DISCUSSION OF THE CYBERCRIMES AND CYBERSECURITY BILL

1. PURPOSE OF BILL

The Cybercrimes and Cybersecurity Bill, 2015 (the "Bill") -

* creates offences and prescribes penalties;
* further regulates jurisdiction;
* further regulates the powers to investigate, search and gain access to or seize items;
* further regulates aspects of international cooperation in respect of the investigation of cybercrime;
* provides for the establishment of a 24/7 point of contact;
* provides for the establishment of various structures to deal with cyber security;
* regulates the identification and declaration of National Critical Information Infrastructures and provides for measures to protect National Critical Information Infrastructures;
* further regulates aspects relating to evidence;
* imposes obligations on electronic communications service providers regarding aspects which may impact on cybersecurity;
* provides that the President may enter into agreements with foreign States to promote cybersecurity;
* repeals and amends certain laws; and
* provides for matters connected therewith.

2. BACKGROUND

2.1 In 2011 more than one third of the world's total population had access to the Internet. It is estimated that mobile broadband subscriptions will approach 70 per cent of the world's total population by 2017. The number of networked devices is estimated to outnumber people by six to one, transforming current conceptions of the internet. In the future hyper-connected society, it is hard to imagine a cybercrime or perhaps any crime, that does not involve electronic evidence linked with internet protocol connectivity. Both individuals and organised criminal groups exploit new criminal opportunities, driven by profit and personal gain. Most cybercrime acts are estimated to originate in some form

of organised activity, with cybercrime black markets established on a cycle of malware creation, computer infection, botnet management, harvesting of personal and financial data, data sale and selling of financial information. Cybercrime perpetrators no longer require complex skills or techniques. Globally, cybercrime shows a broad distribution across financially-driven acts and computer-content related acts, as well as acts against the confidentiality, integrity and accessibility of computer systems. Globally police-recorded crime statistics do not represent a sound basis for determining the precise impact of cybercrime. According to authors cybercrime is significantly higher than conventional crimes. The use of the Internet to facilitate and commit acts of terrorism is a real occurrence. Such attacks are typically intended to disrupt the proper functioning of targets, such as computer systems, servers or underlying infrastructure, especially if they are part of critical information infrastructures of a country, among others, by means of unlawful access, computer viruses or malware. Some countries are taking steps to implement cyber-warfare and defence strategies.

2.2 As part of Government's Outcome Based Priorities, the JCPS Cluster signed the JCPS Delivery Agreement relating to Outcome 3 on 24 October 2010. This agreement focuses on certain areas and activities, clustered around specific outputs, where interventions will make a substantial and positive impact on the safety of the people of South Africa.

2.4 Currently there are various laws on the Statute Book dealing with cyber security, some with overlapping mandates administered by different Government Departments and whose implementation is not coordinated. The legal framework regulating cyber security in the Republic of South Africa is a hybrid mix of legislation and the common law. Some notable statutes in this regard include, among others, the Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002), the Protection of State Information Bill, 2010, the South African Police Service Act, 1995 (Act No. 68 of 1995), the Correctional Services Act, 1998 (Act No. 111 of 1998), the National Prosecuting Authority Act, 1998 (Act 32 of 1998), the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act No. 70 of 2002), the Prevention and Combatting of Corrupt Activities Act, 2004 (Act No.

12 of 2004), the Films and Publications Act, 1996 (Act No. 65 of 1996), the Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007 (Act No. 32 of 2007), the Copyright Act, 1978 (Act No. 98 of 1978), the Civil Proceedings Evidence Act, 1965 (Act No. 25 of 1956), the Criminal Procedure Act, 1977 (Act No. 51 of 1977), the Protection of Personal Information Act, 2013 (Act No. 4 of 2013), the Protection from Harassment Act, 2011 (Act No. 17 of 2011), the Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001), and the State Information Technology Agency Act, 1998 (Act No. 88 of 1998), to name a few.

2.5 The Department of Justice and Constitutional Development was mandated to review the cyber security laws of the Republic to ensure that these laws provide for a coherent and integrated cyber security legal framework for the Republic.

2.6 The Bill is part of a review process of the laws on the Statute Book which deal with cyber security and matters related to cyber security. Further legislation may in due course be promoted to address other relevant aspects, inter alia, cryptography, e-identity management and also a possible review of electronic evidence.

3. OBJECTS OF BILL

3.1 Definitions

Clauses 1, 2 and 26, 50 contain various definitions which will be explained in context with the provisions to which they relate.

3.2. Offences

3.2.1 Personal and financial information or data related offences

The automation of data processing and the development of non-face-to-face transactions have generated increased opportunities to commit various offences with the personal and financial information or data of a person. This information or data can be the subject of several constitutive acts, namely –

* the act of obtaining identity-related or financial information or data;
* the act of possessing or transferring the identity-related or financial information or data; and
* the act of using the identity-related or financial information or data for criminal purposes.

Personal or financial information or data can be obtained, for example, *via* illegal access to computer devices and data bases, the use of phishing or interception tools, or through illicit acquisition, such as dumpster diving, social engineering, theft and online buying of information or data of another person. For example, “phishing” has recently become a key crime committed in cyberspace and describes attempts to fraudulently acquire sensitive information (such as passwords or other personal or financial information or data) by masquerading as a trustworthy person or business (e.g. financial institution) in a seemingly official electronic communication. Examples of personal information or data which is targeted in cyberspace are the following:

* Address particulars, phone numbers, dates of birth and identity numbers: This information can in general be used to commit identity theft if it is combined with other information or data. Having access to information such as a date of birth and address of a person can help the perpetrator to circumvent verification processes. One of the greatest dangers related in this regard is the fact that it is currently available on a large scale on various databases.
* Passwords for non-financial accounts: Having access to passwords for accounts allows perpetrators to change the settings of the account and use it for their own purposes. They can, for example, take over an e-mail account and use it to send out e-mails with illegal content or take over the account of a user of an auction platform and use the account to sell stolen goods.

Financial information or data is a popular target in cyberspace. Financial information or data which is targeted in cyberspace are information regarding saving accounts, credit cards, debit cards and financial planning information.

Personal or financial information or data are mostly used to commit financial cybercrimes.

The following offences aim to address personal or financial information or data related offences:

(*a*) **Clause 3(1)** criminalises the intentional and unlawful acquiring by any means, the possession of or provision to another person, of the personal information of a person for purposes of committing an offence provided for in the Bill.

(*b*) **Clause 3(2)** criminalises the intentional and unlawful acquiring by any means, the possession of or provision to another person, of the financial information of a person for purposes of committing an offence provided for in the Bill.

(c) **Clause 3(3**) criminalises the intentional and unlawful use of the personal or financial information of another person to commit an offence under the Bill.

(*b*) In terms of **clause 3(4)**, a person is guilty of an offence, if he or she is found in possession of personal or financial information of another person in regard to which there is a reasonable suspicion that such personal or financial information–

* was acquired, is possessed, or is to be provided to another person for purposes of committing an offence under the Bill; or
* was used or may be used to commit an offence under this Bill,

and if he or she is unable to give a satisfactory exculpatory account of such possession.

For purposes of this clause, **clause 3(7)** defines –

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

3.2.2 **Unlawful access**

Since the development of computer networks, their ability to connect have been used by hackers for criminal purposes. Hackers need not be present at the crime scene, they just need to circumvent the protection securing the database, network or computer device. Illegal access threatens interests such as the integrity of data, a computer device, a computer network, a database or an electronic communications network. The legal interest is infringed, not only when a person unlawfully interferes or commits other unlawful acts in respect of data, a computer device, a computer network, a database or an electronic communications network, but also when a perpetrator, for example, merely accesses a computer network. Illegal access does not require that the offender

accesses system files or other stored data. The criminalisation of illegal access represents an important deterrent to many other subsequent acts against the confidentiality, integrity and availability of data, a computer device, a computer network, a database or an electronic communications network, and other computer-related offences. It is vital to distinguish between illegal access and subsequent offences, since the other offences have a different focus of protection. In most cases, illegal access is not the end goal, but rather a first step towards further crimes, such as interfering with or intercepting data.

To address this, **clause 4(1)** criminalises the unlawful accessing of the whole or any part of data, a computer device, a computer network, a database, a critical database, an electronic communications network or a National Critical Information Infrastructure. **Clause 4(3)** defines "**access**" as to include, without limitation, the following: 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. **Clause 4(4)** provides that 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.

3.2.3 **Unlawful interception of data**

The use of Information Communications Technologies is accompanied by several risks related to the security of information transfer. Unlike classic mail-order operations, data-transfer processes over the Internet involve numerous providers and different points where the data transfer process could be intercepted. Wireless networks, for example, allow persons to connect to the Internet from anywhere inside a given radius, without the need for cable connections. However, this also allows perpetrators the same

amount of access if adequate security measures are not implemented which will allow access to, inter alia, passwords, bank account information and other sensitive information. The criminalisation of the unlawful interception of data aims to protect the integrity, privacy and confidentiality of data within a computer device, a computer network, a database or an electronic communications network as well as data which is being sent to, over or from the aforementioned. The unlawful interception of data builds on the offence of illegal access, where further actions are taken by the perpetrator in order to acquire data unlawfully.

Clause 5(1) provides that any person who intentionally and unlawfully intercepts data to, from or within 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, is guilty of an offence.

In terms of **clause 5(3)**, the **"interception of data**" is defined as the acquisition, viewing, capturing or copying of data through the use of hardware and software tools 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—

* viewing, examination or inspection of the contents of the data; and
* diversion of the data or any part thereof from its intended destination to any other destination.

"Data" is defined in **clause 1** as 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 traffic data and personal information.

3.2.4 **Unlawful acts in respect of software or hardware tools**

Software and hardware tools which are used to commit crimes in cyberspace are freely available. The criminalisation of such software and hardware is challenging in light of the fact that most of this software or hardware has dual usages, which may not be unlawful. In order to prevent over-criminalisation the Bill, in accordance with various

international and regional instruments, requires a specific intent, namely to commit certain offences provided for in the Bill, to criminalise the manufacturing, assembling, obtaining, selling, purchasing, making available, advertising, using or possessing these devices and software.

In terms of **clause 6(1)**, any person who intentionally and unlawfully manufactures, assembles, obtains, sells, purchases, makes available or advertises any software or hardware tool for the purposes of contravening clauses 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. **Clause 6(2)** provides that any person who intentionally and unlawfully uses or possesses any software or hardware tool for purposes of contravening clauses 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. In terms of **clause 6(3)**, a person is guilty of an offence, if he or she is found in possession of any 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 clauses 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) , and if he or she is unable to give a satisfactory account of such possession.

Clause 6(5) defines **"hardware or software tools"** as 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—

* acquire, make available or to provide personal data or financial data as contemplated in clause 3(1)(*a*) or (*c*), or (2)(*a*) or (*c*);
* access as contemplated in clause 4(3);
* intercept data as contemplated in clause 5(3);
* interfere with data as contemplated in clause 7(3);
* interfere with a computer device, computer network, database, critical database, electronic communications network or National Critical Information Infrastructure as contemplated in clause 8(3); or
* acquire, modify, provide, make available, copy or clone a password, access code or similar data and devices as defined in clause 10(4).

3.2.5 **Unlawful interference with data**

Interference with computer data endangers the integrity and availability of data, as well as the proper operation of computer devices, computer networks, databases or electronic communications networks. Data is vital for users, businesses and public administration, all of which depend on the integrity and availability of data. Lack of access to data can result in considerable pecuniary damage and may disrupt public administration. Perpetrators can violate the integrity of data and interfere with it by deleting data, suppressing data, altering data or restricting access to data. Examples of interference with data are, inter alia –

* a computer virus which is installed on a computer device and which corrupts data; or
* where a hacker accesses a database and deletes files or alters the content of information or a program stored on a database or encrypts information.

Interference with critical data may adversely affect national security and impact on critical services such as electricity, water, transport and financial institutions.

In terms of **clause 7(1)**, the interference with data or critical data is criminalised. In terms of **clause 7(3) "Interference with data"** means to—

* alter data;
* 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
* make vulnerable, suppress, corrupt, damage, delete or deteriorate data.

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

Interference with computer devices, computer networks, databases or electronic communications networks endangers the integrity and availability of data, as well as the proper operation of computer devices, computer networks, databases or electronic communications networks. The same concerns which are relevant to interference with data are applicable to interference with computer devices, computer networks, databases or electronic communications networks. Government and businesses offering services based on electronic communications depend on the functioning of their

communications infrastructure. Interference with communications infrastructures, whether physically or through actions in cyberspace, affect service delivery negatively and may lead to massive losses. Interference with critical databases and National Critical Information infrastructures may compromise national security and impact on critical services.

In terms of **clause 8(1)** of the Bill, the interference with the lawful use of a computer device, a computer network, a database, a critical database, an electronic communications network, or a National Critical Information Infrastructure, is criminalised. In terms of **clause 8(3)**, the "**interference with a computer device, computer network, database, critical database, electronic communications network or National Critical Information Infrastructure**" is defined as to mean 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.

3.2.6 **Unlawful acts in respect of malware**

Malware such as viruses, worms, logic bombs and trojan horses, among others, have different effects on data, computer devices, computer networks, databases or electronic communications networks. On the one hand malware can be regarded as attacks on the integrity of the data but on the other hand it may directly affect the functioning of the hardware. The potential impact of a malware is limited only by the skills, resources and imagination of the programmer who creates it. Viruses and worms cause major economical losses yearly and may be used in cyber terrorist activities to cause widespread disruption of computer systems and the destruction of databases. It may be used to infect computer systems which are used for a critical service or even the defence of the Republic causing these systems to malfunction or become inoperative. A real live example which can be provided is the Stuxnet worm which infected Iran's nuclear facilities, causing centrifuge failure. Physical devices exist which can also be used to compromise data or computer hardware.

In terms of **clause 9(1)** of the Bill, the assembling, obtaining, selling, purchasing, possession, making available, advertising or using malware for the purposes of causing damage to data, a computer device, a computer network, a database, a critical database, an electronic communications network or a National Critical Information Infrastructure, are criminalised. In terms of **clause 9(2)**, a person is guilty of an offence, if he or she is found in possession of malware in regard to which there is a reasonable suspicion that such malware is possessed for the purposes of intentionally and unlawfully causing damage to data, a computer device, a computer network, a database, a critical database, an electronic communications network or a National Critical Information Infrastructure, and the person is unable to give a satisfactory account of such possession. **Clause 9(4)** defines "**malware**" as to mean means any data, electronic, mechanical or other instrument, device, equipment, or apparatus that is designed specifically to—

* create a vulnerability in respect of;
* modify or impair;
* compromise the confidentiality, integrity or availability of; or
* 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.

