government Security Incident Response Teams.

(3) The Cabinet member responsible for State security must enter into service level agreements with—

(*a*) the Head of a department; and

(*b*) any entity or institution,

in respect of the provision of services by the Government Security Incident Response Teams.

(4) (*a*) The Director-General: State Security must, in consultation with the Cabinet member responsible for State security, appoint a person from the State Security Agency—

(i) who, on the grounds of his or her knowledge and experience, is a suitable and qualified person; and

(ii) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State security,

as head for each Government Security Incident Response Team established under this section.

(*b*) The Head referred to in this section must exercise the powers and perform the functions and carry out the duties conferred upon, assigned to or imposed upon him or her by the Director: Cyber Security Centre or under this Act, subject to the control and directions of the Director: Cyber Security Centre.

(*c*) Whenever a Head of a Government Security Incident Response Team is, for any reason, temporarily unable to exercise, perform or carry out his or her powers, functions and duties, the Director-General: State Security must, in consultation with the Cabinet member responsible for State security, appoint a person from the State Security Agency—

(i) who, on the grounds of his or her knowledge and experience, is a suitable and qualified person; and

(ii) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State security,

as acting Head.

(*d*) The Head of a Government Security Incident Response Team must, in the exercise of the powers, performance of the functions and carrying out of the duties conferred upon, assigned to or imposed upon him or her by the Director: Cyber Security Centre or under this Act, be assisted, subject to his or her control and directions, by—

(i) members of the State Security Agency, to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National

Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State security, allocated to the Government Security Incident Response Team;

(ii) any person or a entity—

(*aa*) who or which has particular knowledge and skills in respect of any aspect dealt with in this Act;

(*bb*) who or which is, from time to time, appointed to assist the Head; and

(*cc*) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994, to the satisfaction of the Cabinet member responsible for State security.

(*e*) In order to achieve the objects of this Act, a Head referred to in this section must—

(i) carry out the administrative duties relating to the functioning of the Government Security Incident Response Team;

(ii) exercise control over the members of the State Security Agency allocated to the Government Security Incident Response Team or persons or entities contemplated in subsection (4)(*d*)(ii);

(iii) manage and exercise administrative and technical control over the Government Security Incident Response Team;

(iv) regulate the procedure and determine the manner in which the provisions of this Act must be carried out by the Government Security Incident Response Team; and

(v) co-ordinate the activities of the Government Security Incident Response Team with those of the 24/7 Point of Contact, other Government Security Incident Response Teams, the Cyber Security Centre, the National Cybercrime Centre, the Cyber Command, the Cyber Security Hub and Private Sector Security Incident Response Teams.

(*f*) The Head referred to in this section is, for the purposes of exercising the powers, performing the functions and carrying out of the duties conferred upon, assigned to or imposed upon him or her by the Director: Cyber Security Centre or under this Act, accountable to the Director: Cyber Security Centre.

(*g*) The Head referred to in this section must, on a monthly basis, or as the Director: Cyber Security Centre requires, submit a written report to the Director: Cyber Security Centre regarding —

(i) cyber security-related threats and measures implemented in order to address such cyber security-related threats and shortcomings in addressing such cyber security-related threats;

(ii) any matter relevant to, incidental to or which may impact on the objects and functions of the Government Security Incident Response Team as set out in subsection (5); and

(iii) any other matter relating to this Act which the Head wishes to or may want to bring to the attention of the Director: Cyber Security Centre or Cyber Response Committee.

(5) The objects and functions of a Government Security Incident Response Team are to—

(*a*) develop or acquire and implement measures to deal with cyber security matters impacting on national intelligence and national security;

(*b*) protect and secure National Critical Information Infrastructures;

(*c*) implement measures, on the written request of the Director-General: State Security, in order to assess and test National Critical Information Infrastructures, including vulnerability assessments, threat and risk assessments and penetration testing;

(*d*) provide a reactive service to the State which includes—

(i) responding to alerts and warnings;

(ii) handling incidents by—

(*aa*) incident analysis;

(*bb*) providing incident responses on site;

(*cc*) providing incident response support; and

(*dd*) incident response coordination;

(iii) vulnerability handling by—

(*aa*) analysing vulnerabilities;

(*bb*) mitigating the effect of a vulnerability or repairing a vulnerability; and

(*cc*) coordinating responses to vulnerabilities; and

(iv) artifact handling by—

(*aa*) analysing artifacts;

(*bb*) responding to artifacts; and

(*cc*) artifact response coordination;

(*e*) provide a proactive service to the State which includes—

(i) intrusion alerts, vulnerability warnings, security advice and other similar announcements;

(ii) technical analysis of software, malware, intruder activities and related trends in order to help identify future threats and vulnerabilities;

(iii) the furnishing of security audits and assessments;

(iv) the configuration and maintenance of equipment, software, hardware, configurations and infrastructure;

(v) the development of security tools;

(vi) the provision of an intrusion detection service; and

(vii) the dissemination of security-related information to Government Departments; and

(*f*) provide security quality management services to the State which includes—

(i) a risk analysis service;

(ii) a continuity of service and disaster recovery planning service;

(iii) a security consulting service; and

(iv) a product certification service.

(6) The Cabinet Member responsible for State security may, after consultation with the Cyber Response Committee, make regulations to further—

(*a*) regulate any aspect provided for in subsection (5);

(*b*) impose additional duties upon Government Security Incident Response Teams; and

(*c*) regulate any aspect which is necessary or expedient for the proper implementation of this section.

(7) The Cabinet member responsible for State security may, in consultation with the Cabinet member responsible for national financial matters, make regulations regarding travelling, subsistence, remuneration and other expenses and allowances payable to a person or entity referred to in subsection (4)(*d*)(ii).

(8) The Cabinet member responsible for State security must, at the end of each financial year, submit a report to Chairperson of the Joint Standing Committee on Intelligence established by section 2 of the Intelligence Services Control Act, 1994 (Act 40 of 1994), on the functions of the Government Security Incident Response Teams.

National Cybercrime Centre

54. (1) The Cabinet member responsible for policing must, in consultation with the Cabinet member responsible for national financial matters—

(*a*) establish a National Cybercrime Centre; and

(*b*) equip, operate and maintain the National Cybercrime Centre.

(2) The Cabinet member responsible for policing exercises final responsibility over the administration and functioning of the National Cybercrime Centre.

(3) (*a*) The National Commissioner must appoint a member from the Service—

(i) who, on the grounds of his or her knowledge and experience, is a suitable and qualified person; and

(ii) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State security,

as Director of the National Cybercrime Centre.

(*b*) The Director must exercise the powers and perform the functions and carry out the duties conferred upon, assigned to or imposed upon him or her by the National Commissioner or under this Act, subject to the control and directions of the National Commissioner.

(*c*) Whenever the Director is, for any reason, temporarily unable to exercise, perform or carry out his or her powers, functions and duties, the National Commissioner must appoint a person from the Service—

(i) who, on the grounds of his or her knowledge and experience, is a suitable and qualified person; and

(ii) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State security,

as acting Director.

(*d*) The Director must, in exercising the powers and performing the functions and carrying out the duties conferred upon, assigned to or imposed upon him or her by the National Commissioner or under this Act, be assisted, subject to his or her control and directions, by—

(i) appropriately qualified members of the Service, to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State security, allocated to the National Cybercrime Centre;

(ii) any person or an entity—

(*aa*) who or which has particular knowledge and skills in respect of any aspect dealt with in this Act;

(*bb*) who or which is, from time to time, appointed to assist the Director; and

(*cc*) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994, to the satisfaction of the Cabinet member responsible for State security.

(*e*) In order to achieve the objects of this Act, the Director must—

(i) carry out the administrative duties relating to the functioning of the National Cybercrime Centre;

(ii) exercise control over the members of the Service allocated to the National Cybercrime Centre or persons or entities contemplated in paragraph (*d*)(ii);

(iii) manage and exercise administrative and technical control over the National Cybercrime Centre;

(iv) regulate the procedure and determine the manner in which the provisions of this Act must be carried out by the National Cybercrime Centre;

(v) co-ordinate the activities of the National Cybercrime Centre with those of the 24/7 Point of Contact, the Cyber Security Centre, the Government Security Incident Response Teams, the Cyber Command, the Cybersecurity Hub and the Private Sector Security Incident Response Teams; and

(vi) develop and implement cyber security policies and strategies to investigate and combat cybercrime.

(*f*) The Director is, for the purposes of exercising the powers, performing the functions and carrying out of the duties conferred upon, assigned to or imposed upon him or her by the National Commissioner or under this Act, accountable to the National Commissioner.

