RIGHT2KNOW

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 draft Critical Infrastructure Protection Bill

(Civilian Secretariat for the Police Service)

15 June 2016

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 Alexandria Hotz (alex@r2k.org.za).

Contents

---

1 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.

While the Act was passed in 1980 by the Apartheid Parliament under PW Botha in response to the perceived threat of sabotage to apartheid infrastructure, it was strongly recognised as an undemocratic and unconstitutional law during the transition to democracy but has found a second life in the post-apartheid 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

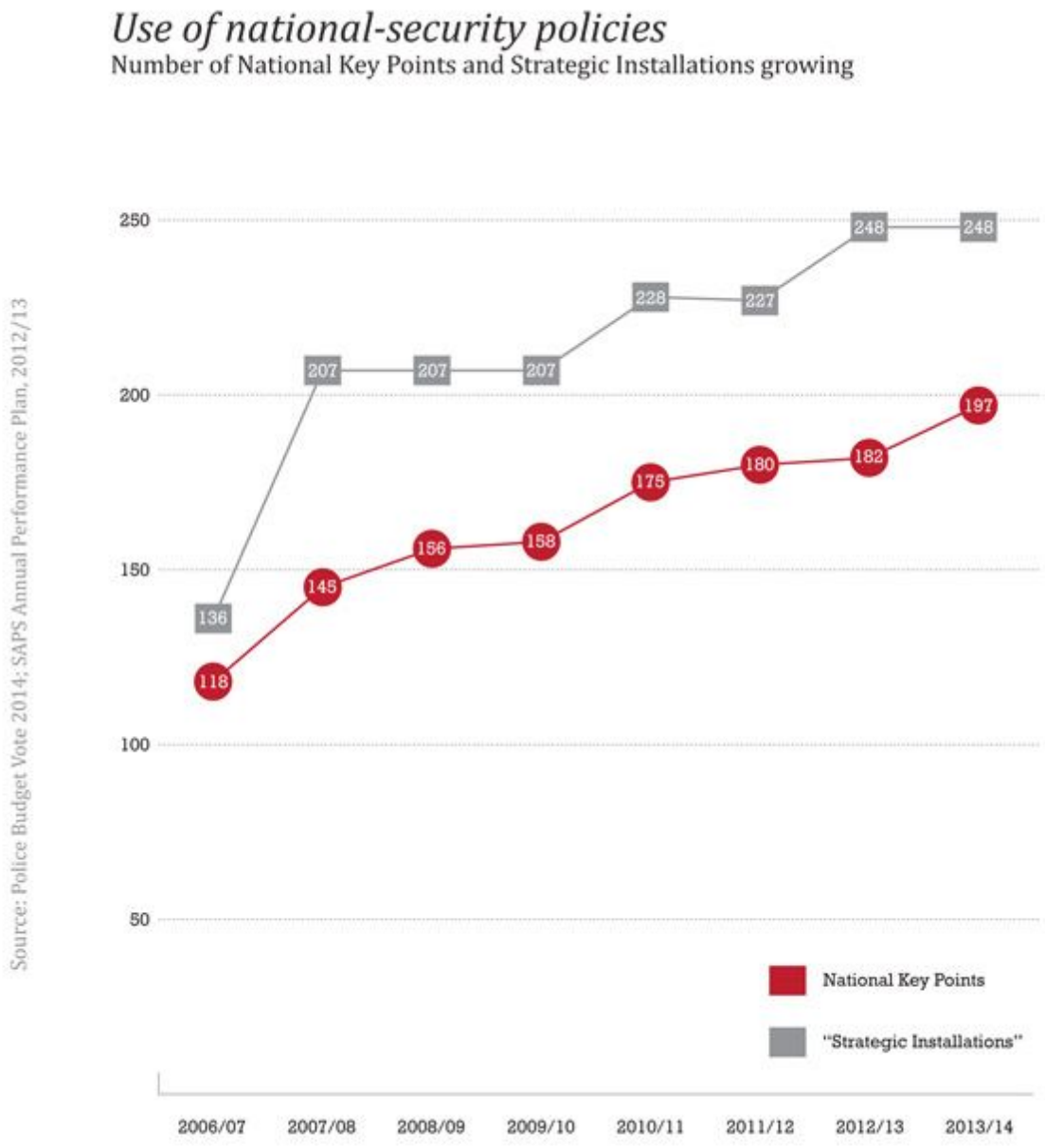
not prohibit gatherings at National Key Points, in many cases the authorities have sought to frame certain protests as being a direct threat to a National Key Point's security).

