A Critical Assessment of the South African Civilian Intelligence Agency

AUTHORS:
Mnr F.G. Loubser
Independent
South Africa
loubserrudolph@gmail.com

Prof André Duvenhage
https://orcid.org/0000-0003-0255-2602
Research Professor
Political Studies
Social Transformation Focus Area
Faculty of Humanities
Potchefstroom Campus
North-West University
South Africa
Andre.Duvenhage@nwu.ac.za

DATES:
Published: 26 September 2025

HOW TO CITE THIS ARTICLE:
Loubser, F.G. & Duvenhage, A., 2025. A Critical Assessment of the South African Intelligence Agency. KOERS — Bulletin for Christian Scholarship, 90(1). Available at: https://doi.org/10.19108/KOERS.90.1.2640

Abstract

This article analyses the state of the intelligence community (IC) in the South African context to determine whether the IC is a failure or whether it is a total disaster. Due to a failed, insufficient intelligence system, the current world order has been severely disrupted by two wars. In this regard, the focus is in particular on the situation in the Middle East, where Israel and the Palestinian group HAMAS are currently involved in a war. According to a Reuters report (Nakhoul & Saul, 2023), Israel was caught off guard by the HAMAS attack on 7 October 2023, and several people have died since then. These types of violent incidents recall the violent riots/protests in South Africa in July 2021, where the severe action of the people involved overpowered the South African Police Service (SAPS) and South African intelligence services. These protest actions / riots inflicted billions of rand in infrastructure damage, and hundreds of people died. The Expert Panel, appointed by the President of South Africa in July 2021, commented as follows on this protest action: "The question, many argue, is not if and whether more unrest and violence will occur, but when it will occur." (Presidency, 2021) A conceptualised intelligence risk management framework (IRMF) is used to analyse the IC of South Africa, with a specific focus on the State Security Agency (SSA). The article aims to explore, describe, and analyse the status and activities from a democratically based framework. Furthermore, the article aims to evaluate the failures of the past decades and draw conclusion regarding the current status of intelligence agencies or services in South Africa. This analysis will determine whether the IC is ready and capable of addressing these types of threats and risks in the future.

Keywords: intelligence community (IC); intelligence failure; intelligence risk management framework (IRMF); risk management (RM); South Africa

Opsomming

Hierdie artikel ontleed die stand van die intelligensiegemeenskap (IM) in die Suid-Afrikaanse konteks om te bepaal of die intelligensiegemeenskap 'n mislukking of 'n volslae ramp is. Vanweë 'n mislukte, ondoeltreffende intelligensiestelsel is die wêreldorde deur twee onlangse oorloë ontwrig. In hierdie verband is die fokus veral gerig op die situasie in die Midde-Ooste, waar Israel en die Palestynse groep HAMAS tans in 'n oorlog gewikkel is. Volgens 'n Reuters-verslag (Nakhoul & Saul, 2023) is Israel onkant betrap deur die HAMAS-aanval op 7 Oktober 2023, en sedertdien het duisende mense gesterf. Hierdie soort gewelddadige voorvalle herinner aan die gewelddadige onluste/protesaksies in Suid-Afrika gedurende Julie 2021, waartydens die ernstige protesoptrede van die betrokke mense die Suid-Afrikaanse Polisiediens (SAPD) en Suid-Afrikaanse intelligensiedienste oorweldig het. Hierdie protesoptrede het infrastruktuur ter waarde van miljarde rande beskadig, en honderde mense het gesterf. Die Deskundige Paneel, wat in Julie 2021 deur die President van Suid-Afrika aangestel is, het soos volg kommentaar gelewer op sodanige protesaksie: "Die vraag, betoog baie, is nie óf en ás onlus en geweld weer sal voorkom nie, maar wánneer dit sal voorkom." (Presidency, 2021) 'n Gekonseptualiseerde intelligensie-risikobestuursraamwerk (IRBR) word gebruik om die intelligensiegemeenskap te ontleed, met spesifieke toespitsing op die Staatsveiligheidsagentskap (SVA). Die artikel beoog om die stand en aktiwiteite vanuit 'n demokraties gebaseerde raamwerk te verken, te beskryf en te ontleed. Voorts het die artikel ook ten doel om die mislukkings oor die afgelope dekades te evalueer en tot 'n gevolgtrekking oor die stand van die intelligensie-agentskappe/-dienste in

Suid-Afrika te kom. Hierdie ontleding sal aandui of die intelligensiegemeenskap (IG) gereed en in staat is om hierdie tipe bedreigings en risiko's in die toekoms te hanteer.

Kernbegrippe: intelligensiegemeenskap (IG); intelligensiemislukking (IM); intelligensie-risikobestuursraamwerk (IRBR); risikobestuur (RB); Suid-Afrika

1. Introduction

Over the past four decades, there have been constant reports about the poor state of South Africa's intelligence services. These views were formed based on incidents from 2005 to date, encompassing corruption, illegal operations, unlawful actions by members of the services, and maladministration (as reported by the Joint Standing Committee on Intelligence (JSCI) in 2021, citing the Inspector-General for Intelligence and the Auditor-General). Adding to these incidents, are aspects of the current international threat picture, which ranges from terrorism, ethnic conflicts within states (Israel and Palestine), violent protest action, strikes, even countries at war (e.g., Ukraine/Russia), and the speedy international technological development, enhanced new threats in e-banking, economic transfers, identity theft, transnational crime, and cyber terrorism. One can only ask whether South Africa's civilian intelligence structures can handle these situations in their current weakened state. Therefore, this article aims to determine the current status of South Africa's intelligence agencies from a democratically conceptualised intelligence risk management framework (IRMF), examining whether the agencies can provide a professional and timely intelligence service to the country. This is done by conducting a critical assessment. The following methodology is used: Firstly, an IRMF is conceptualised, and secondly, this IRMF is used to evaluate South Africa's current legislation framework, structures, and incidents. Thirdly, the status of these agencies is critically analysed to determine whether they are failures or total disasters.

Cleary and Malleret (2006:44) state that the threats and risks mentioned above "diminish or disappear while new risks emerge or come to the fore". These changes impact most international intelligence practices responsible for addressing the aforementioned threats and risks through early warning capabilities and secure communication systems. Intelligence agencies worldwide have implemented specific changes to ensure they can effectively handle these aspects following the end of the Cold War. However, these reforms have not altered the central task of intelligence services, which remains essentially the same.

The South African Intelligence environment has addressed these aspects of change, as outlined in the White Paper on Intelligence (1994), which directs the intelligence community (IC) of South Africa. The White Paper (1994) describes the purpose of intelligence as follows:

In the modern, post-Cold War world, for intelligence to be relevant, it must serve the following purposes:

- To provide the policy-makers with timeous, critical, and sometimes unique information to warn them of potential risks and dangers. Unique information allows the policy-makers to face the unknown and best reduce their uncertainty when critical decisions have to be made;
- To identify opportunities in the international environment by assessing actual or potential competitors' intentions and capabilities. This competition may involve the political, military, technological, scientific, and economic spheres, particularly the field of trade; and

- To assist good governance by providing natural critical intelligence that highlights the weaknesses and errors of government. As guardians of peace, democracy and the Constitution, intelligence services should tell the government what they should know and not what they want to know.

Gilder (2009:46-48) states that the successes were due to the work done by the African National Congress (ANC) regime from 1994 to 2007, as reflected in the statistical data. Gilder (2009:46-47) explains the type of work done by the government during the first decade as follows:

> This is the government that designed one of the best constitutions in the world, that repealed reams of apartheid legislation, that has grown our economy exponentially, that made equity in the workplace obligatory, that has begun to break the minority hold on our economy, that has put billions of rands into providing a cushion for the worst-off of our people, that has dramatically increased access to clean water, to electricity, to education and to health care, that has made the proactive resolution of conflict on our continent and globally one of the key planks of its foreign policy (Cronje, 2017:40-41; Stats SA, 2012a; statistics confirm these developments).

Furthermore, Gilder (2009:46-48) outlines the developments in the intelligence environment and states the following:

> Many of the current leaders of our intelligence services (2007) were involved, even prior to 1994, in designing our democratic intelligence dispensation, drafting the relevant sections of the Constitution, composing the White Paper on Intelligence, and framing the founding legislation, including intelligence oversight mechanisms, that surpass those of many much older and supposedly wiser democracies.

Gilder (2009:46-48) expands his arguments on legislation by stating the following:

> The laws and internal regulations governing the intelligence services disallow spying, except in clearly defined circumstances, notwithstanding relatively recent breaches of those prescripts (breaches that were discovered and dealt with by the oversight mechanisms of the intelligence dispensation).