(*g*) The Director must, on a monthly basis, or as the National Commissioner requires, submit a written report to the National Commissioner regarding any matter relevant to, incidental to or which may impact on the objects and functions of the National Cybercrime Centre as are set out in subsection (4).

(*h*) The Director must, on a quarterly basis, or as the Chairperson of the Cyber Response Committee requires, submit a written report to the Cabinet member responsible for policing and the Chairperson of the Cyber Response Committee regarding—

(i) cyber security-related threats impacting on law enforcement, any measures implemented to address such cyber security-related threats and shortcomings in addressing such cyber security-related threats;

(ii) cyber crime trends;

(iii) successes and shortcomings in investigative measures in order to investigate cybercrime;

(iv) successes and shortcomings in international cooperation in the investigation of cybercrime;

(v) any matter relevant to, incidental to or which may impact on the objects and functions of the National Cybercrime Centre as set out in subsection (4); and

(vi) any other matter relating to this Act which the Director wishes to or may want to bring to the attention of the Cyber Response Committee.

(4) The objects and functions of the National Cybercrime Centre are to—

(*a*) facilitate the operational coordination of cyber security incident response activities with reference to the prevention, combating and investigation of crime in order to maintain public order, to secure the inhabitants of the Republic and their property and to uphold and enforce the laws of the Republic;

(*b*) develop measures in order to deal with cyber security matters impacting on law enforcement;

(*c*) facilitate the analysis of cyber security incidents, trends, vulnerabilities, information-sharing, technology exchange on law enforcement and threats in order to improve technical response coordination;

(*d*) provide coordination and guidance regarding corporate security and policy development, governance, risk management and compliance, identity and security management, security information and events management;

(*e*) establish, develop and maintain an adequate cyber forensics capacity;

(*f*) develop response protocols in order to guide coordinated responses to cyber security incidents and interact with the various stakeholders;

(*g*) develop and maintain cross-border law enforcement cooperation in respect of cybercrime;

(*h*) promote, establish and maintain public-private cooperation in order to fight cybercrime;

(*i*) promote, establish and maintain international cooperation in order to fight cybercrime; and

(*j*) develop capacity and implement measures in order to impede and neutralize cyber security-related incidents and threats.

(5) The Cabinet Member responsible for policing may, after consultation with the Cyber Response Committee, make regulations to further—

(*a*) regulate any aspect provided for in subsection (4);

(*b*) impose additional duties upon the National Cybercrime Centre; and

(*c*) regulate any aspect which is necessary or expedient for the proper implementation of this section.

(6) The Cabinet member responsible for policing may, in consultation with the Cabinet member responsible for national financial matters, make regulations regarding travelling, subsistence, remuneration and other expenses and allowances payable to a person or entity referred to in subsection (3)(*d*)(ii).

(7) The Cabinet member responsible for policing must, at the end of each financial year, submit a report to Parliament regarding progress that has been made towards achieving the objects and functions of the National Cybercrime Centre.

Mark Heyink Comment on Section 54

Subject to the general comments made relating to capacity building, the dearth of expertise and other inhibiting factors dealt with previously, the establishment of a Cyber Crime Centre is to be applauded. However, the siloed nature of the establishment of the various functions, particularly in light of the deficiencies in expertise within the South African Police Service must be raised as a point of concern The difficulty of commenting on these provisions without the benefit of proper background is repeated.

The comment provided by Professor Basie von Solms, pointing out that unless capacity is to deal with this legislation is established in among others the SAPS and NPA the Bill, once enacted, will be nothing more than a "piece of paper" is endorsed.

Cyber Command

55. (1) The Cabinet member responsible for defence must, in consultation with the Cabinet member responsible for national financial matters—

(*a*) establish a Cyber Command as part of the Intelligence Division of the South African National Defence Force contemplated in section 33 of the Defence Act, 2002 (Act 42 of 2002); and

(*b*) equip, operate and maintain the Cyber Command.

(2) The Cabinet member responsible for defence exercises final responsibility over the administration and functioning of the Cyber Command.

(3) (*a*) The Chief of the South African National Defence Force must appoint a member or employee from the South African National Defence Force—

(i) who, on the grounds of his or her technical knowledge and experience, is a suitable and qualified person; and

(ii) to whom a security clearance has been issued in terms of section 37 of the Defence Act, 2002 (Act No. 42 of 2002),

as General Officer Commanding of the Cyber Command.

(*b*) The General Officer Commanding must exercise the powers and perform the functions and carry out the duties conferred upon, assigned to or imposed upon him or her by the Chief of the South African National Defence Force or

under this Act, subject to the control and directions of the Chief of the South African National Defence Force.

(*c*) Whenever the General Officer Commanding is for any reason temporarily unable to exercise, perform and carry out his or her powers, functions and duties, the Chief of the South African National Defence Force must appoint a member or employee from the South African National Defence Force—

(i) who, on the grounds of his or her technical knowledge and experience, is a suitable and qualified person; and

(ii) to whom a security clearance has been issued in terms of section 37 of the Defence Act, 2002 (Act No. 42 of 2002),

as acting General Officer Commanding.

(*d*) The General Officer Commanding must, in exercising the powers, performing the functions and carrying out of the duties conferred upon, assigned to or imposed upon him or her by the Chief of the South African National Defence Force or under this Act, be assisted, subject to his or her control and directions, by—

(i) members and employees of the South African National Defence Force, to whom a security clearance has been issued in terms of section 37 of the Defence Act, 2002 (Act No. 42 of 2002);

(ii) any person or an entity—

(*aa*) who or which has particular knowledge and skills in respect of any aspect dealt with in this Act;

(*bb*) who or which is, from time to time, appointed to assist the General Officer Commanding; and

(*cc*) to whom a security clearance has been issued in terms of section 37 of the Defence Act, 2002 (Act No. 42 of 2002).

(*e*) In order to achieve the objects of this Act, the General Officer Commanding must—

(i) carry out the administrative duties relating to the functioning of the Cyber Command;

(ii) exercise control over the members and employees of the Defence Force or persons or entities contemplated in subsection (3)(*d*)(ii);

(iii) manage and exercise administrative and technical control over the Cyber Command;

(iv) regulate the procedure and determine the manner in which the provisions of this Act must be carried out by Cyber Command;

(v) co-ordinate the activities of the Cyber Command with those of the 24/7 Point of Contact, the Cyber Security Centre, the Government Security Incident Response Teams, the National Cybercrime Centre, the Cyber Security Hub and the Private Sector Security Incident Response Teams.

(*f*) The General Officer Commanding is, for the purposes of exercising the powers, performing of the functions and carrying out of the duties conferred upon, assigned to or imposed upon him or her by the the Chief of the South African National Defence Force or under this Act, accountable to the Chief of the South African National Defence Force.

(*g*) The General Officer Commanding must, on a monthly basis, or as the Chief of the South African National Defence Force requires, submit a written report to the Chief of the South African National Defence Force regarding any matter relevant to, incidental to, or which may impact on the objects and functions of the Cyber Command as set out in subsection (4).

(*h*) The General Officer Commanding must, on a quarterly basis, or as the Chairperson of the Cyber Response Committee requires, submit a written report to the Cabinet member responsible for defence and the Chairperson of the Cyber Response Committee regarding—

(i) cyber security-related threats, any measures implemented to address such cyber security-related threats and shortcomings in addressing such cyber security-related threats which may impact on the defence of the Republic;

(ii) any matter relevant to, incidental to or which may impact on the objects and functions of the Cyber Command as set out in subsection (4); or

(iii) any other matter relating to this Act which the General Officer Commanding wishes to or may want to bring to the attention of the Cyber Response Committee.

(4) The objects and functions of the Cyber Command are to—

(*a*) facilitate the operational coordination of cyber security incident response activities regarding national defence;

(*b*) develop measures to deal with cyber security matters impacting on national defence;

(*c*) facilitate the analysis of cyber security incidents, trends, vulnerabilities, information-sharing, technology exchange and threats on national defence in order to improve technical response coordination;

(*d*) provide guidance to and facilitate the identification, protection and securing of National Critical Information Infrastructures relevant to national defence;

(*e*) ensure, on the written command of the Chief of the South African National Defence Force, regular assessments and testing of National Critical Information Infrastructures relevant to national defence, including vulnerability assessments, threat and risk assessments and penetration testing;

(*f*) ensure the conducting of cyber security audits, assessments and readiness exercises and provide advice on the development of national response plans in so far as they relate to national defence;

(*g*) act as a point of contact regarding matters relating to national defence; and

(*h*) coordinate and implement cyber offensive and defensive measures as part of its defence mandate.

