NATIONAL/W.CAPE
107 Community House
41 Salt River Rd, Salt River,
Cape Town, 7295
Tel: 0214471000
Email: admin@r2k.org.za

KWAZULU NATAL
Room 502, MTB
King George V Ave, Glenwood
Durban, 4041
Tel: 0312603577
Email: Joanne@r2k.org.za

GAUTENG
6th floor, Aspern House
54 De Korte St, Braamfontein
Johannesburg, 2001
Tel: 011 356 5860
Email: bongani@r2k.org.za

Right2Know Campaign

Submission on the Protection of Critical Infrastructure Bill

(Private Member's Bill introduced by the Democratic Alliance)

6 Oct 2015

About the Right2Know Campaign

The Right2Know Campaign (R2K) is a coalition of organisations and people campaigning for information rights — access to information, freedom of expression, and freedom of assembly.

This submission was prepared by R2K's secrecy focus group. For more information please contact Murray Hunter (murray@r2k.org.za).

Executive Summary

The National Key Points Act ("the Act") has privatised and outsourced the use of "national security" as a tool to promote secrecy and undermine freedom of expression and accountability in the public and private sector.

Though the Act was passed in 1980 in response to the perceived threat of sabotage to apartheid infrastructure, and was roundly recognised as an undemocratic law during the transition to democracy, it has found second life in the post-94 democratic era. Its broad, vague and draconian powers have led to numerous abuses grand and small – often inviting officials to exercise powers of secrecy and repression that go far beyond the specific measures of the Act.

These have included countless anti-democratic maneuvers by officials in government and the private sector using the National Key Points Act as a shield from criticism, either by denying access to crucial information (especially in the case of corporate polluters) or by invoking the Act to undermine protests directed at institutions which have been declared National Key Points. (Although the Act does not prohibit gatherings at National Key Points, in many cases the authorities have sought to frame certain protests as being a direct threat to a National Key Point's security.)

R2K calls for the scrapping of the National Key Points Act, and R2K structures have documented, exposed and challenged abuses of the Act on the ground. The apartheid-era Act must be replaced with a new law based on openness and transparency. This new law must be as narrowly applied as possible, with strong, independent oversight – both through formal institutions and through the provision of full public participation and citizen oversight. Above all, activities in the public interest, including whistleblowing, journalism, protest and dissent should be protected from prosecution.

In terms of this Bill, 'National Key Points' would be replaced by 'Critical Infrastructure' — any site deemed to be crucial to national security. If it were enacted tomorrow, roughly 200 National Key Points would be brought under its powers, spanning government buildings, parastatals and the private sector.

Though the Bill makes no mention of them (see section 5.3 of this submission), presumably another 248 Strategic Installations would also be incorporated as 'Critical Infrastructure'.

R2K welcomes any opportunity to further a meaningful public discussion on the National Key Points Act and the broader issue of South Africa's dangerous and expansive national security legislation. This is especially urgent given that the Ministry of Police pledged to replace the Act in May 2013 and to date have not tabled a Bill in Parliament. Unfortunately this Private Member's Bill ("the Bill"), while contributing to that discussion, is fundamentally flawed and dangerous. In some respects the Bill replicates many of the most offensive aspects of the apartheid Act, and in a few instances creates a whole new set of problems.

1. Need for Independent oversight

1.1 Oversight from Parliament

One positive proposal in the Bill is the provision for regular public reporting to the National Assembly identifying the number, name and status of all sites that have been declared 'Critical Infrastructure', per section 12. (However, other clauses detract significantly from this positive proposal – see section 2 of this submission.)

Unfortunately Parliament has often failed to provide meaningful oversight or response to abuses of the Act, except when it was politically expedient to do so – as with the scandal surrounding the President Zuma's private homestead near Nkandla. Many other abuses, such as those alluded to above, have gone unchallenged. A search of committee minutes on PMG.org.za, and the Hansard, suggest that for many years the policy was barely discussed, let alone challenged, in Parliament. At least by legally requiring regular disclosure of Critical Infrastructure to Parliament, this Bill would make it more difficult to neglect that oversight.

However, in other respects the Bill cedes significant power from Parliament to the Minister.

1.2 Parliament's oversight of Critical Infrastructure Board

The Bill's attempt to devolve the unfettered powers which the 1980 Act gives to the Minister of Police, to an appointed Critical Infrastructure Board, is also an encouraging proposal. However, these provisions fall short of giving this Board full independence. Section 5(1) provides that members of the Board are appointed by the Minister "after consultation with the National Assembly." This formulation simply gives no meaningful power to Parliament to influence these appointments, nor is any provision made for public participation and consultation on these appointments.