The above views and explanations by Gilder (2009:46-48) demonstrate that the government performed well during the challenging period from 1994 to 2007 and that the intelligence structures adhered to the necessary legislation and regulations for professional conduct. Furthermore, the intelligence system functioned properly, and the state's oversight organs were actively enforcing the rules of engagement against those who did not comply. Rightfully so, the question can be asked: What went wrong? In this regard, Hulnick (2005:593) warns: "Nothing is more critical in intelligence than preventing surprise. Thus, an intelligence failure is considered more critical if it comes as a surprise." The South African Intelligence is criticised by the media, academics, and even the ANC elite for its poor actions over the past twenty years.

The current war between Israel and HAMAS shows what can happen if intelligence fails and a surprise attack occurs in one's country. According to a Reuters report (Nakhoul & Saul, 2023), Israel was surprised by the attack by HAMAS. In the report, Nakhoul and Saul (2023) state the following: "Hamas used an unprecedented intelligence tactic to mislead Israel over the last months by giving a public impression that it was unwilling to fight or confront Israel while preparing for this massive operation." The retired General Yaakov Amidror told reporters a former national security adviser to Prime Minister Benjamin Netanyahu, further confirmed this intelligence failure. According to Amidror (as quoted by Nakhoul & Saul, 2023), the assault represented "a huge failure of the intelligence system and the military apparatus in the south". Therefore, the criticism of South African intelligence agencies is

significant precisely due to the numerous surprises over the past few decades, including protests, strikes, and riots (such as the Marikana student protests: #FeesMustFall in July 2021), which the security cluster was unable to handle properly and promptly.

The sudden ill actions of some members of the IC created a negative image of the various intelligence agencies, and the media began reporting negatively about the agencies and their members. The downward spiral started with several intelligence failures by the National Intelligence Agency. The following incidents can be referred to: firstly, the 1999-2000 arms deal in the *Sunday Times* ((Mark & Rademeyer, 2014) and in the *Mail & Guardian* (Sole, Timse & Brummer, 2012); secondly, the *spy tapes* that ensured that Mr Jacob Zuma could not be prosecuted for the arms deal corruption; thirdly, the dismissal (2005) of Mr Masetlha (Masetlha vs President, 2008(1) SA 566(CC), the then-Director-General of the National Intelligence Agency (NIA), by President Thabo Mbeki; fourthly, former President Mbeki and his camp miscalculating their support base at Polokwane in 2007 due to a lack of intelligence or withholding of the intelligence available (Joubert & Basson, 2009); and lastly, the creation and operation of the Principle Agent Network (PAN) Unit by Arthur Fraser, who was Deputy Director-General: Operations from 2005-2011 (Pauw, 2017:28-37).

The incidents mentioned above led to questions being asked of the IC, specifically about the members who created the situations that led to poor publicity. After 20 years of adverse reports and research, it is necessary to develop a possible resolution to correct these aspects in the IC, specifically the State Security Agencies (SSA). Therefore, an analysis of the IC is required, and recommendations are needed, as outlined below.

2. An Analysis of the South African Intelligence (specific civilian) Community (IC)

This paper analyses the IC of South Africa by following three basic steps. Firstly, an IRMF is conceptualised to evaluate the current South African intelligence framework, structures, and legislated framework against democratic principles. Secondly, most of the severe incidents of intelligence failures in South Africa and their impact on the IC are identified. Thirdly, the status of the IC and whether it's deemed a failure or whether it is a total disaster is determined.

2.1 A conceptualised IRMF

This article conceptualises an IRMF through an in-depth analysis of Walsh's (2011) frameworks and the Geneva Centre for Security Sector Governance Backgrounders, focusing on how these aspects could influence the field of intelligence risk management (IRM). This analysis provides an enhanced product with a better understanding of the intelligence processes. These IRM products, resulting from the processes, will inform policy-makers and decision-makers on how to manage uncertainty and risk in their environments. This conceptualised IRMF clarifies the core areas in the intelligence processes that need to be enhanced, as shown in Figure 1 below. The adapted figure below by Walsh (2011:148) reflects the required enhancements in a new IRM framework that impacts current intelligence processes followed internationally.

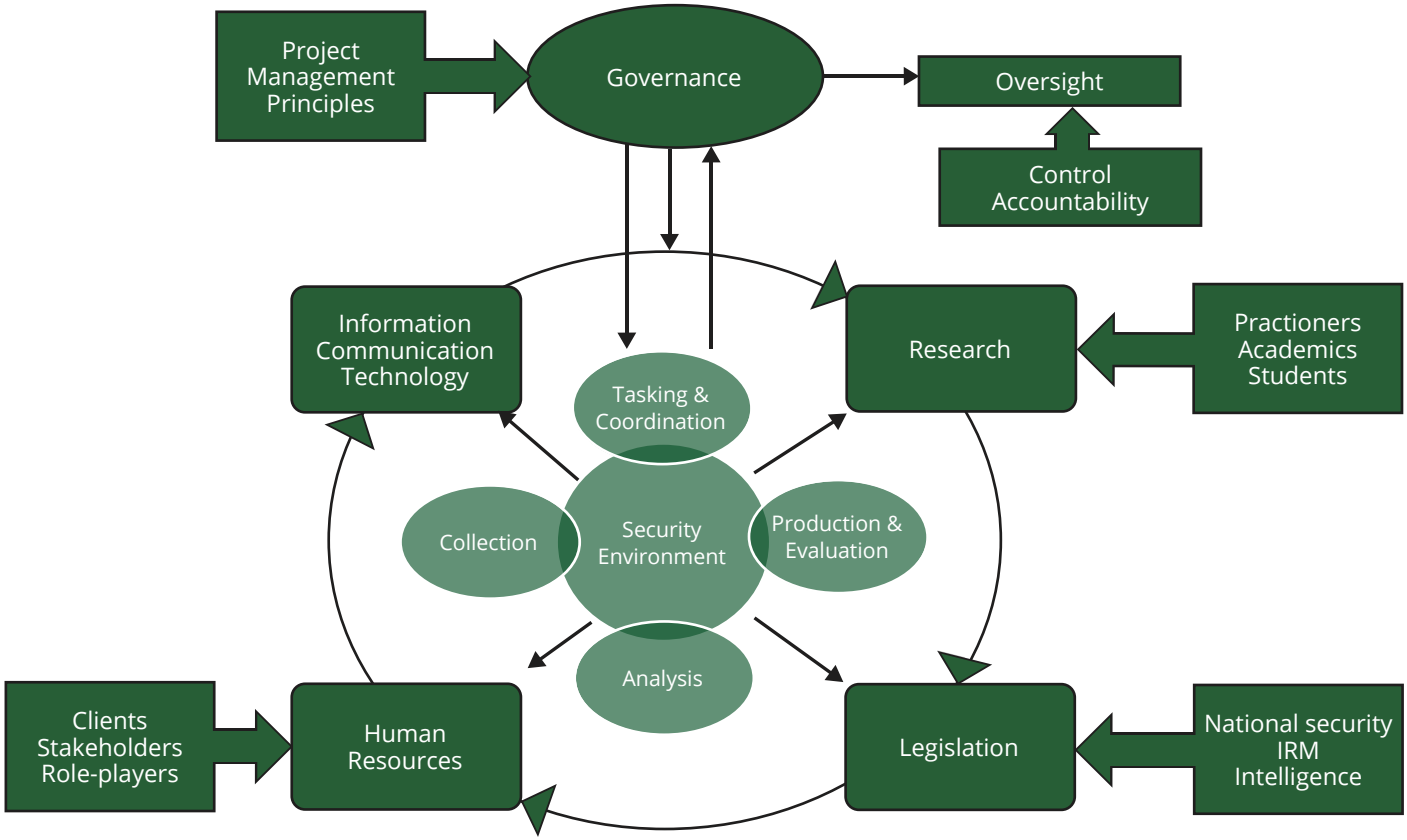

Figure 1: Components of an effective intelligence framework (Loubser, 2023:53, 140)

Figure 1 above illustrates how the new IRM processes will enhance most traditional processes, introducing changes to current intelligence work and approaches. Furthermore, it highlights the changes that must be implemented to create the IRMF in the intelligence environment. The changes and aspects needed to implement an IRMF successfully, are: i) project management principles; ii) good governance with oversight, control and accountability; iii) good coordination and research; iv) changed intelligence processes (a multilayer analysis process); v) well-trained and skilled practitioners; and vi) a legislative framework that captures the intelligence, RM, and national security concepts.

An IRMF should function at three specific levels, as shown in Figure 2 below. These levels are defined by specific tasks, responsibilities, and accountabilities allocated to the structures within these levels.

