

Lighting up the Intelligence Community: A Democratic Approach to Intelligence Secrecy and Openness

Laurie Nathan¹

The most important and vexed issue relating to governance of the intelligence services in a democracy is arguably that of secrecy. It is the most important issue because the higher the level of secrecy, the harder it is to ascertain and assess the features and performance of the services. In the absence of adequate information, it is impossible to have a meaningful discussion on the role and orientation of the intelligence community, on the need for intelligence reform and on the vital question of whether the services are protecting or undermining the security and freedom of citizens.

The subject is vexed because it is characterised by strong competing pressures. On the one hand, certain aspects of the intelligence community and its activities must be kept secret in order to avoid compromising the security of the country, the integrity of operations, and the lives of intelligence officers and their sources. On the other hand, secrecy is antithetical to democratic governance, it prevents full accountability, and it provides fertile ground for abuse of power, illegality and a culture of impunity.

Given these competing pressures, many governmental and non-governmental publications on intelligence assert that ‘a reasonable balance must be struck between secrecy and transparency’. This formulation is too abstract and non-committal to be of any value. In this briefing note I first outline a democratic approach to intelligence secrecy and then make practical recommendations on expanding intelligence transparency without prejudicing the security of the country.

I illustrate the approach and recommendations with reference to South Africa, whose intelligence transformation over the past fifteen years has been substantial, but remains incomplete.² In 2008 the Ministerial Review Commission on Intelligence in South Africa released a report that highlighted a number of areas in which the intelligence dispensation was inconsistent with the Constitution.³ This briefing note is based on that report.

A democratic approach to intelligence secrecy

When we talk about the need to find an ‘appropriate balance between secrecy and transparency’ in the world of intelligence, we are not proceeding from the correct point of departure. The starting point should be the essential tenets of democracy. These tenets include transparent governance and the right of citizens to gain access to information held by the state. They are essential because they are a prerequisite for accountability and oversight, political and personal freedom, democratic contestation of power, robust debate and exchange of ideas, the full exercise of citizenship and the prevention of abuse of power.

The idea that freedom of information is a necessary basis for other rights and freedoms is captured in a 1946 resolution of the United Nations General Assembly, which proclaims that “freedom of information is a fundamental human right and is the touchstone of all the freedoms to which the United Nations is consecrated”.⁴

The same logic is evident in South Africa’s Promotion of Access to Information Act of 2002, which seeks to “actively promote a society in which the people of South Africa have effective access to information to enable them to more fully exercise and protect all of their rights”.⁵ Conversely, according to Act, the system of government under apartheid “resulted in a secretive and unresponsive culture in public and private bodies which often led to an abuse of power and human rights violations”.⁶ The orientation of the Act derives from the Constitution, which is replete with provisions on transparency. These provisions are formulated in such a way as to create an “inseparability of the concepts of democracy and openness”.⁷

Flowing from this understanding of the relationship between openness and democracy, the challenge in the world of intelligence does not lie in ‘finding the right balance between secrecy and transparency’. Rather, secrecy should be regarded as an exception that in every case demands a convincing justification. Whereas the emphasis of intelligence communities throughout the world is on secrecy with some exceptions, in democratic societies the emphasis ought to be on openness with some exceptions. This is a matter of both principle and

pragmatic imperative. The dangers associated with secrecy – lack of accountability, abuse of power, infringement of rights and a culture of impunity – apply to the intelligence organisations no less than to other sectors of the state.

What, then, is the proper basis for intelligence secrecy as an exception to openness? The stock answer in democratic and authoritarian countries alike is ‘national security’.⁸ This answer is endorsed in the International Covenant on Civil and Political Rights, which identifies the protection of national security as a legitimate ground for limiting the right to freedom of expression and access to information.⁹ South Africa’s Constitutional Court similarly views national security as a basis for restricting public access to information about the intelligence services.¹⁰ Even activists campaigning for freedom of expression accept that national security constitutes a justifiable exception.¹¹

This is an unsound and dangerous approach because of the elasticity and ambiguity of the concept of ‘national security’.¹² When ‘national security’ is interpreted narrowly to mean the security of the state, it is often invoked to justify extraordinary measures that suppress civil rights and thereby undermine the security of citizens. On the other hand, if national security is interpreted broadly to cover all aspects of human security, then secrecy based on these expansive grounds might lead to excessive and spurious classification of information.

