OPEN DEMOCRACY ADVICE CENTRE

TRANSPARENCY IN ACTION

Cyber crimes and Cyber Security Bill:

ODAC notes the publication of the draft Bill for comment. ODAC is a non profit organisation established in 2001, which specialises in access to information, whistleblowing and transparency law and policy. We work throughout the continent, and in South Africa.

We would recommend the withdrawal of the Bill, and referral of the matter to the South African Law Reform Commission for investigation by a multi sector project committee. We recommend this for a number of reasons.

1. The Bill fails to protect whistleblowers.
2. The Bill unconstitutionally infringes on the right to impart and receive information.
3. The Bill is not consequent on a public policy process.
4. The Bill clashes with the redrafting of other legislation, as well as provisions in other legislation, especially the Protection of Personal Information Act, 2013. It also repeats offences in other Acts.
5. It does not deal with cyber crime, as it is defined in the Budapest convention on cybercrimes.
6. The Bill is incorrectly tagged, and does not contain costings as required by the Public Finance Management Act.
7. The criminal law onus is reversed in a number of sections.
8. Common law crimes of fraud, forgery, and uttering are drafted as those crimes committed by computer, rather than the cybercrime element identified.
9. The structures created by the legislation will have a draconian and unconstitutional reach into information systems, with particular reference to private sector, and would constitute a violation of the right to informational privacy.
10. The Act will criminalise much legitimate management of computer systems, through its overbroad definitions.

3rd Floor, Springtime Studios
No. 1 Scott Road, Observatory, 7925
Cape Town, South Africa

T +27 21 447 1198 F +27 21 447 1191
www.odac.org.za
NPO Number 021-609-NPO

A. Failure to protect whistleblowers

Clause 16 of the draft Bill introduces a range of offences under the banner of "computer-related espionage" that replicate and deepen problems that still exist in the Protection of State Information Bill and which would seek to criminalise all of these acts.

These provisions make it an offence to "unlawfully and intentionally" possess, communicate, deliver, make available, or receive data "which is in possession of the State and which is classified".

These provisions clearly create penalties,which could ensnare investigative journalists, whistleblowers or other civic actors who may need to access or publish classified information in the public interest. The penalties range from a maximum of 5 to 15 years in jail, depending on whether the information is classified confidential, secret or top secret.

There is no public interest defence nor public domain defence nor whistleblower protection.

Whistleblowing is part of an international framework in terms of International, Continental, Regional law and best practices.

The United Nations Convention against Corruption, 2003

The United Nations Convention against Corruption (UNCAC) was adopted by the General Assembly by resolution no. 58/4 of 31 October 2003. It was ratified by the South African government in November 2004. Whistleblowing is posited as an anti-corruption tool by the Convention.

The purposes of the Convention are, inter alia:

(a) To promote and strengthen measures to prevent and combat corruption more efficiently and effectively; and

(b) To promote integrity, accountability and proper management of public affairs and public property[1].

The scope of the UN Convention is not only limited to the prevention of corruption in the public arena. Article 12 obliges State Parties to take measures to prevent corruption in the private sector.

In terms of Article 5, each State Party is required to establish and promote effective practices aimed at the prevention of corruption in the public and private arena. One of the obligations created by the Convention on State Parties is the incorporation, into their domestic legal system, of appropriate measures to provide protection against any unjustified treatment of whistleblowers, regarded as "any person who reports in good faith and on reasonable grounds to the competent authorities in accordance with the Convention."[2]

---

[1] Article 1

[2] Article 33

The OECD Convention on the Combating Bribery of Foreign Public Officials in International Business Transactions and the compendium of best practices and guiding principles for legislation on the protection of whistleblowers prepared by the OECD at the request of the G20 Leaders at their Seoul Summit in November 2010;

The Organisation for Economic Co-operation and Development (OECD) is made up of thirty member countries, including South Africa[3]. The member states share a commitment to democracy and the market economy to (a) support sustainable economic growth, (b) boost employment, (c) raise living standards, (d) maintain financial stability, (e) assist other countries' (both members and non-members) economic growth and (f) contribute to growth in world trade[4]. The OECD, much like the UN Convention, views whistleblowing as essential to fighting corruption in a democratic society.