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

Passwords, access codes and similar data or devices, have a specific function in cyberspace, namely to protect unauthorised access to, the use of, or interference with data, a computer device, a computer network, a database, or an electronic communications network. In most instances, similar to personal information related offences, this offence can be the subject of several constitutive acts, namely –

* the act of obtaining passwords, access codes or similar data or devices;
* the act of possessing or transferring the passwords, access codes or similar data or devices; and
* the act of using the passwords, access codes or similar data or devices to commit further offences.

Passwords access codes or similar data or devices can be obtained, for example, *via* illegal access to computer devices and databases, the use of phishing or hardware and software tools, or through illegal acquisition, such as dumpster diving, social engineering, the buying of credit card numbers or bank authentication information of another person or theft.

The illicit obtaining and using of credit card numbers and electronic banking information of a person and the subsequent use of this information are everyday examples which clause 9, inter alia, aims to address. **Clause 10(1)** of the Bill criminalises the unlawful acquiring, possession, provision to another or use of access codes, passwords or similar data or devices for purposes of contravening clauses 3(1)(*a*) or (*c*), 3(2)(*a*) or (*c*), 4(1), 5(1), 7(1), 8(1), 11(1), 12(1) or (2) or 13(1) of the Bill. In terms of **clause 10(2)**, a person is guilty of an offence, if he or she is found in possession of an access code, password or similar data or devices in regard to which there is a reasonable suspicion that such access code, password or similar data or devices was acquired, is possessed, or is to be provided to another person or was used or may be used for purposes of contravening section 3(1)(a) or (c), 3(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 account of such possession. In terms of **clause 10(4)** of the Bill **"passwords, access codes or similar data or device"** means without limitation a secret code or pin, an image, a security token, an access card or device, a biometric image, a word or a string of characters or numbers, or a password, used for electronic transactions or user authentication in order to access, as contemplated in clause 4(3), data, a computer device, a computer network, a database, a critical database, an electronic communications network, or a National Critical Information Infrastructure or other device or information.

3.2.8 **Computer related fraud**

Computer-related fraud is one of the most prevalent crimes on the Internet. As in all cyber-related crime, there is a slim chance of catching the perpetrator. The perpetrator can further use various tools to mask his or her identity. Automation enables offenders to make large profits from a number of small acts. One strategy used by offenders is to ensure that each victim's financial loss is below a certain limit. Small-loss-victims are less likely to invest time and energy to report such incidents to the South African Police

Service and the law enforcement agencies do not have the capacity to investigate all cyber related offences but usually prioritize them according to seriousness. The protected legal interest in crimes against the confidentiality, integrity and availability of computer data and systems is the integrity of computer information and data itself. In contrast, criminal provisions on computer-related fraud protect interests in property, financial assets and the authenticity of data or data messages. Common forms of computer related fraud are—

* online auction fraud, where the perpetrator offers non-existent goods for sale and request buyers to pay prior to delivery, or where goods are bought online and where delivery is requested without the intention to pay; or
* advanced fee fraud, where offenders send out e-mails asking for recipients' help in transferring large amounts of money to third parties and promising them a percentage, if they agree to process the transfer using their personal accounts. The offenders then ask them to transfer a small amount to validate their bank account data, which the offender takes.

Section 87 of the Electronic Communications and Transactions Act, 2002, purports to create an offence of computer related fraud, which is more akin to forgery. The common law offence of fraud is used mainly to prosecute offenders in appropriate circumstances. **Clause 11(1),** in line with the common law proscription of fraud, creates the offence of computer related fraud. **Clause 11(1)** provides that any person who intentionally and unlawfully, by means of data or a data message, makes a misrepresentation which causes actual prejudice, or which is potentially prejudicial to another, is guilty of the offence of computer related fraud. **Clause 2(1)** defines **"computer related"** as 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 clause 11. The definition of **"data"** was dealt with under paragraph 3.2.3, above. In terms of **clause 1** a **"data message"** is defined as data in an intelligible form, in whatever form generated, sent, received, communicated, presented, tendered or stored by electronic means. Fraud by means of data will be committed mainly where information is presented to a computer device such as an ATM machine, whilst a data message will be the medium used to mislead another person.

3.2.9 **Computer related forgery and uttering**

Digital documents play an ever increasing role in modern commerce. Computer-related forgery describes the manipulation of digital documents, for example, by creating a document that appears to originate from a reliable institution, or manipulating electronic images, or altering text documents, to purport to be something other than it is. With digital forgeries, digital documents can now be copied without loss of quality and are easily manipulated. It is difficult to prove digital manipulations unless technical protection is used to protect a document from being forged. **Clause 12(1)** criminalises the intentional and unlawful making of a false data document to the actual or potential prejudice of another. A "**data document**" is defined in **clause 12(4)** as a data message containing the depiction of a document which portrays information. **Clause 2(1)** defines **"computer related"** as the use of data, a computer device, a computer network, a database or an electronic communications network to commit the offence in question.

If a forged digital document is brought to the attention of somebody, a further offence is committed, namely computer related uttering. In most cases the person who utters a digital document is also the person who forged the digital document. Phishing is a good example of uttering. "Phishing" entails, inter alia, the act where an e-mail or an SMS which look like a communications from legitimate financial institutions used by the victim is sent to a victim in such a way that it is difficult to identify it as a fake e-mail or SMS. The e-mail asks the recipient to disclose or verify certain sensitive information. Many victims follow the advice and disclose information enabling offenders to make online bank transfers. **Clause 12(2)** criminalises the intentional and unlawful passing of a false data document, to the actual or potential prejudice of another. Section 87(2) of the Electronic communications and Transactions Act, 2002, creates the offence of computer-related forgery. The common law is available to prosecute computer related forgery and uttering, although it is unsure if it has ever been used where a digital document was involved.

3.2.10 **Computer related appropriation**

The elements of the common law offence of theft are the intentional and unlawful act of appropriation (which consists of the deprivation of property with the intention to exercise the rights of an owner in respect of the property), of certain kinds of property (namely movable corporeal property or credit) belonging to another or belonging to the

perpetrator but which is in the lawful possession of another. The issue of theft of incorporeals was dealt with as follows in the South African law: In *S v Mintoor* 1996 1 SACR 514 (C), the court decided that electricity cannot be stolen. In *S v Harper and Another* 1981 (2) SA 638 (D), it was held that shares (as an incorporeal) as opposed to share certificates are capable of being stolen. In *Nissan South Africa (Pty) Ltd v Marnitz NO and Others (Stand 186 Aeroport (Pty) Ltd Intervening)* 2005 (1) SA 441 (SCA) at paragraphs 24 and 25 it was held that, as a result of the fact that ownership in specific coins no longer exists where resort is made to the modern system of banking and paying by cheque or kindred processes, money is capable of being stolen even where it is not corporeal cash but is represented by a credit entry in books of an account. In *S v Ndebele and Others* 2012 (1) SACR 245 (GSJ) at 253 to 257, it was held that incorporeals in the form of electricity credits amount to theft. The courts have not yet developed the offence to include theft of other incorporeals other than money in the form of credits. However, the following examples illustrate the need to criminalise the appropriation of incorporeals:

(a) A hacker accesses a database of a bank where he or she downloads credit card numbers of customers of the bank which he or she subsequently sells over the Internet.

(b) A person physically breaks into the head offices of a pharmaceutical firm, takes a portable data storing device and downloads data which contains all the information about the synthesising of a new drug which cures an incurable disease which he or she subsequently sells to another pharmaceutical company for millions of dollars.

(c) A programmer working for a programming company and who is part of a software development team copies the newly developed computer operating system and sells it to another company.

(d) A person physically steals the only copy of a DVD which contains all the information about the development of a super efficient electro-active polymer which will revolutionise robotic applications which he or she subsequently sells to a country for millions of dollars.

(e) A hacker accesses the electronic database of the Companies and Intellectual Property Commission and substitutes his or her name for that of the patent holder of a patent which he or she later sells.

If the common law offence of theft is applied to the above mentioned examples, the following will result:

* There was no appropriation of property, in examples (a) to (c) in the sense that the owners of the data were deprived of the data or property. The data and property are still in the possession of the owners.
* One cannot steal incorporeal things such as data. The data in examples (a) to (c), which are extremely valuable, are not recognised as capable of being stolen.
* In example (d), the person committing the offence will probably be prosecuted for the theft of a DVD worth R5, 00.
* In example (e), although the hacker can be prosecuted for fraud and forgery, he or she has in fact stolen a patent.

Theft of immovable property is not recognised in the South African Law, mainly “because immovables cannot be carried away” according to a Roman-Dutch law principle. In cyberspace it is possible to assign new ownership to immovable property, for instance, a hacker accesses the electronic database of the deeds office and substitutes his or her name for that of the owner of a farm and who soon afterwards dies intestate.

In terms of section 1 of the General Law Amendment Act, 1956 (Act No. 50 of 1956), the unlawful appropriation of the use of another's property is criminalised. A requirement for this offence is the physical removal of the property from the control of the owner or person competent to consent to such removal. However, in cyberspace it is not necessary to physically remove property and thereby use it without the consent of the owner. For example a computer, server or database within a financial or a state institution can be taken over by a person with the intent to use it for his or her purposes without the consent of the owner or any other person competent to give such consent. Although such conduct may, inter alia, be prosecuted as unlawful access, unlawful interference with data or unlawful interference with a database or electronic communications network, there is no reason for not acknowledging a similar offence as that created by section 1 of the General Law Amendment Act, 1956, in respect of instances where electronic communications infrastructures are unlawfully and without the consent of the owner or legal user used by unauthorised third parties to the detriment of the owners or parties, who have an interest in such resources or property

or resources which can be manipulated or used through such electronic communications infrastructures.

Clause 13 of the Bill therefore creates the offence of computer related appropriation to address the above shortcomings. In terms of **clause 2(1)** of the Bill "**computer related**" is defined as the use of data, a computer device, a computer network, a database or an electronic communications network to commit the offence in question. In terms of clause 13(1) of the Bill, any person who intentionally and unlawfully appropriates, in any manner—

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

* permanently; or
* 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.

Clause 13(3) defines "**property**" as money, credit, any information which can be used to facilitate a financial transaction, or any movable, immovable, corporeal or incorporeal thing which has a commercial value. For purposes of this definitions 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), are excluded from the definition of property. The reason for this exclusion is that the existing legislation in this regard already provides adequate protection against infringements of this nature. However, if such property is appropriated before it is, inter alia, copyrighted it will amount to computer related appropriation. "**Right in property**" is defined in clause 1 as any rights, privileges, claims and securities in property and any interest therein and all proceeds thereof and 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).

3.2.11 The following categories of extortion currently exist:

* A computer network or electronic communications network is used as a medium to extort another person, for instance when one person threatens another person by means of a data message to release certain unflattering personal information about the person if he or she does not meet the demands of the extortionist.
* Data, a computer device, a computer network, a database, a critical database, an electronic communications network or a National Critical Information Infrastructure may become the target of extortion where the owner is threatened with a criminal act which may interfere therewith if the demands of the extortionist are not met. The extortionist may, inter alia, threaten the person that he or she is going to install malware on the person's servers if his or her demands are not met.
* Continuous criminal acts may be committed against a database, a critical database, an electronic communications network, or a National Critical Information Infrastructure and the extortionist undertakes to cease such acts if his or her demands are met. The extortionist may, inter alia, lodge a denial-of-service attack against an online trading entity, which makes it impossible to conduct business.

The perpetrators of Internet extortion can be singular individuals as well as organised criminal groups. The motives behind extortion can be a personal vendetta, monetary in nature or politically or activist motivated. Acts of extortion may be directed at individuals, businesses and government institutions. According to *Snyman, Criminal Law Fifth Edition*, page 427, the common law crime of extortion requires that the advantage must be handed over to the perpetrator before the act is complete. If the perpetrator is apprehended after the threat has been made but before the acquisition of the advantage, he or she can only be convicted of attempted extortion.

Computer-related extortion is dealt with in section 87(1) of the Electronic Communications and Transactions Act, 2002. This offence differs substantially from the common law offence of extortion and requires the acts of extortion to be the unlawful

interception of data, tampering with data, use or distribution of certain devices and denial-of-service attacks to acquire a proprietary advantage by undertaking to cease or desist from such action, or by undertaking to restore any damage caused as a result of those actions as extortion.

Computer-related extortion is dealt with in terms of **clause 14** of the Bill, which broadens the concept of extortion substantially as provided for in section 87 of the Electronic Communications and Transactions Act, 2002. In terms of clause **14(1)** any person who intentionally and unlawfully—

* threatens to commit any offence under the Bill; or
* commits any offence under the Bill,

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

In terms of **clause 2(1)** of the Bill "**computer related**" is defined as the use of data, a computer device, a computer network, a database or an electronic communications network to commit the offence in question.

3.2.12 **Computer related terrorist activity and related offences**

Critical infrastructure is widely recognised as a potential target of a terrorist attack as it is by definition vital for the economy and a state's sustainability and stability. The growing reliance on information technology makes critical infrastructures more vulnerable to attacks. This is especially the case with regard to attacks against interconnected systems that are linked by computer and communication networks. Unlike physical attacks, the terrorists do not need to be present at the place where the effect of the attack occurs and multiple attacks can be carried out simultaneously against various critical infrastructures. Multiple examples exist worldwide where critical infrastructures have been affected adversely by Internet-based attacks. Special software can be designed to circumvent detection and security measures which can cause severe destruction to a critical database or critical infrastructure. Cyber attacks on critical infrastructures do not differ from the traditional concept of terrorism.