In a 1971 judgement the United States Supreme Court raised concerns of this nature about the vagueness of ‘national security’ in relation to restrictions on freedom of speech:

The word ‘security’ is a broad, vague generality whose contours should not be invoked to abrogate the fundamental law embodied in the First Amendment [dealing with freedom of speech]. The guarding of military and diplomatic secrets at the expense of informed representative government provides no real security for our Republic.¹³

National security in a democracy surely encompasses the security of the country, its system of government, its values and all its people. It consequently provides a

compelling basis for openness rather than secrecy. It is not something that has to be *balanced* against rights and freedoms. A democratic approach to national security *embraces* rights and freedoms.

The South African Constitution adopts this approach when it proclaims that “national security must reflect the resolve of South Africans, as individuals and as a nation, to live as equals, to live in peace and harmony, to be free from fear and want and to seek a better life”.¹⁴ A high level of secrecy is incompatible with this injunction.

Instead of being based on the amorphous notion of ‘national security’, secrecy regarding the intelligence community should be motivated with reference to specific and significant harm that might arise from the disclosure of information. It should be confined to those areas where disclosure would cause significant harm to the lives of individuals, the intelligence services, or the state or the country as a whole. Depending on the circumstances, moreover, the harm might have to be weighed against a strong public interest in disclosure. The government cannot seek to avoid all possible harm that might occur from the publication of sensitive information. Some risk of harm has to be tolerated because the dangers posed by secrecy can imperil the democratic order itself.

A minority judgement of the South African Constitutional Court has expressed an opinion along these lines:

In answering this question [concerning disclosure of information about the intelligence services], it is important not to deal with hypothetical damage that could be caused to national security if certain types of information were to be revealed, but rather to verify whether on the facts a real risk exists that non-trivial harm could result. More particularly, it has to be asked whether more harm could well result from disclosure than from non-disclosure.¹⁵

The Ministerial Review Commission argued further that less secrecy and greater provision of information about the intelligence services would be of benefit to the services themselves. A system that over-classifies information lacks credibility, it is difficult to maintain and enforce and it is costly and inefficient. Too much time and effort are

devoted to classifying and protecting innocuous information, potentially at the expense of safeguarding genuinely sensitive information.

In addition, excessive secrecy gives rise to suspicion and fear of the intelligence organisations and this reduces public support for them. In a democracy, unlike a police state, intelligence agencies must rely on public cooperation rather than coercion to be successful. The provision of greater information about the services would raise their profile in a positive way, reduce the apprehension and fears induced by secrecy, improve cooperation with the services and thereby boost their effectiveness.

Expanding intelligence transparency

Debates on intelligence secrecy typically focus on what should be withheld from disclosure. The Ministerial Review Commission focused on what should be published. It argued that in a number of areas a substantial amount of secret information could be disclosed – without compromising intelligence operations or the security of the country – in order to enhance public understanding, critical debate, accountability and oversight. The details are specific to South Africa but the general thrust of the recommendations has broad applicability to democratic states.

National Intelligence Priorities

Every year the South African Cabinet approves a set of National Intelligence Priorities (NIP) that are based on an intelligence estimate prepared by the National Intelligence Coordinating Committee (NICOC). The NIP document provides executive direction for the intelligence organisations’ focus, priorities and allocation of resources in the forthcoming year.

The NIP should not be classified. Parliamentary and public discussion on the executive’s security priorities would deepen accountability and democratic decision-making on an aspect of national policy that effects profoundly the safety and well-being of citizens. Security would not be undermined through disclosure since the NIP does not name individuals and organisations, referring instead to categories such as ‘organised crime’ and ‘nuclear proliferation’. Information that is extremely sensitive could be withheld from the public document.

Ministerial regulations

Since the advent of democracy in 1994, the Minister of Intelligence has issued two sets of regulations: the Intelligence Services Regulations of 2003, the bulk of which is secret, and the Regulations on Liaison with Foreign Intelligence Services of 2007, which is totally secret. This secrecy is permissible in terms of the intelligence legislation but it is contrary to the Constitution, which states that regulations and other instruments of subordinate legislation must be accessible to the public.

