6th Floor
6 Pepper St
8001 Cape Town

Grosvenor Corner
195 Jan Smuts Ave
2193 Johannesburg

South Africa

+27 21 4260802
+27 21 4261274 fax

+27 11 2507300
+27 11 2507502 fax

amabhungane@mg.co.za
www.amabhungane.co.za

November 30, 2015

Mr Sarel Robbertse
Department of Justice
By email CyberCrimesBill@justice.gov.za

Dear Sir,

SUBMISSION: CYBERCRIMES AND CYBERSECURITY BILL

We appreciate this opportunity to comment on the draft Cybercrimes and Cybersecurity Bill. Due to time constraints we limit ourselves to a single aspect: the protection of classified information. However, our concerns are wider and we would not like to limit our right to comment further at later stages of the legislative process.

About us

The MandG Centre for Investigative Journalism NPC (amaBhungane) is a non-profit company founded in 2009 to develop investigative journalism so as to promote a free, capable and worthy media and open, accountable and just democracy.

We pursue this object through three sets of interventions:

- **Investigations programme:** to develop best practice in our field by producing major investigative stories that are accurate and fair, advance methods and standards, set an example to the wider media, expose wrongdoing and enable people to hold power to account;
- **Skills transfer programme:** to impart investigative skills to other journalists through fellowships and extramural transfers.
- **Advocacy programme:** to help secure the information rights investigative journalists need to do their work.

About our advocacy work

This submission is made as part of our advocacy programme.

As we practise investigative journalism, we are ideally placed to identify legal, policy and practical threats to the information flows that are the lifeblood of our field.

We have worked on information rights matters of direct benefit to investigative journalists and often the public at large since 2010. We have interacted with drafters, Parliament and civil society stakeholders i.a. to achieve amendments to the Companies Amendment Act, 2011, the Protection of Personal Information Act, 2013, and the Protection of State Information Bill.

Our submission is attached. We are available to clarify any aspect should you wish.

Yours faithfully,

Stefaans Brümmer, managing partner
stefaansb@amabhungane.org
083 2747438

Karabo Rajuili, advocacy coordinator
karabor@amabhungane.org
082 3656553

Submission on the Draft Cybercrimes and Cybersecurity Bill

M&G Centre for Investigative Journalism (amaBhungane)

Why we are making this submission

We understand the need for legislation regarding cybercrimes and cybersecurity, given the rapid evolution of cyberspace and new threats that have arisen and continue to arise. As investigative journalists we have a particular interest, for example, in the protection of digital communications, given our obligation to protect confidential sources of information.

By the same token we have an abiding interest in there being no unconstitutional or otherwise undue impediments to the flows of information that people need for public and private sector accountability.

The classification of information and its protection is one area where legislators should guard against undue impediment. The outcry over the Protection of State Information Bill ("POSIB") and its tortuous progression though Parliament, after which it remains unsigned by the President, should serve as a reminder of the need to get this aspect of the Cybercrimes and Cybersecurity Bill ("the Bill") right.

This submission is focused exclusively on this aspect of the Bill and refers unless otherwise indicated to cl 16(5), (6) and (7).

The structure of this submission

It appears to us that the Bill's clauses relevant to our concerns rely heavily on the provisions of POSIB, and that this has resulted in two categories of defect:

- Some defects in POSIB were replicated in the Bill.
- Some safeguards (for whistleblowers, journalists and others) in POSIB were "lost in translation".

Below, we detail our concerns relevant to each of the above. Thereafter, we propose a possible solution.

Defects in POSIB replicated in the Bill

1. Simple possession and disclosure by public criminalised

   1.1. International best practice/emerging jurisprudence holds that state information is most effectively and least invasively protected at source, rather than by visiting consequences for a breach on society as a whole.

