OWASP Cape Town Chapter – Comments on “CYBERCRIMES AND CYBERSECURITY BILL”

Authors

Christo goosen

Timo Goosen

Liam Smit

OWASP community members who wish to remain anonymous but are part of our community.

The Cape Town Chapter of OWASP has 167 members currently signed up to receive meeting notifications.

Preface

The Open Web Application Security Project or OWASP is described on its website as the following: “The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. Our mission is to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks” (https://www.owasp.org/index.php/Cape_Town).

OWASP is a NGO comprises of around 42000 volunteers around the world sacrificing their own time and providing the open source knowledge contained in OWASP to improve or create awareness about security beyond just web applications.

OWASP Cape Town (https://www.owasp.org/index.php/Cape_Town) is a local chapter suppored by the global NGO. OWASP Cape Town comprises of a leadership group with local IT professionals attending and contributing to the meetings, talks and projects locally and globally. OWASP Cape Town has access to local and professional knowledge within our community of volunteers and attendees. We aspire to create awareness both locally and internationally in the IT and security community. South Africa is facing growing ICT security concerns in both the government and business sectors.

OWASP Cape Town, comprising a number of well qualified and experienced information security practitioners takes the opportunity of providing its time and experience to ensure that the legal framework that facilitates cybersecurity in South Africa is not only legally correct (which we leave to legal professionals) but also takes account of the practical realities of cybersecurity and the importance of maintaining the democratic freedoms that are part of our open democracy in both the physical and cyber spheres.

Introduction

Various members of the OWASP Cape Town leadership, community and Security community as a whole, started reading and studying the Cyber-Crime Bill in October 2015. We studied the Bill with a technical lens and observed many faults in the wording and aspects covered in the bill. OWASP Cape Town provides comments to the Bill in an effort to draw the drafters and legislators attention to some of the practical realities of information security practices, to prevent unnecessary and harmful prosecutions of security professionals who execute their legitimate duties as whistleblowers in instances of information security breaches or vulnerabilities and to prevent the unconstitutional overreaching by government and private sector organizations of the constitutional rights that govern our open democracy.

OWASP Cape Town acknowledges and confirms the need for cybercrime and cybersecurity legislation but in its current form the Bill is unacceptable. Not only is the wording of the Bill extremely wide but it fails to take into account many of the practical realities of both information security and the use of software in general.

It must be recognized that the information security profession is legitimate and a well regulated part of our information society and is critical to the growing cyber economy. The fact is simply not recognized in the Bill as it stands. Instead it seems to appropriate the right of cybersecurity only to the public sector. This is out of line with what is happening globally. With the greatest respect this attitude betrays the lack of appreciation on the part

of the drafters (and the persons instructing the drafters in the JCPS Cluster) of the realities of the 21st century information security.

Security researchers have been at the forefront of whistleblowing or disclosing vulnerabilities in software which may expose the public and companies to criminal activity. The security industry is dependent on researchers disclosing issues that are kept from the public or haven't been discovered yet. Both the well-publicized Shellshock and Heartbleed vulnerabilities were hidden within open source software used by millions of industries and companies around the world. Without disclosure these critical vulnerabilities could have been exploited by criminal elements and left many users and companies vulnerable.

It is also essential that government and the private Information Security industry work together to secure South African citizens' privacy and security. We can follow the example of Germany where the Hacking Organization "Chaos Computer Club - CCC" is often called into parliament to comment on new laws related to Information Technology. Currently government does not have the capacity on its own. South African IT Security companies have international renown for the work done locally and abroad. Despite recognition of the importance of public/private partnerships in cybersecurity, the Bill does not provide mechanisms for appropriate partnership between government and the private sector and, in the context of our comment, the information security sector specifically. As has been highlighted by Professor Basie von Solms, the capacity and competence to deal with cybersecurity on a nationwide scale simply does not exist within government. The desirability of the public/private partnerships in this regard, well documented in cybersecurity frameworks and affected in implementations in other countries, remains absent in the Bill. The authoritarian approach which is proposed will simply not work.

It is also submitted that some of the penalties (for instance for writing malware) are not aligned to the mischief that needs to be protected against or the severity of the consequences of the crime. It needs also to be understood that the same software may be used for perfectly good and legitimate purposes as well as for committing harm to third parties, which should be punishable. Further, the general assumption of guilt and the reversal of the onus of proof relating to offences that are dealt with in the Bill is likely to create severe injustice, particularly where persons investigating and prosecuting crimes do not have the necessary expertise or experience. From experience in IT and information security, evidence is easily manufactured or faked and the law usually applies to physical items, not virtual issues. The bill is drafted in a way that is contrary to "innocent until proven guilty", in that the bill requires an individual who is suspected of computer related crime to prove their innocence in contrast to the rest of South African law. The Bill will require a significant amount of amendment if unintended consequences which could lead to severe injustice are to be avoided.

Due to our limited legal knowledge we partnered with Mark Heyink, an information attorney and information security consultant. We believe that by virtue of our discussions with Mr Heyink a multidisciplinary approach to some of the issues in the Bill can be achieved.

This is in line with the development of similar frameworks and laws in other jurisdictions, which example the JCPS Cluster has failed to follow in this instance.