The OECD Convention on Bribery of Foreign Public Officials in International Business Transactions is an anti-corruption convention, which provides a "framework for developed countries to work in a coordinated manner to criminalise the bribery of foreign public officials in international business transactions[5]. South Africa has ratified the Convention, which has been in force since August 2007[6]. In terms of the Convention, a further set of "Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions were adopted by the Council on 26 November 2009 and are binding on all signatories to the OECD Convention.

Recommendation IX requires Member countries to ensure that certain whistleblowing channels are in place and certain whistleblowers are protected. More specifically, Member countries must ensure that:

1. Easily accessible channels are in place for reporting of suspected acts of bribery of foreign public officials in international business transactions to law enforcement authorities;
2. Appropriate measures are in place to facilitate reporting by public officials...directly or indirectly through an internal mechanism, to law enforcement authorities of suspected acts of bribery ...;

---

3 http://www.transparency.org/global_priorities/international_conventions/conventions_instruments/oecd_convention

4 http://www.oecd.org/pages/0,3417,en_36734052_36734103_1_1_1_1_1,00.html

5 http://www.transparency.org/global_priorities/international_conventions/conventions_instruments/oecd_convention

6 *Steps taken to implement and enforce the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, South Africa*, 22 May 2009, http://www.oecd.org/document/

3. Appropriate measures are in place to protect from discriminatory or disciplinary action, public and private sector employees who report in good faith and on reasonable grounds to the competent authorities suspected acts of bribery of foreign public officials in international business transactions.

African Union Convention on Preventing and Combating Corruption, 2003

South Africa ratified the African Union Convention on Preventing and Combating Corruption in 2003.

The African Union Convention envisages whistleblowing as central to, not only the fight against corruption, but also to fostering accountability and transparency in the management of public affairs and socio-economic development on the continent. The African Union Convention regards corruption in both the public and private sector as damaging to economic development and commits Member States to develop mechanisms to "detect, prevent, punish and eradicate corruption and related offences in the public and the private sectors".

One of the central mechanisms required by the Convention is whistleblowing legislation. Article 5 requires Members States to take legislative and other measures to:

1. Protect informants and witnesses in corruption and related offences;
2. Ensure that citizens report instances of corruption without fear of consequent reprisals

The SADC Protocol against Corruption

The Southern African Development Community (SADC) Protocol against Corruption ("the SADC Protocol") takes it lead from the AU Convention and locates whistleblowing as a key ingredient within an effective anti-corruption framework. It recognises the negative impact of corruption in the public and private sectors on good governance, accountability and transparency. [7] It commits Member States, including South Africa, to create, maintain and strengthen systems for protecting individuals who, in good faith, report acts of corruption[8].

The Council of Europe's Criminal Law Convention on Corruption, 1999; the Council of Europe's Civil Law Convention on Corruption, 1999 and the Council of Europe's Resolution 1729 (2010): The protection of whistle-blowers, and the Council of Europe Recommendation CM/Rec(2014)7 of the Committee of Ministers to member States on the protection of whistleblowers (Adopted by the Committee of Ministers on 30 April 2014, at the 1198th meeting of the Ministers' Deputies)

Although South Africa is not a member of the European Union and is not a signatory to the Council's Conventions, the anti-corruption conventions and its whistleblowing resolution provide valuable guidance on international best practices. This is especially true given that

[7] Preamble
[8] Article 4(e)

both the Criminal and Civil Conventions adopt a similar approach to whistleblowing as the UN, AU and SADC conventions against corruption. Like the latter, the European conventions recognise the harm that corruption does to democratic societies, the importance of whistleblowing in the fight against corruption and require member states to enact laws that protect whistleblowers against harm ensuing from the making of a disclosure.

The Council of Europe's Resolution 1729: The protection of whistleblowers aims to close the gap between the rhetoric of whistleblowing as contained in the Conventions and the practice in member states by providing guidance to members states on legislative principles that should be practiced to give meaningful effect to the legal protections afforded to whistleblowers[9]. The Resolution aims to provide guidance to member states on necessary legislative principles that will ensure a truly safe alternative to silence for whistleblowers rather than a "shield of cardboard" which would entrap them by giving them a false sense of security.