(5) The Cabinet Member responsible for defence may, after consultation with the Cyber Response Committee, make regulations to further—

(a) regulate any aspect provided for in subsection (4);

(*b*) impose additional duties upon the Cyber Command; and

(*c*) regulate any aspect which it is necessary or expedient for the proper implementation of this section.

(6) The Cabinet member responsible for defence may, in consultation with the Cabinet member responsible for national finance matters, make regulations regarding travelling, subsistence, remuneration and other expenses and allowances payable to a person or entity referred to in subsection (3)(*d*)(ii).

(7) The Cabinet member responsible for defence must, at the end of each financial year, submit a report to Chairperson of the Joint Standing Committee on Defence of Parliament, on the functions of the Cyber Command.

Mark Heyink Comment on Section 55

It is again acknowledged that with regard to defence specific issues, the establishment of Cyber Command has a very definite place. However, it is difficult from a reading purely of the Bill to conceive of the practical working of the Cyber Command.

What is very important to consider is the fact that cyber-warfare is not fought on defined frontiers and is very different to any form of warfare ever experienced by man to date. A vast number of systems critical to the wellbeing of South Africa may be attacked by nation-states or other actors who have the appropriate capability in a myriad of ways. This demands an integration of these defences with parties responsible for national security, police and the private sector and the proper coordination of all of these elements. The framework contemplated in this Bill gives no idea as to how this will work.

What also needs to be considered is that traditionally military defence is responsible for the development of weapons and capability not only to defend the country but where necessary to launch attacks (hopefully in a pre-emptive fashion to act against enemies) against enemies of South Africa. Given the completely different landscape that cyberspace presents, who is responsible for the development of cyber-weapons and cyber-defensive capability? Cyber-command or national security?

Cyber Security Hub

56. (1) The Cabinet member responsible for telecommunications and postal services must, in consultation with the Cabinet member responsible for national financial matters, —

(*a*) establish a Cyber Security Hub; and

(*b*) equip, operate and maintain the Cyber Security Hub.

(2) The Cabinet member responsible for telecommunications and postal services exercises final responsibility over the administration and functioning of the Cyber Security Hub.

(3) The Cabinet member responsible for telecommunications and postal services must enter into service level agreements with—

(*a*) the Heads of departments; and

(*b*) any public or private entity or institution,

in respect of the provision of services by the Cyber Security Hub.

(4) (*a*) The Cabinet member responsible for telecommunications and postal services must appoint a person—

(i) who, on the grounds of his or her technical knowledge and experience, is a suitable and qualified person,

(ii) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State security,

as Director of the Cyber Security Hub.

(*b*) The Director must exercise the powers and perform the functions and carry out the duties conferred upon, assigned to or imposed upon him or her by the Cabinet member responsible for telecommunications and postal services or under this Act, subject to the control and directions of the Cabinet member.

(*c*) Whenever the Director is for any reason temporarily unable to exercise, perform or carry out his or her powers, functions and duties, the Cabinet member responsible for telecommunications and postal services must, appoint a person—

(i) who, on the grounds of his or her knowledge and experience, is a suitable and qualified person; and

(ii) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State security,

as acting Director.

(*d*) The Director must, in exercising the powers, performing the functions and carrying out the duties conferred upon, assigned to or imposed upon him or her by the Minister or under this Act, be assisted, subject to his or her control and directions, by—

(i) officials or employees of the Department of Telecommunications and Postal Services, to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State security, allocated to the Cyber Security Hub;

(ii) members of the law enforcement agencies, to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State security, seconded to the Cyber Security Hub; and

(iii) any person or a entity—

(*aa*) who or which has particular knowledge and skills in respect of any aspect dealt with in this Act; and

(*bb*) who or which is, from time to time, appointed to assist the Director; and

(*cc*) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994, to the satisfaction of the Cabinet member responsible for State security.

(*e*) In order to achieve the objects of this Act, the Director must—

(i) carry out the administrative duties relating to the functioning of the Cyber Security Hub;

(ii) exercise control over the officials or employees, members and persons and entities contemplated in subsection (4)(*d*);

(iii) manage, and exercise administrative and technical control over the Cyber Security Hub and Private Sector Security Incident Response Teams;

(iv) regulate the procedure and determine the manner in which the provisions of this Act must be carried out by Cyber Security Hub and Private Sector Security Incident Response Teams;

(v) co-ordinate the activities of the Cyber Security Hub and Private Sector Security Incident Response Teams;

(vi) co-ordinate the activities of the Cyber Security Hub and Private Sector Security Incident Response Teams with those of the 24/7 Point of Contact, the Cyber Security Centre, the Government Security Incident Response Teams, the National Cybercrime Centre and the Cyber Command; and

(viii) ensure implementation of any national security guidelines which are issued by the Cabinet member responsible for State security, in consultation with the Cabinet member responsible for telecommunications and postal services and after consultation with the Cyber Response Committee.

(*f*) The Director is, for the purposes of exercising the powers, performing the functions and carrying out of the duties conferred upon, assigned to or imposed upon him or her by the Cabinet member responsible for telecommunications and postal services or under this Act, accountable to the Cabinet member.

(*g*) The Director must, on a monthly basis, or as the Cabinet member responsible for telecommunications and postal services requires, submit a written report to the Cabinet member regarding any matter relevant to, incidental to, or which may impact on the objects and functions of the Cyber Security Hub and Private Sector Security Incident Response Teams.

(*h*) The Director must, on a monthly basis, or as the Chairperson of the Cyber Response Committee requires, submit a written report to the Cabinet member responsible for telecommunications and postal services and Chairperson of the Cyber Response Committee regarding—

(i) cyber security-related threats, any measures implemented to address such cyber security-related threats and shortcomings in addressing such cyber security-related threats;

(ii) any matter relevant to, incidental to or which impacts on the objects and functions of the Cyber Security Hub as set out in subsection (5); and

(iii) any other matter relating to this Act which the Director wishes to or may want to bring to the attention of the Cabinet member responsible for telecommunications and postal services or the Cyber Response Committee.

Mark Heyink Comment on Section 56(4)

As a significant amount of oversight and interaction with the private sector will occur, it is not necessarily the case that technical knowledge and experience will qualify the most suitable person. While there is no doubt that exposure to information security principles and various technological frameworks will be important, the ability to engage in and understand issues within the private sector, largely at a non-technological level, will be equally important, if not more important, to this position. As indicated previously, without the benefit of background information these provisions are difficult to comment on. However, the establishment of a function to fulfil the responsibilities of what is described as the responsibilities of the Cybersecurity Hub is long overdue.

(5) The objects and functions of the Cyber Security Hub are to—

(*a*) coordinate general cyber security activities in the private sector;

(*b*) inform Private Sector Security Incident Response Teams, electronic communications service providers, vendors and other persons or entities who may have an interest in cyber security, of cyber security developments;

(*c*) provide best practice guidance on Information and Communications Technology security to Government, electronic communications service providers and the private sector;

(*d*) initiate cyber security awareness campaigns;

(*e*) promote compliance with standards, procedures and policy developed by the Cybersecurity Response Committee regarding cyber security which have a bearing on national security and cybercrime;

(*f*) encourage and facilitate the development of Private Sector Security Incident Response Teams;

(*g*) centralise co-ordination of cyber security activities in the private sector;

(*h*) respond to cyber security incidents;

(*i*) act as a point of contact regarding cyber security activities in the private sector;

(*j*) investigate the activities of cryptography service providers in relation to their compliance or non-compliance with relevant legislation and issue orders to cryptography service providers in order to ensure compliance;

(*k*) conduct cyber security audits, assessments and readiness exercises on request;

(*l*) assist the National Cybercrime Centre, subject to the provisions of subsection (3), in investigations relating to cyber crime; and

(*m*) assist the Cyber Security Centre, the Government Security Incident Response Teams, the National Cybercrime Centre, subject to subsection (3), with any aspect which may impact on their objects and functions.

(6) The Cabinet member responsible for telecommunications and postal services may—

(*a*) after consultation with the Cyber Response Committee and the electronic communications service providers, make regulations to—

(i) further regulate any aspect provided for in subsection (5); or

(ii) impose additional duties on the Cyber Security Hub, not inconsistent with this Act;

(*b*) in consultation with the Cabinet member responsible for national financial matters, make regulations regarding travelling, subsistence, remuneration and other expenses and allowances payable to a person or entity referred to in subsection (4)(*d*)(iii); and

(*c*) make regulations regarding any other relevant matter which is necessary or expedient to prescribe for the proper implementation of this section.