In addition to attacks on critical infrastructures, various acts can take place in cyberspace or the virtual world which enhance the ability of any person, entity or

organisation to engage in a computer terrorist activity. In this regard reference may be made to the following:

* Propaganda: Terrorists use websites, the social media and other forums to disseminate propaganda, to describe and publish justifications for their activities, to recruit new members and to contact existing members and donors. Websites have been used to distribute videos of executions and terrorist attacks.
* Information gathering: Sensitive or confidential information that is not adequately protected from search-robots or hacking attempts can be accessed. Considerable information can be obtained about possible targets through legal as well as illegal access.
* Information dissemination: Training instructions, inter alia, how to make bombs and how to use weapons can be furnished through the Internet. Attacks can be planned and preparations of how to carry out an attack can take place over the Internet. Members can use the Internet to communicate with each other and coordinate terrorist attacks. By using encryption technology and anonymous communication technologies, unwanted access to such communications may be limited.
* Financing: Most terrorist organisations depend on financial resources. The Internet may be used conveniently to receive funds or move funds around with a degree of anonymity.
* Training: Online training is possible over the Internet.
* Distribution of tools to engage in a computer terrorist activity: Programmes which can be used in computer-related terrorist activities can be distributed *via* the Internet.

Clause 15(5) of the Bill defines a "**computer related terrorist activity"** as any prohibited act contemplated in clauses 6(1) (interference with data), 7(1) (interference with computer device, computer network, database, critical database, electronic communications network or National Critical Information Infrastructure), 8(1) (acts in respect of malware) or 13(1) (extortion)—

(*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

(*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,

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.

Clause 15(1) of the Bill aims to criminalise direct computer-related terrorist activities by providing that any person who, intentionally and unlawfully, engages in a computer-related terrorist activity is guilty of the offence of computer-related terrorism. **Clauses 15(2)** and **(3)** create the offences of association with a computer-related terrorist activity and facilitation of a computer-related terrorist activity, respectively. These offences aim to criminalise conduct which does not directly amount to a terrorist attack, but which supports or aids terrorist activities.

The **offence associated with a terrorist activity, as contemplated in clause 15(2)**, consists of acts by a person which will, or is likely to, enhance the ability of any person, entity or organisation to engage in a computer-related terrorist activity, including—

* providing or offering to provide a skill or expertise;
* entering or remaining in any country; or
* 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 which the person 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.

The offence of facilitating a computer-related terrorist activity, as contemplated in **clause 15(3)**, entails—

* the provision or offering to provide any data, an interception device, malware, a password, access code or similar data, a computer device, computer network, a database, an electronic communications network or any other device or equipment or any part thereof to a person for use by or for the benefit of a person, entity or organisation;
* the soliciting of support for or giving of support to a person, entity or organisation;
* providing, receiving or participating in training or instruction, or recruiting a person, entity or an organisation to receive training or instruction;
* the recruiting of any person, entity or organisation; or
* the possession, receiving or making available data, an interception device, malware, a password, access code or similar data 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 which a person knows or ought reasonably to have known or is so connected.

3.2.13 **Computer related espionage and unlawful access to restricted data**

Sensitive information is often stored in computer systems. If the computer system is connected to the Internet, offenders can try to access this information *via* the Internet from almost any place in the world. The Internet is used increasingly to obtain trade secrets, sensitive commercial information and sensitive information in possession of a State. The value of sensitive information and the ability to access it remotely makes data espionage a daily occurrence. Various techniques, which are not limited to technical means, are used to gain access to data. In addition to ordinary hacking attempts, social engineering and specialised software and hardware, are among others, used to gain unauthorised access to sensitive data. **Clause 16(1)(*a*)** criminalises the intentional and unlawful performing or authorising, procuring or allowing another person to perform a prohibited act contemplated in clause 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 clause 4(3), to critical data, a critical database or National Critical Information Infrastructure or to intercept data to, from or within a critical database or National Critical Information Infrastructure, with the intention to directly or indirectly benefit a foreign State or a non state actor engaged in a terrorist activity against the Republic. **Clause 16(1)(*b*)** criminalises the intentional and unlawful possession, communication, delivering, making available or receiving of data to, from or within a critical database or National Critical Information Infrastructure or critical data with the intention to directly or indirectly benefit a foreign State or a non state actor engaged in a terrorist activity against the Republic. **Clause 16(2)(*a*)** criminalises the intentional and unlawful performing or authorising, procuring or allowing another person to perform a prohibited act contemplated in clause 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 clause 4(3), in order to gain access to, as contemplated in clause 4(3), or intercept data, as contemplated in section 5(3) in possession of the State, classified as confidential, with the intention of directly or indirectly benefiting a foreign State or a non state actor engaged in a terrorist activity against the Republic. **Clause 16(2)(*b*)** criminalises the intentional and unlawful possession, communication,

delivering, making available or receiving of data in possession of the State, classified as confidential, with the intention of directly or indirectly benefiting a foreign State or a non state actor engaged in a terrorist activity against the Republic. **Clause 16(3)(*a*)** criminalises the intentional and unlawful performing or authorising, procuring or allowing another person to perform a prohibited act contemplated in clause 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, as contemplated in clause 4(3), or intercept data, as contemplated in clause 5(3), in possession of the State, classified as secret, with the intention of directly or indirectly benefiting a foreign State or a non state actor engaged in a terrorist activity against the Republic. **Clause 16(3)(*b*)** criminalises the intentional and unlawful possession, communication, delivering, making available or receiving of data in possession of the State, classified as secret, with the intention of directly or indirectly benefiting a foreign State or a non state actor engaged in a terrorist activity against the Republic. **Clause 16(4)(*a*)** criminalises the intentional and unlawful performing or authorizing, procuring or allowing another person to perform a prohibited act contemplated in clause 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, as contemplated in clause 4(3), or intercept data, as contemplated in clause 5(3), in possession of the State, classified as top secret, with the intention of directly or indirectly benefiting a foreign State or a non state actor engaged in a terrorist activity against the Republic . **Clause 16(4)(*b*)** criminalises the intentional and unlawful possession, communication, delivering, making available or receiving of data in possession of the State, classified as top secret, with the intention of directly or indirectly benefiting a foreign State or a non state actor engaged in a terrorist activity against the Republic. **Clause 16(5)(*a*)** criminalises the intentional and unlawful performing or authorising, procuring or allowing another person to perform a prohibited act contemplated in clause 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, as contemplated in clause 4(3) or intercept data, as contemplated in clause 5(3), in possession of the State, classified as confidential. **Clause 16(5)(*b*)** criminalises the intentional and unlawful possession, communication, delivering, making available or receiving of data in possession of the State, classified as confidential. **Clause 16(6)(*a*)** criminalises the intentional and unlawful performing or authorising, procuring or allowing

another person to perform a prohibited act contemplated in clause 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, as contemplated in clause 4(3) or intercept data, as contemplated in clause 5(3) in possession of the State, classified as secret. **Clause 16(6)(*b*)** criminalises the intentional and unlawful possession, communication, delivering, making available or receiving of data in possession of the State, classified as secret. **Clause 16(7)(*a*)** criminalises the intentional and unlawful performing or authorising, procuring or allowing another person to perform a prohibited act contemplated in clause clause 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, as contemplated in clause 4(3), or intercept data, as contemplated in clause 5(3), in possession of the State, classified as top secret. **Clause 16(7)(*b*)** criminalises the intentional and unlawful possession, communication, delivering, making available or receiving of data in possession of the State, classified as top secret. **Clause 16(8)** of the Bill defines "**terrorist activity**", for purposes of clause 16, as a "**computer related terrorist activity**" contemplated in section 16(1) of the Act and a "**terrorist activity**" contemplated in the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004 (Act 33 of 2004).

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

Radical individuals and groups use mass communication systems such as the Internet to spread their ideologies. Internet distribution offers several advantages such as lower distribution costs, non-specialist equipment and a global audience. Besides propaganda, the Internet is used to sell certain items such as flags, uniforms and books on auction platforms and web-shops. The Internet is also used to send e-mails and newsletters and distribute video clips through popular archives such as YouTube. Not all countries criminalise these offences. In some countries, such content may be protected by the principles of freedom of speech. Section 16(2)(c) of the Constitution of the Republic of South Africa, expressly provides that the freedom of expression principle does not extend to advocacy of hatred that is, inter alia, based on race and ethnicity and that constitutes incitement to cause harm. **Clause 17(1)** of the Bill criminalises the intentional and unlawful making available, broadcasting or distribution

of a data message which advocates, promotes or incites hate, discrimination or violence against a person or a group of persons. **Clause 17(3)** defines " **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 national or social origin, race, colour, ethnicity, religious beliefs, gender, gender identity, sexual orientation, caste or mental or physical disability.

3.2.15 **Prohibition on incitement of violence and damage to property**

Similar to the offence of advocating, promoting or inciting of hate, discrimination or violence, the Internet or other communications media can be used in order to incite violence against a specific person or a group of persons. The Internet offers a place where negative and violent emotions can be fostered, such as hate group web sites. In some cases, these emotions are followed by actual acts of violence. This can be motivated by a personal feud, political reasons or socially motivated factors. The severity and impact of the offence may differ. The Protection from Harassment Act, 2011, already addresses harassment in cyberspace by means of a civil remedy. **Clause 18** of the Bill takes this further by criminalising the incitement of violence against a specific person or group of persons or damaging of property belonging to a specific person or group of persons.

3.2.16 **Prohibited financial transactions**

The Internet is transforming money-laundering. The regulation of Internet money transfers is currently limited and the Internet offers offenders the possibility of cheap and tax-free money transfers across borders. Online financial services offer the option of enacting multiple, worldwide financial transactions very quickly. The Internet has helped overcome the dependence on physical money transactions. Wire transfers replaced the transport of hard cash as the original first step in suppressing physical dependence on money, but stricter regulations to detect suspicious wire transfers have forced offenders to develop new techniques. The detection of suspicious transactions in the fight against money-laundering is based on obligations of the financial institutions involved in the transfer. Money-laundering is generally divided into three phases, namely, placement, layering (or masking) and integration. With regards to the

placement of large amounts of cash, the use of the Internet might perhaps not offer that many tangible advantages. However, the Internet is especially useful for offenders in the layering phase. In this context the investigation of money-laundering is especially difficult when money-launderers use online casinos and virtual currencies. Unlike a real casino, large financial investments are not needed to establish online casinos. In addition, regulations relating to online and offline casinos often differ between countries. Tracing money transfers and proving that funds are not prize winnings, but have instead been laundered, is only possible if casinos keep records and provide them to law enforcement agencies. Current legal regulation of Internet-based financial services is not as stringent as traditional financial regulation. Apart from gaps in legislation, difficulties arise from –

* accurate customer verification which may be compromised in that the financial service provider and customer never meet and it is difficult to apply traditional customer verification procedures;
* the involvement of providers in various countries with different regulatory provisions applicable to online transfers; and
* instances where peer-to-peer (person-to-person) transfers are allowed.

The use of virtual currencies is similarly problematic in that users may be able to open accounts online, often without registration. Some providers even enable direct peer-to-peer transfer or cash withdrawals. Account holders may also use inaccurate information during registration to mask their identities. **Clause 19** of the Bill supplements the provisions of the Prevention of Organised Crime Act, 1998 (Act No. 121 of 1998) and the Financial Intelligence Centre Act, 2001, in so far as it deals with money laundering. In addition to money laundering, the Internet can further be used as a medium to make payments in order to facilitate a wide array of unlawful activities, inter alia, drug transactions, the buying of stolen credit card numbers, payments made to a criminal to commit an offence, the buying of contraband, the buying of child pornography, etcetera. **Clause 19(1)** criminalises the intentional participating in, processing of, or facilitating of a financial transaction through a computer network or an electronic communications network—

* with the intention of promoting an unlawful activity; or
* which involves the proceeds of any unlawful activity.

Clause 19(3) of the Bill defines "**unlawful activity**" as any conduct which contravenes any law of the Republic.

3.2.17 **Infringement of copyright**

The most common copyright violations include the exchange of copyright-protected songs, e-books, files and software in file-sharing systems. File-sharing systems are peer-to-peer-based network services that enable users to share files, often with millions of other users. After installing file-sharing software, users can select files to share and use software to search for other files made available by others for download from hundreds of sources. Before file-sharing systems were developed, people copied records and tapes and exchanged them, but file-sharing systems permit the exchange of copies by many more users. Peer-to-peer technology plays a vital role in the Internet. File-sharing systems can be used to exchange any kind of computer data, including music, movies and software. Historically, file-sharing systems have been used mainly to exchange music, but the exchange of videos and e-books is becoming more and more important. The technology used for file-sharing services is highly sophisticated and enables the exchange of large files in short periods of time. First-generation file-sharing systems depended on a central server, enabling law enforcement agencies to act against illegal file-sharing. However, the second-generation file-sharing systems are no longer based on a central server providing a list of files available between users. The decentralised concept of second generation file-sharing networks makes it more difficult to prevent them from operating. More recent versions of file-sharing systems enable forms of anonymous communication and make investigations extremely difficult and time consuming. Research has identified millions of file-sharing users and billions of downloaded files. Copies of movies have appeared in file-sharing systems before they are released officially in cinemas at the cost of copyright-holders. The recent development of anonymous file-sharing systems will make the work of copyright holders more difficult, as well as law enforcement agencies. Although various technologies exist to prevent the copying of the contents of CDs and DVDs, software and hardware exist which can override the Digital Rights Management protection. High quality scanners can scan in excess of 30 pages per minute and this allows the scanned product to be saved as a digital file which allows copies of books to be made available. The Copyright Act, 1978 (Act 98 of 1978), regulates copyright in material. Section 23 of the Act determines

when copyright is infringed and sections 24 and 25 deal with the remedies for an infringement of copyright. Section 27 of the Act provide for penalties for the infringement of copyright. **Clause 20** of the Bill aims to supplement the Copyright Act, 1978, by criminalising the infringement of copyright through the use of the Internet and more specifically peer-to-peer file-sharing. **Clause 20(1)** of the Bill provides that any person who intentionally and unlawfully, at a time when copyright exists in any work, without the authority of the owner of the copyright, by means of a computer network or an electronic communications network sells, offers for download, distributes or otherwise makes available, any work, which the person knows is subject to copyright and that his or her actions will prejudicially affect the owner of the copyright, is guilty of an offence. **Clause 20(3)** of the Bill defines "**work**" to mean any literary work, musical work, artistic work, cinematographic film, sound recording, broadcast, programme-carrying signal, published edition or computer program, which is eligible for copyright in terms of section 2 of the Copyrights Act, 1978, or similar legislation of any State designated by the Minister by notice in the *Gazette*.

