

SECRET

---



(This document is the property of  
the Government of the Republic of South Africa and  
the Government of the Republic of Rwanda)

MEMORANDUM OF UNDERSTANDING  
BETWEEN

THE STATE SECURITY AGENCY OF THE REPUBLIC OF SOUTH  
AFRICA  
(SSA)

AND

NATIONAL INTELLIGENCE AND SECURITY SERVICES OF THE  
REPUBLIC OF RWANDA  
(NISS)

ALJAZEERA

SECRET

---

**PREAMBLE**

**WHEREAS** the parties to this Memorandum of Understanding are desirous of the achievement of co-operation on intelligence and security-related matters;

**RECOGNISING** the cordial relations that exist between the countries and their respective people;

**ACKNOWLEDGING** the need for the development, facilitation and consolidation of the alliance of solidarity that exists between the Parties;

**ASPIRING** to develop and strengthen cooperation to mutually promote and protect each other's security and to encourage political and economic development in their respective regions and on the African continent as a whole;

**BASED ON** mutual respect, trust and equality of the two parties;

**ACCEPTING** that this Memorandum of Understanding is in accordance with the domestic laws of the respective Parties and their obligations of in terms of international law

**RECOGNIZING** the need to enhance our cooperation and engage in mutually beneficial present and future sustainable exchange of information;

**HEREBY AGREE** as follows:

**ALJAZEERA**



SECRET

---

Article I  
DEFINITIONS

1.1 In this Memorandum of Understanding unless the context otherwise indicates:

**Agreement** refers to this Memorandum of Understanding;

**Joint project** refers to any joint project that may be undertaken by both Parties with a view to achieve common specified objectives;

**Parties** refers to SSA and NISS, who are responsible for the implementation thereof.

**Third party rule:** refers to the requisite authorisation which the one Party should obtain before releasing to a third party intelligence, information, data or documentation which constitutes the sole property of the other Party.

Article II  
PURPOSE OF THE MEMORANDUM

In furtherance of their common objectives, the Parties commit themselves to cooperate, share information and develop common strategies in the areas specified in Article IV.

Article III  
PRINCIPLES

3.1 The Parties shall cooperate according to the following principles:

- Common interest of the respective states;
- Strategic partnership;
- Mutual assistance, respect, trust and support;
- Confidentiality;
- Third party rule; and
- Reciprocity of treatment.

3.2 All cooperation between the parties shall be beneficial, lawful and reasonable.



- 3.3 The Parties hereby also agree that no party shall carry out intelligence or security-related activities that may endanger or threaten the other party's national interests, national institutions, and their respective Agencies and/or Services.

Article IV  
AREAS OF COOPERATION

- 4.1 Cooperation between the Parties shall *inter alia* apply to the sphere of intelligence and security-related activities, but not be limited to the following:

4.1.1 **Organised Crime and Border Intelligence**

The Parties will identify and share information in regard to organised crime groups as well as individuals suspected of involvement in activities concerning:

- a. Smuggling of illicit goods
- b. Illegal immigration
- c. Human smuggling
- d. Drug trafficking and precursor chemicals used in the manufacturing of drugs
- e. Money laundering.
- f. Combating religious extremism

4.1.2 **Social Stability**

The Parties will share information on organisations existing in both countries that are creating instability within the respective countries or that have suspected links with Foreign Intelligence Services.

4.1.3 **Private Security Companies and Mercenary Activities**

The Parties undertake to exchange information and documents regarding the functioning of private security companies and mercenary activities.

4.1.4 **Counterintelligence**

The Parties agree to cooperate and exchange information and intelligence on the activities of intelligence services that are active against South Africa and the Republic of Rwanda.

The Parties also agree to engage in joint operations and research into the tactics and techniques used by such intelligence services referred to in the previous paragraph as well as the appraisal of countermeasures.



**4.1.5 Human Resources Development**

The Parties agree to cooperate on issues relating to human resources development to evolve best practices in management development and effective performance management systems.