The secrecy is anomalous and undesirable. The primary rules governing the services, particularly in relation to investigative methods that infringe constitutional rights, ought to be available to the public. A distinction should be drawn between rules that must be confidential because they reveal sensitive operational details, and ministerial regulations that should be in the public domain because they are integral to democratic governance.

Executive policies

The Commission noted with concern the absence of ministerial policy on many politically significant topics, such as those relating to the mandates, functions, operations and intrusive methods of the intelligence services. Policies that ought to have been determined by the executive have instead been determined by the heads of the services and appear only in confidential directives.

The Commission recommended that the government publish a White Paper on Intelligence in which the following topics are covered:

- The mandates, functions and powers of the intelligence organisations, including oversight of, and controls over, their powers to infringe constitutional rights.
- Ministerial control and accountability, and the relationship between the intelligence services and the President, Cabinet and the Minister of Intelligence.
- Civilian oversight, including oversight by Parliament and the Inspector-General of Intelligence.
- The relationship and division of responsibilities between the various intelligence bodies in South Africa, the coordination of intelligence and the functions of NICOC.
- Relations with foreign intelligence services and sharing intelligence about South African citizens with foreign governments.

- Secrecy and transparency, covering the provision and protection of information.
- The institutional culture of the intelligence services and ensuring respect for the Constitution and the rule of law.

The process of preparing the White Paper should include parliamentary hearings and a call for public submissions.

Annual reports of the intelligence services

Unlike other government departments in South Africa, the annual reports of the intelligence services are not tabled in Parliament. There is no good reason for this. Security considerations are not at issue since the National Intelligence Agency (NIA) has published some of its annual reports on its website.¹⁶ This is true also of intelligence services in other countries.¹⁷

In a democracy the publication of annual reports by government departments and other organs of state is a necessary means of ensuring accountability to Parliament and citizens. In its submission to the Commission, the National Treasury added that departments should be judged by their outputs and the publication of annual intelligence reports would help taxpayers determine whether they were getting value for money.

Intelligence assessments

Intelligence assessments of individuals and organisations would in many instances be unsuitable for publication because of the risk of compromising operations and crime investigations. However, intelligence assessments that deal with categories of security and threats to security can frequently be published without risk of harm.

By way of example, the Canadian Security Intelligence Service (CSIS) publishes a range of material, including background papers on topics like economic security, weapons proliferation and counter-terrorism; a publication called *Commentary* that focuses on issues related to the security of Canada; and a series of research reports based on CSIS reviews of open source information.¹⁸ The annual reports of the Dutch General Intelligence and Security Service go so far as to include commentaries on radical and terrorist organisations that are mentioned by name.¹⁹

The budgets and financial reports of the intelligence services

The annual budgets and financial reports of the South African intelligence services are confidential and are not presented to Parliament. This is contrary to the constitutional provision which stipulates that national budgets and budgetary processes must promote transparency and accountability. Although the documents are reviewed by the parliamentary Joint Standing Committee on Intelligence (JSCI) behind closed doors, the services are not directly accountable to Parliament for their budgets and spending.

The Commission had an opportunity to read some of the budgets and strategic plans submitted to the JSCI by the intelligence services and did not believe that publication of these documents would in any way compromise intelligence operations or the security of the country. The Commission agreed with the National Treasury's proposal that the budgets and financial reports of the services should be presented openly to Parliament.

The Auditor-General's reports on the intelligence services

The Constitution requires the audit reports of the Auditor-General to be submitted to the relevant legislature and to be made public. The audit reports on the intelligence services, however, are presented only to the JSCI and are classified. The Auditor-General believes that this is inappropriate, noting that the Public Audit Act of 2004 allows for sensitive information to be withheld from audit reports.