   1.2. By way of example, the "Tshwane Principles" provide:[1]

> **Principle 47: Protection Against Sanctions for the Possession and Dissemination of Classified Information by Persons Who Are Not Public Personnel**
> (a) A person who is not a public servant may not be sanctioned for the receipt, possession, or disclosure to the public of classified information.
> (b) A person who is not a public servant may not be subject to charges for conspiracy or other crimes based on the fact of having sought and obtained the information.
> *Note: This Principle intends to prevent the criminal prosecution for the acquisition or reproduction of the information. However, this Principle is not intended to preclude the prosecution of a person for other crimes, such as burglary or blackmail, committed in the course of seeking or obtaining the information.*

   1.3. As such, the "simple" receipt, possession or disclosure of classified information by members of the public (as opposed to state employees and contractors) should not be criminalised. Of course, this does not mean that members of the public may not be sanctioned for aggravated offenses involving classified information, such as espionage and hostile activities.

[1] Global Principles on National Security and the Right to Information, June 2013, http://www.right2info.org/national-security/Tshwane_Principles

1.4. POSIB's simple possession and disclosure offences (s 41) apply to any person, not only state employees and contractors.

1.5. Such generalised criminalisation is particularly invasive of the rights of ordinary people when applied to cyberspace. Large international leaks of classified information such as "Cablegate" and the "Snowden Files" have shown how incredibly widely and fast such information can spread digitally, shared by millions of people. The United States, most affected by these leaks, jailed Bradley (now Chelsea) Manning and seeks to prosecute Edward Snowden, the state employee and contractor responsible for the leaks, but it will not under its laws prosecute members of the public, including journalists, for the simple acts of receiving, possessing or disclosing the information.

1.6. By contrast and like POSIB, the Bill would make members of the public guilty of a serious offence in comparable circumstances. The Bill, at cl 16(5), (6) and (7), makes "any person" who "possesses; communicates, delivers or makes available; or receives" classified information guilty of an offence.

1.7. Such an approach is inconsistent with the limitations clause at s 36(1) of the Constitution and the requirement to use the least restrictive means of limiting competing rights, in this instance the rights of access to information and freedom of expression.

1.8. There is also a practical problem: Criminalising ordinary people without the intention or capacity to prosecute them, or prosecuting them selectively, undermines the rule of law.

2. No public domain defence

2.1. POSIB and the Bill contain no defence that classified information received, possessed or disclosed is already in the public domain.

2.2. This aggravates the problem described above and may contribute to the widespread (and unenforceable) criminalisation of ordinary people.

2.3. Not providing for a public domain defence appears irrational when regard is had to the purpose of legislative provisions for the protection of classified information, namely to prevent such information falling in the wrong hands.

3. No harm test

3.1. International best practice/emerging jurisprudence requires that the disclosure of classified information should be penalised only if there is, and to the extent of, actual harm.[2]

3.2. POSIB contains no harm test relevant to the offence of simple possession and disclosure of classified information (s 41). The Bill replicates this defect.

3.3. This again is problematic when regard is had to the limitations clause of the Constitution and the requirement to use the least restrictive means of limiting competing rights.

4. Penalties for receipt, possession and disclosure of information unconstitutionally classified

4.1. POSIB at s 3 limits the power to classify state information to Cabinet, the security services, certain oversight bodies and, after approval by the Minister on good cause shown, other organs of state excluding municipalities and municipal entities.

4.2. POSIB at s 8 limits the types of information that may be classified and, at s 11, the levels to which information may be classified.

4.3. Thus, while there is debate about whether the limits are sufficiently narrow and properly defined, POSIB's drafters attempted to create a Constitutionally-compliant classification regime.

4.4. However, among its transitional provisions and at s 52(2), POSIB provides for the continued classification of information classified under the apartheid-era Protection of Information Act, 1982, the MISS Guidelines or "any other law". The 1982 Act and the MISS permitted the very widespread classification of information.

[2] See e.g. Principle 46, Global Principles on National Security and the Right to Information, June 2013, http://www.right2info.org/national-security/Tshwane_Principles

4.5. The effect is that POSIB criminalises the receipt, possession and disclosure of much information that would pass muster neither under POSIB nor under the Constitution.

4.6. The Bill, similarly, fails to distinguish between information that was classified under POSIB's attempt at a Constitutionally-compliant classification regime and unconstitutionally classified information. Cl 16(5), (6) and (7) simply refer to data "which is in the possession of the State and which is classified …", without defining the concept.