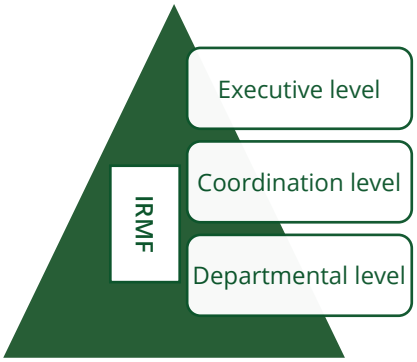

Figure 2: IRMF levels (Loubser, 2023:141)

The three levels of the IRMF were enhanced with democratic principles as researched by the Geneva Centre for the Democratic Control of Armed Forces (DCAF) background papers from 2009-2020 (these background papers were published over this longer period). These research papers revealed that the executive level should be structured as follows:

- presidential: the head of state's or prime minister's responsibilities and accountabilities;
- ministerial responsibilities;
- parliamentary and oversight institutions'/committees' responsibilities; and
- committees, councils, and commissions (National Security Council/Committee, commissions, review panels, and investigative commission / task teams).

Within these structures, persons must fulfil their responsibilities diligently and apply all aspects in accordance with the adapted legislative framework. If those at the executive level do not set the necessary example for the rest of the structures in the IRMF, it will result in the failure of the process.

The analysis of the IRMF reveals that most democratic countries lack a specific governmental structure to coordinate intelligence. It was also found that the functions and responsibilities of this level are not explicitly captured in their legislation. Most countries' intelligence coordination is built into their intelligence processes and policies. These conceptualised coordination structures of the IRMF coordinate all intelligence products and information sent to the executive levels by the departmental levels. Dedicated communication lines were identified and captured in the IRMF. Therefore, this paper views coordination as a national coordination structure. These arrangements will ensure that there is no false reporting or duplication of operations and resources. Furthermore, it will also ensure proper coordination between all role-players and the implementation of a holistic approach.

Furthermore, the research found that the traditional intelligence processes had to be changed at the departmental level. The departments must comply with a multi-layered intelligence process, which will ensure that more IRM products are processed at the executive level, thereby enhancing their decision-making. Figure 3 reflects the findings and proposed structure at this level for implementation. Therefore, this paper postulates its argument based on Lahneman (2010) and Lowenthal (2009), who suggest that intelligence agencies need to change their intelligence processes to a multi-layered approach that integrates and provides a holistic view. The processes will ensure that the IRMF process is followed, enhancing national security in the country. The process is also described by Lowenthal (2009:67) as follows:

> Any intelligence process issues likely to arise (the need for more collection, uncertainties in processing, results of analysis, changing requirements) that cause a second or even third IRM process to take place. Ultimately, one could repeat the process lines repeatedly to portray continuing changes in any of the various parts of the process and the fact that policy issues are rarely resolved in a single neat cycle. It gives a better sense of how the intelligence process operates.

Additionally, Lowenthal (2009:67) finds that an IRMF will enhance several aspects of the intelligence processes, work, and products, which include the following:

- good governance, management, coordination, communication, and lines of communication;
- the development of communication standards and vocabulary;
- new intelligence processes, which include IRM;
- good teamwork and project management; and
- well-trained practitioners.

Furthermore, within the current intelligence framework, practitioners must enhance existing practices and expand their understanding of theory and knowledge to adapt to

an increasingly complex political, economic, and social landscape. For such an IRMF to be functional, it also requires constant refocusing and the ability to adapt to the only known concept of change, which remains the only constant.

Figure 3 below projects the IRMF and gives an overview of the framework. This IRMF can be used to evaluate the current reality of South Africa's intelligence framework and reflect all of the necessary theoretical and conceptual aspects of a properly designed framework.

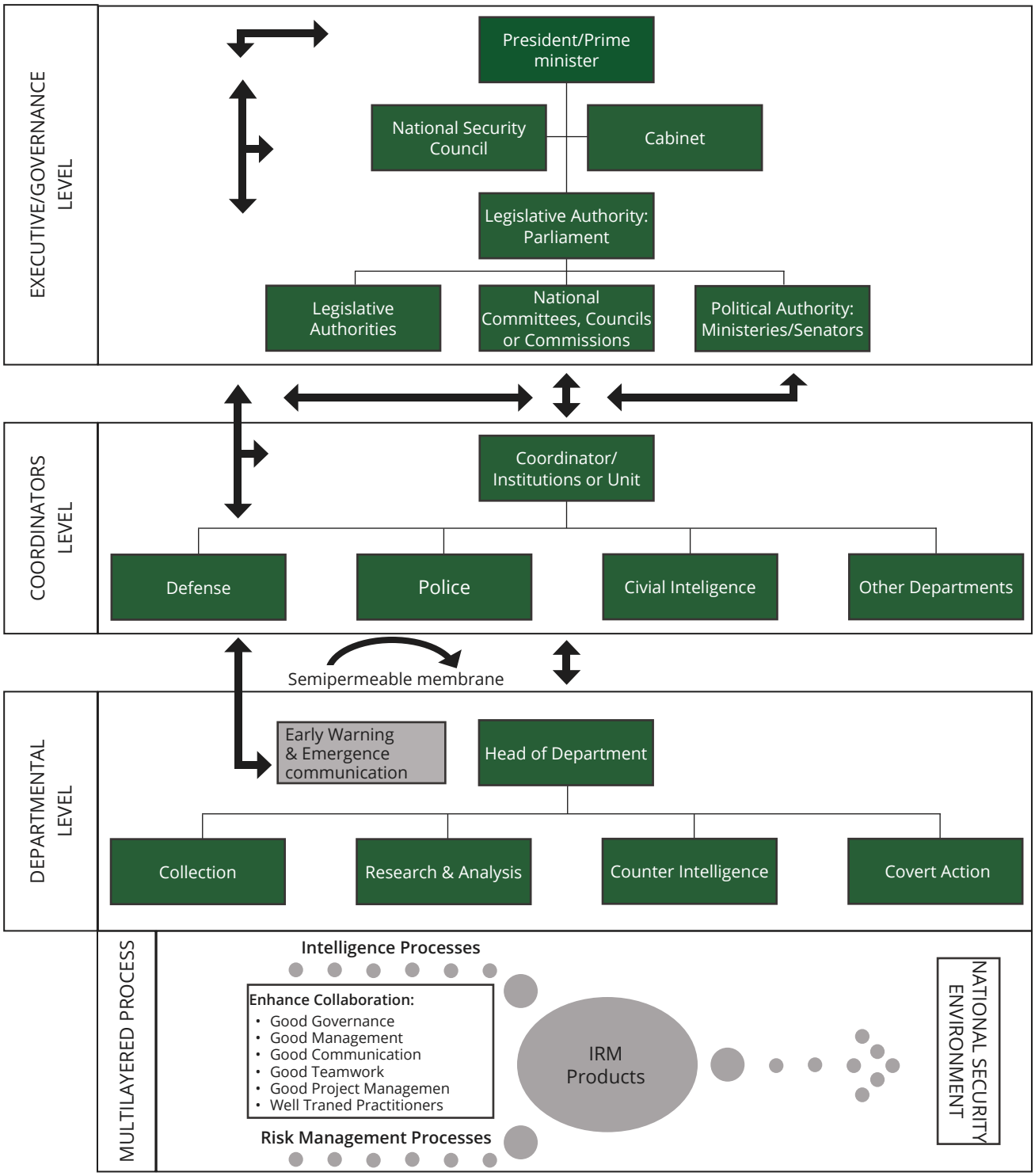

Figure 3: A conceptual IRMF (Loubser, 2023:69, 143)

This conceptualised IRMF will now be used to evaluate the South African intelligence framework and determine the level of compliance within the current framework. The South African intelligence framework is questioned due to the bad publicity the IC has been

receiving in the South African context. Over the past three decades, there has been more negative reporting by all oversight committees, structures (including the Auditor-General and the Inspector-General of Intelligence), and the media than positive reporting. To verify this adverse reporting with the necessary findings is very difficult, due to the secrecy of intelligence work worldwide and legislation frameworks that forbid members, informed political leaders, and other committee members from publicly discussing or announcing this sensitive information.

2.2 An IRMF in the South African context

The analysis from an IRMF perspective in this article clearly demonstrates that an IRMF can be effectively implemented in South Africa's intelligence and security environment. Over the years, the legal framework and structures have been well-drafted, guiding the intelligence, police, and military environments to operate within a democratic state, adhering to its principles and rules. Yet, notwithstanding all of these arrangements, the human failure of the system is evident. Most of the reports were weak in pinpointing the real problems in the intelligence environment, as they focused on frameworks or structures within the IC rather than personnel within the IC. As the High-Level Review Panel (2019) and media reports note, some individuals have alleged that executives and senior personnel exploited the environment to benefit the ANC leadership and themselves.

Against the above background, one would like to mitigate the impact of this personnel misbehaviour and total disregard for the rule of law, even if the arguments of Gill and Phythian (2018:29) are taken into account. The argument of Gill and Phythian (2018:29) is as follows:

> Within the broader context of democratising agencies in former authoritarian regimes, emphasis has been placed on the professionalisation of intelligence officials. The professionalisation involves replacing loyalty to a party or ideology with loyalty to a notion of national security and public safety, which reflects a genuine assessment of a country's needs rather than merely the security in the office of a specific faction.