The Right2Know has consistently called for the scrapping of the National Key Points Act, and Right2Know structures have documented, exposed and challenged abuses of the Act on the ground. The apartheid-era Act must be scrapped in its entirety, not tinkered with, and any new law must be rooted in openness and transparency, as narrowly defined 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 draft 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 6.3 of this submission), presumably another 248 Strategic Installations would also be incorporated as 'Critical Infrastructure'.

The National Key Points Act came under great public scrutiny during the Nkandla scandal, when the homestead of President Jacob Zuma was declared a National Key Point and that the cost for security upgrades needed for such a National Key Point was to be born by the State (essentially public money). But in fact for years the Act had been used to undermine transparency and accountability, at a local level, especially affecting community protesters, environmental activists, and journalists.

The Act has been criticized for lacking transparency (even the list of National Key Points was a secret until released under court order), and for providing a convenient excuse to undermine the right to protest (officials routinely try to stop protests at national key points) and shield certain institutions (including private companies) from criticism or accountability. In 2014, two refineries even refused to release environmental compliance information because they were national key points.

These are no small matters, as the number of National Key Points and Strategic Installations has rapidly increased in the years under record. SAPS annual reports show that between 2007 and 2014, the number of National Key Points grew by 67% and the number of sites designated as Strategic Installations grew by 82%. (See graph.)



The apparent rapid expansion of these policies represent a troubling shift towards greater securitisation, in which 'national security' priorities and structures play an increasingly powerful and visible role in our politics and public life.

The constitutionality and legality of the National Key Points Act have been challenged for a number of reasons as it infringes on a range of rights, including access to information and freedom of expression. The fact that the very list of sites protected by the Act was a closely guarded secret has been a particular point of controversy, and eventually a matter settled by the courts. In *Right2Know Campaign and Another v Minister of Police and Another,* the South Gauteng High Court ordered the Ministry of Police to release the list of National Key Points to the public.

In light of mounting opposition to the 'National Key Points Act', the former Minister of Police, Nathi Mthethwa, promised a review of the Act in May 2013. Now the Civilian Secretariat for Police Service has introduced the draft "Critical Infrastructure Protection Bill'. This draft Bill falls far short of our demands. It does not address the fundamental failings of the previous Act or adequately deal with issues of openness and transparency.

Among other concerns:

- The draft Bill makes very little provision for the oversight role of Parliament, and none for the public.
- While the South Gauteng High Court ordered that the Right2Know Campaign and public have access to the list of National Key Points, the draft Bill leaves the question open of whether or not the list of critical infrastructure will be secret or public.
- This draft Bill still gives huge power to the Minister to declare infrastructure as "Critical Infrastructure" – which is what National Key Points will be now called. These could be public sector bodies or private companies. The policy is likely to cover more than 200 existing national key points, as well as more than 248 secret government sites that are declared 'strategic installations' – and could potentially apply to any other building or location. The criteria for whether a site should be protected, as 'critical infrastructure' is even wider than the National Key Points Act.
- This draft Bill infringes on the Right to Protest, as any disruption or obstruction to

the functioning of “Critical Infrastructure” is an offence under the Bill and one could be prosecuted up to 20 years for interfering in anyway with ‘critical infrastructure’.

- The draft Bill would also infringe on the right to freedom of speech and media freedom as it prohibits the publishing of a wide range of information about ‘critical infrastructure’ and effectively restricts the filming and photographing of ‘critical infrastructure’.
- It infringes on the rule of law as it attempts to apply this Bill retrospectively; this provision is likely unconstitutional. The Separation of Powers must strongly be protected and the powers of the Minister, the National Commissioner must be made clear so that the Executive does not try to change legislation through policy.

We reject policies that invite officials to exercise powers of secrecy and repression. We have to protect our hard-won rights to protest, access to information and media freedom.

Right2Know believes that this draft Bill does not represent a constitutionally sound replacement for the National Key Points Act as it fails to substantially deal with most of the fundamental problems and unconstitutional provisions of the Act, as previously noted. We do not think that the draft Bill will pass constitutional muster as it is still highly focussed on secrecy and furthering South Africa’s dangerous and expansive national security legislation.

There must be a more open process in which policy is developed. This draft Bill is the outcome of a closed process, sparked by public pressure but with no public consultation in the past three years. The initial Ministerial advisory committee’s report has never been made public. With only 30 days for public comment, the public participation process can easily become a tickbox exercise rather than meaningful engagement, consultation and input. Policies that seriously affect human rights, such as the draft ‘Critical Infrastructure Protection Bill’, require an open process not only with stakeholders in government and the private sector but with the broader public,

including public interest groups who have an interest in issues of security and secrecy.