Comments

General

- After reading through the entire bill, it hard not to see it as an attempt by government to obtain complete control over all information systems, with the sweeping powers granted to it from chapter 4 onwards. The broad definitions used, creates the impression that the bill errs on the side of criminalising any act that may be deemed unlawful, even if unreasonably done so, while also allowing government (specifically ill-defined “law enforcement”) almost any action in the name of “cybercrime defense”. It further offers no protection to whistleblowers or personal privacy, and adds significant risk to any person or business who wish to operate in the information security field. This is ironic, since the Bill recognizes the need for many more information security practitioners and the building of the necessary capacity to properly defend South Africa against cybersecurity vulnerabilities. The effect of the Bill as it stands will be to dissuade security practitioners from performing the duties necessary if they are properly to fulfil their role. The onerous penalties will also make this a profession which will be unattractive to practice in South Africa. The result will be that the very people that we need to develop to enhance cybersecurity will find other alternatives rather than run the risk of bad legislation possibly criminalizing their actions. Those that are interested in cybersecurity will in all likelihood leave the country to pursue their profession elsewhere. Considering the importance of the cyber-economy to South Africa and the power of good that the Internet can do for South African citizens that will be a significant blow to South Africa’s aspirations in the cyberworld.
- Quoted from Chapter 2 Offences Section 6: “Unlawful acts in respect of software or hardware tools” below: “It is very important that intent be highlighted within the Cyber Crimes Bill. Tools, data, hardware etc. can be used for both good and bad activities, but intent is what constitutes an unlawful offence.” This is, in summary, this bill’s biggest shortcoming, and could have dire consequences: from criminalising citizens’ arbitrary interactions with almost any digital system, stifling digital innovation, to discouraging business and investment for fears of running afoul of this bill. A simple requirement for intent could be added in the form of “intentional subversion of security measures for personal gain, at the expense of others”, or something to that effect. This would also put some responsibility on information system owners to deploy reasonable security measures, thereby improving the nation’s general information security.

- This bill does not address the very serious issue of the lack of technical knowledge and skills (or access thereto) required by law enforcement (specifically SAPS, prosecutors and judges and magistrates) in the execution of the powers granted. This, combined with the general lack of information security skills in South Africa, leaves the door open for wanton abuse of these powers. It also offers no suggestions to mitigate this skills shortage. In the context of information security professionals, ensuring that appropriate people attend and complete certified ethical hacking courses will not be enough. It is important that appropriate skills are developed at all of the different levels necessary to support the legislation which is proposed.
- With the vague definition of a “critical database” / ”critical network” (vs. just a “database” / ”computer network”), most offences will necessarily be subject to the harsher penalties.
- Multiple instances of “...is liable, on conviction to a fine or imprisonment...”, where “a fine” is not elaborated upon.

Chapter 1 Definitions: "computer device"

Can programs themselves be ”computer devices”?

Chapter 1 Definitions: "critical data"

Critical data seems far too wide a definition.

Critical data should include personal data such as the protections of privacy in POPI.

critical data *“of importance to the protection of*”

How important does it need to be?

f. “records of a financial institution”

Which records? There is a big difference between financial records of individuals or the financial statements of the institution that are published on its website. There are many records that would fall in between those two extremes.

"Record" in itself needs to be defined. It is too vague, especially in the context of semantic or fuzzy data. It could be stretched to mean a paragraph on a website. Also if you consider the POPI legislation, personal information is supposed to be removed from 'records'. Thus what does records of a financial institution constitute? Its accounting or ERP database entries? Payroll system? Client data?

g. "the disclosure of which could cause undue advantage or disadvantage to any person," "Any person" is again hugely broad. What reasonable threshold is there for advantage or disadvantage?

How do you determine whether the advantage / disadvantage gained from disclosure was "undue"?

Is there a limit regarding how such data may be contextualised? There are many ways to gain data of commercial advantage / disadvantage, often this may be achieved through sources that do not belong to affected parties. Is this still "critical data" if it is derived from analysing previously public data, for example?

a. *"the security, defence or international relations of the Republic;"*

How exactly do you validate that data has impact on international relations?

Chapter 1 Definitions: "computer program" means a sequence of instructions which enables a computer device to perform a specified function

We cannot have a definition of Computer Program which does not include inputs and outputs. Both inputs & outputs are non-trivial parts of a program, and in some cases (event-driven programs) are intrinsic to the purpose and behaviour of a program.

We also need to define the specific identity of a program, i.e. where does it begin, when is it complete? Is a method a program? Is an instruction a program? A class? An object?

When is it correct and when is it as defined (buggy)?

What about programs that invoke other programs? Are other programs "computer devices"?

This definition of "computer programs" is a little too close to the definition on Wikipedia: "A computer program is a collection of instructions[1] that performs a specific task when executed by a computer. A computer requires programs to function, and typically executes the program's instructions in a central processing unit.[2]"(https://en.wikipedia.org/wiki/Computer_program).

Additionally the bill's definitions of computer programs performing a "specified function", is flawed when a computer program is used or exploited to perform a different function. A computer program can be targeted to perform a buffer overflow, SQL injection, Cross Site Scripting vulnerability, etc. This highlights the difficulty of overbroad definitions being used to define particular crimes. In this instance the example is that of the criminalization of possession of malware. Often software can be used for both beneficial or malicious

purposes. Therefore the definition of “malware” relates to the intent in the commission of a crime rather than the software itself. An analogy would be that if we outlawed a person possessing a hammer we would prevent the use of the hammer for the many legitimate purposes for which it is intended. However, the hammer could be used for unlawful purposes, such as murdering a person. The same can be said of firearms and many other physical things which may be used for both legitimate and illegitimate purposes. This does not appear to have been taken into consideration by the drafter or persons instructing him in the JCPS Cluster.

What about scripts and / or interpreted programs? In such cases the source code acts as little more than a very complex configuration file. Does it imply that the interpreter becomes “malicious” when a malicious script is executed?

If this goes to court it will be hard to argue exactly what the sequence of instructions will be, there will need to be evidence to prove that the sequence of instructions in question was the one being used in an act of offence and for that to be established. How would that be proven in a court of law?

We would argue that including I/O in the definition is related to the definition of the operation of a program, and not a program as a distinct entity. Is a program no longer a program when it is not executing (without I/O)?

Chapter 1 Definitions: "critical database" means a computer data storage medium or any part thereof which contains critical data;

This is not understandable. Is this a database or a data store? Does such storage have to be persistent, i.e. if you read a copy of the data into computer RAM or cache, does the RAM or cache become critical? Does the RAM become a database? Does the data have to be structured? What if you modify such data structure? Is it still a database? Is it any different from an archive?

Their definition of "database" clearly goes well beyond what we in the industry would use. From the current definition it seems like it refers to anything that could (more accurately?) described as "a collection of data".