The intelligence officers in the intelligence and security cluster have not lived up to these codes, as reflected in the above analysis of the intelligence environment. Reports indicated severe maladministration, corruption, and the operation of illegal units beyond the rule of law, as well as individuals at executive levels who were ill-equipped to manage those positions. There were also reports indicating non-compliance with essential regulatory feedback to Parliament and its committees.

This article found that the legislative framework and structure complied with the Constitution, as reflected in the national legislation controlling the intelligence environment, as shown in Figure 4 below. However, the IC needs to have the will, knowledge, and training of an IRMF to implement it successfully in South Africa. In this regard, Arad (2008:44) states the following:

> This is somewhat surprising, given that practitioners of intelligence and intelligence management are trained in probability thinking and, in need, to use various tools in assessing situations concerning early warning. The modes of thinking about RM and related concepts are exceptionally well suited to the surprise-attack problem.

In the South African context, intelligence services are trained in RM, which is enforced through the country's acts and regulations. However, these services do not apply the acts and regulations in their institutions. When management is non-compliant, the ANC takes no action against them – their wrongdoing is overlooked, and rather than being held accountable, they are placed on paid leave. Arad (2008:44) furthermore states:

A close examination of the various elements in intelligence work discloses that intelligence organisations already tacitly implement fundamentals of risk assessment and management. In addition to probabilistic measurements, evaluation of risks and the use of scenarios, explicit risk-control and risk-management tools are widely used, such as backup systems and risk reduction via diversification and redundancy. Nevertheless, all of these elements have not coalesced into a comprehensive RM doctrine for intelligence.

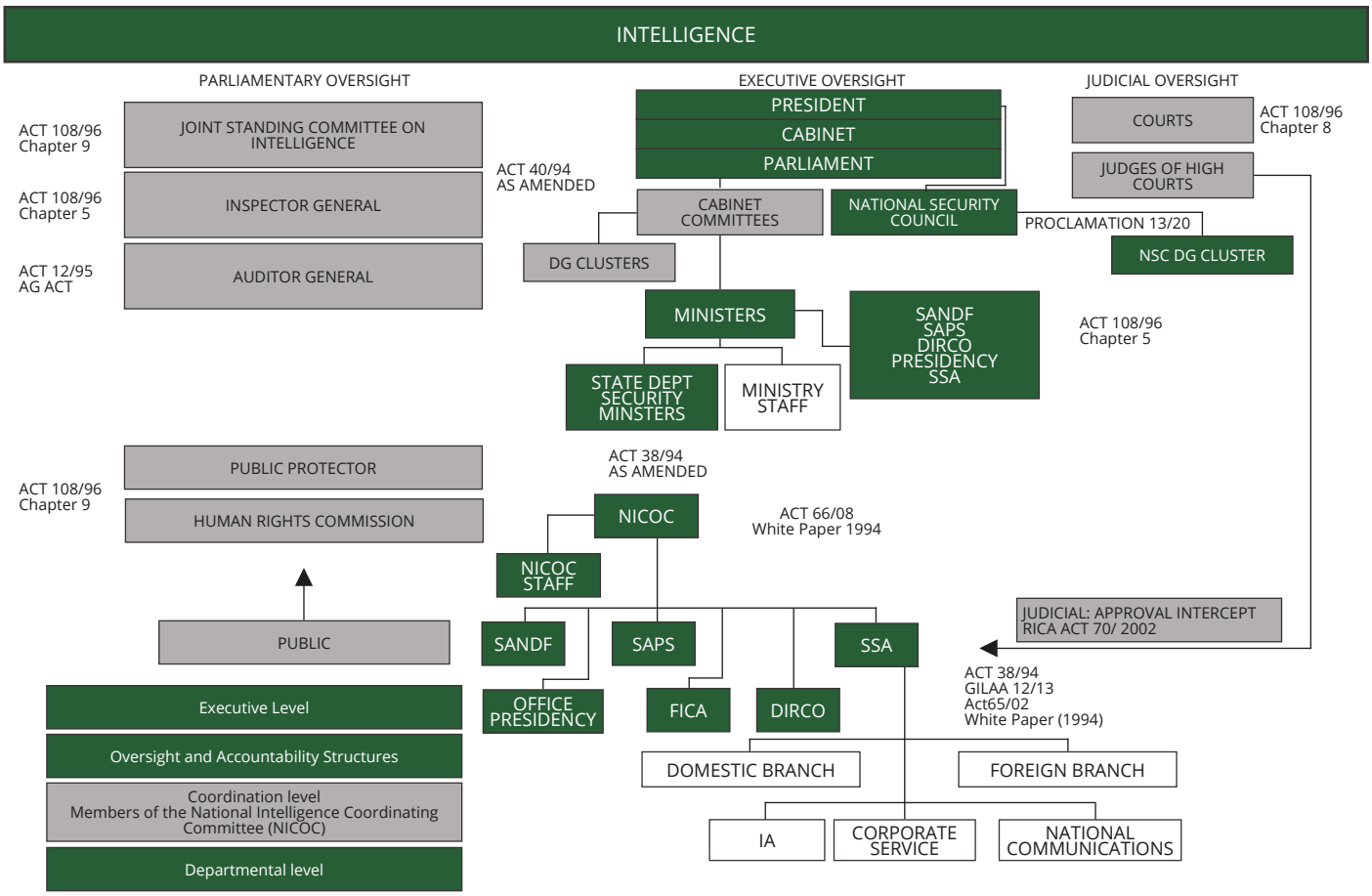

Figure 4: The intelligence structures and legal framework of South Africa in 2022 (Adapted from the SSA ministerial website (2014) and Loubser (2023:100)

2.3 The intelligence legislation and structural framework in South Africa

Malan (2019:97) indicates that the Constitution (Act 108 of 1996) contains the necessary details that provide for every aspect of governmental power, namely legislative, executive, judicial, administrative, policing, intelligence, military, and monetary power, among others. These powers are designated in the Constitution to be exercised by state organs. Therefore, the security and intelligence cluster is responsible for the security and safety of all South African citizens. These aspects are not allocated to any other organs of state or private entities. If the state fails its people, safeguarding themselves becomes crucial for survival. The South African Intelligence Services have failed in their essential task to provide the necessary protection and information to ensure the public's safety, despite all the legal means being provided for them to do so. All past reports that analysed the IC failed to indicate these aspects, which will now be discussed below.

Chapter 11 of the Constitution (1996) outlines the legal standing of intelligence and security services, as well as the relevant frameworks. The Constitution was drafted with democratic principles and control as its guiding foundation. Sub-section 198 (a-d) states what legal

principles must be complied with by all security services to serve the Republic and all of the country's people:

a. National security must reflect the resolve of SA, 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.
b. The resolve to live in peace and harmony precludes any SA citizen from participating in armed conflict, nationally or internationally, except as provided for in terms of the Constitution or national legislation.
c. National security must be pursued in compliance with the law, including international law.
d. National security is subject to the authority of Parliament and the national executive.

These principles guide intelligence and security services to uphold specific ethics, norms, and standards of professionalism. Thus, it is required of all security services in South Africa to respect other people's rights, and they should also adhere to the rule of law (both domestically and internationally), as well as to Parliament and the executives who authorise their work (White Paper, 1994).

Furthermore, Sub-section 199 of the Constitution (1996) establishes structures, directs the conduct of security services, and declares that Parliament will approve structures and that legislation should determine their establishment, structures, and functions:

1. The Republic's security services consist of a single defence force, a single police service, and any intelligence services established in terms of the Constitution.
2. The defence force is the only lawful military force in the Republic.
3. Other than the security services established in the Constitution, armed organisations or services may be established only in terms of national legislation.
4. The security services must be structured and regulated by national legislation.
5. The security services must act and teach and require their members to act, following the Constitution and the law, including customary international law and international agreements binding on the Republic.
6. No member of any security service may obey a manifestly illegal order.
7. Neither the security services nor any of their members, may, in the performance of their functions -
    a. prejudice a political party interest that is legitimate in terms of the Constitution; or
    b. further in a partisan manner, any interest of a political party.
8. To give effect to the principles of transparency and accountability, multi-party Parliamentary committees must have oversight of all security services in a manner determined by national legislation or the rules and orders of Parliament.

The above rules apply to South Africa's intelligence and security services. The Constitution (1996) further expands its rules and direction for security and intelligence services in Chapter 11, which becomes more specific for each service. Therefore, this subsection will focus solely on analysing the intelligence community. Sub-section 209 focuses on the establishment and control of intelligence services, with particular indications for civilian intelligence agencies' rules:

1. Any intelligence service, other than any intelligence division of the defence force or police service, may be established only by the President, as head of the national executive, and only in terms of national legislation.
2. The President, as head of the national executive, must appoint a woman or a man as head of each intelligence service established in terms of Sub-section (1) and must either assume political responsibility for the control and direction of any of those services, or designate a member of the Cabinet to assume that responsibility.