The Resolution locates whistleblowing as central to accountability and the fight against corruption and mismanagement, both in the public and private sectors. Resolution 1 provides that:

The Parliament Assembly recognises the importance of "whistle-blowing" – concerned individuals sounding the alarm in order to stop wrongdoings that place fellow human beings at risk – as an opportunity to strengthen accountability and bolster the fight against corruption and mismanagement, both in the public and private sectors.

South African legislation was introduced in 2000, in the form of the Protected Disclosures Act to protect whistleblowers. It provides that no employee may be subjected to any occupational detriment by his or her employer on account, or partly on account, of having made a protected disclosure.

This legislation is referred to in the Protection of State Information Act (see comment 4), which provides that

> Sec 41. Any person who unlawfully and intentionally discloses or is in possession of classified state information in contravention of this Act is guilty of an offence and is liable to a fine or imprisonment for a period not exceeding five years, except where such disclosure or possession—
> (a) is protected or authorised under the **Protected Disclosures Act, 2000** (Act No. 26 of 2000), the Companies Act, 2008 (Act No. 71 of 2008), the Prevention and Combating of Corrupt Activities Act, 2004 (Act No. 12 of 2004), the National Environmental Management Act, 1998 (Act No. 107 of 1998), or the Labour Relations Act, 1995 (Act No. 66 of 1995);

[9] Omtzigt P, July 2009

(b) is authorised in terms of this Act or any other Act of Parliament; or
(c) reveals criminal activity, including any criminal activity in terms of section 45 of this Act.

Such protections are absent from this legislation. The section instead reads:

38. (1) No person, investigator, member of a law enforcement agency, electronic communications service provider or an employee of an electronic communications service provider may disclose any information which he, she or it has obtained in the exercise of his, her or its powers or the performance of his, her or its duties in terms of this Act, except—
to any other person who of necessity requires it for the performance of his or her functions in terms of this Act;
(*b*) if he or she is a person who of necessity supplies such information in the performance of his or her functions in terms of this Act;
(*c*) if it is information which is required in terms of any law or as evidence in any court of law;
(*d*) if it constitutes information-sharing—
(i) contemplated in Chapter 6 of this Act; or
(ii) between electronic communications service providers, the South African Police Service or any other person or entity which is aimed at preventing, investigating or mitigating cybercrime or relating to aspects of cyber security:
Provided that such information-sharing may not prejudice any criminal investigation or criminal proceedings;
(*e*) to any competent authority which requires it for the institution of criminal proceedings or an investigation with a view to instituting criminal proceedings.

It is not clear whether the drafter intends to cover the terrain of sections (a), (b) and (c) of section 41 of POSIB with this formulation. It appears not, especially when read with section 51 of the Bill which says that, at

51(7)(a) No person referred to in subsection (2) may disclose any confidential information or document obtained by that person in the performance of his or her functions in terms of this Act, except—

i. to the extent to which it may be necessary for the proper administration of any provision of this Act;
ii. to any person who of necessity requires it for the performance of any function in terms of this Act;
iii. when required to do so by order of a court of law; or
iv. with the written permission of the Cyber Response Committee.

(*b*) Any person who contravenes a provision of paragraph (*a*) is guilty of an offence and is liable on conviction to a fine, or to imprisonment for a period not exceeding 2 years or to both such fine and imprisonment.

(*c*) Any person referred to in subsection (2)(*c),* must, before assisting the Cyber Security Committee, make and subscribe to an affirmation of secrecy in the following form:

'I, ... solemnly declare:

i. I have taken cognizance of the provisions of section 51(7) of the Cyber Crimes and Cybersecurity Act, ... (Act No. of .....).

ii. I understand that I may not disclose any information or document, or the contents thereof, of whatever nature that comes to my knowledge or into my possession in consequence of my performance of any function in terms of the Cyber Crimes and Cybersecurity Act, ... (Act No. of .....), whether verbal or in writing, to any unauthorized person without the prior written approval of the Chairperson of the Cyber Security Committee.

iii. I am fully aware of the serious consequences which may follow any breach or contravention of the above-mentioned provisions.

.....

(Signature)'.