Chapter 1 Definitions: “data” means any representation of facts, information, concepts, elements, or instructions

Which is it exactly? For example, based on the previous definition of what a Computer program is, where does the data end and program begin?

Chapter 1 Definitions: "database"

The description of a database is too vague. This could include a hard drive containing your operating system or an external hard drive containing backups, photos, videos etc. This should be further clarified. This should be very well defined as we are living in a time where many types of SQL and NoSQL datastores can be considered a “database”.

Chapter 1 Definitions: "electronic communications service provider"

“(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; “

The overbroad drafting that characterizes the Bill generally, is illustrated graphically by this provision, which in essence makes every person who receives or sends email or SMSs an electronic communications service provider and therefore subject to provisions relating to national critical information infrastructure. This is clearly not only nonsense but is likely to undermine the very purposes for which cybersecurity legislation should be established.

Further, the following definition does not account for the complex array of service providers in South Africa. This does not account for resellers of larger ISPs (Internet Service Provider) or CSPs (Communications Service Provider).

The “any...person or entity who or which transmits, receives, processes or stores data” is a prime example of the lack of knowledge in ICT, applied by the authors of the bill. Under such a definition any entity that submits data is a CSP. By this definition a person’s Internet of Things devices like a mobile weather station, their Smart TV, etc. is a CSP. We cannot allow this definition as that would define any entity that communicates via an electronic or digital medium as a CSP.

Example: Since a person “received, processed and store” an email from their ADSL ISP, they are, under this definition, a CSP. This is clearly wrong.

What about P2P networks? Is someone a CSP for running a Tor node, even though they have no control over the traffic flowing through it? Tor is the software which anonymizes participants in communications and is an acronym for the original software project name “The Onion Router”.

Chapter 1 Definitions section 2 "National Critical Information Infrastructure"

Again this is far too wide. Paragraph b (i) and (ii) are very broad.

This includes the municipal public library! If you want to protect National Critical Information Infrastructure you better know what it is now and be able to define it.

A definition should be thorough in identifying both software and hardware. Eg. 10 Personal Computers accessing a network-server using ethernet via x-network-software

Otherwise this law is open to abuse e.g. throwing the book at some teenager who hacks the library system so that he doesn't have to pay late fees or so that he can loan a few more books.

Or a student who plays a prank at a university by opening all the door locks or setting the copiers to allow any student to print.

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

So any and every possible item of data under government is by default critical? Does prior publication or public accessibility of such data limit this declaration?

This comment applies to Ch2.S2.(3): " *or a National Critical Information Infrastructure —*" How, when this doesn't have to be declared in advance as such?

Considering the Secrecy Bill, and governents open policies (http://www.capetown.gov.za/en/publicparticipation/pages/opendatadraftpolicy.aspx) (http://code4sa.org/2014/09/27/capetown-opendata-policy.html).

Also this will impede the work of organizations like code4sa.org. Government can essentially label all data as critical and lock the public out

Is it linguistically accurate to include "data" in the definition for information infrastructure?

Chapter 2 – General

Through the section references are made to offences "under this Act". What about offences committed under other acts?

Chapter 2 Section 2 Definitions and interpretation

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

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

It is on the very rare occasion that the above holds true in private industry. Most instructions are issued verbally.

How is the employee meant to know that the boss has lawful authority to give consent?

Instructions given to subordinates are highly unlikely to be made in such a way as to clearly define their scope. Which again leaves the employee unable to comply with the definition.

There is a missing “public interest” clause.

What about whitehat (non-malicious) activity?

Academic and private security research?

Chapter 2 Section 3 “Personal information and financial information related offences”

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

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

(b) was used or may be used to commit an offence under this Act, and who is unable to give a satisfactory exculpatory account of such possession, is guilty of an offence.”

Why does someone who is suspected (but not proven) to have intent to commit an offence need to prove their innocence?

Why has the burden of proof been shifted?

What happened to the presumption of innocence?

Question: The problem here is that if you are already sitting on other people's data, you may already be guilty of data theft.

Answer: Correct they may be guilty. Possessing data which might be used to commit an offence should not be an offence in and of itself. If the government wishes to prove you guilty then it should do so. It should not rely on laws which force you to have prove your innocence. The road to hell is paved with good intentions…

Answer 2: This is analogous to having your house or car searched (legally), yielding possible evidence for prosecution. In such a scenario, possessing suspected contraband is not an offence itself, but evidence towards the prosecution of the real crime.

What if this person is in charge of making offsite backups? Also what is “financial information” or what is “personal information”, this needs to be defined better.

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

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

Do these fines and prison terms match those for the same action which does not involve a computer? E.g. if an individual finds another individual’s financial information in the trash. There should also be fines for system administrators and CEOs that make poor decisions i.e. negligence that leads to people’s financial information being leaked onto the internet. Is this not more applicable to privacy legislation like POPI?

Chapter 2 Offences Section 4: “Unlawful access”

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

In terms of this definition a user of a system could accidently access or view an amount of data through merely exploring the system. If the systems administrator or software developer has incorrectly developed or configured a feature, the user could access the data and be liable to the Unlawful Access offence. The wording puts the responsibility of the user / accidental offender to thus prove that the access was not unlawful, and in terms of the wording of the offence, this will be nearly impossible.

There should be limitations of this clause where it concerns Research & Development, and educational purposes. As citizens we have the right to verify that our assets are sufficiently secure. Our intention to verify this needs not be a criminal offence. We have historical cases where well-intended citizens have exposed zero-day incidents. This behaviour should not be criminalised.

Also, when applying or performing due diligence, you should be able to investigate, verify and validate the services, software, computing and communication devices, etc. that you are legally allowed access to (Banking services, TV, servers, etc.).

The internet is the computer equivalent of a public thoroughfare. If one connects a private road to a public road and does not put up a gate or a sign then one would be in a poor position to argue that someone travelling on their private road is at fault.