Section 6 further provides that the Chair of the Board can only be appointed on recommendation of the National Assembly, but the National Assembly can only recommend candidates who are have already been appointed to the Board by the Minister – Parliament can only nominate candidates who have already received the Minister's endorsement. This means that Parliament's role would be little more than ceremonial.

The Board should also table its reports directly to Parliament.

2. Transparency

2.1 Reports to Parliament

While section 12(1) provides for quarterly reports to the National Assembly disclosing the total number, names and category of all sites declared to be 'Critical Infrastructure', section 13(1) essentially undoes this gain, by empowering the Minister to withhold any information on almost no grounds:

> "The Minister must ensure that a list of the names and categories of all the places and areas declared as 'Critical Infrastructure' must be made available on the website of the South African Police Service unless he or she, after consultation with the Committee, decides that the publication of the name and category will increase the vulnerability of the place or area to such an extent that national security will be threatened."

This clause provides a loophole that cedes power to the Minister to invoke the same secrecy that has been at the centre of criticism of the National Key Points Act.

It is worth noting that the Minister of Police and South African Police Service have consistently held that merely identifying sites as National Key Points harms their security, and this was a key dispute in the 2014 High Court case that resulted in public access to the list of National Key Points. In the end Judge Sutherland found that SAPS and the Minister had simply failed to show why it was important to shield National Key Points from public scrutiny:

> "A serious flaw in the efforts to justify non-disclosure is the absence of an argument to support the conclusion that the NKP Act objectives include keeping secret the status of places as key points… All the respondents offer are platitudes and a recitation of the provisions of the statutes."[1]

In effect, section 13(10) of this Bill may finally provide a legal basis for the Minister to claim secrecy powers that may not even have been provided by the 1980 National Key Points Act.

2.3 Need to disclose location of 'Critical Infrastructure'

Section 12(1) and section 13(10) of the Bill call for the public release of the names and categories of 'Critical Infrastructure', but not the locations. From this it can be assumed that the Bill intends to keep this information secret. This secrecy is both unnecessary and wrong.

In Right2Know Campaign and Another v Minister of Police and Another, the court found little reason to uphold this secrecy:

> "In my view, the alleged anxiety about disclosure of addresses is misplaced. It may be correct that the only way to describe a particular key point is by reference to its address per se. The applicants have no interest in addresses per se, and where the key point can be identified without such reference, no obligation exists to do so. However, it is correctly surmised by the respondents that even without an address it is possible

[1] Right2Know Campaign and Another v Minister of Police and Another (2013/32512) [2014] ZAGPJHC 343, para 36

for an inquisitive person to find out where a place is located."[2]

Essentially, when the information can be pieced together in any case, such secrecy is irrational.

However, given the extremely harsh penalties this Bill seeks to impose, such secrecy can also do real harm. The full harm contained in the Bill's proposed offences will be dealt with in more detail below, but for now let it be noted that a law cannot seek to criminalise people for doing certain things in certain places, if those places are a secret kept under lock and key. Simply put, you cannot propose to keep the location secret, if taking a photo of it could put someone in jail to 10 to 25 years.

2.4 Closed meetings for Parliament?

It is right to delegate oversight to the Portfolio Committee on Police, rather than the Joint Standing Committee on Intelligence, which has a poor track record on transparency.

However, section 12(2) the Bill gives the Police Committee a legal requirement to meet behind closed doors to get detailed reports on 'Critical Infrastructure'. section 19 gives further detail on the obligation of the Committee to close its doors in certain conditions.

On principle R2K objects to closed meetings in Parliament.

2.5 Potential contradictions and loose ends

While the Bill has stated that it aims to create a more transparent regime than the 1980 National Key Points Act, it would end up creating several different overlapping official records of National Key Point-like sites, with varying levels of secrecy that do not appear to match up.

Section 16 says that the Critical Infrastructure Board must create an official 'Register' of Critical Infrastructure - but that this will be kept secret, accessible

[2] Right2Know Campaign and Another v Minister of Police and Another (2013/32512) [2014] ZAGPJHC 343, para 31

only to a select few. But there is also a partial report that the Minister of Police must table in Parliament (section 12(1)), a more complete but secret report that the Minister must table in a closed Parliamentary committee (section 12(2)), and another list that the Minister of Police which must publish on the SAPS website after making whatever redactions he wishes (section 13(10)). Aside from the obvious transparency concerns that this formulation raises, it is also somewhat messy. A better regime would focus on a single source of information, which should be made as public as possible.

3. Offences

The offences and penalties of the Bill offer the deepest problems yet, and are worth replicating here in full.