3.2.18 **Harbouring or concealing person who commits offence**

It is a well established principle in legislation which aims to address terrorist activities and espionage to criminalise the harbouring and concealing of a suspected spy or terrorist. See in this regard section 11 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004 (Act 33 of 2004) and clause 34 of the Protection of State Information Bill. Section 51(2) of the Criminal Procedure Act, 1977 (Act 51 of 1977), similarly criminalises the harbouring or concealing of a person who escapes from custody. Although offences in cyberspace are usually committed by individuals, there is a growing tendency of a concerted approach to cybercrime where support is given to the cybercriminal to evade justice, which includes giving refuge to or concealing the perpetrator. **Clause 21** of the Bill criminalises the intentional and unlawful harbouring or concealing of a person by another 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 clauses 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 17, 18, 19 or 20 or any offence contemplated in section 15 or 16 of the Bill.

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

In terms of **clause 22** of the Bill any person who intentional and unlawful attempts, conspires with any other person or aids, abets, induces, incites, instigates, instructs, commands, or procures another person, to commit an offence in terms of Chapter 2 of the Bill, is guilty of an offence and liable on conviction to the punishment to which a person convicted of actually committing that offence would be liable.

3.2.20 **Aggravating circumstances when offence committed in concert with other persons**

Cyberspace lends itself to coordination across a dispersed area. An organized cybercrime group may be a highly structured organisation that engages in cybercrime or it could be a short-lived group established specifically to commit certain crimes in cyberspace. Various online communities exist which assist or facilitate cybercrimes, sometimes in accordance with their ideological principles. An example of cooperation in cybercrime is where a person obtains information through social engineering and gives it to a hacker to gain access to a server where certain information is copied who, in turn, gives it to another person who sells the information or use the information to commit fraud or computer related appropriation. **Clause 23(1)** of the Bill aims to address concerted and organised efforts to commit cybercrime by providing that if an offence in terms of the Bill is committed in concert with other persons it must be considered as an aggravating circumstance for purposes of sentencing.

A position of trust is not normally given to individuals unless they have unblemished integrity and an offence committed by persons in a position of trust may be seen as a betrayal of those very characteristics. Society operates in certain spheres largely on the basis of trust and one of the burdens of a position of trust is an undertaking of incorruptibility. The individual who puts himself or herself forward as trustworthy is trusted by others and if he or she takes advantage of his or her power for his or her own personal gain it can be said to offend in two ways, namely not only does he or she commit the crime in question, but in addition he or she breaches the trust placed in him or her by society and by the victims of the particular offence. According to various judgments of the High court it is an aggravating circumstance if a person, who is in a

position of trust, to abuse this position by committing an offence. Persons who are responsible for the processing of personal information or financial information or who are in charge of, in control of, or have access to data, a computer device, a computer network, a database, a critical database, an electronic communications network, or a National Critical Information Infrastructure as part of their daily duties are persons in a position of trust. To date, various serious cybercrimes have been committed in the Republic by persons in a position of trust, either by themselves or in collusion with or with the assistance of other persons. Cybercrimes committed by persons in trust is a serious concern to both the private and public sector. Persons in trust may have unrestricted and unlimited access to data, information, access codes or computer systems of an institution. The reasons for these persons committing these offences and the kind of offences which commit, vary. Crimes by persons in trust may be committed for purposes of self-enrichment, as a vendetta against their employer, or as part of an organised criminal syndicate, among others. In terms of **clause 23(2)** of the Bill a court which imposes any sentence in terms of clause 3, 4, 5, 7, 8 or 10 of the Bill 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 clause 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 clause 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 clause 10.

In terms of **clause 23(3)**, a court must, unless substantial and compelling circumstances exist which justify the imposition of another sentence as prescribed in paragraphs (*a*) or (*b*) of clause 23(3), impose, with or without a fine, in the case of—

(*a*) a first contravention of clause 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 clause which is contravened; and

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

3.2.21 **Criminal liability in terms of the common law or other legislation**

In terms of **clause 24**, the savings provision, the provisions of Chapter 2 of the Bill do not affect criminal liability in terms of the common law or other legislation. This means that the offences in terms of Chapter 2 of the Bill can be used in addition to other existing offences to prosecute a person for an offence which is committed in cyberspace. This clause aims to preclude any possible argument that, because the Bill creates certain specific offences which can be committed in cyberspace, that such offences are the only offences for which a person can be prosecuted when an offence is committed by electronic means.

3.3 Jurisdiction

Cybercrime is a typical transnational crime that involves different jurisdictions. It is not unusual that several countries may be affected. The term “jurisdiction” refers to the authority of a state to enforce its domestic law. Traditionally, the legal concept of jurisdiction involves territory, with the scope of a country's jurisdiction being defined by the limits of its territorial boundaries. This territorial notion of jurisdiction is ineffective to prosecute cybercriminals. Determining where a cybercrime is committed can be difficult, since the perpetrator and the victim can be located in different countries and also because the perpetrator may utilize computer systems in several countries in the course of attacking a victim, for instance the offender might have acted from country A, used an Internet service in country B which connects to a server in country C which connects to the victim’s computer device in country D. This is a challenge with regard to the application of criminal law and leads to questions about which of the countries has jurisdiction, which country should take forward the investigation and how are disputes resolved. Various theories exists in respect of jurisdiction, namely:

* The territoriality theory: In terms of this theory jurisdiction is determined by the place where the offence is committed, in whole or in part.
* The nationality theory or active personality theory: In terms of this theory, due to the fact that a country has unlimited control over its nationals it is considered that

such a country has the right to exercise jurisdiction over its nationals, wherever they are and whatever they do.

* The passive personality theory: This theory is concerned with the nationality of the victim and the courts of a country, to which the victim belongs, assume jurisdiction.
* The protective theory: A country assumes jurisdiction if its national or international interest are adversely affected.
* Universality theory: This theory is based on the international character of offences and allows every country to assume jurisdiction over offences, even if those offences have no direct effect on a specific country. The requirements for assuming jurisdiction in terms of this theory are, firstly, that the State assuming jurisdiction must have the perpetrator in custody, and secondly, the offensive conduct must adversely affect the international community.

Countries, in general, deal with cyber jurisdiction issues by broadening as much as possible the notion of jurisdiction in accordance with the first four jurisdiction theories to investigate and prosecute cybercrime effectively. **Clause 25** of the Bill follows suit and extends the traditional concept of criminal jurisdiction to accommodate cybercrime. **Clause 25** of the Bill provides as follows:

(*a*) A court in the Republic trying an offence in terms of the Bill has jurisdiction where—

* the offence was committed in the Republic;
* any act of preparation towards 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;
* 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
* 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.

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

* is a citizen of the Republic;
* is ordinarily resident in the Republic;
* 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;
* is a company, incorporated or registered as such under any law, in the Republic; or
* is any body of persons, corporate or unincorporated, in the Republic.

(*c*) Any act alleged to constitute an offence under the Bill and which is committed outside the Republic by a person, other than a person contemplated in paragraph (*b*), , regardless of whether or not the act constitutes an offence or not at the place of its commission, is deemed to have also been committed in the Republic if that—

* act affects or is intended to affect a public body, a business or any other person in the Republic;
* person is found to be in South Africa; and
* person is for one or other reason not extradited by South Africa or if there is no application to extradite that person.

(*d*) Where a person is charged with attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding, 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.

3.4 Powers to investigate, search and gain access to or seize and international cooperation

3.4.1 In a constitutional dispensation where the powers of the law enforcement agencies to investigate crime are regulated by statute, adequate statutory provisions should be adopted to give them these investigative powers and also to guard against abuses in the investigative process. The evidence relating to cybercrime is almost always in electronic, or digital, form. This data can be stored or are transient, and can exist in the form of computer files, transmissions, logs, metadata, or network data.

Obtaining such evidence requires an amalgamation of traditional and new policing techniques. Law enforcement agencies may use traditional policing investigation methodologies (interviewing victims or undercover visual surveillance of suspects) in some stages of an investigation, but require electronic-specific approaches for other parts. These can include accessing, and seizing or copying of data from devices belonging to suspects, obtaining data from third parties such as Internet service providers, and where necessary intercepting electronic communications. While some of these investigative actions can be achieved by means of traditional powers, many procedural provisions do not translate well from a spatial, object-oriented approach to one involving electronic data storage and real-time data flows. In addition, investigative powers must be able to address challenges such as the volatile nature of electronic evidence, the use of obfuscation techniques by perpetrators such as the use of encryption, proxies, cloud computing service, 'innocent' computer systems infected with malware, and multiple (or 'onion') routing of internet connections. These aspects require cyber-specific laws to provide a clear scope of application of the power, in order to guarantee legal certainty in its use and sufficient legal authority for actions such as ensuring access to data, preservation of data, and the collection of data.

Chapter 2 of the Criminal Procedure Act, 1977 (Act No. 51 of 1977), in general, sets out the powers of law enforcement agencies in the investigation of criminal offences. Although an "article" as intended in section 20 of the Criminal Procedure Act, will include anything which is involved in or which may afford evidence of the commission of an offence, Chapter 2 is object based and does not readily lend itself to the investigation of cybercrime. In so far as it relates to investigations of cybercrime, the Criminal Procedure Act, 1977, is supplemented by the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (the RICA). The RICA provides, inter alia, for the obligations of electronic communications service providers to record and store certain information in respect of customers and communications of customers, the interception of communications, the provision of communication-related information and obligation on decryption key holders. It must be mentioned that there is currently no obligations on Internet service providers to store any communication-related information. Cumulatively viewed these two Acts do not provide adequate measures for the investigation of cybercrime. Chapter 4 of the Bill

aims to rectify this position and to bring the law of the day in line with the international position regarding the investigation of cybercrime.

3.4.2 **Clause 26** contains definitions which are relevant to the interpretation of Chapter 4 of the Bill. In terms of **clause 26**—

(*a*) "**access**" is defined as making use of, gaining entry to, viewing, displaying, retrieving, copying data, or otherwise making 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;

(*b*) "**article**" is defined as 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—

* is concerned with or is, on reasonable grounds, believed to be concerned in the commission or suspected commission;
* may afford evidence of the commission or suspected commission; or
* 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 the Bill 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.

(*c*) "i**nvestigator**" is defined as 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, as the case may be, due to his or her expertise to, subject to the control and directions of a member of a law enforcement agency who accompanies him or her, assist a law enforcement agency in an investigation in terms of the Bill;

(*d*) "**designated judge**" is defined as the 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);

(*e*) "**law enforcement agency**" is defined as —

* the South African Police Service referred to in section 5 of the South African Police Service Act, 1995 (Act No. 68 of 1995); and
* the State Security Agency referred to in section 3(1) of the Intelligence Services Act, 2002 (Act No. 65 of 2002);

(*f*) "**magistrate**" includes a regional court magistrate;

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

(*f*) "**specifically designated member of a law enforcement agency**" means—

* 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
* 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—

- make oral applications for a search warrant or an amendment of a warrant contemplated in **clause 30**;
- issue expedited preservation of data directions contemplated in **clause 40**; or
- serve a disclosure of data direction from the designated judge on a person or electronic communications service provider contemplated in **clause 41(7)**.

3.4.3 Various other laws contain provisions which may be used to investigate aspects relating to cybercrime, see in this regard, inter alia, sections 82 and 83 of the Electronic Communications and Transactions Act, 2002, the RICA, section 11 of the Intelligence Services Act, 2002 (Act 65 of 2002), Chapter 2 of the Criminal Procedure Act, 1977. The purpose of Chapter 4 is to establish additional procedures which cater specifically for the investigation of cybercrime. In terms of **clause 27** the provisions in Chapter 4 of the Bill apply in addition to Chapter 2 of the Criminal Procedure Act, 1977, or any other applicable law that regulates the search and seizure of articles connected with offences. **Clause 27** further provides that Chapter 4 also applies in addition to Chapter 2 of the International Co-operation in Criminal Matters Act, 1996 (Act 75 of 1996), which

regulates requests to and from foreign States to provide evidence in criminal matters. **Clause 28** of the Bill provides that a 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.

3.4.5 The warrant requirement in criminal investigations is a tried and tested method to protect individuals against the power of the State, ensuring that the police cannot invade private homes or private communications upon a whim, or to terrorise. Open democratic societies throughout the world have fashioned the warrant process as the mechanism to balance the public interest in combating crime with the individual's constitutional rights. The warrant process guarantees that the State must justify and support intrusions upon individuals' rights under oath before a neutral judicial officer prior to the intrusion. It furthermore governs the time, place and scope of the search, limiting the intrusion of rights, guiding the State in the conduct of the inspection and informing the subject of the legality and limits of the search. In similar trend to section 21 of the Criminal Procedure Act, 1977, **clause 29** of the Bill, provides that an article can only be accessed or seized in terms of a search warrant. Clause 29, however, differs in various aspects from section 21 of the Criminal Procedure Act, in order to provide for the search and access or seizure of evidence relevant to cybercrime. **Clause 29(1)** provides that an article referred to in clause 28 can only be accessed or seized by virtue of a search warrant issued—

* 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 that there are reasonable grounds for believing that an article is—
    - within his or her area of jurisdiction; or
    - being used or is involved in the commission of an offence within his or her area of jurisdiction, or 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
* 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.

Clause 29(2) provides that a search warrant issued by a magistrate or judge 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, authorizes the member of a law enforcement agency or an investigator who is accompanied by a member of the law enforcement agency to—

* search any person identified in the warrant;
* enter and search any container, premises, vehicle, facility, ship or aircraft identified in the warrant;
* 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 a container, on or at such premises, vehicle, facility, ship or aircraft;
* 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 nearby, who uses or who is in possession of or in direct control of any data, a computer device, a computer network, a database, a critical database, an electronic communications network or a National Critical Information Infrastructure identified in the warrant to the extent as is set out in the warrant;
* access and search any data, a computer device, a computer network, a database, a critical database, an electronic communications network or a National Critical Information Infrastructure identified in the warrant to the extent as is set out in the warrant;
* 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, a computer device, a computer network, a database, a critical database, an electronic communications network or a National Critical Information Infrastructure identified in the warrant to the extent as is set out in the warrant;
* copy any data or other information to the extent as is set out in the warrant; or
* seize an article identified in the warrant to the extent as is set out in the warrant.