(7) The Cabinet member responsible for telecommunications and postal services must, at the end of each financial year, submit a report to Parliament regarding progress that has been made towards achieving the objects and functions of the Cyber Security Hub.

Mark Heyink Comment on Section 56

With regard to the staffing of the Cybersecurity Hub, at this stage finance has not been made available to establish the physical presence and facilities necessary for the Cybersecurity Hub to function appropriately. Considering the wide remit of the Cybersecurity Hub's functions and its interaction with the private sector and citizens at all levels, it should be anticipated that the task of the Cybersecurity Hub will be significant and will require staffing of persons with expertise and experience across a broad spectrum of issues. This will require significant budget, as is evidenced in the countries that have established facilities of this nature. It is assumed that this budget will have to be made available by the Department of Telecommunications and Postal Services but the question is raised whether a separate appropriation specifically for cumulative effort of government towards establishing cybersecurity and combatting cybercrime would not be preferable? As there are significant dependencies between the various agencies established in this Bill, the failure of one may lead to the failure of the other. Therefore the failure to coordinate the apportionment of appropriate budget to streamline the efforts between the various agencies in this regard is likely to lead to gaps and consequential failure. It is also submitted that it will be necessary to coordinate regulation between the various agencies if the desired cooperation and integration is to be achieved.

It appears that the very important responsibility for awareness creation within the private sector and civil society will also fall on the Cybersecurity Hub. In this regard, there has been a very broad document relating to awareness which has been developed by the DPTS. I further understand that there is a draft implementation document, which has not been made available as yet. Thus it is not clear how the Cybersecurity Hub will be expected to deal with the awareness creation that is its responsibility. These are issues that will require significant budget and effort to reach and educate citizens across the country. Unless this is done, equipping citizens to recognise the dangers inherent in our new information society and to combat these dangers will adversely impact on cybersecurity efforts across the board.

Whatever the Bill may say, ultimately success of these endeavours will depend on the political will within government and ministries responsible for the Cybersecurity Hub. To date this political will has been conspicuous by its absence.

It is also submitted that it will require establishment of public/private partnerships to achieve the goals. This is not a power that is established in this legislation. The interaction with the private sector is at arm's length and relates to "encouragement" and instruction rather than the joint development of appropriate cybersecurity interventions. At this early stage I warn that this approach will fail. It is out of line with international recommendations and frameworks in this regard. The Department of Justice has to understand and accept that much of the infrastructure on which the country's economy and societal communication is dependent, is not owned by government. It will be unconstitutional not to deal with this jointly and to agree appropriate cybersecurity measures. This is particularly the case as these measures have to be implemented at the cost of parties within the private sector. This Bill does not adequately address the necessity to establish public/private partnerships, their structures and mechanisms to attain agreement relating to the management and security of infrastructure which is in the hands of the private sector.

Aside from this, considering that the Minimum Information Security Standards applicable to government published in 1996, have not been amended or replaced or any amended security standards implemented within government for almost 20 years little confidence can or should be placed on government agencies to establish appropriate cybersecurity. The fact is that the cybersecurity measures in the private sector are largely significantly superior to those in government.

The reality is that while government has to provide the leadership, which so far has been conspicuous by its absence, in dealing with the development of our information economy and the security thereof, it cannot do it on its own. For it to attempt to do so will simply stamp it as an authoritarian regime, completely devoid of consideration for its constitutional duties.

Private Sector Security Incident Response Teams

57. (1) (*a*) The Cabinet member responsible for telecommunications and postal services must, by notice in the *Gazette*, declare different sectors which provide an electronic communications service for which Private Sector Security Incident Response Teams must be established.

(*b*) The declaration of different sectors referred to in paragraph (*a*) must be done in consultation with the Cabinet member responsible for the functional area of the sector and after consultation with the Cyber Response Committee.

(2) (*a*) Each sector must, within six months from the date of the publication of a notice referred to in subsection (1)(*a*) at own cost establish one or more Private Sector Security Incident Response Teams for that sector.

(*b*) The Cabinet member responsible for telecommunications and postal services must, by notice in the *Gazette*, recognise any Private Sector Security Incident Response Team which is established in terms of paragraph (*a*), for a sector.

(3) (*a*) If a sector fails to establish a Private Sector Security Incident Response Team, contemplated in subsection (2), the Cabinet member responsible for telecommunications and postal services may, after consultation with the sector, establish a Private Sector Security Incident Response Team for that sector on such terms and conditions as he or she deems fit to give effect to the objects of this Act.

(*b*) The particular sector is responsible for the operational costs of a Private Sector Security Incident Response Team which is established in terms of paragraph (*a*).

(4) A Private Sector Security Incident Response Team recognised in terms of subsection (2)(*b*) or established under subsection (3)(*a*), must—

(*a*) act as a point of contact between the sector entities in the sector for which it is established and the Cyber Security Hub;

(*b*) be a contact point for that specific sector on cyber security matters;

(*c*) coordinate cyber security incident response activities within that sector;

(*d*) facilitate information-sharing and technology-sharing within the sector;

(*e*) facilitate information-sharing and technology-exchange with other Private Sector Security Incident Response Teams established for other sectors and the Cyber Security Hub;

(*f*) establish minimum security standards and best practices for the sector for which it is established in consultation with the Cyber Security Hub;

(*g*) report all cyber security threats in the sector for which it is established and measures which have been implemented to address such threats to the Cyber

Security Hub and Private Sector Security Incident Response Teams established for other sectors;

(*h*) immediately report new cybercrime trends which come to its attention to the Cyber Security Hub, Private Sector Security Incident Response Teams established for other sectors and the National Cybercrime Centre;

(*i*) provide sector entities within the sector for which it is established with best practice guidance on cyber security; and

(*j*) perform any other function conferred on or assigned to it by the Cabinet member responsible for telecommunications and postal services by notice in the *Gazette*.

(5) (*a*) The Cabinet member responsible for telecommunications and postal services may make regulations after consultation with the relevant sector and the Cyber Security Hub, and after consultation with the Cyber Response Committee—

(i) to further regulate any aspect provided for in subsection (4);

(ii) regarding different grades of security clearances to be issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State security, to persons involved in the Private Sector Security Incident Response Teams; and

(ii) regarding any other relevant matter which is necessary or expedient to prescribe for the proper implementation of this section.

(*b*) The regulations contemplated in paragraph (*a*), may provide that any person or entity who contravenes or fails to comply with a regulation is guilty of an offence and is liable on conviction to a fine or to imprisonment not exceeding one year or to both such fine and imprisonment.

Mark Heyink Comment on Section 57

While the sentiment of establishing capability within the private sector to deal with responses which are specific to the private sector, is understood, it is foolish to believe that there will be always be a division of responses which are appropriate in the private sector and those that are appropriate in the public sector. This is simply not the case

and as was seen with the well-publicised Sony-hack in the USA. While the hack may have been perpetrated against a private company, it is now fairly certain that it was perpetrated by North Korea. The implications of a nation-state attacking private citizens, as was the case in this instance, has national security, defence and other critical implications.

The provisions as they stand allow for the Minister to make regulations after consultation with the private sector. This is simply not good enough. At the meeting of the 18th February a Director General in the Department of Telecommunications and Postal Services indicated the intention was to consult with the private sector and "work with the private sector" to achieve appropriate interaction. This is not what the Bill says and it allows for the situation where government may consult with the private sector but choose to ignore what the private sector requirements may be. The necessity for the establishment of proper public/private partnerships to deal with cybersecurity issues is repeated.

It is strongly recommended that these provisions be redrafted in their entirety to ensure that the aims established in credible cybersecurity frameworks are properly reflected in the Bill.

CHAPTER 7

NATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

Identification and declaring National Critical Information Infrastructures

58. (1) The Cyber Security Centre—

(*a*) in consultation with the Cyber Response Committee; and

(b) after consultation with any information infrastructure which is identified as a potential National Critical Information Infrastructure,

must within 12 months of the date of commencement of this Act, submit to the Cabinet member responsible for State security, information and recommendations regarding information infrastructures which need to be declared as National Critical Information Infrastructures.

(2) The Cabinet member responsible for State security may, subject to subsection (3), after considering any information and recommendations made to him or

her in terms of subsection (1) or at any time, by notice in the *Gazette*, declare any information infrastructure, or category or class of information infrastructures or any part thereof, as National Critical Information Infrastructures if it appears to the Cabinet member that such information infrastructure or information infrastructures are of such a strategic nature that any interference with them or their loss, damage, disruption or immobilization may—

(*a*) prejudice the security, the defence, law enforcement or international relations of the Republic;

(*b*) prejudice the health or safety of the public;

(*c*) cause interference with or disruption of, an essential service;

(*d*) causes any major economic loss;

(*e*) cause destabilization of the economy of the Republic; or

(*f*) create a public emergency situation.