Only the President can approve the above rules and the establishment of these structures, which must comply with the aspects necessary to conceptualise an IRMF. These aspects of the Constitution also align with democratic principles for controlling and establishing intelligence agencies worldwide. Sub-section 210 states that national legislation must control these agencies, which determines their objects, powers, and functions.

The IC has complied with the Constitution (1996) by developing the necessary national legal framework, which determines its structures, mandates, functions, responsibilities, and areas of focus regarding national security threats. The legislative framework was developed between 1994 and 2002, which included a framework that established the necessary control mechanisms. These Acts, regulations, and policies were aligned with the Constitution and are listed below:

- Protection of Information Act No. 82 of 84, Replacement Bill on the table: Protection of State Information [B6-2010]. The Bill was passed on 29 November 2012 with amendments by the National Council of Provinces. On 25 April 2012, the National Assembly approved it. However, in September 2013, the then-President, Jacob Zuma, refused to sign the Bill into law, sending it back to the National Assembly for review. After all these years, this Bill has still not been approved or republished for approval (a typical government action of not applying any urgency to necessary legislative changes).
- Public Finance Management Act No. 1 of 1999
- Regulation of Interception of Communications and Provision of Communication-related Information Act No. 70 of 2002
- Intelligence Services Act No. 65 of 2002
- Intelligence Services Oversight Act No. 40 of 1994
- National Strategic Intelligence Act No. 39 of 1994
- Public Service Act No. 103 of 1994
- Public Service Regulations (issued in 2016)
- Treasury Regulations as amended (issued in 2001)
- White Paper on Intelligence (1994)

From 1994 to 2023, several incidents stood out in the IC environment, highlighting the legal downward spiral of the IC environment, with its severe impact on the environment and the country's security. Africa and Mlombile (2001:8-9) report the first incident: A senior executive of the military provided direct intelligence reports to President Mandela that the ANC elites were planning to undermine the negotiation process; sometime later, it was revealed that executive officers of the South African National Defence Force (SANDF) were "plotting a coup". Upon investigation, these reports were found to be false and were dismissed. The senior member of the SANDF was replaced and left the service soon after. This incident demonstrates that the intelligence framework of South Africa was designed to prevent false reporting from reaching the President. Furthermore, it also shows that reports should be scrutinised by the coordinators (National Intelligence Coordinating Committee (NICOC)) of intelligence products in South Africa. There should also be better coordination between the different intelligence and security structures in South Africa to ensure that direct access to the President is not abused.

The second incident that illustrated the legal downward spiral of the IC environment was the dismissal of the Director-General of the NIA (Mr Masetlha) by former President Mbeki in 2005. Mister Masetlha questioned his dismissal in court (Masetlha v President of RSA and Another, 2008 [1] SA 566 [CC]). The courts ruled that the President can appoint or dismiss a director-general within the powers granted to them by the Constitution. Notwithstanding this, Mr Masetlha was exempted from all wrongdoing. The manner in which this incident was handled demonstrates that the South African intelligence framework operates in accordance with the democratic principles outlined in the Constitution, the White Paper (1994), and other relevant intelligence legislation (Loubser, 2023:83). Despite official inquiries, the ruling party (ANC) conducted its own investigation into the e-mail sag: "This blurring of the lines between state and party business left many South Africans confused and suspicious that state institutions served at the behest of the ruling party." (Africa & Mlombile, 2001:8-9)

Pauw (2017:37-38) points out a third incident, indicating that someone was covering up for Zuma, and that the intelligence structures under Fraser could easily be those protecting him. This incident serves as a stark example of how political leaders have misused intelligence for their own personal and political agendas.

A fourth incident arose from the Browse Mole Report (Africa & Mlombile, 2001:8-9), which was investigated, drafted, and communicated by the Directorate of Special Operations (DSO), also known as the Scorpions. The Scorpions led an operation using intrusive intelligence methods, although they were not an intelligence agency. The report claims that certain African governments (Libya and Angola) were funding a conspiracy by the ANC's Deputy President (Jacob Zuma). Following an investigation by Fraser, the Deputy Director-General of the NIA at the time, the Cabinet approved the disbandment of the DSO. Pauw (2017:36-39) states that:

> During Fraser's investigation into the Browse Mole report, the NIA tapped the phones of several high-ranking officials mentioned in the report, including those of Ngcuka (the Head of the National Prosecuting Authority) and McCarthy, the Scorpions boss. On the tapes, they discussed when it would be the most politically damaging time to charge Zuma. Fraser had unearthed what amounted to gold for Zuma.

These aspects of the investigation halted Zuma's prosecution and enabled him to dethrone Mbeki at the ANC conference in 2007, which was held in Polokwane.

The analyses from an IRMF perspective of the above incidents clearly demonstrate that an IRMF needs to be implemented in South Africa's intelligence and security environment. Gilder (2009:45-46) also states that the legal framework and structures have been well-drafted over the years, directing the intelligence, police, and military environments to operate within a democratic state with its established principles and rules. However, notwithstanding all of these arrangements, the system's human failure (also in terms of cadre deployment) is evident. Yet, most reports fail to pinpoint the real problems in the intelligence environment. Additionally, commissions, panels, and reviews often fail to hold the personnel and the ANC government accountable for these failures, as they do not accept any responsibility for them. Instead, the legal framework and structures are blamed for the problems, despite personnel being the most significant issue, not the legal framework or structures within the IC. Malan (2019:105) refers to the fact that the intelligence services "descended into an instrument of the ruling party, and that its officials were working for the ANC rather than the state". Then the Minister of Intelligence, Ronnie Kasrils (2005), appointed the Ministerial Matthews Commission that published a report in 2008, confirming these aspects. As the High-Level Review Panel (2019) and media reports note, some individuals have alleged that the political elite, executives, and senior personnel have exploited the environment to benefit the ANC leadership and themselves.

An analysis of the commissions and panels over the past decades reveals a lack of political will among deployed cadres in the intelligence and security environment. These individuals have failed to act on recommendations aimed at improving governance and at managing and controlling the environment in which several severe incidents occurred between 2005 and 2022. Despite various interventions over the years, the IC has made no changes or corrections, apart from some legislative amendments and structural adjustments. These interventions include the Ministerial Commission appointed in 2008 by the Minister of Intelligence, Ronnie Kasrils; the High-Level Review Panel appointed by the President in 2018; and the 2020 Constitutional Court ruling on the Regulation of Interception of Communications and Provision of Communication-related Information Act (hereinafter referred to as RICA).

More than 15 years ago, the Ministerial Review Commission on Intelligence (2008:298-299) noted that several aspects of intrusive intelligence measures require legislative control. The Commission made the following recommendation in this regard:

The Minister should introduce legislation that uniformly regulates the use of intrusive measures by the intelligence services. The legislation should be consistent with Constitutional Court decisions regarding infringements of the right to privacy and should, therefore, contain the following elements:

- The use of intrusive measures should be limited to situations where there are reasonable grounds to believe that a) a severe criminal offence has been, is being or is likely to be committed; b) other investigative methods will not enable the intelligence services to obtain the necessary intelligence; and c) the gathering of the intelligence is essential for the services to fulfil their functions as defined in law.
- The intelligence services should be prohibited from using intrusive measures against persons and organisations involved solely in lawful activity. An alternative formulation would be that intelligence services may not use intrusive measures concerning lawful activities unless these activities are reasonably believed to be linked to the commission of a serious offence.
- Intelligence services should be prohibited from interfering in the political processes of other countries, whether through intrusive methods or other means.
- The use of intrusive measures by the intelligence services should require the approval of the Minister. The Minister must be satisfied that the criteria for using these measures have been met.
- The use of intrusive measures should require the prior authorisation of a judge. The legislation should prescribe the information that the applicant must present to the judge in writing and on oath or affirmation. The application must provide sufficient detail to enable the judge to assess whether the circumstances warrant the independent use of intrusive measures.
- As with RICA, the legislation should stipulate that intrusive methods may only be used as a last resort.
- The legislation should require intrusive measures to be carried out strictly, regarding decency and respect for a person's rights to dignity, personal freedom, security, and privacy.
- The legislation should state that the intelligence services must delete within specified periods a) private information about a person who is not the subject of investigation where the information is acquired incidentally through the use of intrusive methods; b) private information about a targeted person that is unrelated to the investigation or planning of a serious criminal offence; and c) all information about a targeted person or organisation if the investigation yields no evidence of the commission or planning of a serious offence.