Given the growing concern at heightened secrecy and securitisation in our politics and public life, as well as the contested nature of this particular policy, it is important to build a more participatory, open and transparent approach to policy development and law making.

Policy-making is a contested terrain, thus power relations and political interests play a big role in determining outcomes of policies. Therefore space must be created for more inclusive deliberation so as to democratise the process and level the unequal playing field.

2 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.

2.1 What is a security measure?

> "security measures" means any measure to preserve the availability of, the integrity of and confidentiality of a critical infrastructure and includes but not limited to—
> (a) information security at a critical infrastructure;
> (b) securing any part or component of a critical infrastructure;
> (c) information and communications technology infrastructure security at or to and from a critical infrastructure;
> (d) securing personnel or other persons at or nearby a critical infrastructure;
> (e) contingency plans for a critical infrastructure; and
> (f) administration of, provision of and implementation of security procedures at a critical infrastructure;

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 26.

As we see in section 1, the definition of "Security Measures" is purposefully broad and open ended, "includ[ing] but not limited to" the descriptions that follow. This open ended definition is contrary to the principle that 'security' laws should have as narrow an application as possible. This open ended definition will allow for an abuse of the Bill in order to protect State and private sector interests.

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

2.2.1 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 at the criteria for determining which sites can be declared 'Critical Infrastructure' and how it attempts to transfer National Key Point-like powers to these institutions.

Section 16(2) spells out the very wide and vague grounds in which the Minister of Police may declare any site to be 'Critical Infrastructure'. These include whether damage or disruption to the site would "prejudice" national security (which is not defined in the draft Bill, but which is unacceptably broadly defined in related legislation such as the Protection of Information Act of 1982 or the Protection of State Information Bill which has not been signed into law). But the draft Bill also provides that the Minister may take into consideration whether the site is important to "significant economic operations", the nature of which are not specified, or "the provision of goods or services essential for the daily operations, economic activity, livelihood or well-being of the public". These broad definitions may be drafted with the best intentions, but in a national security law they are a recipe for abuse.

3 Need for Transparency

The outrageous and unjustifiable secrecy surrounding the National Key Points has been a key grievance with the Act. This includes the basic question of which sites are protected by the Act, but also broader questions of how the Act is being implemented and overseen.

The draft Bill entirely fails to address this issue.

3.1 Failure to require minimum transparency

Publishing a list of sites protected by such a law is a very minimum level of transparency. The secrecy surrounding which sites were protected by the National Key Points Act has shown to be both unnecessary and wrong. In *Right2Know Campaign and Another v Minister of Police and Another*, the court found little reason to uphold this secrecy. This includes not just the names of the entities, but their locations as well. Judge Roland Sutherland found:

> "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 for an inquisitive person to find out where a place is located."

Yet the draft Bill is silent on whether or not such a list would be public. Section 27 of the Bill gives discretion to the Minister of Police to determine, without consultation or oversight, whether to make regulations regarding "the publication of areas and places declared as critical infrastructure and the requirements for information to the public". This unfettered power for the Minister to determine whether or not be transparent and provide information around 'critical infrastructure' is unconstitutional and undemocratic.

Section 21 (5) makes it clear that police will keep a register of which sites are declared Critical Infrastructure. But It is unclear who has access to such a register,

and whether such a register would be kept secret or made public.

However, it is clear that in terms of Section 24 (8) and Section 25 (8) that any site that is protected as Critical Infrastructure will be easily identifiable to a passerby.

Section 24 (8) provides that:

> A person in control of a critical infrastructure must demarcate and place a notice, in the prescribed format and manner, on premises constituting a critical infrastructure in order to notify persons that the premises are declared a critical infrastructure.

In Section 25 (8) provides that:

> The person in control of a critical infrastructure must indicate in a notice in the prescribed form and manner at every entry point of a critical infrastructure that the critical infrastructure may only be entered upon in accordance with the provisions of subsection (2) and the conditions determined by the security manager.

This section appears to contradict the need to classify any information around Critical Infrastructure as it discloses the identity and location of any particular site protected by the draft Bill. It makes any attempt to withhold that information irrational.

The provision that Critical Infrastructure be clearly identified on the ground is, on principle, an important measure. If the public is unaware of what 'critical infrastructure is and where it is located, they could unknowingly be committing offences.

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.