(3) (*a*) Before the Cabinet member responsible for State security declares an information infrastructure to be a National Critical Information Infrastructure as contemplated in subsection (2), he or she must—

(i) with the exception of the State Security Agency, as referred to in section 3(1) of the Intelligence Services Act, 2002 (Act No. 65 of 2002), where the information infrastructure, or any part thereof, belongs to a Department of State, consult with the Cabinet member responsible for that Department;

(ii) where the information infrastructure, or any part thereof belongs to a company or entity that is not a state-owned or a person—

(*aa*) consult with the company, entity or person;

(*bb*) afford the company, entity or person the opportunity to make written representations on any aspect relating to the Cabinet member's intention to declare the information infrastructure, as a National Critical Information Infrastructure;

(*cc*) consider the representations of the company, entity or person; and

(*dd*) give a written decision to the company, entity or person; or

(iii) where the information infrastructure, or any part thereof, belongs to a bank as defined in section 1(1) of the Banks Act, 1990 (Act No. 94 of 1990), a mutual bank as defined in section 1(1) of the Mutual Banks Act, 1993 (Act No. 124 of 1993), a co-operative bank as defined in section 1(1) of the Co-operative Banks Act, 2007 (Act No. 40 of 2007) or the South African Reserve Bank as contemplated in the South African Reserve Bank Act, 1989 (Act No. 90 of 1989)—

(*aa*) consult with the Cabinet member responsible for finance, the South African Reserve Bank as contemplated in the South African Reserve Bank Act, 1989 (Act No. 90 of 1989), and the Financial Services Board established by section 2 of the Financial Services Board Act, 1990 (Act 97 of 1990);

(*bb*) consult with the bank in question;

(*cc*) afford the bank the opportunity to make written representations on any aspect relating to the Cabinet member's intention to declare the information structure, as a National Critical Information Infrastructure;

(*dd*) consider the representations of the bank; and

(*ee*) give a written decision to the bank.

(*b*) (i) A company, entity, person or bank may appeal against any decision of the Cabinet member in terms of paragraph (*a*)(ii)(*dd*) or (*a*)(iii)(*ee*) to the High Court.

(ii) An appeal in terms of paragraph (*b*)(i) must—

(*aa*) be lodged within 180 days from the date on which the decision was made known by the Cabinet member or such later date as the High Court permits; and

(*bb*) set out the grounds for the appeal.

(iii) The appeal must be proceeded with as if it were an appeal from a magistrate's court to the High Court.

(4) Any information infrastructure declared to be a National Critical Information Infrastructure must, notwithstanding any other law, comply with the regulations made in terms of subsection (5).

(5) The Cabinet member responsible for State security, in consultation with the relevant Cabinet members and the Cyber Response Committee must, within six months of the declaration of any information infrastructure, or category or class of information infrastructures or any part thereof, as National Critical Information Infrastructure, make regulations regulating—

(*a*) the classification of information on National Critical Information Infrastructures;

(*b*) security policies and procedures to be applied to National Critical Information Infrastructures;

(*c*) access to National Critical Information Infrastructures;

(*d*) the storing and archiving of information on National Critical Information Infrastructures;

(*e*) cyber security incident management and continuation with service provision;

(*f*) minimum physical and technical security measures that must be implemented in order to protect National Critical Information Infrastructures;

(*g*) the period within which the owner of, or person in control of a National Critical Information Infrastructure must comply with the regulations; and

(*h*) any other relevant matter which is necessary or expedient to prescribe for the proper implementation of this section.

(6) The owner of, or person in control of, a National Critical Information Infrastructure, which includes National Critical Information Structures under control of a Department of State, must in consultation with the Cabinet member responsible for State security, at own cost, take steps to the satisfaction of the Cabinet member for purposes of complying with the regulations contemplated in subsection (5).

(7) If the owner of, or person in control of, the National Critical Information Infrastructure, which includes a National Critical Information Structure under control of a Department of State, fails to take the steps referred to in subsection (6), the

Minister may, by written notice, order him or her to take such steps in respect of the National Critical Information Infrastructure as may be specified in the notice, within the period specified in the notice.

(8) If the owner of, or person in control of, the National Critical Information Infrastructure, which includes a National Critical Information Structure under control of a Department of State, without reasonable cause refuses or fails to take the steps specified in the notice within the period specified therein he or she is guilty of an offence and is liable on conviction to a fine or to imprisonment for a period not exceeding two years or to both such fine and such imprisonment.

(9) If the owner of, or person in control of, the National Critical Information Infrastructure fails or refuses to take the steps specified in the notice within the period specified therein, the Cabinet member responsible for State security may take or cause to be taken those steps which the owner or person failed or refused to take, irrespective of whether the owner or person has been charged or convicted in connection with that failure or refusal, and the Cabinet may recover the costs of those steps from the owner or person on whose behalf they were taken.

(10) For purposes of this section—

(*a*) "**information infrastructure**" means any data, computer data storage medium, computer device, database, computer network, electronic communications network, electronic communications infrastructure or any part thereof or any building, structure, facility, system or equipment associated therewith or part or portion thereof or incidental thereto; and

(*b*) **"relevant Cabinet members"** means the Cabinet members responsible for defence, telecommunications and postal services, justice and correctional services, policing, State security and includes the National Director of Public Prosecutions.

Mark Heyink Comment on Section 58

These provisions reflect in principle at least the provisions in the ECT Act which, interestingly, are not repealed in the draft legislation. The reference to National Critical Information Infrastructure as opposed to Critical Databases in the ECT Act, much

criticised before the Parliamentary Portfolio Committee, which comment was simply ignored by Parliament, is clearly a step in the right direction. Nonetheless, these provisions suffer the same defects as indicated in dealing with the prior Section 55. National Critical Information Infrastructures are not confined to government owned infrastructure and therefore the authoritarian and dictatorial approach reflected in the legislation is simply not constitutionally acceptable. As with Section 55, these provisions should be considered and redrafted in their entirety.

Establishment and control of National Critical Information Infrastructure Fund

59. (1) There is hereby established a fund to be known as the National Critical Information Infrastructure Fund.

(2) The Fund must be credited with—

(*a*) moneys appropriated by Parliament for the National Critical Information Structure Fund;

(*b*) interest derived from the investment of money in the Fund;

(c) any costs recovered in terms of section 58(9); and

(*d*) money accruing to the Fund from any other source.

(3) (*a*) The money in the Fund must be utilised—

(i) for purposes of section 58(9) on behalf of the owner or person who fails or refuses to take steps referred to in section 58; or

(ii) to implement disaster management measures in respect of National Critical Information Infrastructures in disaster situations.

(*b*) The Cabinet member responsible for State security must, before the Fund can be utilised for the purposes contemplated in paragraph (*a*)(ii), obtain the permission of the Cabinet member responsible for national financial matters.

(4) The Director-General: State Security is the accounting officer of the Fund in terms of the Public Finance Management Act, 1999 (Act No. 1 of 1999).

(5) The Fund is, subject to the directions of the Cabinet member responsible for State security, after consultation with the Cyber Response Committee, under the control and management of the Director-General: State Security, who—

(*a*) must utilise the money in the Fund in accordance with subsection (3);

(*b*) is charged with the responsibility of accounting for money received in, and payments made from, the Fund; and

(c) must cause the necessary accounting and other related records to be kept.

(6) Any money in the Fund which is not required for immediate use must be invested by the Director-General: State Security with a banking institution approved by the Cabinet member responsible for State security, in consultation with the Cabinet member responsible for national financial matters, and may be withdrawn when required.

(7) Any unexpended balance of the money in the Fund at the end of any financial year must be carried forward as a credit in the Fund to the next financial year.

(8) The Fund and the records referred to in subsection (5)(*c*) must be audited by the Auditor-General.

(9) For purposes of this section—

(*a*) **"disaster management measure"** means any measure aimed at—

(i) preventing or reducing the risk of a disaster;

(ii) mitigating the severity or consequences of a disaster;

(iii) emergency preparedness;

(iv) rapid and effective responses to a disaster; and

(v) post-disaster recovery and rehabilitation; and

(*b*) "**disaster situation**" means a progressive or sudden, widespread or localised occurrence, which takes place or is imminent and which causes or may cause substantial damage to a National Critical Information Infrastructure or any part thereof and which is of such a magnitude that it exceeds the ability of such a National Critical Information Infrastructure affected by the disaster to cope with its effects using its own resources only.