**4.1.6 Technical Resources Development**

The Parties agree to cooperate in the areas of research and development, signals intelligence and information communication technology.

**4.1.7 Reciprocal Visits**

The Parties agree to encourage reciprocal visits of technical professionals and experts.

**Article V**

**MECHANISMS OF COOPERATION**

5.1 The co-operation between Parties shall include and not be limited to the following mechanisms:

- Regular meetings of the Heads of the respective Services and/or Agencies;
- Regular meetings of the experts of the respective Parties;
- Reciprocal nomination and accreditation of liaison officers in their respective Countries; and
- Setting up of Task Teams to carry out joint projects.

**Article VI**

**PROCEDURES**

6.1 On the basis of this Agreement the Parties agree that the implementation and execution of the provisions herein contained will be entrusted to the Heads of the Parties.

6.2 Action plans may be developed between the Parties as and when necessary.

**ALJAZEERA**



SECRET

- 6.3 The action plan will incorporate intelligence cooperation, joint projects and procedures to exchange intelligence as indicated in Article IV of this Agreement.

**Article VII**  
**INFORMATION EXCHANGE**

- 7.1 Information exchange on intelligence expertise and assessments shall be effected in the following manner:
- Written requests and responses shall be directed to the Heads of the Parties;
  - Mutual Briefings followed by exchange of documentation on themes and subjects of common interest to the Parties.

**Article VIII**  
**ACCREDITATION**

- 8.1 Each Party shall apply for or bestow accreditation prior to placement of their respective liaison officers.

**Article IX**  
**OTHER AGREEMENTS**

- 9.1 The signing of this Agreement takes precedence over all other arrangements pertaining to the aforesaid matters.
- 9.2 In the same vein, the conclusion of this Agreement does not preclude the possibility of other agreements between the two parties on any related matters.

**ALJAZEERA**



SECRET

---

Article X

DURATION, MODIFICATION AND RENUNCIATION

- 10.1 This Agreement for cooperation is entered into for the duration of five years (5) and will be deemed to be renewed, unless advance notice is given to the contrary in writing by either Party, of at least three (3) months prior to the termination.
- 10.2 The Parties may at any time amend or revise this MOU to expand the scope of their understanding to encompass any other mutually agreed terms provided that such amendment shall be by mutual written consent signed by the Heads of the Parties..
- 10.3 In addition, the Parties explicitly agree that operational and organisational changes within a Party shall not constitute any obstacle to the continuation of the cooperation, unless they prove to hinder its execution.

Article XI

SETTLEMENT OF DISPUTES

11. Any dispute that occurs in the execution and/or the interpretation of this agreement will be settled amicably.
- (a) A dispute shall be deemed to have arisen when either Party notifies the other Party in writing to that effect; and
- (b) Any dispute that occurs in the execution and/or the interpretation of this Agreement will be settled in an amicable manner by the respective Heads of the Parties.

**ALJAZEERA**



SECRET

---

Article XII  
NOTICES

12.1 On the basis of reciprocity, each Party shall take the necessary measures to facilitate the stay and mission of the liaison officers accredited to the respective countries.

Article XIII

DISCLOSURE OF INFORMATION

13.1 Information and expertise exchanged between the Parties in fulfilling this Agreement and any information about the nature and contents of cooperation is confidential and shall be treated according to the conventional classification and may not be disclosed to any third party without prior written consent of the other Party.

13.2 The Parties also agree not to use any exchanged information for the purpose of judicial processes without written consent of the other Party.

13.3 All provisions contained in this Article, 13.1 and 13.2, will remain in force even after the termination of this Agreement.

**ALJAZEERA**



SECRET

---

**Article XV**  
**ENTRY INTO FORCE**

This Agreement shall enter into force upon the date of its signing by the Heads of the two Parties.