Clause 29(3) provides that whenever a search warrant, issued under **clause 29(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 **clause 35(2)**, be carried out by a member of the law enforcement agency accompanying the investigator.

In terms of **clause 29(4)**, a search warrant may be executed at any time, unless the person issuing the warrant in writing specifies otherwise.

In terms of **clause 29(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 clause 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.

3.4.6 In some instances it is necessary to search and gain access to or seize items immediately or urgently. The procedures for obtaining a search warrant under **clause 29(1)(*a*)** on information on oath will, in such circumstances, defeat the objects of the search. This is especially applicable to crimes committed in cyber space, where a real possibility exists that evidence may be lost. In many instances highly relevant information is often deleted automatically after a short period of time. The reason for this automatic deletion is because after the end of a process (e.g. the sending out of an e-mail, accessing the Internet or downloading child pornography), the traffic data that has been generated during the process and that ensures that the process could be carried out is no longer needed. There is also the possibility that a perpetrator of cybercrime may cover his or her tracks by deleting or altering highly incriminating data. Although section 22 of the Criminal Procedure Act, 1977, provides that a member of a law enforcement agency may, without a search warrant, conduct a search it is highly undesirable to afford such powers to the law enforcement agencies where databases of banks, electronic communications service providers or National Critical Information Infrastructures may be involved.

Clause 30 of the Bill aims to balance the interests of natural and legal persons to ensure the privacy and confidentiality of information in their possession and control with the interests of the law enforcement agencies to search for and access or seize an article involved in a cybercrime. To this end **clause 30** provides for the oral application for, or for the amendment of search warrants contemplated in **clause 29(1)(*a*)**, 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. In terms of this clause:

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

(*b*) A magistrate or judge of the High court may, upon an oral application made to him or her, issue the warrant applied 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—

* within his or her area of jurisdiction; or
* 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
* 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 warrant applied for; and

(iii) on condition that the member of the law enforcement agency concerned submits a written application to the magistrate or judge of the High Court concerned within 48 hours after the issuing of the oral warrant.

(*c*) A warrant issued following an oral application must be in writing and must be transmitted electronically to the member of the law enforcement agency.

(*d*) A magistrate or judge of the High Court who issued a warrant under this clause 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 paragraph (*b*)(iii) reconsider that application whereupon he or she may confirm, amend or cancel that warrant.

Clause 31 of the Bill, however, provides that a 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 the Act, subject to any other law if the person who has the lawfully authority to consent to the—

* search for and access to or seizure of the article in question; or
* 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.

3.4.7 **Clause 32**, similar to section 23 of the Criminal Procedure Act, 1977, provides that, on the arrest of any person on suspicion that he or she has committed an offence under the Bill or any other offence, a member of a law enforcement agency may search the arrested person and seize any article referred to in clause 28 which is in the possession of, in the custody of or under the control of the arrested person. This clause further authorises a member of a law enforcement agency or or an investigator who is accompanied by a member of a law enforcement agency to access and search the seized article. The definition of “article” is relevant to the interpretation of this clause since it restricts the ambit thereof which may otherwise have unforeseen consequences. An article can only be seized and can only be accessed if it qualifies as an article, in that it—

* is concerned in or is, on reasonable grounds, believed to be concerned in the commission or suspected commission;
* may afford evidence of the commission or suspected commission; or

* 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 the Bill or any other offence which may be committed by means of or facilitated through the use of an article.

3.4.8 Electronic communications networks and are relatively complicated and may consist of various servers and associated infrastructure which makes it extremely difficult for law enforcement agencies to locate and access or seize the required evidence. Electronic devices which store and transmit data are protected by passwords, access devices or encryption from unauthorised access. Data is, in many instances, encrypted which make intelligible access to data virtually impossible. In most instances the person in control of an electronic communications network or a database can assist the law enforcement agencies to locate as well as access or seize the required evidence. In terms of **clause 33** of the Bill an electronic communications service provider or person, other than the person who is suspected of having committed an offence under the Bill, who is in control of any container, premises, vehicle, facility, ship, aircraft, data, computer device, computer network, database, critical database, electronic communications network or a National Critical Information Infrastructure or any other information, instrument, device or equipment that is subject to a search authorised in terms of clause 29(1) or 30(3) or which takes place in terms of clause 31 must, if required, provide—

* technical assistance; and
* 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—

* access, or use any data, computer device, computer network, database, critical database, electronic communications network or a National Critical Information Infrastructure or any other information, instrument, device or equipment;
* copy data or other information;
* obtain an intelligible output of data; or
* remove a computer device, any part of a computer network, a database, a critical database, an electronic communications network or a National Critical Information Infrastructure.

3.4.9 **Clause 34** of the Bill contains the following provisions to ensure that law enforcement agencies and investigators who are accompanied by members of a law enforcement agency are not hindered in an investigation:

* **Clause 34(1)** of the Bill provides that 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 performing of his or her duties or functions in terms of Chapter 4 or who refuses or fails to comply with a search warrant issued in terms of clause section 29(1), section 30(3) or which takes place in terms of section 31, is guilty of an offence.
* **Clause 34(2)** provides that 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 clause 29(2) of the Bill, may use such force as may be reasonably necessary, proportional to all the circumstances relating to the execution of such powers.

Similar to the Criminal Procedure Act, 1977, and various other laws which authorise the use of force to enter premises, this clause further provides that no member of a law enforcement agency may enter upon or search any premises, vehicle, ship or aircraft unless he or she has audibly demanded admission to the premises, vehicle, ship or aircraft and has notified the purpose of his or her entry. However, due to the fact that electronic evidence may easily be altered or destroyed, provision is further made that a member of a law enforcement agency may enter premises without demanding admission, if he or she 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.

3.4.10 In a democratic society it is a requirement that the powers conferred upon the State to investigate crime should be tempered in order to ensure that an unfettered discretion is not given to law enforcement agencies in the execution of their powers. This is done by introducing additional conditions that balance these powers. In this regard these powers are further regulated by **clauses 35 and 36**.

Clause 35 of the Bill provides that 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 clause 29(2) of the Bill, must be conducted with strict regard to decency and order and with due regard to the the rights, responsibilities and legitimate interests of other persons in proportion to the severity of the offence. This clause further provides that if a female needs to be physically searched, such search must be carried out by a female.

Clause 36 of the Bill criminalises the conduct of a member of a law enforcement agency or an investigator—

* who acts contrary to the authority of a search warrant issued under clause 29(1) or clause 30(3) of the Bill or the provision of any other law which affords similar powers to a member of a law enforcement agency or investigator; or
* who, without being authorized thereto under Chapter 4 of the Bill or the provision of any other law which affords similar powers to a member of a law enforcement agency or investigator—
    - 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;
    - obtains any instrument, device, password, decryption key or other information that is necessary to access or use 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
* who obtains and uses any instrument, device, password, decryption key or other information contemplated in clause 29(2)(*f*), for other purposes as set out in warrant, or does not destroy all information if such information will not be required for purposes of court proceedings or for purposes of an order of court.

The clause further provides that if a member of a law enforcement agency or an investigator is convicted of an offence in terms of this clause, 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, applies *mutatis mutandis* with reference to such award.

3.4.11 The impact of an investigation relating to cybercrime is of such a nature that a lot of specialised manpower is necessary to investigate the offence in question which may impact on the availability of electronic resources and adversely affect the productivity of a company or the State. Furthermore, cybercrime investigations, to a greater or lesser extent, will almost always make inroads on the privacy and other rights of a person. **Clause 37** of the Bill therefore aims to counter these adverse effects by criminalising the giving of false information on oath or by way of affirmation which results in a search warrant being issued, or being issued and executed on the basis of such information. The clause further provides that if a person is convicted of an offence in terms of this clause, 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, applies *mutatis mutandis* with reference to such award.

3.4.12 In order to protect the integrity of the investigation process and to ensure that offenders are not warned in advance of an investigation which may lead to the tampering with or destruction of evidence, **clause 38** of the Bill provides that 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 obtained in the exercising of his, her or its powers or the performance of his, her or its duties in terms of the Bill, except—

* to any other person who of necessity requires it for the performance of his or her functions in terms of the Bill;
* if he or she is a person who of necessity supplies such information in the performance of his or her functions in terms of the Bill;
* if it is information which is required in terms of any law or as evidence in any court of law; or
* to any competent authority which requires it for the institution of criminal proceedings or an investigation with a view to instituting criminal proceedings.

3.4.13 User interaction with computer devices produces a wealth of computer generated digital traces. These digital traces are relevant to the investigation of cybercrime and can, in some instances, indicate the origin, destination, content of a communication and underlying service used. Computer data potentially relevant to a criminal act may include photographs, videos, emails, chat logs and system data. This evidence can be altered or obliterated easily. Locating relevant information within this data can further be extremely time-consuming, requiring long periods of availability of data. The identification of an offender who has committed a cybercrime usually requires an analysis of data. One of the main difficulties that investigators face is the fact that data which can be used to identify the cyber-offender or the criminal act is more often than not available after a short period of time only. Although there are obligations on electronic communications service providers to record and store certain information in terms of section 30 of the RICA, no such obligations were imposed on Internet service providers in terms of section 30(2) of the RICA. Furthermore, obligations imposed on electronic communications service providers in this regard do not provide for the preservation of all digital evidence which may be relevant to a cyber offence. In so far as electronic communications service providers are obliged to intercept, record and store data, **clause 39** of the Bill provides that the provisions of the RICA must be utilized to obtain obtain this information.

Clause 40 of the Bill provides for an expedited preservation of data mechanism, where persons or electronic communications service providers are under no obligation to intercept, record or store information as required by the RICA. This mechanism, in so far as it relates to traffic data, forms part of most international instruments and various international laws dealing with cybercrime. This procedure does not only guarantee the availability of digital evidence but also ensures that it must be retained as is on the electronic communications network of the electronic communications service provider or on the database of a person who stores such information in order to ensure the integrity and availability of the information. Seen from an Internet service provider's perspective, data preservation is a less intensive instrument compared to data retention. Internet Service Providers do not need to store all data for all users, but instead have to ensure that specific data is not deleted as soon as they receive a preservation request. However, the proposed legislative intervention is wider than the international notion of

data preservation, in that it applies, in addition to traffic data, also to other forms of data, for instance information that is stored on a computer device or a database or which may become available. **Clause 40** provides that a specifically designated member of a law enforcement agency, may if he or she, on reasonable grounds, believes that any person or electronic communications service provider may be in possession of, or is in control of data concerned in the commission or intended commission of an offence in the Republic or an offence substantially similar to an offence recognized in the Republic committed in a foreign State, issue an expedited preservation of data direction to a person or electronic communications service provider. The effect of an expedited preservation of data direction is that the person or electronic communications service provider must immediately, from the moment of service of the direction, and for a period of 120 days (which may be extended by a preservation of evidence direction issued by a judicial officer in terms of clause 42 of the Bill), preserve the current status of data in order to preserve the integrity of the data. However, no data may be disclosed to a law enforcement agency on the strength of a preservation of data direction. The clause further provides that a person or electronic communications service provider to whom an expedited preservation of data direction 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.

The Bill provides for separate procedures for the expedited preservation of data and the expedited disclosure of data. Although the immediate availability of data will enable law enforcement agencies to respond faster to an alleged cybercrime, the rights of the concerned individual, most notably the right to privacy should be protected. Prior judicial authorization for a procedural intervention on the rights of an individual is usually a prerequisite. **Clause 41** of the Bill therefore requires prior judicial authorization before data can be disclosed. This clause provides that a judicial officer may, on written application by a law enforcement agency, if it appears to the judicial officer 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 be in possession of data which is relevant to or which may afford evidence of, the

commission or intended commission of an offence, issue a disclosure of data direction. This clause sets out the conditions which an application must adhere to, inter alia, giving a description of the data which must be provided and a description of the offence which has been or is being or will probably be committed. In considering the application the judicial officer must satisfy himself or herself of the reasonableness of the grounds for believing that an offence is or was committed by means of, or facilitated by the use of an article or that it is necessary to determine whether such an offence has been so committed, and that it will be in the interests of justice if a disclosure of data direction is issued. The power of a magistrate or a judge of the High Court to authorize the disclosure of data is however subject to the provisions of sections 15(2), 16 and 17 of the RICA. This means that content of a communication, or real-time communication-related information on an ongoing basis, which was preserved in terms of clause 40, can only be provided in terms of a direction of a designated judge. Clause 40(4) further authorizes the designated judge, on request of an authority, court or tribunal of a foreign State, on 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 be in possession of data which is relevant to, or which may afford evidence of, the commission or intended commission of an offence similar to those contemplated in Chapter 2 of this Bill, or 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, to issue a disclosure of data direction. However, a disclosure of data direction on request of an authority, court or tribunal of a foreign State, can only be issued if there is further compliance with this clause which, inter alia, requires—

* a description of the data which must be provided and a description of the offence (which must be similar to an offence in the Republic) which has been or is being or will probably be committed;
* that the request is, where applicable, in accordance with—
    - any treaty, convention or other international agreement to which that foreign State and the Republic are parties, or any agreement with any foreign State entered into in terms of clause 64 of the Bill; and
    - that it will be in the interests of justice if a disclosure of data direction is issued; and

* that the Cabinet member responsible for the administration of justice, is informed of the—
  - fact that he or she intends to issue a disclosure of data direction; and
  - reasons for such decision.

A disclosure of data direction must—

* direct the person or electronic communications service provider to provide the data identified in the direction to the extent as is set out in the direction to an identified member of the law enforcement agency;
* must set out the period within which the data must be provided; and
* may specify conditions or restrictions relating to the provision of data authorised therein.

The clause further provides that a person or electronic communications service provider to whom disclosure of data direction is addressed, may in writing apply to the judicial officer 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. Non-compliance with a disclosure of data direction is criminalized.