Mark Heyink Comment on Section 59

The idea of a National Critical Information Infrastructure Fund is noble but the comments relating to a general appropriation of funds for the purposes of cybersecurity and ensuring that the various agencies which may be required to establish

cybersecurity are properly funded should also be given consideration. Currently these are individually dealt with by the various Departments and the Minister of Finance. The Minister of Finance will be responsible for the allocation of appropriate funding and the fact that on the current drafting there is no appropriate mechanism of coordination for the finances required which need to be applied to cybersecurity. This needs to be addressed to accommodate appropriate coordination.

Auditing of National Critical Information Infrastructures to ensure compliance

60. (1) The owner of, or person in control of, a National Critical Information Infrastructure must, at least once a year, cause an audit to be performed on the National Critical Information Infrastructure in order to evaluate compliance with the provisions of section 58(6) of this Act.

(2) Before an audit referred to in subsection (1) is performed on a National Critical Information Infrastructure, the owner of, or person in control of, a National Critical Information Infrastructure must, at least 30 days in advance of the date of the audit, notify the Director-General: State Security, in writing of—

(*a*) the date on which an audit is to be performed; and

(*b*) the particulars and contact details of the person who is responsible for the overall management and control of the audit.

(3) The Director-General: State Security may designate any member, person or entity, referred to in section 52(4) of this Act, to monitor, evaluate and report on the adequacy and effectiveness of any audit referred to in subsection (1).

(4) The owner of, or person in control of, a National Critical Information Infrastructure must, within 30 days after an audit referred to in subsection (1) has been completed, report in the prescribed form and manner to the Director-General: State Security regarding the outcome of the audit referred to in subsection (1).

(5) The Director-General: State Security may request the owner of, or person in control of, a National Critical Information Infrastructure to provide such additional information as may be necessary within a specified period, in order to evaluate the report referred to in subsection (4).

(6) If the owner of, or person in control of, a National Critical Information Infrastructure—

(*a*) fails to cause an audit to be performed on a National Critical Information Infrastructure in order to evaluate compliance with the provisions of section 58(6) of this Act as contemplated in subsection (1);

(*b*) fails to give a report referred to in subsection (3) to the satisfaction of the Director-General: State Security after he or she has been requested to do so in terms of subsection (5), to provide additional information; or

(*c*) requests the Director-General: State Security to perform an audit referred to in subsection (1),

the Director-General: State Security must cause an audit to be performed on the National Critical Information Infrastructure in order to evaluate compliance with the provisions of section 58(6) of this Act.

(7) No person may perform an audit on a National Critical Information Structure pursuant to the provisions of subsection (6) unless he or she—

(*a*) has been authorised in writing by the Director-General: State Security to perform such audit;

(*b*) is in possession of a certificate of appointment, in the prescribed form, issued by the Director-General: State Security, which certificate must be produced on demand; and

(*c*) is accompanied by a person in control of the National Critical Information Infrastructure or a person designated by such a person.

(8) The person contemplated in subsection (7)(*c*) and any other employee of the National Critical Information Structure must assist and provide technical assistance and support to a person who is authorised to carry out an audit in terms of subsection (7)(*a*).

(9) The National Critical Information Structure which is audited pursuant to the provisions of subsection (6) is responsible for the cost of the audit.

(10) The owner of, or person in control of, a National Critical Information Infrastructure who—

(*a*) fails to cause an audit to be performed on a National Critical Information Infrastructure in order to evaluate compliance with the provisions of section 58(6) of this Act as contemplated in subsection (1);

(*b*) fails to notify the Director-General: State Security, in writing of an audit to be performed as contemplated in subsection (2);

(*c*) fails to—

(i) report on the outcome of the audit within 30 days; or

(ii) report in the prescribed form and manner to the Director-General: State Security regarding the outcome of the audit,

as contemplated in subsection (4);

(*d*) furnishes—

(i) a report referred to in subsection (4); or

(ii) any additional information referred to in subsection (5),

to the Director-General: State Security which he or she knows to be false or which he or she does not know or believe to be true; or

(*e*) fails to provide, within the specified time period the additional information requested by the Director-General: State Security as contemplated in subsection (5),

is guilty of an offence and is liable on conviction to a fine or to imprisonment for a period not exceeding three years, or to both such fine and such imprisonment.

(11) Any person who—

(*a*) hinders or obstructs any member, person or entity to monitor, evaluate and report on the adequacy and effectiveness of an audit as contemplated in subsection (3);

(*b*) hinders or obstructs a person authorised to carry out an audit in the exercise of his or her powers or the performance of his or her functions or duties in terms of subsection (6);

(*c*) fails to accompany a person authorised to carry out an audit as contemplated in subsection (7)(*c*); or

(*d*) fails to assist or provide technical assistance and support to a person authorised to carry out an audit as contemplated in subsection (8),

is guilty of an offence and is liable on conviction to a fine or to imprisonment for a period not exceeding two years, or to both such fine and such imprisonment.

Mark Heyink Comment on Section 60

The concept of audit is accepted but the provisions do not take account of what occurs when audits fail (as they will in many cases within government) in the private sector. Are the failures immediately criminalised? One of the points of information security is constant review and improvement. This is not the manner in which this has been addressed in the Bill.

These provisions and the establishment of control in the National Critical Information Infrastructure falls to be dealt with by both the public and the private sector. It is recognised in the NCFP there is a necessity for public/private partnerships. However, this is simply not the way that this issue is addressed in this Bill. There is no doubting that government should be leading (a role which it has not performed to date in so far as cybersecurity is concerned) but it cannot be authoritarian or attempt to dictate to the private sector how to deal with issues of information security without proper consultation. Information security is by its very nature a discipline that depends on the type of information being processed, the technology used, the processes employed and the training of people processing the information. It is not something that can simply be foisted on the entity without proper consideration of all of the different facets of properly implemented information security. The fact that the legislation itself fails to address this issue properly is testament to the fact that this is a multidisciplinary issue and cannot be dealt with by lawyers (who not only do not understand the information security principles applicable but do not have any idea of the information which it is necessary to secure in this regard), it demands to be addressed in terms of public/private partnerships as is stated government policy.

It should also be recognised that implementation of unnecessary or inappropriate information security will be hugely expensive. So too will the cost of audits that are contemplated in terms of the Bill. To foist these costs on business, particularly when government has not shown any aptitude in dealing with these issues, is simply unacceptable.

CHAPTER 8

EVIDENCE

Mark Heyink Comment on Chapter 8

Also under the ambit of the Department of Justice through the South African Law Reform Commission is Discussion Paper 131 which examines the Law of Evidence and makes proposals relating to possible changes. With great respect, many of the proposals made do not pass muster when examined in light of the full background of their establishment in the ECT Act. The Department of Justice is urged to liaise with the South African Law Reform Commission to address the deficiencies in its addressing evidence in this chapter.

While the provisions of Sections 61, 62 and 63 do relate to administrative issues addressing the admissibility of certain evidence and reflect the provisions of Section 15 of the ECT Act, they deviate from the intention of those provisions relating to the provisions of printouts of data messages to court and betray the same lack of consideration and understanding of the background of the ECT Act as is evidenced in the Discussion Paper. While it is accepted that in certain instances printouts may derive from foreign countries, the principles applying to printouts in terms of Section 15(4) of the ECT Act have been ignored because the electronic documents in question can be displayed on screens in South Africa and certified in terms of Section 15(4) in terms of our current law without having to be dealt with by resorting to the verification principles applicable to documents executed outside of the Republic.

Unless the issue of evidence is very carefully dealt with and is dealt with in light of the provisions of the ECT Act and information security principles relating to the integrity of information, the provisions as they stand will create huge difficulty in our courts.

Admissibility of affidavits

61. (1) Whenever any fact established by any examination or process requiring any skill in—

(*a*) the interpretation of data;

(*b*) the design of, or functioning of data, a computer device, a computer network, a database, an electronic communications network;

(*c*) computer science;

(*d*) electronic communications networks and technology;

(*e*) software engineering; or

(*f*) computer programming,

is or may become relevant to an issue at criminal proceedings or civil proceedings as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act, 1998 (Act No. 121 of 1998), a document purporting to be an affidavit made by a person who, in that affidavit, states that he or she—

(i) is in the service of a body in the Republic or a foreign State designated by the Cabinet member responsible for the administration of justice, by notice in the *Gazette*;

(ii) possesses relevant qualifications, expertise and experience which make him or her competent to make the affidavit; and

(ii) has established such fact by means of an examination or process,

is, upon its mere production at such proceedings, *prima facie* proof of such fact.