3.2 Reports to Parliament

No doubt it will be argued by some that the draft Bill does make adequate provision for transparency, through Section 15 which requires the Minister of Police to report to Parliament's Joint Standing Committee on Intelligence:

> "The Minister must, on an annual basis, table a report in Parliament through the Joint Standing Committee on Intelligence on the activities of the Critical Infrastructure Council, substantially corresponding with the format of the report in section 7(g)".

Section 7 (g) of the Bill provides the functions of the Critical Infrastructure Council, it states that the council must:

> "compile and submit a report to the Minister at the end of each financial year regarding—
> (i) the activities of the Council during the preceding financial year;
> (ii) particulars pertaining to the number of declarations as critical infrastructure;
> (iii) particulars pertaining to any limitations or revocation as critical infrastructure;
> (iv) financial statements;
> (v) the level and extent of public-private sector cooperation; and
> (vi) any other matter that may impact on the functioning of the Council;

This simply is not adequate. Firstly, these guidelines suggest that this report will not include identifying the sites and locations protected by the draft Bill. Secondly, the Joint Standing Committee on Intelligence is a closed-door committee whose meetings and documents are not publicly available. This is not a transparency measure.

On principle, the Right2Know objects to closed door meetings in parliament as the public should be able to access information especially as the offences and penalties of this Bill prejudice them seriously.

4 Need for Independent oversight

4.1 Almost no oversight role for Parliament

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.

The draft Bill's attempt to devolve powers to the secretive Joint Standing Committee on Intelligence, and the serious transparency implications thereof, are dealt with above. However, it is worth noting that even this is limited to receiving a report. The Minister receives almost unfettered powers to implement this policy.

All operational powers are delegated to a Council, appointed by the Minister; he does not need to consult with Parliament. This gives no power or oversight to Parliament to influence these appointments, nor is there any provision made for public participation and consultation on these appointments.

5 Offences

Section 26 of the Bill provides for the offences and penalties in relation to Critical Infrastructure. This provision of the Bill offers the deepest problems yet, and are worth replicating here in full.

> (1) Any person who unlawfully and intentionally—
> (a) tampers with, damages or destroys critical infrastructure; or
> (b) colludes with or assists another person in the commission, performance or carrying out of an activity referred to in paragraph (a), and who knows or ought reasonably to

have known that it is critical infrastructure, is guilty of an offence and liable on conviction to a period of imprisonment not exceeding 30 years.

(2) Any person who—
(a) unlawfully hinders, obstructs or disobeys a person in control of a critical infrastructure in taking any steps required or ordered in terms of this Act in relation to the security of any critical infrastructure;
(b) unlawfully hinders, obstructs or disobeys any person while performing a function or in doing anything required to be done in terms of this Act;
(c) unlawfully furnishes, disseminates or publishes in any manner whatsoever information relating to the safety and security measures applicable at or in
respect of a critical infrastructure;
(d) takes or records, or causes to take or record, an analog or digital photographic image, video or film of a critical infrastructure or critical infrastructure complex with the intent to use or distribute such analog or digital photographic image, video or film for an unlawful purpose;
(e) takes or records, or causes to take or record, an analog or digital photographic image, video or film of a critical infrastructure or critical infrastructure complex in contravention of the notice contemplated in sections 24(8) or 25(8);
(f) unlawfully damages, endangers, disrupts or threatens the safety or security at a critical infrastructure or part thereof;
(g) unlawfully threatens to damage critical infrastructure;
(h) unlawfully enters in or onto, or gains access to critical infrastructure, commits an offence and is liable upon conviction to a fine or to imprisonment for a period not exceeding 20 years, or to both a fine and such imprisonment.

These offenses potentially criminalise legitimate disclosures of information and acts of protest and dissent in a variety of ways. They offer many of the same problems as the offences contained in section 10(2) of the 1980 National Key Points Act – and some new ones.

5.1 Criminalising freedom of expression and access to information

Blanket secrecy on ‘safety and security’ measures

The offence in section 26(2)b replicates the bulk of the same egregious offence of the 1980 Act, which places an almost total veil of secrecy on any information *related* to the safety and security measures of ‘Critical Infrastructure’.

The inappropriate broadness of the information that could be classified as a security measure is dealt with elsewhere. For now, it is worth pointing out two things.

Firstly, many security measures are things visible to the passerby: a fence around the Engen refinery in South Durban, a security camera in the parking lot of a SABC station, a turnstile at Parliament. To disclose their very existence, when they are actually not secret, nor sensitive, could be a construed as an act against ‘national security’ in terms of this Bill.

Secondly, let it be noted that there are clearly instances where it is in the public interest for information, including sensitive 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. No demonstrable harm was done by these disclosures, and they served a vital role in informing the public, yet these acts would be criminalised under this Bill.