This provides none of the protections of the POSIB, and appears to contradict the section in the Protected Disclosures Act , which states

(3) **<u>Any provision in a contract of employment or other agreement between an employer and an employee is void</u>** in so far as it-

(a) purports to exclude any provision of this Act, including an agreement to refrain from instituting or continuing any proceedings under this Act or any proceedings for breach of contract; or

(b) (i) purports to preclude the employee; or

(ii) has the effect of discouraging the employee, from making a protected disclosure.

Employee making protected disclosure not to be subjected to occupational detriment

B. Gaps in overall framework of the Bill.

ODAC understands the National Cyber Security Policy framework and Draft National Critical Information Infrastructure Policy to be the policy framework for this Bill. Unfortunately we have only had sight of the first, which was published in the Government Gazette months after the Bill was published for comment. We have not had sight of the latter despite a request to the drafter. We have also not had sight of the National Cyber Security Implementation Plan, which apparently remains classified.

This is particularly concerning for several reasons:

- There is other legislation currently enacted which appears to deal with the same subject matter;
- There are legislative processes which are proposing amendment to the issues dealt with in the Bill, which are not referenced;
- There is no extant structure which is being used which brings together the various stakeholders dealing with the many issues raised in this legislation, for the purposes of preventing duplication, contradiction, and lack of clarity.

We raise a number of overlapping provisions:

1. As an example, the relationship between this legislation and the Minimum Information Security Standards is not addressed. These have not been updated since their introduction, as a Cabinet Policy. Despite the view of the previous head of Sate Security, Barry Gilder, as expressed to the parliamentary committee in 2009 that the MISS standards are ultra vires, given that they have no legislative framework, nor have updated standards have been introduced. These standards are one of the most important tools the State has in terms of the practical implementation of information security, and apply across the state. The failure to reference these in any way leave a concerning lacuna as to how the MISS and this legislation cohere.

2. We also note that the Protection of Personal Information Act appears not to have been considered in relation to this legislation. While we appreciate that the majority of the legislation is not in operation, we anticipate that POPI will be brought into operation. Under those circumstances, the primary responsibility for the protection of private information, will be managed by the Information Regulator (IR), who is currently in the process of being appointed by Parliament. The distinction between the mandate of the IR and the various structures proposed in Chapter 6, especially given the provisions relating to personal information in section 3, 5, 7, and 8, is not clear.

POPI regulates the definition and processing of personal information, including financial information in great detail. The Act's long title is:

- To promote the protection of personal information processed by public and private bodies;
- to introduce certain conditions so as to establish minimum requirements for the processing of personal information;
- to provide for the establishment of an Information Regulator to exercise certain powers and to perform certain duties and functions in terms of this Act and the Promotion of Access to Information Act, 2000;
- to provide for the issuing of codes of conduct;
- to provide for the rights of persons regarding unsolicited electronic communications and automated decision making;
- to regulate the flow of personal information across the borders of the Republic;
- and to provide for matters connected therewith.

POPI does not directly criminalise the unlawful processing of personal information, but rather makes in an offence to fail to comply with an enforcement notice served in terms of section 95 of POPI. The thorough scrutiny of the question of criminalising the processing of personal information has been considered by the South African Law Reform Commission, as well as Parliament, and the resultant legislation already signed as an Act. A responsible party who contravenes the provisions of section 8 of POPI insofar as those provisions relate to the processing of an account number of a data subject is already guilty of an offence. Section 3 therefore appears redundant.

3. We would also draw the attention of the drafters to section 38 of the Protection of State Information Bill, as follows:

> 38. (3) Any person who unlawfully and intentionally produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component, which is specifically designed to overcome security measures for the protection of state information, for the purposes of contravening this section, is guilty of an offence and liable on conviction to imprisonment for a period not exceeding 10 years.
> (4) Any person who intentionally utilises any device or computer program mentioned in subsection (3) in order to unlawfully overcome security measures designed to protect state information, is guilty of an offence and liable on conviction to imprisonment for a period not exceeding 10 years.
> (5) Any person who contravenes any provision of this section with the intent to interfere with access to an information system so as to constitute a denial, including a

partial denial, of service to legitimate users commits an offence and is liable on conviction to imprisonment for a period not exceeding 10 years…..