**IN WITNESS WHEREOF** the Director General of the National Intelligence and Security Services of the Republic of Rwanda and the Director-General of the State Security Agency of the Republic of South Africa, sign this agreement.

This ..... day of ..... 2012.

---

Mr Dennis T Dlomo  
Acting Director-General  
State Security Agency  
Republic of South Africa

---

Lt General EK Karezi  
Director General  
National Intelligence & Security Services  
Republic of Rwanda

**ALJAZEERA**



ANNEX III



**state security**

State Security Agency  
REPUBLIC OF SOUTH AFRICA

Office of the General Manager  
Central and East Africa

25 October 2012

SSA: SSA/YF10/IN/IC/FI

Head Liaison : [REDACTED]

**RE: FEEDBACK ON MOU WITH RWANDA SERVICE**

1. The Chief Directorate took note of the comments and proposals by the Rwandan service. The Chief Directorate is of the view that the proposals are not acceptable and not operationally appropriate, given the current circumstances. The intention of the proposal especially on fugitive's issues seem much more difficult to pursue
2. The Chief Directorate is therefore proposing that the MOU be processed as is and be presented for further discussion by both services legal teams at the date to be agreed.

Regards

[REDACTED]  
GENERAL MANAGER – CENTRAL AND EAST AFTRICA

**ALJAZEERA**



## ANNEX II

### OBSERVATIONS ON THE MOU PROPOSED BY THE STATE SECURITY AGENCY OF THE REPUBLIC SOUTH AFRICA (SSA)

The Preamble as proposed has no problem. It is brief and spells out the background for our cooperation.

Article III Principles of cooperation (3.3) can be modified as follows:

No party shall engage in any intelligence and security related operations/covert activities, which are likely to endanger the interests of the other Party without prior consultation and consent of that other Party.

Article IV (4.1.1) Areas of cooperation can be modified to include:

g- Tracking of genocide fugitives/negationists

4.1.2 can be modified to include "and individuals".

Article Vii (7.1) provides that each party shall bestow accreditation prior to placement of their respective liaison officers. This article implies that a designated officer can be rejected because the receiving Service carries out vetting before accreditation is given.

The remaining part of document has no problem. Typing errors can be rectified as well as the designation of the SG- NISS.

The logo for Al Jazeera, featuring the word "ALJAZEERA" in a bold, blue, sans-serif font. The letters are slightly shadowed, giving it a three-dimensional appearance. The logo is positioned at the bottom of the page, centered horizontally.



SECRET

SECRET

THIS DOCUMENT IS THE PROPERTY OF THE ORIGINATOR. IT CONTAINS CLASSIFIED INFORMATION AND MUST BE HANDLED IN ACCORDANCE WITH ESTABLISHED SECURITY PROCEDURES. IT IS LOANED TO YOUR AGENCY IN CONFIDENCE AND MAY NOT BE FURTHER DISSEMINATED WITHOUT PRIOR CONSENT OF THE ORIGINATOR.

DATE 30 JULY 2012

REPORT NO. 6960

URGENCY

SUBJECT **EGYPT/POLITICAL**

EGYPT: MORSI'S FIRST STEPS AS PRESIDENT REFLECT AN AGGRESSIVE POLITICAL STANCE ALONGSIDE A POPULIST AND PRAGMATIC FOREIGN POLICY

IN OUR UNDERSTANDING, MORSI'S CONDUCT SO FAR EXPRESSES THE MUSLIM BROTHERHOOD'S DETERMINATION TO TRANSLATE ITS SUCCESS IN WINNING THE PRESIDENCY INTO A PROFOUND CHANGE IN THE BALANCE OF POWER BETWEEN THE PRESIDENCY AND THE MILITARY AND CURRENT JUDICIARY. THE MUSLIM BROTHERHOOD IS READY TO ADOPT AN AGGRESSIVE APPROACH (WHETHER THROUGH A CONSCIOUS DECISION OR BECAUSE IT UNDERESTIMATES ITS RIVALS), EVEN AT THE COST OF DAMAGING ITS MODERATE AND DEMOCRATIC STATE IMAGE.