3.4.15 In the investigation of cybercrime, other evidence, which may be hardware related, may be relevant to prove the commission of the offence, inter alia, a router with a backdoor, a hardware interception device connected to a computer or a computer network or a server with information on it. It is a well establish principle in the investigation of cybercrime that collated evidence should be preserved in as close to its original state as possible. In order to ensure the proper preservation and collection of evidence, computer devices or other hardware must be preserved as is, for purposes of a forensic investigation. The mere switching a computer device on or off may alter the evidence. If a computer device is switched off information in the Random Access Memory of the computer will, in most cases, be lost. The reason for preserving the evidence in as close to its original state as possible is that it may affect the admissibility of evidence (the chain of custody of evidence) if it was further handled by other persons or subjected to further processes before the investigation takes place. **Clause 42** of the Bill provides that a magistrate or judge of the High Court, may on written application by a law enforcement agency, if it appears to the magistrate or judge, from information on oath or by way of affirmation that that there are reasonable grounds for believing that

any person or electronic communications service provider may be in possession of, or in control of an article which may afford evidence of the commission or intended commission of an offence contemplated in the Bill, issue a preservation of evidence direction. 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. The preservation of evidence direction will direct the person or electronic communications service provider, from the moment of service of the direction, and for the time period specified in the direction, to—

* preserve the current status of;
* not to deal in any manner with; or
* to deal in a certain manner with,

an article in order to preserve the integrity of the evidence. Non-compliance with preservation of evidence direction is criminalized. The person or electronic communications service provider on whom a preservation of evidence direction is served may in writing apply to a magistrate or judge of the High Court for an amendment or the cancellation of the direction on the ground that he, she or it cannot timeously or in a reasonable fashion comply with the order. **Clause 43** makes provision for an oral application for a preservation of evidence direction in urgent cases.

3.4.16 **Clause 44(1)** of the Bill provides that a member of a law enforcement agency or an investigator may—

* access public available data regardless of where the data is located geographically;
* access or receive non-public available data, regardless of where the data is geographically located, if the person who has the lawful authority to disclose the data, voluntarily, in writing, consents to such accessing of data, or provides the data to a member of a law enforcement agency or an investigator; or
* access any data, regardless of where the data is located geographically, if such data is lawfully accessible from, or 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 in terms of clause 29, 30, 31 or 32.

The first two grounds of access are in line with Article 32 of the European Convention on Cybercrime. Access to public available data, is defined as data which is without restriction accessible in the public domain, does not require further elaboration. If everybody else can access such data so can the law enforcement agencies. On similar grounds access to non-public available data with the voluntary consent of the person who has lawful authority to allow access to or to provide data, can be justified.

Since cybercrimes often have an international dimension which, in turn, implies that the cybercriminal and the victim may be in separate countries, whilst the electronic resources of a third country may primarily be used to commit the offence in question. Cybercrime is by no means the first type of crime to demand a global response. Over the past decades, global action has been required to address challenges such as illicit drug trafficking, trafficking in persons and transnational organized crime, through the development of international agreements. Nonetheless, cybercrime presents unique international cooperation challenges. One of the key demands of investigators in transnational investigations is the need for immediate reaction of their counterparts in the country where the offender is located. The European Convention on Cybercrime (Article 23 and 25) contains the following principles regarding international cooperation in cybercrime investigations among the members:

* Cooperation in international investigations to the widest extent possible should be provided;
* this cooperation does not only apply in cybercrime investigations but in any investigation where evidence in electronic format needs to be collected;
* parties must co-operate with each other on the basis of international instruments on international co-operation in criminal matters, arrangements agreed to on the basis of uniform or reciprocal legislation, and domestic laws; and
* fast communication in cybercrime investigations is necessary.

In many instances the country in which the offences are committed may not even be aware of the conduct of the cyber criminal who may have committed similar offences in that country or other countries. Within cybercrime investigations carried out on a national level, links to offences related to another country might be discovered. If law enforcement agencies, for example, investigate a child pornography case, they might find information about pedophiles from other countries that have participated in the

exchange of child pornography. Article 26 of the European Convention provides for the law enforcement agencies to inform foreign law enforcement agencies without jeopardizing their own investigation. In addition to forms of formal international cooperation, parts of the process of extraterritorial law enforcement investigations may be undertaken by informal police-to-police communications. Such communications can be used prior to a formal mutual legal assistance request to a competent authority, or to facilitate a formal request. In similar vein the Bill provides for a mechanism which may be used by the South African law enforcement agencies to cooperate with any foreign law enforcement agency for purposes of investigating cybercrime and offences which may be committed or facilitated by means of an article. The network of informal bilateral relationships between law enforcement agencies, INTERPOL, currently serves this purpose and facilitates informal police-to-police requests. In this regard **clause 44(2)** of the Bill provides that a law enforcement agency may, after obtaining the written approval of the National Director of Public Prosecutions, forward any information obtained during any investigation to a law enforcement agency of a foreign State when the law enforcement agency is of the opinion that the disclosure of such information may—

* assist the foreign State in the initiation or carrying out of investigations regarding an offence committed within the jurisdiction of a foreign State;
* lead to further cooperation with a foreign State to carry out an investigation regarding the commission or intended commission of an offence contemplated in terms of the Bill which was committed within the Republic; or an offence which was committed in a foreign State.

In terms of **clause 44(3)**, the information may only be forwarded to the foreign State if the National Director of Public Prosecutions approves it in writing after he or she is satisfied that the forwarding of information —

* will not affect any pending criminal proceedings or investigations adversely regarding criminal offences committed within the Republic; and
* is in accordance with any applicable law of the Republic.

Clause 44(4) provides that a law enforcement agency may receive any information from a foreign State which will—

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

* lead to further cooperation with a foreign State to carry out an investigation regarding the commission or intended commission of an offence contemplated in the Bill.

Where informal police-to-police networks are used in matters such as locating witnesses or suspects, conducting interviews, or sharing police files or documentation, two particular concerns are frequently raised, namely—

* that the request is not perceived in the requested state as an attempt to conduct foreign criminal investigations without the proper authority; and
* that any evidence obtained for use in a court of law may not meet the required standard of admissibility.

Subclauses (2) to (4) are, however, not intended to provide formal evidence or receive formal evidence which may be used in a criminal trial. Their purpose is to provide information which enables a law enforcement agency to become aware of an offence which can then be investigated further.

3.4.17 Cybercrime investigations at international level fail because the investigations take too long and important data is therefore lost before procedural measures are instituted to preserve or access or seize data or other information. Investigations that require mutual legal assistance do in general take long due to the time-consuming formal requirements. Informal police-to-police investigations, for the reasons set out in paragraph 3.4.16, cannot be used for formal legal assistance. International cooperation is, in many instances, based on international or regional Conventions or agreements, which set out the obligations of the respective parties. South Africa has signed the European Convention on Cybercrime but has not ratified the Convention. The African Union Convention on Cyberspace Security and Personal Data Protection has not yet been finalized, which would, on a regional basis, cater for cooperation within the African Union. The Republic is further not a party to any other International or Regional instrument that specifically deals with cooperation in cybercrime matters. Chapter 2 of the International Co-operation in Criminal Matters Act, 1996 (Act No. 75 of 1996), regulates international co-operation in criminal matters in the Republic. **Clauses 45 to 48** of the Bill deal with formal international cooperation.

Clause 45 of the Bill provides for the manner in which foreign assistance and cooperation in cyber related matters must be requested. The clause makes provision for an ordinary procedure and an expedited procedure for requesting foreign assistance and cooperation. In terms of **clause 45(1)**, a judicial officer may if it appears from information on oath or by way of affirmation that there are reasonable grounds for believing that an article necessary for the investigation and prosecution of an offence contemplated in the Bill is in the possession of, under the control of or upon any person, in a container, upon or at any premises, vehicle, 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 judicial officer may issue a direction in the prescribed form, in which assistance from that foreign State is sought to preserve an article or to intercept or obtain and provide data, as is stated in the direction. In terms of **clause 45(2)**, the direction must specify that—

* there are reasonable grounds for believing that an offence contemplated in the Bill has been committed in the Republic or that it is necessary to determine whether an offence has been committed;
* an investigation in respect thereof is being conducted; and
* 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.

In terms of **clause 45(3)**, in the case of an ordinary request for assistance, a direction is sent to the National Director of Public Prosecutions for transmission to—

* the court or tribunal specified in the direction;
* the appropriate authority in the foreign State which is requested to provide assistance and cooperation; or
* a designated 24/7 contact point in the foreign State which is requested to provide assistance and cooperation.

In terms of **clause 45(4)**, in a case of urgency, a direction may be transmitted directly to the court or tribunal, the appropriate government body or designated 24/7 contact point and the National Director of Public Prosecutions must, as soon as practicable be notified of that fact and a copy of the direction must be furnished to him or her. In terms of **clause 45(5)**, the Cabinet member responsible for the administration of justice must

be informed of the fact that a direction, as contemplated in clause 44 has been sent to a court or tribunal or the appropriate authority in the foreign State.

Clause 46 provides for the converse situation contemplated in clause 45, namely, where the Republic is requested to provide foreign assistance and cooperation. This clause also makes provision for an ordinary procedure and an expedited procedure for requesting assistance and cooperation. In terms of **clause 46(1)**, a request by an authority, court or tribunal exercising jurisdiction in a foreign State for assistance in preserving, obtaining and providing or intercepting and providing an article in the Republic for use in such foreign State must be submitted—

* to the 24/7 point of contact established in terms of **clause 49** of the Bill, which must submit it to the National Director of Public Prosecutions or, in case of urgency, to the designated judge;
* the National Director of Public Prosecutions; or
* in case of urgency, to the designated judge,

for consideration.

In terms of an ordinary application for assistance which is submitted to the National Director of Public Prosecutions, **clause 46(2)** provides that he or she must satisfy himself or herself—

* that proceedings have been instituted in a court or tribunal exercising jurisdiction in the requesting State or territory; or
* that there are reasonable grounds for believing that an offence has been committed in the requesting State or territory 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 State or territory.

Similar considerations are applicable, in terms of **clause 46(3)** of the Bill, if an urgent application serves before the designated judge. In addition this clause requires the designated judge to obtain the recommendations of the National Director of Public Prosecutions on the request. In terms of **clause 46(4)**, 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 State or territory concerned, stating the facts contemplated in the said subsections. In terms of the general procedure for assistance, **clause 46(5)** requires that the National Director of Public Prosecutions must, if he or she approves of

the application, submit the request together with his or her recommendations, to the Cabinet member responsible for the administration of justice, for his or her approval. If the request is approved by the Minister it must be submitted to the designated judge for approval. In terms of **clause 46(6)**, the designated judge may, subject to the conditions set out in **clause 46(7)**, issue any order which he or she deems appropriate to ensure that the requested article is preserved for a period or obtained and provided or intercepted and provided. In the case of a urgent request which was submitted directly to the designated judge. Before the designated judge may issue an order as contemplated in clause 46(6)(a), the designated judge must inform the Cabinet member responsible for the administration of justice, in writing, of the fact that he or she intends to issue an order and the reasons for the decision. In terms of **clause 46(8)**, the order of the designated judge must be executed by a member of the South African Police Service who was specifically designated in writing by the National Commissioner to execute such orders.

Clause 47 criminalizes non-compliance with an order of a designated judge. Provision is, however, made that a person or electronic communications service provider to whom an order 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. If the application for the amendment or the cancellation of the order is successful the National Director of Public Prosecutions must be informed of the outcome of the application.

Clause 48 provides for the manner in which a foreign State must be informed of the outcome of a request for assistance and cooperation and also provides for the manner in which information must be provided to the foreign State. In terms of **clause 48(1)** of the Bill, the National Director of Public has the responsibility of informing a foreign State of the outcome of its request for assistance and cooperation. **Clause 48(2)** provides that the data which was obtained or intercepted pursuant to the order of the designated judge must be provided to the 24/7 Point of Contact, for provision 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. The information must be accompanied by the order of the designated

judge and 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. **Clause 48(3)** obliges a person or electronic communications service provider to keep copies of any the information which is furnished to the 24/7 Point of Contact, in a manner which will ensure the authenticity, integrity and reliability of the information. **Clause 48(4)** provides that the information, together with the copy of the order and affidavit, must be provided to the authority, court or tribunal exercising jurisdiction in a foreign State who requested the assistance.

3.5 Establishing of a 24/7 Point of Contact

Cybercrime investigations often require immediate reaction. In order to expedite international investigations, various international and regional instruments, inter alia, Article 35 of the European Convention on Cybercrime, propose that countries should designate a contact point for mutual assistance requests, which contact point should be available on a twenty-four hour, seven days a week basis, in order to ensure assistance in cyber related matters. The purpose behind 24/7 Points of Contact is mainly to address the challenges relating to the investigation of cybercrime which has an international dimension, especially in so far as it relates to information exchange. 24/7 Points of Contact usually ensure immediate action against the investigation of cybercrime. The current position in the Republic is that a 24/7 Contact Point is not institutionalised. In terms of the European Convention the functions of a 24/7 Point of Contact are to provide technical assistance and advice, assist with the preservation of data and collection of evidence, the provision of legal information and the location of suspects. In order to ensure that 24/7 Points of Contact can carry out their functions they must be adequately equipped to receive and make available requested information and must have trained personnel, both technical and legal, to carry outs their functions. **Clause 49** of the Bill makes provision for the establishment of a 24/7 Point of Contact for the Republic. In terms of **clause 49(1)**, the Cabinet member responsible for policing must, at State expense, establish a 24/7 Point of Contact and equip, operate and maintain the 24/7 Point of Contact. In terms of **clause 49(3)**, a member of the South African Police Service, who on the grounds of his or her technical knowledge and experience is a suitable and qualified person, must be appointed as the

Director of the 24/7 Point of Contact. The Director is 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. The clause further provides that the Director must, in the exercise of his or her powers, the performance of his or her functions and carrying out of his or her duties, be assisted by –

(a) appropriately qualified members of the South African Police Service;

(b) a member of the National Prosecuting Authority who has particular knowledge and skills in respect of any aspect dealt with in this Act and who is seconded or designated to the 24/7 Point of contact to assist the Director; and

(c) persons or entities who are, from time to time, appointed to assist the Director.

Due to the nature of the work involved it is a requirement that a security clearance should be issued to these persons. The functions of the 24/7 Point of Contact are set out in **clause 49(4)**, which provides that 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 an offence contemplated in the Bill, which assistance includes—

* the provision of technical advice and assistance;
* the facilitation or provision of assistance regarding anything which is authorised under Chapter 4 of the Bill;
* the provision of legal information;
* the identification and location of an article;
* the identification and location of a suspect; and
* cooperation with appropriate authorities of a foreign State.

In terms of **clause 49(5)**, the Cabinet member responsible for policing may, after consultation with the Cyber Response Committee, make regulations to further regulate any aspect which is necessary or expedient for the proper implementation of this provision. In terms of **clause 49(6)**, 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 to report on the functions and activities of the 24/7 Point of Contact.