Computing devices and especially networks are all about providing access to information. According to the wording of the Bill, merely accessing a computer network connected to the internet in an insecure manner could constitute an offence.

This is problematic when you consider the vague definition of databases in the context of this Act. If you get hold of a lost memory stick and access it to identify its owner (intentional but inadvertently unlawful), you may contravene this Act.

Also consider that any and every part of data store / medium that could have a data footprint is considered a database. That means if you access and read a memory module, and retrieve any data, image or program, you could be in contravention.

Consider also that to be considered an "electronic service provider..." if you look into someone's browser history, and discover through their cookies what may or may not fall into the vague definition of critical data, you could also be in contravention.

Are the fines and imprisonment terms equal to the real world analogies e.g. of simple trespass?

Again this is a nebulous concept of authority. Who determines who has authority to grant access? Who determines what is unlawful access? This appears to be circular reasoning. I.e. something is unlawful therefore it is an offence which then renders it unlawful.

How does an individual know if something connected to the internet is meant to be accessed (e.g. a public website) or is meant not to be accessed (e.g. a private intranet site). The onus should fall on the information system owner to secure their computer or network.

The drafters have taken a very aggressive stance here on the person who accesses protected data but not those who fail to protect it. Other laws don't work this way i.e. we don't arrest the drug addict and ignore the dealer. What if somebody is given the data without asking for it and they should not legally be allowed to view the data for example a journalist who is emailed data without asking for it, or for example viewing classified documents of the South African government which are posted on wikileaks?

This has a large impact for everything from cloud storage solutions to simple browser caching bugs - basically if I can get something stored as an attacker that now becomes a viable means of exploitation. <script>alert('SOMEONE’S CREDIT CARD')</script>

- Simpler and more disturbing example: If going to a .gov.za site (intentionally) includes information loaded from the intranet (protected under this vague Bill), you are now a criminal.
- Again, whitehat (and whistleblower) activities are not covered. Responsibly disclosing a vulnerability in a large, economically active city's municipality website would render you liable.
- How about limiting this to access with criminal intent?

Chapter 2 Offences Section 5: "Unlawful interception of data"

"...a hardware or software tool…."

What is the definition of Software?

This section is completely vague and does not consider the technical implications of such an offence. Under this section a Firewall or Proxy could constitute such an offence and the system administrator would be liable for accidentally capturing packets from external sources. This wording will also have to consider that ISPs (Internet Service Providers) will automatically be capturing client data when it passes through their servers, network switches, Firewalls etc. This section should also make a clear distinction between encrypted data and clear text data, SSL interception for example should be illegal and this is done on many corporate networks in South Africa.

Additionally a couple of local South African companies produce software for the interception of network traffic, cellphone GSM traffic, landline calls and interception of VOIP traffic. This would make the activities of these companies (funded by the South African Government) illegal and contrary to South African laws. These companies test most of their equipment and software in South Africa.

Network diagnostic tools capture packets. The intent is to diagnose a network problem. However the data could be "critical".

A security researcher could capture packets with the intent of checking that the communications are encrypted and thus secure. The data could turn out to be unencrypted and sensitive personal or financial data. If the security researcher informs the institution of the problem then that should not be considered an offence.

Chapter 2 Offences Section 6: "Unlawful acts in respect of software or hardware tools"

This section is exceptionally inaccurate and does not consider the implications of open source software models. Additionally obtaining, possessing and even use of software does not constitute unlawful intent. The user could merely acquire software for research and analysis. For example a white hat researcher who is in possession of malware samples or source code for the purpose of research.

Many open source software projects are distributed via a global network of download mirrors. South Africa has many open source software mirrors hosted on university or company servers for public access. These mirrors give faster access to users within geographic locations. Within the wording of the bill, universities or the administrators who host software mirrors could be held liable.

The following description is incredibly vague: *"For purposes of this section "software or hardware tools" means any data, electronic, mechanical or other instrument, device, equipment, or apparatus, 19 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".*

When considering that many tools can be operated on Windows / Linux, within this definition then Microsoft Windows would be unlawful if hacking tools are used on the Operating System. It is very important that intent be highlighted within the Cyber Crimes Bill. Tools, data, hardware etc. can be used for both good and bad activities, but intent is what constitutes an unlawful offence.

As mentioned before the, South African companies manufacture and sell software for national mass surveillance, thus the following statements could make such activity unlawful: *"Any person who unlawfully and intentionally manufactures, assembles, obtains, sells, purchases, makes available or advertises any software or hardware tool for the purposes of contravening the provisions of section 3(1)(a) or (2)(a), 4(1), 5(1), 7(1), 8(1), 10(1), 11(1), 12(1) or (2) or 13(1), is guilty of an offence"*

6.1. Tools are multi-purpose. E.g. a hammer can knock in a nail or knock in a skull. Likewise a piece of a software can be used to gather information for purposes such as diagnostics, fault, finding, routine system monitoring, performance investigations, academic research, security research, etc.

6.2 and 6.3. The burden of proof should rest with the state to prove that an offense has occurred rather than the mere possession of tools that might (or might not) be used to commit an offense, shifting this burden to the accused who then has to prove his or her innocence.

These types of tools have legitimate uses. E.g. identifying the source of attack or diagnosing problems.

With reference to paragraphs 6.4. & 6.5, are these fines and prisons terms in line with owning a crowbar, screwdriver or other physical device which could be used to break into a building? If not then why not?

The definition of the affected tools are so vague that it includes almost all software, including operating systems, diagnostics tools and even web browsers. All of these have features that would include them in this definition.

On a point of principle: Tools and their use should not be outlawed, only their malicious use.

Chapter 2 Offences Section 7 & 8: "Unlawful interference with data, etc "

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

(a) alter data;

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

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

Can this be contextualised? Power outages may offend. Where data is transmitted wirelessly, interference, or blocking of spectrum may contravene this. Such interference or blockage may be inadvertent. Other bands of electromagnetic spectrum, e.g. C-bands (https://en.wikipedia.org/wiki/C_band), may be affected by home appliances, unbeknown to the user.