(2) Any person who makes an affidavit under subsection (1) and who in such affidavit wilfully states anything which is false, is guilty of an offence and is liable on conviction to a fine or imprisonment not exceeding two years.

(3) The court before which an affidavit is produced as *prima facie* proof of the relevant contents thereof may, in its discretion, cause the person who made the affidavit to be subpoenaed to give oral evidence in the proceedings in question or may cause written interrogatories to be submitted to such person for reply and such interrogatories and any reply thereto purporting to be a reply from such person are likewise admissible in evidence at such proceedings.

(4) No provision of this section affects any other law under which any certificate or other document is admissible in evidence and the provisions of this section are deemed to be additional to and not in substitution of any such law.

(5) (a) For the purposes of subsection (1), a document purporting to be an affidavit made by a person who in that affidavit alleges that he or she is in the service of a body in the Republic or foreign State designated by the Cabinet member responsible for the administration of justice, by notice in the *Gazette,* have no effect unless—

(i) it is obtained in terms of an order of a competent court or on the authority of a government institution of the foreign State concerned, as the case may be; and

(ii) it is authenticated—

(*aa*) in the manner prescribed in the rules of court for the authentication of documents executed outside the Republic; or

(*bb*) by a person and in the manner contemplated in section 7 or 8 of the Justices of the Peace and Commissioners of Oaths Act, 1963 (Act No. 16 of 1963).

(*b*) The admissibility and evidentiary value of an affidavit contemplated in paragraph (*a*) are not affected by the fact that the form of the oath, confirmation or attestation thereof differs from the form of the oath, confirmation or attestation prescribed in the Republic.

(*c*) A court before which an affidavit contemplated in paragraph (*a*) is placed may, in order to clarify any obscurities in the said affidavit and at the request of a party to the proceedings, order that a supplementary affidavit be submitted or that oral evidence be heard: Provided that oral evidence may only be heard if the court is of the opinion that it is in the interests of the administration of justice and that a party to the proceedings would be prejudiced materially if oral evidence is not heard.

Admissibility of evidence obtained as result of direction requesting foreign assistance and cooperation

62. (1) Evidence which is provided in response to a direction contemplated in section 45 of this Act from a foreign State is deemed to be evidence under oath if—

(*a*) it is obtained in terms of an order of a competent court of a foreign State; or

(*b*) it is accompanied by a statement in which it appears that the witness was, in terms of the law of the foreign State, warned to tell the truth and which is authenticated —

(i) in the manner prescribed in the rules of court for the authentication of documents executed outside the Republic; or

(ii) by a person and in the manner contemplated in section 7 or 8 of the Justices of the Peace and Commissioners of Oaths Act, 1963 (Act No. 16 of 1963); or

(iii) in terms of the laws of the foreign State,

which verifies the correctness of any evidence which has been furnished; and

(*c*) the person, according to the law of the foreign State, would be guilty of an offence for which he or she could be prosecuted if he or she makes a false statement or representation, or furnishes false information, knowing it to be false.

(2) Any evidence received in response to a direction, together with the statement contemplated in subsection (1)(*b)* and the direction issued in terms of section 45(1) must be open to inspection by the parties to any proceedings.

(3) Evidence obtained in terms of subsection (1) must be admitted as evidence at any proceedings and forms part of the record of such proceedings if—

(*a*) the party against whom the evidence is to be adduced agrees to the admission thereof as evidence at such proceedings; or

(*b*) the court, having regard to—

(i) the nature of the proceedings;

(ii) the nature of the evidence;

(iii) the purpose for which the evidence is adduced;

(iv) any prejudice to any party which the admission of such evidence might entail; and

(v) any other factor which in the opinion of the court should be taken into account,

is of the opinion that such evidence should be admitted in the interests of justice.

(4) The provisions of subsection (2) do not render admissible any evidence which would be inadmissible had such evidence been given at the subsequent proceedings by the witness from whom it was obtained.

(5) The court before which evidence is produced as *prima facie* proof of the relevant contents thereof may, in its discretion—

(*a*) cause the person who made the statement to be subpoenaed to give oral evidence in the proceedings in question; or

(*b*) cause written interrogatories to be submitted to such person for reply and such interrogatories and any reply thereto purporting to be a reply from such person, are likewise admissible in evidence at such proceedings.

(6) The provisions of this section do not affect any other law in terms of which evidence may be admitted as evidence at any proceedings and the provisions of this section are additional to and not in substitution for, any such law.

Admissibility of evidence

63. (1) In any criminal proceedings under this Act, the rules of evidence do not apply in a manner so as to preclude the admissibility of data, a data message or data document in evidence—

(*a*) merely on the grounds that it is data or a data message; or

(*b*) if it is the best evidence that the person adducing it could reasonably be expected to obtain on the grounds that it is not in its original form.

(2) Evidence in the form of data or a data message must, subject to subsection (3), be given due evidential weight.

(3) In assessing the admissibility or evidential weight of data or a data message regard must be had to—

(*a*) the reliability of the manner in which the data or data message was generated, stored or communicated;

(*b*) the reliability of the manner in which the integrity of the data or data message was maintained;

(*c*) the manner in which the originator or recipient of the data or data message was identified; and

(*d*) any other relevant factor.

(4) A copy or printout of data or a data message is rebuttable proof of the contents of such data or data message if it is accompanied by a declaration that is authenticated—

(a) in the manner prescribed in the rules of court for the authentication of documents executed outside the Republic;

(*b*) by a person, and in the manner, contemplated in section 7 or 8 of the Justices of the Peace and Commissioners of Oaths Act, 1963 (Act No. 16 of 1963); or

(*c*) in terms of the laws of the foreign State regulating the integrity and correctness of the data or data message and the correctness of the copy or printout.

(5) The provisions of this section do not affect any other law in terms of which data or a data message may be admitted as evidence at any proceedings and the provisions of this section are additional to and not in substitution for, any such law.

CHAPTER 9

GENERAL OBLIGATIONS OF ELECTRONIC COMMUNICATIONS SERVICE PROVIDERS AND LIABILITY

Mark Heyink Comment on Chapter 9

Several efforts were made to attend meetings that were convened between the Department of Justice and electronic communication service providers. I place on record that I have barred by the Department of Justice from these meetings. I further place on record that I requested minutes of the meetings to enable comment to be made relating to these provisions but my requests were not even met with the courtesy of a reply.

This notwithstanding, the amendments that appear to have come from that meeting are an improvement on the drafting of the conditions contained in a previous draft of the Bill relating to the notification of potential cybercrimes.

This having been said it is notable that the provisions relating to the liability of electronic communication service providers have been deleted in their entirety. It is requested that this issue be properly debated in dealing with public comment.

General obligations of electronic communications service providers and liability

64. (1) An electronic communications service provider must—

(*a*) take reasonable steps to inform its clients of cybercrime trends which affect or may affect the clients of such an electronic communications service provider;

(*b*) establish procedures for its clients to report cybercrimes with the electronic communications service provider; and

(*c*) inform its clients of measures which a client may take in order to safeguard himself or herself against cybercrime.

(2) An electronic communications service provider that is aware or becomes aware that its computer network or electronic communications network is being used to commit an offence provided for in this Act must—

(*a*) immediately report the matter to the National Cybercrime Centre; and

(*b*) preserve any information which may be of assistance to the law enforcement agencies in investigating the offence, including information which shows the communication's origin, destination, route, time date, size, duration and the type of the underlying services.

(3) An electronic communications service provider which fails to comply with subsection (1) or (2), is guilty of an offence and is liable on conviction to a fine of R10 000, for each day on which such failure to comply, continues.

(4) The Cabinet member responsible for policing, in consultation with the Cabinet member responsible for the administration of justice, must make regulations regulating the manner in which an electronic communications service provider must report the use of its computer network or electronic communications network to commit an offence, to the National Cybercrime Centre.