6 (b) Any person who wilfully gains unauthorised access to any computer which belongs to or is under the control of the State or to any programme or data held in such a computer, or in a computer to which only certain or all employees have restricted or unrestricted access in their capacity as employees of the State, is guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding two years.
(c) Any person who wilfully causes a computer which belongs to or is under the control of the State or to which only certain or all employees have restricted or unrestricted access in their capacity as employees to perform a function while such person is not authorised to cause such computer to perform such function, is guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding two years.
(d) Any person who wilfully performs an act which causes an unauthorized modification of the contents of any computer which belongs to or is under the control of the State or to which only certain or all employees have restricted or unrestricted access in their capacity as employees of the State with the intention to—
(i) impair the operation of any computer or of any programme in any computer or of the operating system of any computer the reliability of data held in such computer; or
(ii) prevent or hinder access to any programme or data held in any computer, is guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding five years.

These issues appear to be dealt with in a different form in section 4 through 7, 16 and 22 of this Bill, in so far as state information is concerned. Again, the rationale behind this duplication is unclear.

4. The Promotion of Equality and Prevention of Unfair discrimination Act (PEPUDA) is also duplicated in section 17 (Prohibition on dissemination of data message which advocates, promotes or incites hate, discrimination or violence) The provisions dealing with hate speech in the PEPUDA, which in section 10 provides that

….no person may publish, propagate, advocate or communicate words based on one or more of the prohibited grounds, against any person, that could reasonably be construed

1) to demonstrate a clear intention to-
a) be hurtful;
b) be harmful or to incite harm;
c) promote or propagate hatred.

5. We also note that section 20 deals with the infringement of copyright. There is no reference to the Copyright Amendment Bill, published for comment on the 17 July 2015, and containing provisions dealing with technological protection. For example section 20 of this Bill introduces measures, which deal with technological protection measures that protect copyright, as follows:

> Prohibited conduct in respect technological protection measure
> (1) The prohibited conduct in respect of the technological protection measure, the use of a technological protection measure circumvention device and the exceptions related to technological protection measure, contemplated in sections 280 and 28P of the Copyright Act, 1978 (Act 98 of 1978), shall mutatis mutandis apply in respect of performances fixed or fixed in audio-visual fixations.
> (2) Contravention of the technological protection measure provisions contemplated in subsection (1) shall be an offence and a person convicted thereof shall be liable in terms of the provisions of this Act.

It is not clear if this legislation intends to improve on or anticipate the Copyright Amendment Bill.

6. The Bill also appears to duplicate in section 5 and 7, section 49 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act which reads:

> 49.(1) Any person who intentionally intercepts or attempts to intercept, or authorises or procures any other person to intercept or attempt to intercept, at any place in the Republic, any communication in the course of its occurrence or transmission, is guilty of an offence.

7. Section 15 appears to duplicate the Protection of Constitutional Democracy against Terrorist and Related Activities Act where any act which

> is designed or calculated to cause serious interference with or serious disruption of an essential service. facility or system, or the delivery of any such service. facility or system, whether public or private, including. but not limited to -
> (aa) a system used for, or by, an electronic system. Including
> (bb) a telecommunication service or system;
> (cc) a banking or financial service or financial system;
> (dd) a system used for the delivery of essential government
> (ee) a system used for, or by, an essential public utility or
> (8) an essential infrastructure facility; etc.

This definition does not include the exemption provided for in the Act:

> Any act which is committed in pursuance of any advocacy, protest. dissent or industrial action and which does not intend the harm contemplated in paragraph (o)(i) to (v) of that definition, shall not be regarded as a terrorist activity within the meaning of that definition, which excludes advocacy or dissent. Acts committed in the context of legitimate struggles for national self-determination or national liberation should not be considered terrorist acts.

8. Definitions

We also note the definition of malware as:

“Malware” means malicious software, and is programming (code, scripts, active content or other software) designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, and other abusive behaviour.”

Computer software is a tool, and cannot be malicious, just as a gun or knife is not malicious.

Many systems used by network operators to manage the network, and test for security flaws, would fall into this definition.