THE CHALLENGES FACING THE STATUS AND AUTHORITIES OF THE PRESIDENT AND PARLIAMENT ARE EXPECTED TO CONTINUE AND DEMAND MOST OF THE MUSLIM BROTHERHOOD'S ATTENTION, GIVEN THAT THEY ARE ESSENTIAL FOR PROMOTING ITS OTHER GOALS. THIS, IN ADDITION

SECRET

PAGE 1 OF 1



SECRET

TO THE DIFFICULTY IT WILL HAVE MEETING PUBLIC EXPECTATIONS REGARDING A SIGNIFICANT IMPROVEMENT IN THE ECONOMIC-SECURITY SITUATION, ARE EXPECTED TO KEEP THE MUSLIM BROTHERHOOD PREOCCUPIED WITH DOMESTIC AFFAIRS FOR THE TIME BEING, AND LIMIT THE AMOUNT OF ATTENTION IT CAN GIVE TO FOREIGN AFFAIRS.

- SOME THREE WEEKS SINCE BECOMING PRESIDENT, MORSI IS TAKING A CONFRONTATIONAL LINE WITH THE MILITARY AND THE JUDICIARY, STRIVING TO EXPAND HIS AUTHORITY AND RE-ESTABLISHING PARLIAMENT (CONTROLLED BY THE MUSLIM BROTHERHOOD) THROUGH PRESIDENTIAL DECREE. HE HAS HAD NO SUCCESS IN FORMING A COALITION GOVERNMENT OR APPOINTING VICE PRESIDENTS TO REPRESENT ALL THE DIFFERENT SECTORS OF EGYPTIAN SOCIETY, AS PROMISED BY THE MOVEMENT IN THE PAST.
- MEANWHILE, MORSI HAS PUT A SERIES OF POPULIST MEASURES IN MOTION TO ACHIEVE FAST RESULTS: A 100-DAY PLAN TO ADDRESS THE FUNDAMENTAL PROBLEMS OF SECURITY, TRANSPORTATION, FOOD, FUEL, AND GARBAGE; SALARY RAISES FOR THE MILITARY AND THE PUBLIC SECTOR; AND AMNESTY FOR HUNDREDS OF PRISONERS IN RECOGNITION OF RAMADAN.
- MORSI'S FOREIGN POLICY IS CHARACTERIZED BY ACTIVE MEASURES TO ALLAY CONCERN REGARDING AGGRESSIVE FOREIGN POLICY; GUARANTEE ECONOMIC AID (VISIT TO SAUDI ARABIA AND MEETINGS WITH CLINTON AND ASHTON); AND PROTECT EGYPT'S INTERESTS WITH REGARD TO THE NILE'S WATERS (VISIT TO ETHIOPIA). ALL THESE ISSUES HAVE DIRECT IMPLICATIONS FOR EGYPT'S INTERNAL SITUATION.
- MORSI'S FIRST STEPS WITH REGARD TO THE PALESTINIAN ISSUE (MEETINGS WITH ABU MAZEN AND MASH'AL) REFLECT AN ATTEMPT TO ADOPT A CAUTIOUS AND NEUTRAL STANCE, AND AVOID SHOWING



SECRET

UNEQUIVOCAL SUPPORT FOR HAMAS. ANY DIRECT REFERENCE BY MORSI TO ISRAEL IS CONSPICUOUS IN ITS ABSENCE.

- AT THE MOMENT, THE MUSLIM BROTHERHOOD IS PLAYING A KEY ROLE IN FORMULATING AND IMPLEMENTING MORSI'S DECISIONS. THE MOVEMENT'S TRAINING BUREAU AND SHURA COUNCIL APPEAR TO HAVE DRAWN UP MO'S FOR MORSI TO CONTEND WITH THE POLITICAL CRISIS; AND ITS ORGANIZATIONAL DISPOSITION HAS BEEN HARNESSSED TO PROMOTE THE 100-DAY PLAN DECLARED BY THE PRESIDENT.