CHAPTER 10

AGREEMENTS WITH FOREIGN STATE

President may enter into agreements

65. (1) The President may, on such conditions as he or she may deem fit, enter into any agreement with any foreign State regarding—

(*a*) the provision of mutual assistance and cooperation relating to the investigation and prosecution of—

(i) an offence under Chapter 2 of this Act;

(ii) any other offence in terms of the laws of the Republic which is or was committed by means of, or facilitated by the use of an article; or

(iii) an offence—

(*aa*) similar to those contemplated in Chapter 2 of this Act; or

(*bb*) any other offence substantially similar to an offence recognised in the Republic which is or was committed by means of, or facilitated by the use of an article,

in that foreign State;

(*b*) the implementation of cyber threat response activities;

(*c*) research, information and technology-sharing and the development and exchange on cyber security related matters;

(*d*) the protection and securing of National Critical Information Infrastructures;

(*e*) the establishment of 24/7 contact points;

(*f*) the implementation of emergency cross-border response mechanisms to address cyber threats;

(*g*) the reciprocal implementation of measures to curb cybercrime; and

(*h*) the establishment of emergency centres to deal with cyber-related threats.

(2) The Cabinet member responsible for the administration of justice must, as soon as practical after Parliament has agreed to the ratification of, accession

to or amendment or revocation of an agreement referred to in subsection (1), give notice thereof in the *Gazette*.

CHAPTER 11

GENERAL PROVISIONS

Repeal or amendment of laws

66. The laws mentioned in the Schedule are hereby repealed or amended to the extent reflected in the third column of the Schedule.

Regulations

67. (1) The Cabinet member responsible for the administration of justice must make regulations, prescribing the—

(*a*) form of the expedited preservation of data direction and the manner in which it must be served by a member of a law enforcement agency as contemplated in section 40(2);

(*b*) form of the disclosure of data direction and the manner in which it must be served by a member of a law enforcement agency as contemplated in section 41(7);

(*c*) form of the preservation of evidence direction and the manner in which it must be served by a member of a law enforcement agency as contemplated in section 42(2);

(*d*) form of the direction as contemplated in section 45(1); and

(*e*) form of the affidavit which must accompany the information furnished to the 24/7 Point of Contact as contemplated in section 48(2)(*b*)(ii).

(2) The Cabinet member responsible for State security must, in consultation with the Cabinet member responsible for the administration of justice, make regulations, prescribing the—

(*a*) form of the report and manner of reporting to the Director-General: State Security as contemplated in section 60(4); and

(*b*) form of the certificate as contemplated in section 60(7).

(3) The Cabinet member responsible for State security must make regulations as contemplated in section 58(5).

Short title and commencement

68. (1) This Act is called the Cybercrimes and Cybersecurity Act, 20..... (Act No. ..... of .....), and comes into operation on a date fixed by the State President by proclamation in the *Gazette*.

(2) Different dates may be fixed under subsection (1) in respect of different provisions of this Act.

Schedule

LAWS REPEALED OR AMENDED

Number and year of law	Short title	Extent of repeal or amendment
Act No. 68 of 1995	South African Police Service Act, 1995	The deletion of section 71.
Act No. 32 of 1998	National Prosecuting Authority Act, 1998	The deletion of sections 40A and 41(4).
Act No. 111 of 1998	Correctional Services Act, 1998	The deletion of section 128.
Act No. 38 of 2001	Financial Intelligence Centre Act, 2001	The deletion of sections 65, 66 and 67.
Act No. 25 of 2002	Electronic Communications and Transactions Act, 2002	(*a*) The amendment of section 1 by the deletion of the definitions of "critical data", "'critical database" and "critical database administrator". (*b*) The deletion of Chapter IX. (*c*) The deletion of sections 85, 86, 87, 88 and 90. (*d*) The substitution for section 89 of the following section: "Penalties **89. [(1)]** A person convicted of an offence referred to in sections 37 (3), 40 (2), 58 (2), 80 (5)**[,]** or 82 (2) **[or 86 (1), (2) or (3)]** is liable to a fine or imprisonment for a period not exceeding 12 months. **[(2) A person convicted of an offence referred to in section 86 (4) or (5) or section 87 is liable to a fine or imprisonment for a period not exceeding five years.]**.
Act No. 70 of 2002	Regulation of Interception	The addition of the following items

Number and year of law	Short title	Extent of repeal or amendment
	of Communications and Provision of Communication related Information Act, 2002	to the Schedule to the Act: "15 any offence referred to in section 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 19, 21(2)(*b*) or 22 (in so far as the attempt, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding, or procuring to commit offence relates to any of the aforementioned offences) of the Cybercrimes and Cybersecurity Act, 20… (Act …… of ….); and 16 any offence which is substantially similar to an offence referred to in item 15 which is or was committed in a foreign State.".
Act No. 32 of 2007	Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007	(**a**) The insertion of the following section after section 16, in Part 2 of Chapter 3 of the Act: **"Definitions** **16A**. For the purposes of this Part and unless the context indicates otherwise— (*a*) "computer data storage medium" means any article, device or location from which data is capable of being reproduced or on which data is capable of being stored, by a computer device, irrespective of whether the article or

Number and year of law	Short title	Extent of repeal or amendment
		device is physically attached to or connected with the computer device; (*b*) "computer device" means any electronic programmable device used, whether by itself or as part of a computer network, a database, a critical database, an electronic communications network or a National Critical Information Infrastructure or any other device or equipment or any part thereof, to perform predetermined arithmetic, logical, routing or storage operations in accordance with set instructions and includes all— (i) input devices; (ii) output devices; (iii) processing devices; (iv) computer data storage mediums; (v) programs; and (vi) other equipment and devices, that are related to, connected with or used with such a device or any part thereof; (*c*) "computer network" means two or more inter-connected or related computer devices, which allows these inter-connected or related computer devices to— (i) exchange data or

Number and year of law	Short title	Extent of repeal or amendment
		any other function with each other; (ii) exchange data or any other function with another computer network; or (iii) connect to an electronic communications network; (*d*) "database" means a collection of data in a computer data storage medium; (*e*) "electronic communications network" means electronic communications infrastructures and facilities used for the conveyance of data; (*f*) "electronic communications service provider" means any person who provides an electronic communications service under and in accordance with an electronic communications service licence issued to such person under Chapter 3 of the Electronic Communications Act, 2005 (Act No. 36 of 2005), or who is deemed to be licensed or exempted from being licensed as such in terms of the Electronic Communications Act, 2005.”. (*b*) The insertion of the

Number and year of law	Short title	Extent of repeal or amendment
		following section after section 20: "**Cybercrimes involving child pornography** **20A.** (1) Any person who unlawfully and intentionally takes steps to procure, obtain or access or in any way, knowingly assists in, or facilitates the procurement, obtaining or accessing of child pornography through a computer network or electronic communications network, is guilty of an offence. (2) Any person who unlawfully and intentionally possesses child pornography on a computer data storage medium, a computer device, a computer network, a database or an electronic communications network, is guilty of an offence. (3) Any person who unlawfully and intentionally produces child pornography for the purpose of making it available, distributing it or broadcasting it by means of a computer network or an electronic communications network, is guilty of an offence. (4) Any person who unlawfully and intentionally— (*a*) makes available, distributes or broadcasts; (*b*) causes to be made available, broadcast or distributed; (*c*) assists in making available, broadcasting or distributing, child pornography by means of a

Number and year of law	Short title	Extent of repeal or amendment
		computer network or an electronic communications network, is guilty of an offence. (5) Any person who unlawfully and intentionally advocates, advertises, encourages or promotes— (*a*) child pornography; or (*b*) the sexual exploitation of children, by means of a computer network or an electronic communications network, is guilty of an offence. (6) Any electronic communications service provider who unlawfully and intentionally— (a) makes available, distributes or broadcasts; (b) causes to be made available, broadcast or distributed; (c) assists in making available, broadcasting or distributing, child pornography through a computer network or an electronic communications network, is guilty of an offence. (7) Any electronic communications service provider who unlawfully and intentionally advocates, advertises, encourages or promotes child pornography or the sexual exploitation of children, is guilty of an offence. (8) Any person who unlawfully and intentionally processes or facilitates a financial transaction, knowing that such transaction will facilitate access to, or the distribution or possession

Number and year of law	Short title	Extent of repeal or amendment
		of, child pornography, by means of a computer network or an electronic communications network, is guilty of an offence. (9) Any person or electronic communications service provider who, having knowledge of the commission of any offence referred to in subsections (1) to (8), or having reason to suspect that such an offence has been or is being committed and unlawfully and intentionally fails to— (*a*) report such knowledge or suspicion as soon as possible to a police official; or (*b*) furnish, at the request of the South African Police Service, all particulars of such knowledge or suspicion, is guilty of an offence. (*c*) The amendment of section 56A of the Act, by the addition of the following subsection: "(3) Any person or electronic communications service provider who contravenes the provisions of section 20A(9), is liable, on conviction to a fine not exceeding R 5 million or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment.".