C. Tagging, and the PFMA

We note that the proposed tagging of the Bill is as a section 75 Bill. We would suggest that the Bill will have a significant impact on the Provinces. As an example:

National Critical Information Infrastructure is defined in section 1 (our emphasis at b(i)) as follows:

> "National Critical Information Infrastructure" means means any data, computer data storage medium, computer device, database, computer network, electronic communications network, electronic communications infrastructure or any part thereof or any building, structure, facility, system or equipment associated therewith or part or portion thereof or incidental thereto—
> (a) which is specifically declared a National Critical Information Infrastructure in terms of section 58(2) of this Act; or
> (b) which, for purposes of Chapters 2 and 4 of this Act, are in possession of or under the control of—
>
> (i) any department of State or administration in the national**, provincial** or local sphere of government; and
> (ii) any other functionary or institution exercising a public power or performing a public function in terms of any legislation,
> irrespective whether or not it is declared a National Critical Information Infrastructure as contemplated in paragraph (a);

We would draw you attention to the decision of the CC in Tongoane and Others v National Minister for Agriculture and Land Affairs and Others [10]

> To summarise: any Bill whose provisions substantially affect the interests of the provinces must be enacted in accordance with the procedure stipulated in section 76. This naturally includes proposed legislation over which the provinces themselves have concurrent legislative power, but it goes further. It includes Bills providing for legislation envisaged in the further provisions set out in section 76(3)(a)-(f), over which the provinces have no legislative competence, as well as Bills the main substance of which falls within the exclusive national competence, but the provisions of which nevertheless substantially affect the provinces.

We therefore submit the Bill is incorrectly tagged.

---

[10] **(**CCT100/09) [2010] ZACC 10; 2010 (6) SA 214 (CC) ; 2010 (8) BCLR 741 (CC) (11 May 2010)

It is also not clear that the question as to whether the requirements of the PFMA, section 35, have been dealt with.

D. Reversal of onus.

The possession offences outlined in Chapter 2 propose a framework whereby the possession of information or software is guilty, unless they can give an 'exculpatory account' of the possession.

The presumption falls into the class of "reverse onus" provisions, which are now settled in law as being unconstitutional.

> which have been held by this Court to infringe the right of an accused person to be presumed innocent as envisaged in section 25(3)(c) of the Constitution. The function and effect of the presumption is to relieve the prosecution of the burden of proving all the elements of the offence with which the accused is charged. [11]

In a 2014 judgement from Judge Raulinga

> [41] The state bears the onus of establishing the guilt of the accused beyond a reasonable doubt and the converse is that he is entitled to be acquitted if there is a reasonable possibility that he might be innocent or if his version might be reasonably possibly true. In S *v Van Aswegen* **2001 (2) SACR 97** *(SCA),* the Supreme Court of Appeal reiterated that in whichever form the test if applied a court must be satisfied upon the consideration of all the evidence. In as much as a court does not look at the evidence implicating an accused person in isolation in order to determine whether there is proof beyond reasonable doubt, so too does it not look at the exculpatory evidence in isolation to determine whether it is reasonably possible that it might be true.

---

[11] S v Coetzee and Others (CCT50/95) [1997] ZACC 2; 1997 (4) BCLR 437; 1997 (3) SA 527 (6 March 1997)

E. Specific concerns: definitions of common law crimes as cybercrimes.

Clauses 11, 12, 13 and 14 appear to advance the proposition that a cyber crime is a common law crime, committed with a computer. This is not consonant with the Budapest Convention on Cybercrime (to which South Africa is a signatory), which requires parties to

> establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible.

The criminal offence is the changing of the data. It is not the fraud, committed by computer. This is correctly identified in the policy document as **not** cybercrime. The policy document says

> However, cybercrime comprises also offences committed by means of computer data and systems, ranging from the sexual exploitation of children to fraud, hate speech, intellectual property rights (IPR) infringements and many other offences.
>
> Furthermore, any crime may involve electronic evidence in one way or the other. **While this may not be labelled "cybercrime",** a cybercrime strategy would nevertheless need to ensure that….evidence in relation to any crime, or that all law enforcement officers, prosecutors and judges are provided at least with basic skills in this respect….

Similar logic must be applied to the sections dealing with forgery and uttering, appropriation, and extortion.