WE WOULD APPRECIATE RECEIVING YOUR COMMENTS ON THE FOLLOWING:

1. FURTHER STEPS YOU EXPECT THE MUSLIM BROTHERHOOD TO TAKE TO WEAKEN THE INFLUENCE OF THE MILITARY, THE COURTS, AND EGYPT'S DEEP STATE.
2. BEYOND THE 100-DAY PLAN ANNOUNCED BY MORSI, WHAT OTHER TARGETS IS THE MUSLIM BROTHERHOOD SETTING, TO ENSURE QUICK ACHIEVEMENTS WITH WHICH TO IMPRESS THE PUBLIC?
3. DETAILS ON THE RELATIONS BETWEEN PRESIDENT MURSI AND THE MUSLIM BROTHERHOOD, INCLUDING KHAYRAT AL-SHATA'AR AND MUHAMMAD BADEEA. WHAT IS THE DECISION-MAKING PROCESS IN THE PRESIDENCY?
4. DETAILS ON MURSI'S CIRCLE OF ADVISERS: NAMES, FUNCTIONS IN THE PRESIDENCY, TIES WITH THE MUSLIM BROTHERHOOD, TIES WITH MURSI HIMSELF.
5. DETAILS ON THE STEPS THE MUSLIM BROTHERHOOD IS TAKING TO PENETRATE THE SECURITY SYSTEM (MILITARY, DEFENSE MECHANISMS, AND POLICE), LEGAL SYSTEM, AND CIVILIAN BUREAUCRATIC SYSTEM. PEOPLE IN THESE SYSTEMS WHO ARE

SECRET

PAGE 3 OF 3



SECRET

KNOWN TO HAVE/ARE SUSPECTED OF HAVING TIES WITH THE  
MUSLIM BROTHERHOOD.

6. THANK YOU. REGARDS.



**ALJAZEERA**



CONFIDENTIAL

(This document is the property of the Governments of the  
Republics of Zimbabwe and South Africa)



REPORT OF THE 3<sup>RD</sup> MEETING OF THE JOINT INTELLIGENCE  
TASK TEAM OF THE STATE SECURITY COMMITTEE OF THE 6<sup>TH</sup>  
SESSION OF THE ZIMBABWE-SOUTH AFRICA JOINT  
PERMANENT COMMISSION ON DEFENCE AND SECURITY,  
ELEPHANT HILLS HOTEL, VICTORIA FALLS, ZIMBABWE

29-30 OCTOBER 2011

**ALJAZEERA**

1  
CONFIDENTIAL



CONFIDENTIAL

**REPORT OF THE 3<sup>RD</sup> MEETING OF THE JOINT INTELLIGENCE TASK TEAM (JITT) OF THE STATE SECURITY COMMITTEE OF THE 6<sup>TH</sup> SESSION OF THE ZIMBABWE-SOUTH AFRICA JOINT PERMANENT COMMISSION ON DEFENCE AND SECURITY, ELEPHANT HILLS HOTEL, VICTORIA FALLS, ZIMBABWE**

**1. INTRODUCTION**

1.1 The third meeting of the Joint Intelligence Task Team (JITT) of the Zimbabwe-South Africa Joint Permanent Commission on Defence and Security (JPCDS), was held at Elephant Hills Hotel, Victoria Falls, Zimbabwe from 29 to 30 October 2011. The Zimbabwean delegation was led by [REDACTED] Director External of the Central Intelligence Organisation (CIO), who chaired the meeting. The South African delegation was led by [REDACTED] the General Manager at the State Security Agency (SSA), who co-chaired the meeting.