3.6 Structures to deal with cyber security

3.6.1 In order to centralise the coordination of cybersecurity activities, relevant structures are established in terms of **clauses 51 to 57** in order to deal with cybersecurity.

3.6.2 In terms of **clause 51** a dedicated Cybersecurity Response Committee (hereinafter referred to as the "CRC") will be established to coordinate cybersecurity activities and manage the implementation of Output 8. The CRC will be chaired by the State Security Agency and it will be supported operationally by a Cyber Security Centre, situated within the State Security Agency. Various Departments will be represented on the Cybersecurity Response Committee. The CRC consists of a Chairperson, who is the Director-General: State Security, members of various Departments, who are the Heads of such Departments and their nominees, and persons who have particular knowledge and skills in respect of any aspect dealt with in the Bill who are, from time to time, requested to assist the Committee. **Clause 51(6)** set out the objects and functions of the CRC, which are to—

(*a*) implement Government policy relating to cyber security;

(*b*) identify and prioritise areas of intervention;

(*c*) coordinate cyber security activities and be a central point of contact on all cyber security matters pertinent to national security;

(*d*) identify and prioritise areas of intervention and promote focussed attention and guidance where required regarding cyber security related threats and incidents;

(*e*) promote, guide and coordinate activities aimed at improving cyber security measures by all role players, which would include amongst others, the strengthening of intelligence collection and improve the State's 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, Government Security Incident Response Teams, the National Cybercrime Centre, the Cyber Command, Cyber Security Hub and Private Sector Security Incident Response Teams established in the Republic;

(*g*) promote and provide guidance to the process of the development and implementation of—

* the protection of the National Critical Information Infrastructure Plan;

* situational analysis and awareness campaigns concerning the risk environment of South African cyberspace;
* a cyber security culture and compliance with minimum security standards;
* public-private partnerships and national and regional action plans in line with Government policy;
* appropriate technical and operational cyber security standards;
* cyber security training, education, research and development and skills development programmes; and
* international cooperation initiatives;

(*h*) facilitate interaction on cyber security, both nationally and internationally and to develop policy guidelines 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.

Clause 51(9) provides that the Cabinet member responsible for State security must oversee and exercise control over the performance of the functions of the CRC. **Clause 51(10)** provides that the Cabinet member responsible for State must, at the end of every financial year, submit a report to Chairperson of the Joint Standing Committee on Intelligence, regarding progress that has been made towards achieving the objects and functions of the CRC.

3.6.3 **Clause 52** provides for the establishment of a dedicated structure, namely the Cyber Security Centre, whose responsibilities are, inter alia—

* to develop measures to deal with cyber security matters impacting on national security;
* to facilitate the identification of and protection and securing of National Critical Information Infrastructures; and
* to respond to and to provide coordination and guidance pertaining to cyber security aspects which may affect the State.

In terms of **clause 52(1)** of the Bill, the Cabinet member responsible for State security, must establish and equip, operate and maintain a Cyber Security Centre**. Clause 52(3)** provides that the Cabinet member responsible for State security must enter into service

level agreements with the head of a department or any entity or institution, in respect of the provision of services by the Cyber Security Centre. In terms of **clause 52(4)**:

* A person must be appointed as Director of the Cyber Security Centre, subject to the control and directions of the Cabinet member responsible for State security.
* The Director will, in the exercise of his or her duties, be assisted by members of the State Security Agency designated to the Cyber Security Centre and other persons to whom security clearances have been issued and who, from time to time, are appointed to assist the Director.
* The Director is responsible for the day to day functioning of the Cyber Security Centre and must 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.
* The Director must 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 Private Sector Security Incident Response Teams.
* The Director must also, on a quarterly basis, or as the Chairperson of the CRC requires, submit a written report to the Cabinet member responsible for State security and the Chairperson of the CRC regarding matters relevant to, incidental to the functioning of the Cyber Security Centre.

Clause **52(5)** provides for the objects and and functions of the Cyber Security Centre which, inter alia, includes the development of measures to deal with cyber security matters impacting on national security and to act as a point of contact regarding matters relating to national intelligence.

3.6.4 **Clause 53** envisages that the existing Government Security Incident Response Teams will continue to exist and that additional Government Security Incident Response Teams should be established. In terms of **clause 53(1)**, the Cabinet member responsible for State security must, in consultation with the Cabinet member responsible for national financial matters, at State expense establish on or more Government Security Incident Response Teams and equip, operate and maintain the Government Security Incident Response Teams. In terms of **clause 53(3)**, the Cabinet member responsible for State security must enter into service level agreements with the

head of a department and any entity or institution, in respect of the provision of services by the Government Security Incident Response Teams. **Clause 53(4)** requires that the Director-General: State Security, must appoint a person from the State Security Agency who, on the grounds of his or her knowledge and experience is a suitable and qualified person, as head for each Government Security Incident Response Team, who is subject to the control and directions of the Director: Cyber Security Centre. The head of a Government Security Incident Response Team will be assisted in his or her daily functions by members of the State Security Agency designated to the Government Security Incident Response Team and knowledgeable persons who are, from time to time, appointed to assist the head. The head must, on a monthly basis, or as the Director: Cyber Security Centre requires, submit a written report to the Director: Cyber Security Centre—

* regarding cyber security related threats, and measures implemented to address such cyber security related threats and shortcomings in addressing such cyber security related threats;
* any matter relevant to, incidental to or which may impact on the objects and functions of the Government Security Incident Response Team; and
* any other matter relating to the Bill which the head wishes to or may want to bring to the attention of the Director: Cyber Security Centre or Cyber Response Committee.

The objects and functions of a Government Security Incident Response Team are set out in **clause 53(5)**, which are to—

* develop or acquire and implement measures to deal with cyber security matters impacting on national intelligence and national security;
* protect and secure National Critical Information Infrastructures;
* implement measures, on the written request of the Director-General: State Security, to assess and test National Critical Information Infrastructures, including vulnerability assessments, threat and risk assessment and penetration testing;
* provide a reactive service to the State, which includes responding to alerts and warnings, handling incidents, vulnerability handling and artifact handling;
* provide a proactive service to the State which includes intrusion alerts, vulnerability warnings, security advice and other similar announcements and

technical analysis of software, malware, intruder activities and related trends in order to help identify future threats and vulnerabilities;

* provide security audits and assessments;
* configure and maintain equipment, software, hardware, configurations and infrastructure;
* develop security tools;
* provide an intrusion detection service; and
* disseminate security related information to Government Departments; and
* provide security quality management services to the State .

Clause 53(6) provides that the Cabinet Member responsible for State security may, after consultation with the CRC make regulations to further regulate the objects and functions of a Government Security Incident Response Team. **Clause 53(8)** provides that the Cabinet member responsible for State security must, at the end of every 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.

3.6.5 **Clause 54** of the Bill provides for the establishment of a National Cybercrime Centre. The aim of establishing this structure within the South African Police Service is to ensure that a dedicated structure is created which focuses on cybercrime as opposed to other forms of crime. In terms of **clause 54(1)**, the Cabinet member responsible for policing must, in consultation with the Cabinet member responsible for national financial matters, at State expense establish a National Cybercrime Centre and equip, operate and maintain the National Cybercrime Centre. **Clause 54(3)**, among others, provides for—

* the appointment of a member from the Service, who on the grounds of his or her knowledge and experience, is a suitable and qualified person, as Director of the National Cybercrime Centre;
* the staffing of the National Cybercrime Centre;
* the powers and duties of the Director, which includes the co-ordination of the activities of the National Cybercrime Centre with those of the other structures established in terms of Chapters 5 and 6 of the Bill and the development and

implementation of cyber security policies and strategies in order to investigate and combat cybercrime.

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. The Director must further, on a quarterly basis, or as the Chairperson of the CRC requires, submit a written report to the Cabinet member responsible for policing and the Chairperson of the CRC regarding—

* 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;
* cyber crime trends;
* successes and shortcomings in investigative measures in order to investigate cybercrime, as well as successes and shortcomings in international cooperation in the investigation of cybercrime; and
* any matter relevant to, incidental to or which may impact on the objects and functions of the National Cybercrime Centre.

The objects and functions of the National Cybercrime Centre are set out in **clause 54(4)**, which are to—

.* facilitate the operational coordination of cyber security incident response activities with regard to the prevention, combating and investigation of crime;
* develop measures to deal with cyber security matters impacting on law enforcement;
* 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;
* provide coordination and guidance regarding corporate security and policy development, governance, risk management and compliance, identity and security management, security information and event management;
* establish, develop and maintain an adequate cyber forensics capacity;
* develop response protocols to guide coordinated responses to cyber security incidents and interact with the various stakeholders;

* develop and maintain cross-border law enforcement cooperation in respect of cybercrime;
* promote, establish and maintain public-private cooperation to fight cybercrime;
* promote, establish and maintain international cooperation to fight cybercrime; and
* develop capacity and implement measures to impede and to neutralize cyber security related incidents and threats.

In terms of **clause 54(5)**, the Cabinet Member responsible for policing may, after consultation with the CRC, make regulations to further regulate the objects and functions of the National Cybercrime Centre.

In terms of **clause 54(7)**, the Cabinet member responsible for policing must, at the end of every financial year, submit a report to Parliament regarding progress that has been made towards achieving the objects and functions of the National Cybercrime Centre.

3.6.6 In order to protect the interests of the Republic in the event of a cyber-war, a cyber-warfare capacity has to be built. The Department of Defence has overall responsibility for the coordination, accountability and implementation of cyber defence measures in the Republic as an integral part of its National Defence Mandate. A Cyber-warfare Strategy, that is informed by the National Security Strategy of South Africa, should be developed under guidance of the CRC. **Clause 55** of the Bill aims to establish a dedicated structure within the Department of Defence which has the responsibility of implementing and developing the cyber offensive and defensive capabilities of the South African National Defence Force. In terms of **clause 55(1)**, the Cabinet member responsible for defence must, in consultation with the Cabinet member responsible for national financial matters, at State expense, establish a Cyber Command and equip, operate and maintain the Cyber Command. **Clause 55(3)** provides for the appointment of the General Officer Commanding of and the staffing of the Cyber Command and also sets out the responsibilities of the General Officer Commanding and the reporting functions of the General Officer Commanding. **Clause 55(4)** sets out the objects and functions of the Cyber Command, which are to—

* facilitate the operational coordination of cyber security incident response activities regarding national defence;

* develop measures to deal with cyber security matters impacting on national defence;
* facilitate the analysis of cyber security incidents, trends, vulnerabilities, information sharing, technology exchange and threats on national defence to improve technical response coordination;
* provide guidance to and to facilitate the identification, protection and securing of National Critical Information Infrastructures relevant to national defence;
* 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 assessment and penetration testing;
* 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;
* act as a point of contact regarding matters relating to national defence; and
* coordinate and implement cyber offensive and defensive measures as part of its defence mandate.

Clause **55(5)** provides that the Cabinet Member responsible for defence may, after consultation with the CRC, make regulations to further regulates the objects and functions of the Cyber Command.

The Cabinet member responsible for defence must, in terms of **clause 55(7)**, at the end of each financial year, submit a report to Chairperson of the Joint Standing Committee on Defence, to report on the functions of the Cyber Command.

3.6.7 There is a need to ensure appropriate cooperation between Government, the private sector and civil society regarding cybersecurity matters. To that end there should be coordination and consultation between Government, the private sector and civil society regarding cybersecurity. **Clause 56** of the Bill provides for the establishment of a Cyber Security Hub within the Department of Telecommunications and Postal Services, the appointment of a person in charge of the Cyber Security Hub and his or her responsibilities and the staffing of the Cybersecurity Hub. The objects and functions of the Cyber Security Hub are set out in **Clause 56(5)**, which are, among others to—

* coordinate general cyber security activities in the private sector;

* 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;
* provide best practice guidance on Information and Communications Technology security to Government, electronic communications service providers and the private sector;
* initiate cyber security awareness campaigns;
* 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;
* encourage and facilitate the development of Private Sector Security Incident Response Teams;
* centralise co-ordination of cyber security activities in the private sector;
* respond to cyber security incidents;
* act as a point of contact regarding cyber security activities in the private sector; and
* assist the structures established under Chapter 6 of the Bill, with any aspect which may impact on their objects and functions.

3.6.8 In terms of **clause 57**, the Cyber Security Hub, has the responsibility of encouraging and facilitating the development of appropriate additional Private Sector Security Incident Response Teams. Clause 57 of the Bill provides for the recognition or establishment of Private Sector Security Incident Response Teams and also provides for the objects and functions the Private Sector Security Incident Response Teams. The functions of Private Sector Security Incident Response Teams are, among others, to—

* be a contact point for that specific sector on cyber security matters;
* coordinate cyber security incident response activities within that sector;
* facilitate information-sharing and technology-sharing within the sector;
* facilitate information-sharing and technology-exchange with other Private Sector Security Incident Response Teams established for other sectors and the Cyber Security Hub;
* establish minimum security standards and best practices for the sector for which it is established in consultation with the Cyber Security Hub;

* 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;
* 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; and
* provide sector entities within the sector for which it is established with best practice guidance on cyber security.

3.7 National Critical Information Infrastructure Protection

Information infrastructures are an essential part of the overall infrastructures supporting modern society. Ever more critical information resources are supplied and operated in partnership between the Government and the private sector and even in some instances across borders. Furthermore, infrastructure and information infrastructure have a necessary dependency on each other. There are many critical sectors whose operations depend on Information and Communication Technologies and it is therefore essential to protect these sectors from threats in cyberspace. Every developed and developing country across the world has already or is taking drastic steps to implement such protective measures. Ultimately, the goal is to protect these structures against all possible intrusions which may affect their day to day functions adversely. The critical need for information infrastructures and the measures of protection afforded thereto differs from jurisdiction to jurisdiction. Traditionally infrastructures which are of paramount importance to a country include defence, law enforcement, communications, energy (such as electricity and fuel), economy, transportation, water, food supplies, emergency services and Government services are also usually regarded as critical infrastructures. The aim of **Chapter 7 of the Bill** is to deal with information infrastructures which form part of these traditional infrastructures or which can be regarded as a critical information infrastructure. Information infrastructures enable large scale processes throughout the economy, facilitating complex interactions between systems across global networks. Their interactions propel innovation in industrial design and manufacturing, e-commerce, e-governance, communications, and many other

economic sectors. The information infrastructures provide for processing, transmission, and storage of vast amounts of vital information used in every domain of society and enable government agencies to interact with each other rapidly, as well as with industry, citizens, states and local governments. Information infrastructures encompass interconnected computer devices, computer networks, data bases and electronic communications systems. Various steps are necessary in order to provide for the protection of critical information infrastructures which, broadly speaking, encompass the following:

* An adequate legal framework to deal with critical information infrastructure protection;
* the implementation of a process of identifying the relevant information infrastructures which can be considered critical;
* the implementation of security measures to provide for the protection of critical information infrastructures and ensure compliance with these measures; and
* disaster management.