The IC had not complied with these recommendations, which led to the creation and abuse of the intelligence structures. The following aspects occurred from 2005 until 2022:

- The Principal Agent Network (PAN) under Fraser was implemented (2005-2011).
- The PAN misused the situation, resulting in maladministration, unlawful operations, and the covering up of activities within this unit under the guise of national security (secrecy).
- The Special Operational (SO) Unit (2016) was created, and its activities were implemented.
- The RICA constitutionality (2019) was questioned in court by the AmaBhungane Centre for Investigative Journalism.
- According to Ensor (2022), administration and service delivery were poor between 2005 and 2022 (service delivery protests and the Financial Action Task Force (FATF)).
- Several intelligence failures occurred between 2005 and 2022: the Marikana mine tragedy (16 August 2012), the #FeesMustFall protests by students countrywide (2016-2017), the riots in KwaZulu-Natal and Gauteng (July 2021), the South African spies who were busted in Mozambique (July 2021), and organised crime in South Africa (2022).

However, the most significant change in the civilian intelligence legal framework, also identified by the High-Level Review Panel (2019), occurred between 2010 and 2013. The change was made through the General Intelligence Laws Amendment Act (GILAA, 2013). It impacted the names of the civilian intelligence agencies, from the National Intelligence Agency (NIA), the South African Secret Service (SASS), the South African National Academy for Intelligence (SANAI), and the National Communications (NC) to the State Security Agency (SSA). The GILAA amended the National Strategic Intelligence Act, explicitly defining the national threats upon which the services should focus. These changes broadened the scope of the civilian intelligence agency to encompass anything perceived as a threat, risk, or vulnerability that it must address. The original definition in the National Strategic Intelligence Act (39/1994:s 1) states that the intelligence agencies must focus on:

> counterintelligence measures and activities conducted, instituted or taken to impede and to neutralise the effectiveness of foreign or hostile intelligence operations to protect intelligence and any classified information, to conduct [security screening] vetting investigations and to counter [subversion, treason, sabotage and terrorism aimed at or against personnel, strategic installation or resources of the Republic].

The GILAA (2013) amended the Act so that it read*:* "any threat or potential threat to national security". The definition provides the agency with a vast threat target field to counter anything it deems a threat. These aspects also influence the structuring of the civilian intelligence environment, as well as its policies and regulations.

In this regard, the incidents regarding the Special Operations (SO) Unit and its activities come to mind. They disregard the professional conduct of intelligence officers as prescribed by the Constitution. Furthermore, the Unit focuses on all threats and risks as the agency sees fit. These actions disregard the proper understanding of the laws applicable to these operations. The High-Level Review Panel (2019:55) states:

> The SSA Special Operations (SO) Unit, in terms of its serious breaches of the Constitution, legislation, and other prescripts, is mainly related to the politicisation and factionalisation of intelligence and executive overreach. It just needs to be noted here that the SO became a law unto itself, particularly in utilising and accounting for SSA funds, and its very existence and functioning were a prime example of the devastating impact.

The Unit's actions directly breach the Constitution, the White Paper, relevant legislation, and the principles of good government intelligence functioning. As indicated above, these aspects could be controlled and corrected by ministers or the President, who have extensive political authority.

Despite its changes, South Africa's intelligence framework from 1996 to 2021 has been divided between executive, coordination, and departmental levels, with communication and control lines for these intelligence and security services. The structures from 2014 (Figure 4) demonstrate that democratic principles were adhered to in the design of these different levels, in line with the legislative framework, as Gilder (2009:45-46) states. Figure 4 also illustrates the executive political command and control, communication lines, oversight, coordination, and departmental levels within the intelligence environment up to 2014. It also complies with the legal framework. The IC was manipulated to provide services not in the interest of securing South Africa as a state, but in the interest of certain individuals and structures. The High-Level Review Panel (2019:64-66) was informed and provided with information regarding an SSA SO Unit, which was first established in the NIA in 1997. This unit was subsequently shut down (the exact date is unknown), reopened in or around 2002/03, and carried over into the SSA. The notion of a SO Unit in intelligence, military and police services is not unusual. It typically involves units that operate under deeper cover than other service units and conduct operations against severe targets or issues, often at a national level. This unit's activities were not legitimate, and many questions were raised about how they operated and precisely which target areas they were focusing on.

Therefore, the High-Level Review Panel (2019:54-56) recommends that the competent authorities conduct urgent forensic and other investigations into the financial and other control breaches evident from some of the information available to the Panel. These investigations were to focus primarily on the PAN Project and the SO Unit, as they could have led to disciplinary and criminal prosecutions.

Ten years after the Ministerial Commission of 2008 was appointed, the High-Level Review Panel (2019:49-50) reiterates the same issues and recommends intrusive intelligence measures that require urgent attention from the IC. The Panel states the following:

Heads of Services/Agencies to issue directives for the conduct of intelligence operations that:

i. Determine specific internal processes for priority-setting and targeting arising from the National Intelligence Priorities.
ii. Specify the criteria to be applied in authorising intrusive intelligence techniques.
iii. Outline the levels of authority required to authorise such intrusive operations, dependent on the risk of compromise involved.
iv. Determine the level of supervision of the conduct of high-risk intelligence operations and the system of such supervision.
v. Specify the procedures to be followed in authorising specific methods of intrusive intelligence collection.
vi. Determine the requirement and procedure for discarding incidental information collected during intrusive operations unless such information indicates a new threat.
vii. Detail the record-keeping system of all processes authorising and managing intrusive intelligence operations.
viii. Obligate the Services to establish internal mechanisms for monitoring compliance with these directives and dealing with compliance failures.

If the recommendations mentioned above had been followed, the South African IC would have prevented all problems related to the operation of SO units. Furthermore, there would

have been proper control during the Marikana mine tragedy, the #FeesMustFall protests, the riots of July 2021 in KwaZulu-Natal and Gauteng, and the exposure of South African spies in Mozambique (Stone, 2021).

The 2019 RICA court ruling is a further incident illustrating South Africa's downward spiral in terms of its IC. In this regard, *Business Tech* (Staff Writer, 2021) reports the following: "SA's spy problems are well documented and were brought to the fore in the 2019 court case challenging the constitutionality of RICA."

The AmaBhungane Centre for Investigative Journalism also challenged RICA's constitutionality by taking the government to court regarding a journalist being spied on (the Zuma "spy tapes" saga). The case was only brought to court in 2019, and the High Court ruled as follows, according to *Business Tech* (Staff Writer, 2021):

- The Act fails to adequately prescribe the procedure for notifying a person whose information has been intercepted.
- The Act fails to adequately prescribe the proper procedures to be followed when state officials examine, copy, share and sort data obtained through interceptions.
- The Act fails to adequately address situations where the subject of surveillance is a practising lawyer or a journalist.

The above ruling of the High Court was upheld by the Constitutional Court in 2020. The IC (government) was given 36 months to rectify the Act. When drafting this paper, two specific Bills (GILAA 2023 and the RICA Amendment 2023) were published on 23 August 2023, which need to correct all necessary intelligence legislation and the RICA to comply with the Constitutional Court's 2020 ruling. If they comply, the above incidents and rulings show that the IC has a prolonged response time to "law-and-order" issues. The Ministerial Commission of 2008 indicated these shortcomings of the RICA. If the cadres had attended to it, the problem of lousy publicity regarding these intelligence operation aspects would not have occurred. Furthermore, the High-Level Review Panel confirmed these views ten years later, stating that the Panel was aware of several processes for reviewing and amending the legislative prescripts over the years. The High-Level Review Panel (2019:21) states: "Many of the high-level recommendations of these previous processes are identical or similar but have never been finalised or implemented, and the Panel has come to similar conclusions."

A recent shortcoming of the South African government was highlighted in the 2019 Financial Action Task Force (FATF) report. This report sets standards and promotes the effective implementation of legal and operational measures for combating money laundering, terrorist financing, and the financing of weapons of mass destruction internationally (Ensor, 2022). According to this report, South Africa was non-compliant with the set of standards and legal frameworks. Hence, the South African government was grey-listed, despite the government providing feedback to the FATF by the end of December 2022. In this regard, Ensor (2022) states: "Treasury acting DG Ismail Momoniat says that SA has made significant and real progress in meeting the requirements laid down by the FATF to avoid grey-listing." However, these efforts were in vain because the FATF (2019) reported that SA had not complied and that there were several concerns that "SA members are poorly trained, with no experience in international cases in this field". In this regard, it is worth noting that this South African listing will expose financial institutions and companies to risk and hinder the effective operation of South African IC and security services (Loubser, 2023:113).

3. Conclusion

In summary, against the above background, one would like to soften the impact of this personnel misbehaviour and total disregard for the rule of law, even if Gill and Phythian's argument (2018:29) is considered. Malan (2019:104) states that: "South Africa has developed a crippling shortage of suitable, qualified public officials with the required specialised knowledge and know-how to sustain a functioning public sector." These officials may be loyal to the party and leadership, but they are not well-suited to manage these government institutions adequately. According to Ronnie Kasrils (Minister of Intelligence from 2003-2008), the IC members descended into an instrument working for the party rather than the state. These actions by members of the IC led to severe maladministration, corruption, the operation of illegal units operating outside the rule of law, and non-compliance with essential regulatory feedback to Parliament and its committees.