The websites of the intelligence organisations

The website of the South African Ministry for Intelligence Services contains a fair amount of information, including the intelligence legislation, an organogram of the intelligence community, ministerial statements, court judgements that have a bearing on the intelligence services, speeches by the President and the Minister, and parliamentary questions and answers regarding intelligence.²⁰

NIA and the South African Secret Service (SASS) have websites that contain information about their work and orientation.²¹ This is not true of NICOC, the JSCI and the Office of the Inspector-General of Intelligence, with the result that members of the public cannot learn about their activities and results. The Commission recommended that all the intelligence bodies, including the JSCI, should have websites and that these sites should include a section that assists members of the public who want to request information under the Promotion of Access to Information Act.

Conclusion

In the course of the past fifteen years over twenty-five countries have enacted legislation aimed at giving their citizens greater access to government information. As the sphere of access and transparency has expanded and thereby strengthened democracy, intelligence organisations have lagged behind and remain a major exception. There are certain intelligence matters that should be kept secret, but the obsession with secrecy goes way beyond what is justified in a democracy and way beyond what is required to protect operations and security. This obsession should be replaced by a more rational approach that views secrecy as an exception that has to be justified on the basis of significant and specified harm arising from the disclosure of information.

Footnotes

- ¹ The author is a research fellow at the University of Cape Town and the London School of Economics. In 2006-8 he served on the Ministerial Review Commission on Intelligence in South Africa. He acknowledges with gratitude a research grant from the Global Facilitation Network for Security Sector Reform (GFN-SSR) at the University of Birmingham.
- ² Kenneth R. Dombroski, 2006, ‘Reforming Intelligence: South Africa after Apartheid’, *Journal of Democracy*, vol. 17, no. 3, pp. 43-57.
- ³ Ministerial Review Commission on Intelligence, 2008, ‘Intelligence in a Democracy: Final Report of the Ministerial Review Commission on Intelligence to the Minister for Intelligence Services, the Honourable Mr Ronnie Kasrils, MP’, available at www.crisisstates.com/Resources/intelligenceReport.htm.
- ⁴ United Nations General Assembly resolution 59(1), 14 December 1946.
- ⁵ Republic of South Africa, Promotion of Access to Information Act of 2002, Preamble.
- ⁶ *Ibid.*
- ⁷ Mr Justice Sachs in *Independent Newspapers (Pty) Ltd v Minister for Intelligence Services and Freedom of Expression Institute (Amicus Curiae)*, CCT 38/07 [2008] ZACC 6, at para 154.
- ⁸ See Sandra Coliver, Paul Hoffman, Joan Fitzpatrick and Stephen Bowen (eds), 1999, *Secrecy and Liberty: National Security, Freedom of Expression and Access to Information*, The Hague: Martinus Nijhoff Publishers.
- ⁹ International Covenant on Civil and Political Rights, 1976, article 19(3)(b).
- ¹⁰ *Independent Newspapers v Minister for Intelligence Services*, op cit.
- ¹¹ Article 19, 1996, ‘The Johannesburg Principles on National Security, Freedom of Expression and Access to Information’, available at <http://www.article19.org/pdfs/standards/joburgprinciples.pdf>.
- ¹² Arnold Wolfers, 1952, “‘National Security’ as an Ambiguous Symbol”, *Political Science Quarterly*, vol. 67, no. 4, pp. 481-502.
- ¹³ *New York Times Co vs United States* 403 US 713 (1971) at 719, quoted in *Independent Newspapers v Minister for Intelligence Services*, op cit, note 23 at pg. 21.
- ¹⁴ Section 198(a) of the Constitution.
- ¹⁵ *Independent Newspapers v Minister for Intelligence Services*, op cit, para 163.
- ¹⁶ These reports are not up-to-date, however. In March 2009 the most recent annual report on the NIA website was for the 2003/4 financial year.
- ¹⁷ The annual reports of the Dutch intelligence service are a good example of a comprehensive and useful report. See www.fas.org/irp/world/netherlands/aivd2004-eng.pdf.
- ¹⁸ See the website of the Canadian Security Intelligence Service at www.csis-scrs.gc.ca.
- ¹⁹ See www.fas.org/irp/world/netherlands/aivd2004-eng.pdf.
- ²⁰ The Ministry website can be viewed at www.intelligence.gov.za.
- ²¹ The website of NIA can be viewed at www.nia.gov.za. The website of SASS can be viewed at www.sass.gov.za.