With regards to section "3 (a) alter data;"
What about Network Address Translation (NAT) or Session Initiation Protocol (SIP) packet header rewriting performed by network routers, firewalls or other devices? Most of computing exists to transform (alter) data. For more information on NAT and SIP refer to the following two links: https://en.wikipedia.org/wiki/Network_address_translation, https://en.wikipedia.org/wiki/Session_Initiation_Protocol.

With regards to section "3 (b) hinder block, impede …. data;"

What about spam filtering or filtering objectionable content using something like Dan's Guardian on a proxy server?

With regards to section “3 (b) confidentiality …. data;”

What about companies doing deep packet inspection of SSL traffic? They need to decrypt it to do that which breaks any confidentiality.

With regards to section “3 (c) deteriorate data;”

What about applying lossy compression to images, video audio or other data?

Chapter 2 Offences Section 9: “Unlawful acts in respect of malware”

In regards to the following incorrectly written section:

“For purposes of this section "malware" means any data, electronic,

mechanical or other instrument, device, equipment, or apparatus that is designed specifically to—(a) create a vulnerability in respect of;

(b) modify or impair;

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

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

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

In terms of the above definition a software developer could accidentally/unintentionally create a software vulnerability and it could be regarded as malware. This definition of malware is flawed, creating a vulnerability should not be a crime, but rather exploiting it. Some of the best malware research from the 90’s comes from the virus writing group 29A that wrote proof of concept code for would be viruses that did not contain payloads and also did not spread their viruses, by this definition their research would be illegal. This section should also outline punishment for the government’s use of malware. There are strong suspicions and allegations have been raised on several occasions that the South African government is making use of malware to spy on individuals. Without the constitutional protections of privacy of personal information government can act unlawfully without any sanction. Therefore it should be made clear what the limits are on legitimate law enforcement and national security agencies in this regard.

Additionally software in security companies is developed to find vulnerabilities (vulnerabilities are not created by exploits; the only person who can create a vulnerability is the developer, we merely find them) for testing, penetration testing or proof of concept.

This should not constitute malware as the intent is not to cause immediate harm but rather to identify vulnerabilities to prevent harm.

The following section is also inaccurate as the description is too wide: *“Any person who assembles, obtains, sells, purchases, possesses, makes available, advertises or uses malware for the purposes of unlawfully and intentionally causing damage to”*.

In terms of obtains malware, simply opening emails or surfing the web could cause your computer to “obtain” malware. Additionally relating to “possesses”, in terms of the definition of malware within the bill, having a bug database like Bugzilla would constitute possessing or acquiring malware.

While this section is somewhat clearer in terms of its wording (“for the purposes of unlawfully and intentionally causing damage to”), it does not include protection for whitehat activities. These legitimate information security activities are critical to cybersecurity. As previously mentioned they are not confined to government. On the contrary, around the world it is the private sector that provides this type of legitimate research, development of anti-virus software and penetration testing that is considered critical in the fight against cybercrime.

Chapter 2 Offences Section 10 Unlawful acquisition, possession, provision, receipt or use of passwords, access

Passwords are often shared amongst a group of people e.g. a team.

Systems often have common passwords. It would be easy to log into the wrong system with the right password.

Not all passwords secure important things. If someone types in a pin code on a photocopier to access it are they guilty of an offense?

Passwords are stuck on sticky notes on monitors and keyboards. Does viewing these constitute receipt?

Passwords are cached in browsers. If someone else using the same browser clicks on a site and it automatically logs them in due to the saved password then would that be a crime?

10.2 “or may be used for purposes of contravening the provisions of section”

A password may always be used to provide access. This is akin to finding someone guilty of an offense because they posses a key which could be used to unlock a door which could facilitate theft.

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

The above section of the law is the biggest issue created by the authors. The burden of proof falls to the accused now? This is unconstitutional.

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

(a) a secret code or pin;

(b) an image;

(c) a security token;

(d) an access card or device;

(e) a biometric image;

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

(g) a password,

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

(a) ”without limitations” The issue with this is that it enables this clause to be all-encompassing, and delimits this clause ambiguously, and unquantifiably.

(b) Can this be clarified? The onus of developing (implementing) a secure access mechanism cannot be transferred to the one who has the means to gain access. i.e. you cannot penalise people for having keys.

(f) & (g) These are not universally unique, so it's not implausible that a person may possess such records that also incidentally provide access elsewhere

“any other device or information”

This is too wide and vague, for example it encompasses any random alphanumeric word generator.

Chapter 2 Offences Section 11 “Computer related fraud”

This section makes a lot of sense. However we’d be inclined to amend section 276 of the Criminal Procedure Act, 1977 (Act No. 51 of 1977) to include misrepresentation via data or data messages (using a computer or not) to constitute fraud. Even better would be to amend that section so that no matter the medium, if misrepresentation is made for the purpose of unjustified enrichment then that constitute fraud. No need for a separate law each time a new medium of communication arrises.

“(1) Any person who unlawfully and intentionally, by means of data or a data message, makes a misrepresentation which— (a) causes actual prejudice; or (b) which is potentially prejudicial, to another person is guilty of the offence of computer related fraud.”

This seems to encroach a lot on freedom of expression, since almost any opinion piece and even advertising has the aim of creating prejudice with regards to something. And, just because such an email was used, this is now distinguished from fraud as an “offence of computer related fraud.”

Clearly this is not logical. Don’t redefine fraud that is better dealt with in other legislation.

“(b) A court which imposes any sentence in terms of this section must, without excluding other relevant factors, consider as aggravating factors— (i) the fact that the offence was committed by electronic means;”

How is fraud *“committed by electronic means”* an *“aggravating factor”* when compared to any other fraud?

Chapter 2 Offences Section 12 “Computer related forgery and uttering”

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

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

This section, like section 11 seems reasonable at first glance. However forgery should be forgery regardless of the medium used to perpetrate it. As such we would recommend amending section 276 of the Criminal Procedure Act, 1977 (Act No. 51 of 1977) to include falsified electronic documents.