> *Offences and penalties*
> *20. (1) Any person who in the course of their duties under this Act, intentionally or negligently—*
> *(a) hinders, obstructs or disobeys any person in the fulfillment of their functions in terms of this Act;*
> *(b) unlawfully discloses, in any manner, any information relating to the security measures implemented at a Critical Infrastructure without being legally obliged or entitled to do so, or as may be necessary for the performance of functions under this Act; or*
> *(c) commits any act which damages, endangers, disrupts or threatens a Critical Infrastructure,*
> *is guilty of an offence.*
> *(2) Any person who, intentionally or negligently—*
> *(a) hinders, obstructs or disobeys any person in the fulfillment of their functions in terms of this Act;*
> *(b) unlawfully discloses, in any manner, any information relating to the security measures implemented at a Critical Infrastructure without being legally obliged or entitled to do so, or as may be necessary for the performance of functions under this Act; or*
> *(c) commits any act which damages, endangers, disrupts or threatens a 'Critical Infrastructure',*
> *is guilty of an offence. (3) Any person found guilty of an offence referred to in subsection (1) or*
> *(2) is liable on conviction to—*
> *(a) a fine not exceeding R1 000 000;*
> *(b) imprisonment of not less than 10 years but not exceeding 25 years; or*
> *(c) both such a fine and imprisonment.*

It is worth noting that section 20(2) is identical to section 20(1) and is

presumably a typographical error.

More substantively, these offenses criminalise legitimate disclosures of information, and as well as protest. They also bear a startling similarity to the offences contained in section 10(2) of the 1980 National Key Points Act – offering many of the same problems and some new ones.

3.1 Criminalising freedom of expression and access to information

3.1.1 Criminalising journalism and whistleblowing

The offence in section 20(1)b replicates the bulk of the same egregious offence of the 1980 Act, which places an almost total veil of secrecy on any information whatever *related* to the security measures of 'Critical Infrastructure'.

The inappropriate broadness of the information that could fall under this section is dealt with elsewhere.

For now, let it be noted that there are clearly instances where it is in the public interest for information about security measures at 'Critical Infrastructure' to be made public. The most famous example is the disclosure by investigative journalists of security features and other upgrades at the President's private homestead at Nkandla, which were vital to exposing possible waste of public funds and abuse of power.

These provisions also replicate another key problem from the Secrecy Bill — often referred to as "reversing the onus". Simply put, like section 43 of the Secrecy Bill which would made it a criminal offence to make secret information public unless protected by a few narrow exemptions, the section may exempt certain people from prosecution, but puts the onus on them to prove that their action was exempted.

Placing the burden on the accused to prove their action should be exempt violates the presumption of ignorance, and places an unjustifiable restriction on freedom of expression.

3.1.2 Criminalising ordinary public acts

These criminal clauses do not only ensnare courageous public acts of journalism and the like. The simple fact is that a great many National Key Points – and 'Critical Infrastructure' – are public places; these provisions make a criminal of ordinary people who take a selfie outside Parliament, at the airport, and hundreds of other sites.

3.2 Criminalising protest

The Bill adds new categories of offences not contained in the 1980 National Key Points Act, criminalising any act that "damages, endangers, disrupts or threatens" 'Critical Infrastructure'.

It goes without saying that sites that meet the Bill's envisaged criteria for 'Critical Infrastructure' are often the target of legitimate public protest and criticism. This includes government departments, financial institutions, and industrial pollutants.

Almost all effective forms of protest are disruptive by their nature, and institutions which are targets of protest can expect to be disrupted – albeit it temporarily. If protest that is disruptive but non-violent is still a Constitutionally protected form of free speech, it would be extraordinary to criminalise such action – especially with such heavy-handed sentences.

The offence of "endangering" or "threatening" 'Critical Infrastructure' are so especially vague that they surely invite officials to abuse the powers of the Act. Even if such abuses could be challenged in court, this is too high a cost. Practical experience has shown that the justice system simply does not mete out fair treatment to the poor and marginalized. The correct remedy is not to propose legislation with broad and expansive powers that invites officials to abuse them.

3.3 No public interest defence

These offences are not subject to a public interest defence. In this respect, the Bill raises similar concerns to those at the centre of opposition to the draconian Secrecy Bill. While there are limited (albeit deficient) exemptions to those section 20(1)b that criminalises the disclosure of information, there are no

exemptions or protections whatsoever for section 20(1)c which potentially criminalises forms of protest. Effectively the Bill cannot distinguish between security threats and legitimate acts of dissent, protest, advocacy, whistleblowing and journalism.

3.4 Harsh penalties

The penalties are outrageously high – significantly higher, in fact, than the 1980 National Key Points Act, which did not exceed three years – and carried no prescribed minimum sentence.

Without labouring the point, R2K believes these offences are drastically out of kilter with the values of our Constitution and hard-won democracy.

4. Scope of the Bill

The problems with the broadness of what the Bill seeks to criminalise are closely linked with broadness of what the Bill seeks to protect.