F. Structures as created by the Bill.

The policy document and law creates 5 structures, as follows:

1. The JCPS Cybersecurity Response Committee, with the DG of SSA heading it up, and the secretariat provided by SSA. In the policy they oversee the RSA Government Electronic Communications Security Computer Security Incident Response Team (ECS –CSIRT) and any other CSIRT established in South Africa.
2. The Cybersecurity Hub, run by DTPS. (the policy document mentions DOC in this context, but this appears to be in error. – "Cybersecurity Hub within the Department of Telecommunications and Postal Services (DOC). The Cybersecurity Hub will be operated within the DOC in accordance with national security guidelines"
3. The Cyber command, run by SANDF.
4. The National Cybercrime Centre, run by SAPs, who also run the 24/7-point of contact.
5. The Cybersecurity Centre, run by the SSA.

The sector, which provides an electronic communications service must establish a Private Security Computer Security Incident Response Team (PSCSIRT). If they do not do so within six months of being so instructed, the Department of Telecommunications and Postal Services (DTPS) can establish the Security Computer Security Incident Response Team for the sector. The sector is responsible for costs of the Team. It is not clear by what mechanism the costs will be recovered. The team have to perform 'any other function conferred' on it by DTPS.

While according to sec 56 the Cybersecurity Hub (DTPS) will "manage and exercise administrative control over Private Security Computer Security Incident Response Teams, and regulate the way they carry out Act. In other sections the
24/7 centre ensures it is coordinated with PCSIRT (sec 49) and the committee oversees and guides functioning of PCSIRT (sec 51), while the cyber security centre co ordinates activities with the PCSIRT (sec 52).
The Government Computer Security Incident Response Team (one or more) also co ordinates with the Private Security Computer Security Incident Response Teams (sec 53) and the National Cyber Crime Centre must also co ordinate with the Private Security Computer Security Incident Response Team (sec 54).

We would suggest that this structure is so complex and unclear in terms of what it will do, and how it is funded that these sections are vague to the extent that they would be unlawful.

<u>National Critical Information Infrastructure</u>

The Cyber Security Centre, after consultation, can refer potential National Critical Information Infrastructure to the SSA, and they can declare it National Critical Information Infrastructure (NCII). The definition of a NCII is vague and overbroad.

> Sec 58 The Cabinet member responsible for State security may… declare any information infrastructure… as National Critical Information Infrastructures if it **appears** to the Cabinet member that such information … are of such a strategic nature that **any** interference with them or their loss, damage, disruption or immobilization **may**
> (*a*) prejudice the security, the defence, law enforcement or international relations of the Republic;
> (*b*) prejudice the health or safety of the public;
> (*c*) cause interference with or disruption of, an essential service;
> (*d*) causes any major economic loss;
> (*e*) cause destabilization of the economy of the Republic; or
> (*f*) create a public emergency situation.

There is no criteria for the test 'appears'. The threshold for the interference is 'any' is too wide. The harm test is too low in that it uses the word 'may' instead of a demonstrable harm test, which may be proved by evidence.

The definition of National Critical Information Infrastructure is also overbroad and vague. They include any institution performing a public power or a public function. This would include private hospitals, and private security companies. This would also include the South African Police Services including the Hawks, the Public Protector, Independent Police Investigative Directorate and other such institutions. The principle that the State Security Agency be given access to all the data, computers and buildings in NCIIs is not in line with the principle of proportionate and reasonable processing of personal information and specifically would be a violation of the right to informational privacy.

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

The powers given to SSA are overbroad, and as below, include access to databases, which creates less security against cybercrime rather than more. .

> 58(5) The Cabinet member responsible for State security, in consultation with the relevant Cabinet members and the Cyber Response Committee must, within six months of the declaration of any information infrastructure, or category or class of information infrastructures or any part thereof, as National Critical Information Infrastructure, make regulations regulating—
> (*a*) the classification of information on National Critical Information Infrastructures;
> (*b*) security policies and procedures to be applied to National Critical Information Infrastructures;
> **(*c*) access to National Critical Information Infrastructures**;
> (*d*) the storing and archiving of information on National Critical Information Infrastructures;
> (*e*) cyber security incident management and continuation with service provision; (*f*) minimum physical and technical security measures that must be implemented in order to protect National Critical Information Infrastructures;
> (*g*) the period within which the owner of, or person in control of a National Critical Information Infrastructure must comply with the regulations; and
> (*h*) any other relevant matter which is necessary or expedient to prescribe for the proper implementation of this section.