However the phrase “potential prejudice” is concerning. Making laws that result in potential prejudice becoming an offense is open to abuse by both the state and individuals wanting to use the law for their own ends.

This must have limitations, especially when it comes to Freedom of Speech. Consider that parody, or practical jokes, fall under this definition, but the intention is not forgery but humour or comment. The summary finding towards forgery is over-reaching. This must be explored under appropriate procedures before it's attributed the type of offence.

There isn't a definition / context for False. Seems trivial at face value, but let's consider that truth is also relative. E.g. if my one car breaks down, that's 100% of my population, but << 1% for the manufacturer.

The definition of Data Document is also very limited, or otherwise vague and ambiguous. given how the phrase "data" is used throughout this Act.

Chapter 2 Offences Section 13 "Computer related appropriation"

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

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

If anything using electronic means to appropriate someone else's property could be considered a mitigation of sentence because it precludes the possibility of physical violence.

Chapter 2 Offences Section 14 "Computer related extortion"

Seems redundant with existing law on extortion.

This seems to target responsible disclosure practices directly: telling a party responsible for a vulnerable system that "We shall disclose this vulnerability publicly in [insert time frame], or as agreed between us" will be tantamount to extortion in this section.

Whistleblowing for systems which have been reported as insecure (vulnerable) but which have not fixed (and are thus exposing customers, the public, etc) could also fall afoul of this section.

Chapter 2 Offences Section 15 "Computer related terrorism"

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

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

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

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

(c) making himself or herself available, for the benefit of, at the direction of, or in association with any person, entity or organisation engaging in a computer related terrorist activity, and who knows or ought reasonably to have known or suspected, that such act

was done for the purpose of enhancing the ability of such person, entity or organisation to engage in a computer related terrorist activity, is guilty of the offence of association with a computer related terrorist activity."

Are ordinary South African citizens to check potential employers' terrorist status? What resources and supporting infrastructure is provided for this? Otherwise this law imposes an unreasonable burden on the public to investigate and explore potential crimes without really ascertaining skill or resources available to the public to execute this assignment.

"(3)(b) solicits support for or gives support to a person, entity or organisation"

They aren't terrorists until they are. The expectation that the public will see through facades of terrorist entities is unreasonable.

"(5) For purposes of this section "computer related terrorist activity" means…."

This definition is too vague. If a person writes software that crashes the stock exchange, how does that make them a terrorist? It could be a sincere defect, miscalculation, etc. Indeed this has happened through some High Frequency Trading (HFT) systems on the NYSE e.g. on 24 August 2015 when HFT systems withdrew from the market to protect themselves. Another example would be the Microsoft SQL Server worm which propagated itself in January 2003. Here follows a couple of links on the above terms and events: https://en.wikipedia.org/wiki/High-frequency_trading, http://www.microsoft.com/en-us/server-cloud/products/sql-server/, http://www.zerohedge.com/news/2015-08-25/cutting-through-hft-lies-what-really-happened-during-flash-crash-august-24-2015, https://en.wikipedia.org/wiki/2010_Flash_Crash

"and who knows or ought reasonably to have known or suspected"

Is this Bill asking us to profile our fellow citizens? Are ordinary citizens empowered to deduce or distinguish a terrorist?

This section is more appropriate in an anti-terrorism act, than a cybercrime act. Just as was mentioned above regarding fraud.

This section also does nothing to protect security research, researchers and the publication of their results (which may be used by a terrorist organisation). Maybe we'll be

required to add a “No terrorist may use this work” disclaimer to security related publications…?

Does this section apply to enemies of the State in a situation of war?

Computer related espionage and unlawful access to restricted data (s.16)

“… with the intention of directly or indirectly benefiting a foreign state or any person engaged in a terrorist activity ... “

This entire section should be treated in another legislation altogether.

There are just too many classification terms, that are not defined within this Act.

With regards to indirect benefit, how is that deduced?

This section contains **NO PROTECTION** for whistleblowers.

Chapter 2, Section 17: *“Prohibition on dissemination of data message which advocates, promotes or incites hate, discrimination or violence”*

1.c. “assists in making available, broadcasts or distributes, through a computer network or an electronic communications network, to a specific person or the general public, ...”

This will criminalise any social network, CSP and even software/hardware vendors used by a person to publish an offending message.

This section does not belong in a cybercrime bill, but rather legislation regarding hate speech. It also fails to address the intricacies of hate speech, such as satire, comedy and general differences in opinion.

As a results, this will criminalise (almost) anyone with a social media account, the SA government itself, and now me for the previous item in this list.

Chapter 2, Section 18: *"Prohibition on incitement of violence and damage to property"*

Mostly the same as comments as Section 17 apply.

Chapter 2 Offences Section 20 "Infringement of copyright"

The bar for infringing copyright seems is set exceptionally low. Someone emailing an email with attached photographs would be infringing copyright.

There seems no provision for fair use.

If it included the requirement "for commercial gain" then that would eliminate the above concerns.

This whole section overlaps the Copyright Act, and should rather be handled there. The Copyright Act provides for rights conferred by various forms of Copyright, exceptions, sui generis.

Chapter 2 Offences Section 21 "Harbouring or concealing person who commits offence"

How does one prove *"reasonable grounds to believe or suspect"*?

This question is doubly so for offences which have not even been committed! It makes an offense of harbouring someone who has not yet committed an offense (thought crime?).

This clause could be used to finger encryption and protection of a potential offender's privacy as an offence.

Concealing a person who commits offence can be done by encrypting one's hard drive, or communications. With this clause they can argue this and by law force you to decrypt!

Forcing decryption is tantamount to preventing the right to remain silent thus forcing self incrimination.

Basically it could become a well worn excuse for forcing some to decrypt under mere suspicion of committing an offence or simply associating with someone who is suspected of committing an offence e.g. chatting to them on facebook, tweeting them, tagging them in a instagram post, etc could and probably would be considered as means to establish association to suspicious parties.