**2. OPENING REMARKS**

2.1 In his opening remarks, the Chairperson, [REDACTED] welcomed the South African delegation to Zimbabwe and particularly, to Victoria Falls. He highlighted that JITT provides the two sister Services with the opportunity to review progress on the implementation of the Joint Action Plan adopted at the last meeting held in November 2010 in Durban, South Africa. The Chairperson then underscored the role played by the Southern African Development Community (SADC) at continental gatherings, such as the African Union (AU) related meetings, where SADC, made meaningful and significant contributions.

2.2 In his reciprocal remarks, the Co-Chairperson, [REDACTED] expressed appreciation over the warm hospitality accorded his delegation. He urged the



**CONFIDENTIAL**

delegates to engage in discussions in a candid manner, reflective of the mutual cooperation enjoyed by the two Services. The co-Chair made reference to the Zambezi River, which he said could easily be the liberation route for SADC if proper research is done. He then expressed, once again, his condolences on the passing on of CIO Deputy Director General, [REDACTED]

**3. CONSIDERATION OF THE AGENDA**

**3.1** The JITT considered and adopted the following agenda items:-

- Opening Remarks
- Adoption of the Agenda
- Presentation on the 17<sup>TH</sup> Conference of the Parties to the United Nations Framework Convention on Climate Change (COP17)
- Review of the Joint Action Plan
- Break away into Subcommittees
- Report back from Subcommittees
- Preparation of the Joint Action Plan and JITT report
- Presentation and adoption of the Joint Action Plan and the JITT report
- Any Other Business
- Closing Remarks

**4. PRESENTATION ON COP17**

**4.1** The SSA presented an overview on the COP17 Summit scheduled for 28 November to 9 December 2011 in Durban, South Africa. The presentation highlighted the significance and opportunities offered by the event, especially with regard to tourism and diplomacy, as well as the security implications and challenges thereof.



CONFIDENTIAL

- 4.2 The meeting noted the need for the exchange of information on risks and threats associated with hosting a global event of such magnitude. These include, *inter alia*, possible terror attacks, border management challenges, transnational organised crimes and disruptive acts by non state actors.
- 4.3 The committee emphasized the need to monitor the activities of pressure groups stationed in either country or those that might want to use regional countries as transit to South Africa. The report cited the three African caravans as having the potential for disruptive behaviour thus meriting the attention of intelligence Services.
- 4.4 The meeting then expressed hope that South Africa will host a successful COP17 and that the conference will yield positive views on issues of climate change that would benefit Africa.

5. REVIEW OF THE 2010/2011 JOINT ACTION PLAN

- 5.1 The meeting noted, with appreciation, considerable progress made in the implementation of the 2010/2011 Joint Action Plan. These included:
- Enhancing cooperation through training and development
  - Cooperation in respect to combating international terrorism and proliferation of Weapons of Mass Destruction
  - Monitoring activities aimed at subverting constitutional order
  - Cooperating and exchanging information on border intelligence
  - Enhancing cooperation on the hosting of COP17



CONFIDENTIAL

- Exchanging intelligence on bilateral, regional and international developments through analysis exchange meetings
- Enhancing technological cooperation.

5.2 The meeting noted the challenges faced in the implementation of the Joint Action Plan, such as the adoption of the Joint Operational Guidelines and the financial constraints in fulfilling some of the agreed objectives. The meeting resolved to address the challenges in the new Joint Action Plan.

5.3 The meeting recommended some changes to the Joint Action Plan. These included the realigning of objectives and the provision of specific dates, wherever possible. The committee then agreed that, for purposes of clarity, the timeline of the Joint Action Plan should be the JITT calendar.