Aside from the lack of a public interest defence or other safety mechanisms dealt with in Section 5.3 of this submission, 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 make 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.

‘Banning’ videos and photographs of anything

Section 26(2)c extraordinarily goes even further than the 1980 Act, by prohibiting the photographing, filming or recording of *any* aspect of a Critical Infrastructure -- not just the security measures -- if it is for an “unlawful purpose”. This is an absurd provision. On many occasions, Right2Know members or supporters have been harassed by police or private security when taking videos in public places near or at National Key Points. It is a key way that the Act has been used to shield these institutions from public scrutiny. The qualification that the act is only prohibited if it is for an “unlawful purpose” is no relief. Who will determine at the time that someone filming a Critical Infrastructure has an unlawful purpose in mind? How can a security official be expected to risk an unlawful act being commissioned when he or she observes someone taking video footage at OR Tambo airport or the Gauteng provincial legislature or any other location? In practical terms, this clause draws a veil of secrecy around any institution that would be protected by this draft Bill.

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 potential criminal of ordinary people who take a selfie outside Parliament, at the airport, and hundreds of other sites.

5.2 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, refineries and other large-scale industrial and energy sites.

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. Protest that is disruptive but non-violent is still a Constitutionally protected form of free speech. It would therefore 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 is most often inaccessible due to cost and 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.

5.3 No public interest defence

These offences are not subject to a public interest defence. In this respect, the draft Bill raises similar concerns to those at the centre of opposition to the draconian Secrecy Bill. The draft Bill also lacks other possible safety mechanisms, such as a ‘harm test’ which would determine whether or not an offence had been committed by the demonstrable harm that is caused by an action, rather than an action itself which may cause no harm. Effectively the draft Bill cannot distinguish between security

threats and legitimate acts of dissent, protest, advocacy, whistleblowing and journalism.

5.4 Harsh penalties

The penalties are outrageously high – significantly higher, in fact, than the 1980 National Key Points Act, which did not exceed three years. One may ask, what has changed since 1980 that we need a harsher piece of security legislation?

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

6 Additional Concerns

6.1 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.

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 correspondence between R2K and the SAPS suggests that most Strategic Installations are national and provincial government buildings.

'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.

6.2 Breach of the Rule of Law

In the section that provides for Transitional Arrangements under section 30 (5) (a) it states that the Bill will apply retrospectively; this is reiterated in section 30 (5) (b), in that it states:

> Despite the repeal of the previous Act, any person who, before such repeal, committed an act or omission which constituted an offence under that Act and which constitutes an offence under this Act, may after this Act takes effect be prosecuted under the relevant provisions of this Act.

This is an infringement on the ordinary rule of our law that statutes operate only prospectively and not retrospectively and that one cannot rely on an Act retrospectively.

6.3 Cost to Implement the Bill

Beyond the constitutional issues around the Bill, what is of grave concern is that there has been no consideration to the cost of implementing this Bill and where the budget for the implementation of this Bill will come from. The Bill outlines a number of instances in which a budget would be required for the functioning of the Critical Infrastructure Council, upgrades to Critical Infrastructure and the labeling of 'Critical Infrastructure'. This is will be an incredibly expensive Bill to implement that will most likely come from public funds that could be spent on other urgent social welfare issues like education, health, housing and sanitation.

The other huge expenditure that will come from public money as seen with Nkandla is the cost of security upgrades to critical infrastructure. Provision 4 states that:

> (4) The Minister may, if the person in control of a critical infrastructure shows good cause in the application contemplated in sections 18(1) and 19(1), and in consultation with the Cabinet Minister of Finance and the Minister of the affected department, determine that a Head of a Government Department is, subject to such conditions as the Minister may determine regarding the recovery of cost from that person, responsible for all or some of the expenses necessary to implement the steps contemplated in subsection (1) and in writing inform the person in control of that critical infrastructure of the decision.

This provision could mean that the public could have to bear the cost of security upgrades of the private sector.

7 Conclusion

Despite our fervent opposition to the National Key Points Act and longstanding demand to see it scrapped, Right2Know believes that this draft Bill does not represent a constitutionally sound replacement to that Act. It fails to substantially deal with most of the fundamental problems and unconstitutional provisions of the Act, as previously noted. It represents a continuation, not a departure, of the security-statist thinking that drove opposition to the National Key Points Act. It is a matter of deep concern that, far from being closely monitored and regulated at the margins of our society, security laws and security politics play an increasingly prominent role in South Africa's public life, often at the expense of South Africa's people.

#End