Chapter 2 Offences Section 22: "Attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding, or procuring to commit offence"

This section is a gross injustice as the vague wording of it will likely be used to persecute whistleblowers, competitors, opposition parties, political opponents or civil society. This section grossly violates the rights of an individual, in terms of the person being guilty of the offence before being found guilty. This section of the bill will be exploited against individuals when an opponent with questionable ethics employs legal counsel. Additionally the evidence to support such a claim (system logs) can easily be falsified and the paper based nature of our courts will deter a defendant's ability to defend him/herself.

This section should be struck from the bill or redrafted to protect the privacy and constitutional rights of the individual. Additionally Government needs to set minimum IT Security and Forensics standards to be applied with the law. Currently consulting with an expert, the expert's certifications or ability needs to be established to allow a court to receive proper information on technical matters.

Chapter 4: "Powers to investigate, search and access or seize and international cooperation"

Section 26: *"Definitions and interpretation"*

"article"

It is hopefully an omission that (b) does not include the requirement of “believed, on reasonable grounds”. Without it, the definition seems to include anything (as “any other information, instrument, device or equipment” seem to indicate) that anyone deems an “article”, since it “may afford evidence”, even with no reasonable belief to that effect.

“law enforcement agency”

As a matter of accuracy, is the SSA a law enforcement agency? It doesn’t seem to be the case from http://www.ssa.gov.za/AboutUs.aspx, but we can’t be sure. Reading the following sections makes such an inaccuracy seem very important, since a “member of a law enforcement agency” is granted a lot of powers.

*“**investigator**”*

“on the strength of his or her expertise”

How is this expertise determined, proven, documented, etc? Where is this defined?

Section 28: “Search for and access to or seizure of, certain articles”

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

Considering that the definition of article is all-encompassing, this provides for the law agents to seize even non-offending articles, or adversely affect parties and articles that were not partisan to potential commitment of alleged crimes.

Section 29: “Article to be accessed or seized under search warrant”

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

Section 29 is too vague and will have dangerous consequences. To a hammer everything looks like nails. You cannot violate privacy and confiscate every item from an individual near a premise. If a crime is committed on the premise of a ISP, do you raid the ISP and

confiscate all the servers in the data centre, as well as all personal items on the systems administrators on premise?

This could become a legal weapon for a competitor. To cripple an opponent you merely have to fabricate an offence and all assets will be seized until the entity can prove its innocence. This also relates to political opponents or non governmental organizations.

What does “nearby” mean?

What makes this section really worrying is the potential for abuse. Without technical knowledge about what magistrates or judges are signing warrants for, this could create an easy avenue to search/seize anything and everything an agent wants. Don’t have any hard evidence on person A? Don’t worry! Person B (completely unrelated to person A) sent a racist tweet using an ADSL line. Since person A lives “nearby” a Telkom line, he is covered by the warrant for person B!

“2 (f) obtain and use any instrument, device, equipment, password, decryption key, data or other information that is believed, on reasonable grounds, to be necessary to access or use any part of any data, computer device, computer network, database, critical database, electronic communications network or National Critical Information Infrastructure identified in the warrant to the extent as is set out in the warrant;”

This seems to ride roughshod over privacy.

How are they going to ”obtain” passwords to decrypt things? The right to remain silent exists for good reason...

Section 30: “Oral application for search warrant or amendment of warrant”

Without a time limit for reconsideration in (6), it may “postponed” until the articles in question has already been searched and privacy violated, without a magistrate/judge’s oversight.

Surely there should be one set of procedures for getting a warrant from a magistrate or judge regardless of whether it is an offence described in cybercrime bill or an offense described in some other bill.

Section 31: Search and access or seizure without search warrant

"Any member of a law enforcement agency or an investigator who is accompanied by a member of a law enforcement agency may, without a search warrant, execute the powers referred to in section 29(2) of this Act, subject to any other law if the person who has the lawful authority to consent to the— (a) search for and access to or seizure of the article in question; or (b) search of a container, premises, vehicle, facility, ship, aircraft, data, computer device, computer network, database, critical database, electronic communications network or a National Critical Information Infrastructure, consents, in writing, to such search and access to or seizure of the article in question"

How is the legal authority established for the above section?

What about the case where a document storage company grants permission for their systems to be searched? The actual owner of the information won't have given permission. This raises serious issues especially regarding privacy.

Section 32: Search and seizure for and access to article on arrest of person

1.b: "any other offence"

So, when being arrested for some petty crime, any member of law enforcement (as implied by (2)) can search the arrestee's phone, laptop and even their bank account (assuming they've got their bank card on their person), compel them to relinquish their passwords/PINs/encryption keys/whatever, without it even having anything to do with the offence they're being arrested for!? Also, if that person happen to be working on a bank's mainframe at that time, they are allowed search and seize that too!? This seems exceptionally broad and ripe for abuse.

This section provides is a giant loophole which is going to prove too tempting not to be (ab)used.

Section 33: Assisting member of law enforcement agency or investigator

"(1) An electronic communications service provider or person, other than the person who is suspected of having committed an offence under this Act, who is in control of any container, premises, vehicle, facility, ship, aircraft, data, computer device, computer network, database, critical database, electronic communications network or National Critical Information"

Regarding the above section, considering the earlier definition of who an ECSP may be, this over-arches and gives the state the power to compel anybody who has ever stored any other person's data to assist the state.

Section 36: "Wrongful search and access or seizure and restriction on use of instrument, device, password or decryption key or information to gain access"

"(2)(b) must destroy all information if -"

Clarify "all information".

Section 38: "Prohibition on disclosure of information"

"he, she or it"

What does this mean? Very vague

This section contains no protections for whistleblowers.

Section 43: "Oral application for preservation of evidence direction"

We find it hard to believe that it's not possible to write down an application in the vast majority of cases. In those very occasional situations where the member or law enforcement would have to make an oral submission (e.g. over the phone from a crime scene) then we would suggest that at a minimum the conversation be recorded and transcribed so as to provide an accurate record of the application. This should then be followed up with an additional (supplemental) written application with 48 hours.