These steps are provided for in **clauses 58 to 60** of the Bill.

Clause 1 of the Bill defines a "National Critical Information Infrastructure as 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).

In terms of **clause 58(1)** of the Bill, the Cyber Security Centre, in consultation with the CRC and after consultation with any information infrastructure which is identified as a

potential National Critical Information Infrastructure, must within 12 months of the fixed date, submit to the Cabinet member responsible for State security, recommendations regarding information structures which need to be declared as National Critical Information Infrastructures. In terms of **clause 58(2)**, the Cabinet member responsible for State security may, after considering recommendations made to him or her by the Cyber Security Centre, by notice in the *Gazette*, declare any information structure, or category or class of information structures, as National Critical Information Infrastructures if it appears to the Cabinet member that an information infrastructure is so important that any interference therewith, or that its loss, damage, disruption or immobilization may—

* prejudice the security, defence, law enforcement or international relations of the Republic;
* prejudice the health or safety of the public;
* cause interference with or disruption of an essential service;
* causes any major economic loss;
* cause destabilization of the economy of the Republic; or
* create a public emergency situation.

Clause 58(3) makes it mandatory for the Cabinet member responsible for State security to follow a just administrative process before he or she declares an information infrastructure as a National Critical Information Infrastructure. The decision of the Cabinet member is subject to appeal to the High Court. In terms of **clause 58(4)**, an information infrastructure which is to be declared as a National Critical Information Infrastructure must comply with the regulations which the Cabinet member may make in terms of clause 58(5). In terms of **clause 58(5)**, the Cabinet member responsible for State security must make regulations regulating—

* the classification of information on National Critical Information Infrastructures;
* security policies and procedures to be applied to National Critical Information Infrastructures;
* access to National Critical Information Infrastructures;
* storing and archiving of information on National Critical Information Infrastructures;
* cyber security incident management and continuation with service provision;

* minimum physical and technical security measures that must be implemented in order to protect National Critical Information Infrastructures; and
* the period within which the owner of, or person in control of a National Critical Information Infrastructure must comply with the regulations.

The owner of, or person in control of, a National Critical Information Infrastructure must, in consultation with the Cabinet member responsible for State security and at own cost, take steps to the satisfaction of the Cabinet member in order to comply with these regulations (**clause 58(6)**). An 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, commits an offence if he or she fails to comply with the regulations and the Cabinet member may, at the cost of the owner or person, take the necessary steps to comply with the regulations (**clauses 58(7), (8) and (9)**).

Clause 59 provides for the establishment and control of a fund to be known as the National Critical Information Infrastructure Fund which must, among others, be utilised to implement disaster management measures in respect of National Critical Information Infrastructures in disaster situations. **Clause 59(9)** defines—

(a) **"disaster management measure"** as any measure aimed at—
* preventing or reducing the risk of a disaster;
* mitigating the severity or consequences of a disaster;
* emergency preparedness;
* rapid and effective responses to a disaster; and
* post-disaster recovery and rehabilitation; and

(b) "**disaster situation**" as 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.

Clause 60 of the Bill provides for an auditing process in order to evaluate compliance with the provisions of clause 58(6) of the Bill.

3.8 Evidence

Evidence is the means by which facts relevant to the guilt or innocence of an individual at a trial are established. Electronic evidence is all material that exists in electronic, or digital form, for instance data which makes up a virus and which deletes other data as opposed to real evidence, like a computer device. The South African common and statutory law (most notably Chapter III Part 1 of the Electronic Communications and Transactions Act, 2002), governs admissibility of electronic evidence. The current laws dealing with electronic evidence are, in general, sufficient for the purposes of criminal proceedings. However, the Bill proposes two clauses which provide for evidence by means of affidavits. The possibility of giving evidence by way of affidavit is recognised in various laws of the Republic. The rationale behind these provisions is to avoid an unnecessary waste of resources and time, especially where evidence needs to be adduced which originates from a foreign State. In many instances such evidence is not disputed and is sometimes formally admitted through admissions by the defence.

Sections 212 and 212A of the Criminal Procedure Act, 1977, make provision for the admissibility of certain affidavits. These sections provide for the reception of affidavits on their production as *prima facie* proof of their contents. Since these affidavits, at common law, constitute hearsay evidence whenever their probative value depends upon the credibility of any person other than the testifying witness, these sections make inroads on the hearsay rule. These affidavits can therefore only be regarded as *prima facie* proof of their contents if there strict is compliance with the prerequisites which are provided for their admissibility. As opposed to sections 212 and 212A of the Criminal Procedure Act, clause 61 caters specifically for disciplines relevant to information communications technologies which may be received in evidence by way of affidavit. Aspects relating to information communication technologies are not addressed adequately by section 212 or 212A of the Criminal Procedure Act. Section 212(4)(*a*)(iii) of the Criminal Procedure Act, as the only possible relevant provision, is restricted in its ambit to “computer science” which does not include all the other relevant disciplines which may play a role in, or which are relevant to, evidence relating to cybercrime. Section 212A, concerns itself with an act, transaction or occurrence which took place in a government institution, court of law or a bank of a foreign State, which also

substantially limits its relevance in sofar as it relates to the furnishing of evidence by affidavit in criminal proceedings involving cybercrime. **Clause 61** of the Bill aims to address this lacuna by further regulating the admissibility of an affidavit relating to facts established by any examination or process requiring any skill in—

* the interpretation of data;
* the design of, or functioning of data, a computer device, a computer network, a database, an electronic communications network;
* computer science;
* electronic communications networks and technology;
* software engineering; or
* computer programming.

In terms of this clause an affidavit made by a person who has certain expertise and who has established facts by means of an examination or process, is, upon its mere production at such proceedings, *prima facie* proof of such facts. The making of a false statement in an affidavit is criminalised. The clause gives a court before which an affidavit is produced as *prima facie* proof of the relevant contents thereof, the discretion to subpoena the person who made the affidavit to give oral evidence in the proceedings 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. **Clause 61(5)** sets out the prerequisites which must be met for such an affidavit to be admissible and also gives a court a discretion in order to clarify any obscurities in the affidavit, to order that a supplementary affidavit should be submitted or that oral evidence be heard at the proceedings.

Clause 62 provides for the admissibility of evidence which is provided in response to a direction contemplated in clause 45 of the Bill. In terms of this clause such evidence is deemed to be evidence under oath if—

* it is obtained in terms of an order of a competent court of a foreign State; or
* 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 is authenticated; and

* the person who makes the statement 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.

Evidence which is so obtained must be admitted as evidence at any proceedings and forms part of the record of such proceedings if—

* the party against whom the evidence is to be adduced agrees to the admission thereof as evidence at such proceedings; or
* the court, having regard to the nature of the proceedings, the nature of the evidence, the purpose for which the evidence is tendered, any prejudice which a party may suffer and any other factor which the court deems necessary to take into account, is of the opinion that such evidence should be admitted in the interests of justice.

The court before which evidence is produced as *prima facie* proof of the relevant contents thereof may, in its discretion—

* cause the person who made the statement to be subpoenaed to give oral evidence in the proceedings in question; or
* cause written interrogatories to be submitted to the person for reply and such interrogatories and reply are likewise admissible in evidence at such proceedings.

Clause 63 urges the courts not to apply the rules of evidence too strictly so as to preclude the admissibility of data, a data message or data document in evidence in criminal matters. The clause further provides for—

(a) general considerations which must be taken into account in assessing the admissibility and the evidential weight of data, a data message or a data document; and
(b) the admissibility of a copy or printout of data, a data message or a data document,

in criminal proceedings.

3.9 General obligations of electronic communications service providers and liability

Due to the mechanics of the Internet, the transmission of a communication involves a number of entities. For instance, in order to download child pornography, the content provider who uploaded the material (for example on a web storage facility), the access provider who provides access to the Internet, the hosting provider who provides the storage facility, the access provider who provides a person with access to the web storage facility halfway across the globe, are involved. Because of this involvement electronic communications service providers are always part of the investigation of criminal offences and law enforcement agencies are dependent on the cooperation of electronic communications service providers. Electronic communications service providers cannot monitor communications unless they are authorised to do so under judicial authority. On the other hand electronic communications service providers operate in a highly regulated environment which imposes obligations on them regarding the way in which they conduct their daily business, which are aimed at protecting their customers in cyberspace. For purposes of the Bill, electronic communications service providers are defined broadly so as to encompass other persons and entities, which are not traditionally regarded as electronic communications service providers. **Clause 1** of the Bill defines an electronic communications service provider as any—

"**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.

Clause 64 of the Bill sets out the general obligations of an electronic communications service provider which are—

* to take reasonable steps to inform its clients of cybercrime trends which affect or may affect the clients of such an electronic communications service provider;
* establish procedures for its clients to report cybercrimes with the electronic communications service provider;
* inform its clients of measures which a client may take in order to safeguard himself or herself against cybercrime; and
* when it becomes aware of the use of its computer network or electronic communications network to commit an offence, to—
    - immediately report the matter to the National Cybercrime Centre; and
    - 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.

Non-compliance with these obligations is criminalised.

3.10 Agreements with foreign State

As pointed out above, cybercrime most often involves an international dimension and, to that extent, international cooperation is essential for the investigation and prosecution of cybercrime. Although the Republic has signed the European Convention on Cyber Crime, it has not ratified the Convention. The Republic is further not a party to any regional or international agreement which deals specifically with measures to address cybercrime. To address cybercrime, other measures, in addition to the investigation of and prosecution of cybercrime, are necessary. Other strategies and measures which reduce the risk of crimes occurring and their potential harmful effects on individuals and society, on an international and regional basis, are also necessary. The United Nations Guidelines for the Prevention of Crime highlight that government leadership plays an important part in crime prevention, combined with cooperation and partnerships across countries. In terms of **clause 65** of the Bill, the President may enter into any agreement with any foreign State regarding—

* the provision of mutual assistance and cooperation relating to the investigation and prosecution of offences contemplated in the Bill;
* the implementation of cyber threat response activities;

* research, information and technology sharing, development and exchange on cyber security related matters;
* the protection and securing of National Critical Information Infrastructures;
* the establishment of 24/7 contact points;
* the implementation of emergency cross-border response mechanisms to address cyber threats;
* reciprocal implementation of measures to curb cybercrime; and
* the establishment of emergency centres to deal with cyber related threats.

3.11 General Provisions

3.11.1 **Clause 66** of the Bill proposes—

(a) the deletion of the following provisions—
  (i) section 71 of the South African Police Service Act, 1995;
  (ii) sections 40A and 41(4) of the National Prosecuting Authority Act, 1998;
  (iii) section 128 of the Correctional Services Act, 1998;
  (iv) sections 65, 66 and 67 of the Financial Intelligence Centre Act, 2001; and
  (v) sections 85, 86, 87, 88 and 90 of the Electronic Communications and Transactions Act, 2002; and

(b) amendments to—
  (i) the Electronic Communications and Transactions Act, 2002 and the RICA, which are consequential in nature; and.
  (ii) the Criminal Law (Sexual Offences and Related Matters) Amendment Act Amendment Act, 2012.

The provisions which are deleted deal with substantially the same matters which are provided for in the Bill.

The amendments to the Criminal Law (Sexual Offences and Related Matters) Amendment Act Amendment Act, 2012, aims to criminalise various aspects relating to child pornography in cyberspace. Initiatives seeking to regulate the distribution of child pornography over the Internet have had little deterrent effect on perpetrators. The Internet is the medium which is preferred for the distribution of child pornography. The

online sale of child pornography is highly profitable, with collectors willing to pay great amounts for videos, pictures and literature depicting children in a sexual context. Search engines find such material quickly. Most material is exchanged in password-protected closed forums, which regular users and law enforcement agencies can rarely access. The following factors in the use of the Internet to exchange of child pornography pose difficulties for the investigation of these crimes, namely—

***** the use of virtual currencies and anonymous payments which make it difficult for law enforcement agencies to trace financial transactions in respect of child pornography;

* the use of encryption or other technologies to make information which is sent and stored, inaccessible; and

* technologies or procedures which can be used to hide the identities of perpetrators.

The amendments to the Criminal Law (Sexual Offences and Related Matters) Amendment Act Amendment Act, 2012, aim to supplement section 24B of the Films and Publications Act, 1996, which contains provisions criminalising child pornography. The amendments proposed by the Bill, aims to criminalise the intentional and unlawful—

* taking of steps to procure, obtain or access or in any way knowingly assisting in, or facilitating the procurement, obtaining or accessing of child pornography through a computer network or electronic communications network;

* possession of child pornography on a computer data storage medium, a computer device, a computer network, a database or an electronic communications network;

* production of 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;

* making available, distribution or broadcasting of child pornography by means of a computer network or an electronic communications network;

* advocating, advertising, encouraging or promotion of child pornography or the sexual exploitation of children, by means of a computer network or an electronic communications network;

* making available, distribution or broadcasting by an electronic communications service provider of child pornography through a computer network or an electronic communications network;
* advocating, advertising, encouraging or promotion child pornography or the sexual exploitation of children, by an electronic communications service provider; and
* processing or facilitation of a financial transaction which will facilitate access to, or the distribution or possession of, child pornography.

The proposed amendments further oblige a person or an electronic communications service provider who, have knowledge of the commission of an offence, or have reason to suspect that an offence has been or is being committed, to report such knowledge or suspicion as soon as possible to a police official of the South African Police Service.

3.11.2 **Clause 67** provides that the Cabinet members responsible for the administration of justice and State security must make regulations where these are required in terms of the Bill.

3.11.3 **Clause 68** provides for the short title and commencement.