4.7. We submit that such an indiscriminate approach will not pass Constitutional muster.

Safeguards in POSIB "lost in translation"

5. No limited public interest defence or whistleblower protection

5.1. A key demand of the civil society and popular campaign against POSIB was for the inclusion of a "public interest defence" and whistleblower protection. The former is usually understood as a method for extinguishing the offences of (simple) receipt, possession and disclosure of classified information where the public interest in disclosure outweighs the harm contemplated. Whistleblower protection is a universally accepted mechanism for combating corruption and other forms of wrongdoing.

5.2. In response, legislators included the exceptions now found at s 41 of POSIB:

> 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); 35
> *(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.

5.3. These exceptions do not meet the test for a true public interest defence and reservations have been expressed about the workability of the whistleblower protection by reference to the Protected Disclosures Act. Nevertheless, these had the effect of ameliorating POSIB.

5.4. The Bill, however, contains no public interest defence nor any of the exemptions found in POSIB, including reference to the Protected Disclosures Act.

5.5. This leads to the iniquitous possibility that a person who may not be prosecuted under POSIB or who would have a valid defence, may be prosecuted and convicted under the Bill on the same set of facts. The Constitutional implications are substantial.

6. Excessive penalties

6.1. POSIB was criticised during its Parliamentary passage for its harsh penalties. In response, legislators reconsidered the sentencing regime and included explicit provision for the courts to apply lesser sentences in relation to espionage and related offences at s 34(4).

6.2. POSIB's arguably still very harsh penalties distinguish between those for aggravated offences, where the sentence is matched to the level of classification, and that for simple possession or disclosure, which attracts a comparatively light penalty regardless of the level of classification.

6.3. In POSIB, espionage and related offences (where the beneficiary is a foreign state) attract imprisonment of three to five years if the information is confidential, 10 to 15 if it is secret, and 15 to 25 years if it is top secret. Hostile activity offences (where the beneficiary is a terrorist organisation) attract sentences of up to five, 15 and 20 years.

6.4. Cl 16(2), (3) and (4), however, attract sentences of up to 10, 15 and 25 years – regardless of whether the beneficiary is a foreign state or a terrorist organisation.

6.5. The contrast is much more stark when it comes to simple possession and disclosure. S 41 of POSIB provides for a fine or imprisonment of up to five years regardless of the level of classification. The Bill provides for sentences of up to five years if the information is confidential, 10 if it is secret, and 15 if it is top secret. In cl 16(5)(b), (6)(b) and (7)(b) the offence in each instance is clearly of simple receipt, possession or disclosure.

6.6. The latter grossly compounds the iniquity described at (5.5) above. Not only, if prosecuted under the Bill for simple possession or disclosure, will a defendant be unable to avail him or herself of a defence that would have been available under POSIB, but he/she may be sentenced to 15 years on the same set of facts that would have attracted no more than a fine or five years under POSIB.

Towards a solution

7. It is probably no exaggeration to say that POSIB attracted more controversy than any other legislation before Parliament since 1994. First introduced in March 2010 and finalised at the end of 2013 after the President had referred it back to Parliament, the President has still not signed it into law two years later.

8. Organisations such the Right2Know Campaign have prepared Constitutional Court challenges to it; opposition parties have vowed to force a Constitutional Review; and indications are that an Amendment Bill may be introduced by the Minister before the President signs POSIB into law.

9. As indicated above, there are provisions of the Bill that are, intentionally or not, substantially harsher than equivalent provisions of POSIB and would likely attract similar levels of contestation.

10. Given that POSIB has not yet been enacted and remains subject to amendment/review, it appears that the concurrent processing of legislation that traverses the same terrain of the protection of classified information may be an exercise in futility and invite the duplication of contestation.

11. We recommend that, in so far as there is a need for the Bill to deal with the protection of classified information by making offences specifically applicable to cyberspace, it does so by reference to POSIB and not by duplicating any of its provisions. In that way, contestation can be properly limited to POSIB and not impede the passage of valid aspects of the Bill.