This is still probably open for abuse. E.g. not giving a judge sufficient time or reasons to consider as a means to obtain the desired *"preservation of evidence direction*".

Section 44: "Access to data and receipt and forwarding of unsolicited information"

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

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

An interesting mention of *"public available data"* how does this (non) definition relate to the access related offence in chapter 2?

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

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

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

investigator; or"

Privacy implications?

How is lawful authority confirmed?

Chapter 6

One big overarching question: Is it feasible?

This chapter mandates the creation of 7 types of bodies, in several different government departments, with large overlaps in responsibilities, in a country with a) no money to accomplish this with, b) an undersupplied infosec capability, and c) a poor record of creating such capability.

It should be suggested that most (if not all) of these bodies either be combined, dropped, or absorbed into their relevant departments.

If penetration testing companies cannot even find capable employees, where will government find them for all these new bodies/teams?

It is also concerning that most of these bodies are clearly geared toward protecting, servicing, and providing information to government, with very little effort flowing from government to the citizenry/private sector. This creates the impression that this bill is aimed at giving government more powers and capabilities, without affording the same to its citizens.

Another concern are all these “incidents” that come to light. Will they be communicated to the public? How will they learn of incidents in the private sector where their disclosure will generally have negative consequences for the affected institution?

Section 51 “Cyber Response Committee”

Information and communication technology touches just about every business, organisation and individual in South Africa, therefore there are some far reaching consequences that stem from such a committee.

Any such committee needs strong oversight from the highest levels i.e. a parliamentary committee to ensure accountability and prevent abuses.

How about transparency measures, in the form of anonymised records released to the public?

Section 52: "Cyber Security Centre"

"(6) The Cabinet Member responsible for State security may make regulations to further—

...

(b) impose additional duties upon the Cyber Security Centre;..."

While we're sure "legally" is implied and intended, but given the broad definitions in this act, this point seems to create the possibility of the minister of State Security to setup the ZA NSA in the Cyber Security Centre, since it is all covered under this act.

Section 53: Government Security Incident Response Teams

"(5) The objects and functions of a Government Security Incident Response Team are to—"

These functions are currently being tended to by SITA. Admittedly, they're doing a very poor job of it. Regardless, how does this GSIRT affect SITA's mandate and operations? Will we simply have double the "capability" (tax burden)?

Section 55: Cyber Command

Will this be our cyber army? What about offensive capabilities?

Section 56: Cyber Security Hub

"(5) The objects and functions of the Cyber Security Hub are to—

(j) investigate the activities of cryptography service providers in relation to their compliance or non-compliance with relevant legislation and issue orders to cryptography service providers in order to ensure compliance;"

The term "cryptographic service provider" is not defined, nor used anywhere else in the bill. Does it include CSPs allowing encrypted traffic over their networks? Website operators that support HTTPS? Tor users/operators?

What “activities” are being to be investigated? What is the “relevant legislation” that is being referred to?

This smells like an attack on cryptography akin to what we’ve seen in the US and now in the UK, with the associated threats to personal privacy. Such vague, overarching statements cannot be allowed.

Section 58: Identification and declaring National Critical Information Infrastructure

Parastatals are not directly addressed. From the wording it would seem that Telkom would also be classified as National Critical Information Infrastructure, since the government owns a stake therein. Together with section (5)(d), allowing “regulations regulating… the storing and archiving of information on National Critical Information Infrastructure”, this will effectively put a large piece of public traffic under government control.

We tend to put things like power, water, medical care, communications under the critical infrastructure category.

Knocking out the PSTN and mobile network operators plus a good chunk of the internet in SA would be a problem of critical proportions.

However we do not see a company's infrastructure as a monolithic whole. E.g. a core switch network is very important whereas a training room, staff information portal, etc would all be very non critical.

Companies do tend to distinguish between levels of criticality for their disaster recover plans. Core business functionality e.g. providing your services to your customers and being able to bill for it is critical. The tools to plan next year's capacity expansion is far less critical.

We do not take issue with the declaration of National Critical Information Infrastructure in principle, but are concerned about the effects of the overlap with public infrastructure and the implications for us as ordinary citizens.

Chapter 7

Section 60: "Auditing of National Critical Information Infrastructures to ensure compliance"

We agree that auditing is important, but merely finding and reporting on problems is not enough.

What about resolving negative findings of audits?

Are the board members of private industry held responsible and accountable?

Are the directors or other government officials held responsible and accountable for their ministries, departments or public sector organisations?

Chapter 9

Section 64: "General obligations of electronic communications service providers and liability"

"(2) An electronic communications service provider that is aware or becomes aware that its computer network or electronic communications network is being used to commit an offence provided for in this Act must"

Regarding the above section based on that arbitrary definition that makes a teenager backing up his/her grandmother's tablet an ECSP, these obligations seem impractical and unreasonable. This conflicts earlier provisions of the Act that prohibits inspection of third-party data.

Conclusion

In conclusion while OWASP Cape Town Chapter does not oppose the bill in its entirety, we do oppose the current draft of the bill. Many areas of the bill need to be redrafted and a longer period of public comment must follow.

A longer time for public comment will allow private enterprise and experts in Information Security to contribute knowledge to create a better bill. South Africa has many strong private Information Security firms (Sensepost, MWR, Nclose, TelSpace, etc.) that can assist the government in redrafting the bill with the assistance of experts in law (http://privacyonline.co.za/). OWASP Cape Town, has the unique opportunity to proxy the knowledge of hundreds of Information Security professionals in South Africa, to assist in technical and legal issues related to ICT.

We need to protect our ICT infrastructure from enemies both local and abroad, but we must draft the bill to protect other actors such as whistleblowers, penetration testers, security and academic researchers, curious citizens who cause no harm, etc. We need the rights tools, people and legislation to do the job, inaccurate legislation can allow further loopholes for criminals to perpetrate the crimes that the Bill seeks to protect against.