The reports by the JCSI regarding the activities of the IC have identified some of these problem areas over the last two decades, and changes have been recommended. However, the IC has not implemented these changes, with severe consequences for the state and the agencies' image. The riots and looting that occurred in July 2021 in KwaZulu-Natal and Gauteng can be directly linked to poor management and a lack of focus among members in the various agencies (Presidency, 2021). The same influence from the descent in the Counter Intelligence (CI) agencies is their implementation and application of RM in their institutions.

In the South African context, intelligence services are trained in RM, which is enforced through South Africa's financial acts and regulations. However, these services do not apply the acts and regulations in their institutions. When management is non-compliant, the ANC takes no action against them for their wrongdoing. Rather than being held accountable, management stays at home and is paid full salaries. The National Treasury's 2001 regulations and the substituted guidelines for implementing RM in government institutions cover these aspects regarding RM. Therefore, one can only ask: What went wrong, and how could it have gone wrong? In this regard, the benefits of IRMF will be an essential management tool for the future of intelligence in South Africa, as it will nudge the government to act against these wrongdoers.

In The prince, Niccolò Machiavelli (1998) argues as follows:

> [I]t ought to be remembered that there is nothing more challenging to take in hand, more perilous to conduct, or more uncertain in its success than to take the lead in the introduction of a new order of things. Because the innovator has enemies, all those who have done well under the old conditions, and lukewarm defenders in those who may do well under the new. This coolness arises partly from fear of the opponents, who have the laws on their side, and partly from the incredulity of men, who do not readily believe in new things until they have had a long experience of them.

Over the years, Parliament was briefed on successes, but more about intelligence failures. The NIA provided information to Parliament during 2001-2004 regarding the successful counteractions of threats of violence (People Against Gangsterism and Drugs: PAGAD), specifically in the Western Cape. The actions of the NIA resulted in the arrest and prosecution of several individuals involved. Furthermore, the NIA played an essential role in collecting intelligence regarding violence in the taxi industry. Africa (2011:24) mentions that the NIA was also involved in joint operations with the South African Police Service (SAPS) to combat internal stability issues and organised crime. Malan (2019:105) expands upon the problems experienced in the government sector, as these cadres have been responsible for poor service delivery since 2007. Malan (2019:105) states the following: "Cadre deployment with the accompanying deployment of incompetent staff is one of the foremost causes of the widespread collapse of government institutions on all levels, including the intelligence environment."

Despite successes, the NIA faced embarrassment and adverse media reports regarding its counterintelligence operations. Following these operational failures in 2004-2005, the Minister of Intelligence took action against several senior management members, including the Director-General of the NIA. These cases demonstrate that members did not follow or comply with the rules and regulations of the Constitution and the intelligence legislation. However, in the end, the members were acquitted of wrongdoing. These situations have occurred several times over the past decades, and as Malan (2019:106) points out, the ANC would not part with their cadre deployment strategy.

The analysis from an IRMF perspective in this article clearly shows that an IRMF can be implemented in the intelligence and security environment of South Africa. Over the years, the legal framework and structures have been well-drafted, guiding the intelligence, police, and military environments to operate within a democratic state, adhering to its principles and rules (Loubser, 2023:98-99). Notwithstanding all of these arrangements, the human failure of the system is evident. Although the High-Level Review Panel and media reports have pointed out that some individuals have alleged that executives and senior personnel have abused the environment to benefit the ANC leadership and themselves, most reports did not state this. Many reports were thus insufficient in pinpointing the real problems in the intelligence environment; they focused on the IC's legal framework and structures, but not on the personnel within the IC, which was the most severe issue. In this regard, the High-Level Review Panel (2019:ii) states:

> We think it prudent to highlight here that our key finding is that there has been a severe politicisation and factionalisation of the intelligence community over the past decade or more, based on factions in the ruling party, resulting in an almost complete disregard for the Constitution, policy, legislation and other prescripts, and turning our civilian intelligence community into a private resource to serve the political and personal interests of particular individuals.

Finally, it is worth noting that the deterioration of the IC in South Africa has led to several security and safety-related issues, which in turn impact the country's socio-economic development. These aspects further show that the IC in South Africa cannot provide the required intelligence to neutralise these severe threats. These aspects are listed below:

- Researchers, academics, and journalists refer to South Africa as the protest capital of the world (Sole, 2010). Neethling (2016:52) states: "Social risk in the form of service delivery protests has increased markedly, and this phenomenon remains a factor of the most significant concern in any consideration of forces and events that could negatively influence investors' confidence."
- The Institute for Security Studies (Chipkin, Vidojević, Rau, & Saksenberg, 2022) has conducted research on violent crime and protest actions, finding that these threats and risks significantly influence the country's political stability. There were indications that some of the ANC faction's political elites were involved. The elite's involvement in these crimes also placed the police and intelligence services in a complicated position.
- A severe threat and risk to the South African environment was published in the *Sunday Times* (Shaw & Rademeyer, 2022:13-14) regarding organised crime in South Africa. In this article, Shaw and Rademeyer (2022:13-14) argue that these organised crimes can be linked to an underground economy and activities. Shaw and Rademeyer (2022:13-14) further note that these crime syndicates are threatening everyone in South Africa, tarnishing the country's reputation and harming the tourist industry, which is still trying to recover after the COVID-19 pandemic.

- Furthermore, recent surveys and research indicated that between 2000 and 2008, xenophobic attacks (and murders) became another severe political issue in the South African context. Neethling (2016:66-97), the South African Reconciliation Barometer (SARB) (2021) and Afrobarometer (2021) show that xenophobia and violence against immigrants have increased in recent years, with a marked escalation occurring from late 2000 to 2008 (Human Rights Watch, 2021). These aspects will impact the tourism industry and international companies seeking to invest and establish operations in South Africa.
- The alarming unemployment rate in South Africa is a severe situation that can spill into violent protests and severe interaction between the security organs of the state and the protestors. These protests will harm the already struggling economy and the country's international image.
- If they comply, the government responds slowly to law-and-order issues. Some legislation changes take a very long time to finalise, leading to international grey-listing and Constitutional Court rulings against the IC.
- Slow to no action is taken by the government against members, executives, and political leaders who are guilty of disregarding the legal framework for intelligence in South Africa.

Lastly, the following question can be asked: Is there hope for the ill civilian intelligence environment in South Africa, which has been tarnished by unfavourable reports, maladministration, and corruption over the past few decades? The IC will continue to malfunction under an ANC government with policies that prioritise total control over all spheres of government power and the deployment of cadres in sensitive and managerial positions within intelligence agencies. The only hope for the civilian intelligence agencies lies in the regime's willingness to implement the following measures and to ensure strengthened oversight and management of these agencies through the following steps:

- Cadre deployment should be reconsidered. A new approach to appointing individuals in critical positions is required, as these positions necessitate individuals with the appropriate qualifications who prioritise ethics and norms, enabling them to lead agencies in providing the necessary quality intelligence products that support good governance.
- They need to implement a new approach (intelligence risk management) in the intelligence environment with a multi-level approach.
- They must not prolong the legal process and the drafting of the regulations and directives for the agencies.
- They need to take severe action against any member of staff who does not comply with the legal framework and policies.
- Close coordination and cooperation must exist within the security cluster with the NICOC, which is responsible for central coordination functions.

The ANC will not easily implement the above recommendations, as history shows that they are reluctant to make changes; they tend to stick to their views on central control and socialist political practices. The non-functioning of the agencies will continue in future. Therefore, no good changes will materialise soon. In summary, the political regime needs to change, and a new government must address this crucial central provider of professional intelligence products.

4. BIBLIOGRAPHY

Africa, S. 2011. *The transformation of the South African security sector: Lessons and challenges.* Policy Paper no. 33. Geneva: Geneva Centre for the Democratic Control of Armed Forces (DCAF).

Africa, S. & Mlombile, S. 2001. *The transformation of the South African Intelligence Services.* Paper presented to the Round Table on the Reform of the Guatemalan Intelligence Services: 31 March – 2 April. Boston, MA: Harvard University Law School.

Afrobarometer. s.a. *South Africa website: In partnership with the Institute for Justice and Reconciliation (IJR) in South Africa.* https://www.afrobarometer.org/countries/south-africa/ Date of access: 30 Sept. 2022.

Arad, U. 2008. Intelligence management as risk management: The case of surprise attack. (*In* Bracken, P., Bremmer, I. & Gordon, D., *eds*. *Managing strategic surprise: Lessons from risk management and risk assessment.* London: Cambridge University Press. pp. 43–77) https://doi.org/10.1017/CBO9780511755880.003

Chipkin, I., Vidojević, J., Rau, L. & Saksenberg, D. 2022. *The near future of South Africa: Protest and political stability.* Government and Public Policy (GAPP). https://issafrica.org/research/southern-africa-report/dangerous-elites-protest-conflict-and-the-future-of-south-africa Date of access: 20 Oct. 2022.