4.1 What is a security measure?

The first place to look is the problematic, broad and vague definition of what could be considered a security measure – and information which would be protected with criminal sanctions under section 20.

As we see in section 1, the definition of "Security Measures" is purposefully broad and open-ended, "not limited to" the descriptions that follow. This open-ended definition is anthemia to the principle that 'security' laws should have as narrow an application as possible.

4.2 On what grounds can a place be declared 'Critical Infrastructure'?

4.2.1 Replicating flaws from the "Secrecy Bill"

The question of the Bill's narrowness of application is critical in determining whether the Bill would be open to abuse if passed into law – meaning that we must look closer what the criteria for determining which sites can be declared

'Critical Infrastructure' and imbued with National Key Point-like powers.

The relevant section, 13(5), is similar to a corresponding section in the Protection of State Information Bill, and bears a similar problem – it encourages over-classification with a broad notion of 'security'. In particular section 13(5)c, is overkill, for several reasons.

- Practically every government department currently classifies documents as confidential, secret or top secret under the broad and likely unconstitutional Minimum Information Security Standards. If every government department classifies information, every government department is at some level of risk of leaking that information – effectively this clause would see every single government department be declared 'Critical Infrastructure'

- For government departments and officials who deal with classified information, a range of provisions already exist that oblige them to take adequate measures to protect this information.

- However, section 13(5)d goes even further, adding the consideration of whether 'Critical Infrastructure' is vulnerable to "an act that would expose information that would threaten the constitutional order of the Republic".

  This kind of drafting simply invites officials to paranoid thinking and abuse of power – exactly the kind of overreach that was a hallmark of the National Key Points Act. In addition to worrying about information in section 13(5)c that has actually been formally classified – albeit through a draconian procedure – officials will now be invited to speculate about protecting other forms of information which have not been formally classified but which would threaten the constitutional order of the Republic if exposed. This begs the question: what kind of information would threaten the constitutional order of the Republic? And why was it not classified in the first place?

4.2.2 Encouraging more National Key Points?

It is worth noting that sections 13(2)a to 13(2)i contain more categories and sub-categories of sites than currently used by the South African Police Service in administering the National Key Points Act (including, for example, railway stations and commercial banks). Furthermore, this Bill envisages a number of types of site which are not to be found on the current list of National Key Points – such as medical, police, fire and rescue systems; networks providing electricity to end users; commercial banks and trading houses; traffic movement systems, and ports, waterways or railway stations.

The risk is that these provisions get carried away in detail, and may encourage officials to over-classify and declare more 'Critical Infrastructure' than ever before -- potentially creating thousands of new sites, at great public cost and administrative bureaucracy, and with severe consequences for democratic values.

5. Additional concerns

5.1 Exempting the private sector from costs

Section 17 exempts private companies from having to pay for their own security upgrades. Quite simply it is unacceptable to expect the public to pay to maintain the security of the private firms that this Bill would seek to protect -- including, but not limited to, private banks, corporate polluters, and companies that make biological weapons and munitions.

5.2. Need to ensure public information about disasters and public safety issues at 'Critical Infrastructure'

According to Section 14(4)a:

> *"Notwithstanding the provisions in the Disaster Management Act, 2002 (Act No. 57 of 2002), all emergency services must assist in an emergency at a declared 'Critical Infrastructure', when so requested in writing by the South African Police Service, State Security Agency, or the South African National Defence Force without a disaster being declared in the Gazette."*

The Disaster Management Act requires the authorities to publicly declare all disasters by national or provincial gazette. It may be that Section 14(4)a intends that emergency services should respond rapidly to emergencies at Critical Infrastructure even before the authorities have declared a disaster in the gazette. At the very least this drafting creates an ambiguity about whether or not disasters at Critical Infrastructure should be publicly declared. Needless to say, it is crucial to the public interest that any disasters or public safety issues at Critical Infrastructure should be publicly declared immediately.

5.3 Bill does not account for 248 secrets sites declared to be Strategic Installations

As R2K has stated elsewhere, National Key Points are just one category of secret 'security' sites. Another category of sites exists called Strategic Installations – with 248 sites across the country[3].

At R2K's behest, the South African History Archive (SAHA) has submitted a PAIA request to the police for a list of these Strategic Installations. Police have refused to disclose this information, but it is believed that most Strategic Installations are mostly national and provincial government buildings[4].

'Strategic Installations' were a feature of the Police Ministry's 2007 draft Bill to amend the National Key Points Act. Though the Bill was withdrawn, it would appear that SAPS has implemented aspects of the Bill without any law to underpin it.

Any attempt to repeal the National Key Points Act should be cognisant of the need to roll back this unregulated practice.

#Ends

[3] Police Budget Vote, 2014/15

[4] R2K Factsheet on Strategic Installations, 3 Feb 2015: www.r2k.org.za/?p=4315