Cleary, S. & Malleret, T. 2006. *Resilience to risk.* Cape Town: Human & Rousseau.

Cronje, F. 2017. *A time traveller's guide: South Africa in 2030.* Cape Town: Tafelberg.

Ensor, L. 2022. Real progress is being made to avoid greylisting. *Business Day:* 24 Oct. https://www.businesslive.co.za/bd/economy/2022-10-24-real-progress-is-being-made-to-avoid-greylisting-says-momoniat/ Date of access: 26 Oct. 2022.

Geneva Centre for the Democratic Control of Armed Forces (DCAF). 2017. *Intelligence services.* SSR Backgrounder Series. Geneva: DCAF.

Gilder, B. 2009. Are our intelligence services really that bad? (*In* Hutton, L., *ed*. *To spy or not to spy? Intelligence and democracy in South Africa.* Monograph 157. Pretoria: Institute for Security Studies (ISS) pp. 45-54)

Gill, P. & Phythian, M. 2018. *Intelligence in an insecure world.* 3rd ed. Cambridge: Polity Press.

High-Level Review Panel. 2019. *High-level Review Panel into the State Security Agency:* https://www.politicsweb.co.za/documents/report-of-the-highlevel-review-panel-on-the-ssa Date of access: 25 June 2022.

Hofstatter, S., Wa Afrika, M., Rampedi, P. & Jurgens, A. 2014. Exposed: How arms dealer Thales bankrolled Zuma. *Sunday Times:* 28 Sept. https://www.timeslive.co.za/politics/2014-09-28-exposed-how-arms-dealer-thales-bankrolled-zuma/ Date of access: 2 Jul. 2022.

Hulnick, A.S. 2005. Indications and warning for homeland security: Seeking a new paradigm. *International Journal of Intelligence and Counterintelligence,* 18(4):593–608. https://doi.org/10.1080/08850600500177101

Human Rights Watch. 2021. *World report: South Africa 2020.* https://www.hrw.org/world-report/2021/country-chapters/south-africa Date of access: 13 Sept. 2023.

Joubert, P. & Basson, A. 2009. The spy who saved Zuma. *Mail & Guardian:* 9 April. https://mg.co.za/article/2009-04-09-the-spy-who-saved-zuma/ Date of access: 20 Oct. 2023.

Lahneman, W.J. 2010. The need for a new intelligence paradigm. *International Journal of Intelligence and Counterintelligence,* 23(2):201–225. https://doi.org/10.1080/08850600903565589

Loubser, R.G. 2023 *An intelligence risk management framework for SA: An exploratory perspective.* Potchefstroom: North-West University. (MA – Dissertation)

Lowenthal, M.M. 2009. *Intelligence: From secrets to policy.* 4th ed. Washington, DC: CQ Press.

Machiavelli, N. 1998. *The prince.* Translated by W.K. Marriott. [e-book] Project Gutenberg. https://www.gutenberg.org/files/1232/1232-h/1232-h.htm Date of access: 16 Aug. 2022.

Malan, K. 2019. *There is no supreme constitution: A critique of statist-individualist constitutionalism.* Stellenbosch: African Sun Press.

Nakhoul, S. & Saul, J. 2023. How Hamas duped Israel as it planned devastating attack. *Reuters: 10 Oct.* https://www.reuters.com/world/middle-east/how-israel-was-duped-hamas-planned-devastating-assault-2023-10-08/ Date of access: 26 June 2025.

Neethling, T. 2016. An update on South Africa's political risk profile in 2015/6. *New Contree*, (75):66-97. https://doi.org/10.4102/nc.v75i0.145

Parliament of South Africa. s.a. *Annual Report of the Joint Standing Committee on Intelligence (JSCI) for the financial year ending 31 March 2020, including the period to December 2020.* https://www.parliament.gov.za Date of access: 4 Jul. 2022.

Pauw, J. 2017. *The President's keepers: Those keeping Zuma in power and out of prison.* Cape Town: Tafelberg.

Presidency. 2021. *Expert Panel: Report of the Expert Panel into the July 2021 civil unrest.* https://www.thepresidency.gov.za/content/report-expert-panel-july-2021-civil-unrest Date of access: 20 Jan. 2022.

Rodrigues, C. 2010. Black Boers and other revolutionary songs. *Mail & Guardian*: 4 Apr. https://thoughtleader.co.za/on-revolutionary-songs/ Date of access: 31 Oct. 2022.

SAFLII. 2008. *Masetlha v President of the Republic of South Africa and Another, 2008 (1) SA 566 (CC).* http://www.saflii.org/za/cases/ZACC/2007/20.html Date of access: 20 Jul. 2022.

Shaw, M. & Rademeyer, J. 2022. The dark, tangled web strangling SA. *Sunday Times, Insight*: 25 Sept. https://www.timeslive.co.za/sunday-times/opinion-and-analysis/insight/2022-09-25-the-dark-tangled-web-strangling-sa/ Date of access: 30 Sept. 2022.

Sole, S. 2010. Zuma's new spy purge. *Mail & Guardian*: 5 Feb. https://mg.co.za/article/2010-02-05-zumas-new-spy-purge/ Date of access: 23 Feb. 2023.

Sole, S., Timse, T. & Brummer, S. 2012. Swedish TV reveals fresh claims in South Africa's arms deal. *Mail & Guardian*: 22 Nov. https://mg.co.za/article/2012-11-22-swedish-tv-reveals-fresh-arms-deal-claims/ Date of access: 20 Jul. 2022.

South Africa. s.a. *State Security Agency (SSA).* http://www.ssa.gov.za/ Date of access: 7 Oct. 2020.

South Africa. 1984. Protection of Information Act No. 82 of 1984. Pretoria: Government Printer.

South Africa. 1994a. The Intelligence Services Oversight Act 40 of 1994. Pretoria: Government Printer.

South Africa. 1994b. The National Strategic Intelligence Act 39 of 1994. Pretoria: Government Printer.

South Africa. 1994c. The Public Service Act 103 of 1994. Pretoria: Government Printer.

South Africa. 1994 (Approved by the Cabinet in December 1994). *White paper on intelligence.* http://www.info.gov.za/whitepapers/1995/intelligence.htm or http://www.nia.gov.za/SSA-web-Legislation%20and%20Oversight.html Date of access: 5 Oct. 2014.

South Africa. 1996. Constitution of the Republic of South Africa Act 108 of 1996. Pretoria: Government Printer.

South Africa. 1999. Public Finance Management Act No. 1 of 1999. Pretoria: Government Printer.

South Africa. 2001. The treasury regulations as amended (issued in 2001). Pretoria: Government Printer.

South Africa. 2002a. Intelligence Services Act 65 of 2002. Pretoria: Government Printer.

South Africa. 2002b. National Strategic Intelligence Amendment Act 67 of 2002. Pretoria: Government Printer.

South Africa. 2002c. Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002. Pretoria: Government Printer.

South Africa. 2013. General Intelligence Laws Amendment Act No. 11 of 2013 (GILAA). Pretoria: Government Printer.

South Africa. 2016. The public service regulations. Pretoria: Government Printer.

South Africa. 2023a. General Intelligence Laws Amendment Bill (GILAA). Cape Town: Parliament.

South Africa. 2023b. Regulation of Interception of Communications and Provision of Communication-related Information Bill. Cape Town: Parliament.

South African Reconciliation Barometer (SARB). 2021. South African Reconciliation Barometer survey 2021 report. Institute for Justice and Reconciliation. https://www.ijr.org.za/portfolio-items/south-african-reconciliation-barometers-survey-2021-report/ Date of access: 12 Sept. 2022.

Staff Writer. 2021. Intelligence report reveals "shocking reality" around the interception of communication in South Africa. Business Tech: 14 Sept. https://businesstech.co.za/news Date of access: 11 Aug. 2022.

Statistics South Africa (Stats SA). 2012. Millennium development goals: Country report 2013. http://www.statssa.gov.za/MDG/MDGR_2013.pdf Date of access: 2 Aug. 2022.

Statistics South Africa (Stats SA). 2022. Census 2022: South Africa's youth continues to bear the burden of unemployment. https://www.statssa.gov.za/?p=15407 Date of access: 4 Nov. 2022.

Stone, S. 2021. SA spies bust in Mozambique. City Press: 4 Jul. https://www.news24.com/citypress/news/sa-spies-bust-in-mozambique-20210704 Date of access: 20 Jan. 2023.

The Minister of Intelligence. 2008. Ministerial Review Commission on Intelligence. https://www.r2k.org.za/wp-content/uploads/Matthews-Commission-Report-10-Sept-2008.doc Date of access: 20 Oct. 2016.

Walsh, P.F. 2011. Intelligence and intelligence analysis. New York: Routledge. https://doi.org/10.4324/9780203815939

Author Contributions

This article originates from the completed master's study of Rudolph Loubser, a former M-student who achieved a distinction. I served as the study leader and am presently a Research Professor.