**6. JITT SUB-COMMITTEES**

- 6.1 A new sub-committee namely, Domestic Intelligence, was established. The meeting broke into the following sub-committees
- a) Counter Intelligence;
  - b) Training;
  - c) Technical;
  - d) Domestic Intelligence; and
  - e) Economic Intelligence

**7. THE 2011/2012 JOINT ACTION PLAN**

- 7.1 The JITT reviewed the 2010/2011 Joint Action Plan, developed and adopted the 2011/2012 Plan. These included new training requirements and enhanced co-operation in the exchange of information on threats and opportunities of social media networks, illicit textile and



**CONFIDENTIAL**

tobacco industries as well as best practice visits. The committee noted the need to develop and implement operational plans to counter poaching.

7.2 The meeting further agreed that respective Heads of branches should meet regularly to discuss matters at their level. Hitherto, meetings were being held at lower levels without much participation at the level of Heads of branches.

**8. CONSIDERATION OF THE DRAFT AGENDA FOR THE STATE SECURITY COMMITTEE**

8.1 The JITT proposed the following agenda items for the State Security Committee:

- 1) Opening Remarks;
- 2) Adoption of the Agenda;
- 3) Presentation of Security Situation Briefs;
  - a) Zimbabwe
  - b) South Africa
- 4) Presentation and Adoption of the 2010-2011 JITT Report
- 5) Presentation and Adoption of the 2011-2012 Joint Action Plan;
- 6) Any Other Business;
- 7) Closing Remarks

**9. CLOSING REMARKS**

9.1 The co-Chairperson, [REDACTED] expressed satisfaction that the meeting had deliberated on key issues pertaining to the Joint Action Plan. He underscored the need for continued engagement on issues of mutual cooperation and reiterated the challenges the region was facing. He thanked the Chairperson for successfully steering deliberations of the JITT meeting.



CONFIDENTIAL

9.2 In his concluding remarks, the Chairperson, [REDACTED] [REDACTED] thanked the South African delegation for the fruitful engagement and expressed hope that the two Services will work to implement the agreed work plans. He thanked both teams for displaying commitment to JITT deliberations.



**ALJAZEERA**





**ALJAZEERA**

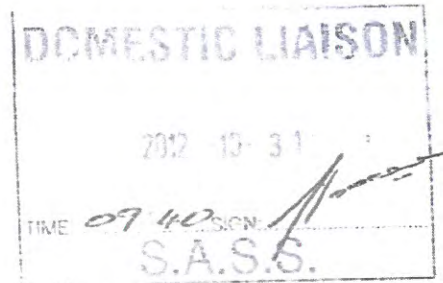
---



SECRET

DAY ONE:

**DRAFT REPORT OF MEETING HELD  
IN ADDIS ABABA, ETHIOPIA**



ON 24 OCTOBER 2012

## PURPOSE

The multi-disciplinary team headed by Director: Mr S NTOMBELA SSA:FB) consisted of [REDACTED] General DLADLA (SAPS), Colonel (Special Forces); Lt-Colonel , [REDACTED] FB and Mr M APHANE (DIRCO). The team left South Africa for Addis Ababa on 24-10-2012 in order to engage with the Security Establishment of Ethiopia on security matters related to concerns around the Chairperson of the African Union Commission (AUC), Dr NC DLAMINI-ZUMA.

The following meetings were scheduled by the Head of Station;

- Meeting Ambassador PEPANI
- Meeting with National Intelligence and Security Services (NISS)
- Meeting with Head of AUC Safety and Security Division (AUC SSD)

## Meeting on arrival 24 Oct 2012

On arrival the team convened a meeting with Acting Director Mr NTOMBELA, outlining the purpose of the visit. He mentioned that the visit was aimed at meeting the local state security apparatus to discuss all security related issues around the Chairperson of the AUC. This was also aimed at making an overall intervention for the security of the AUC Chair and this also included getting the assurances from the host country service

The Acting Director then requested [REDACTED] to make remarks on the purpose of the visit. [REDACTED] remark was that the team needed to ask the question of security around the AUC Chairperson in a manner that is not intrusive but asked in good faith. Furthermore, the General said the team needed to unbundle the issues as they are raising them with the Host Service so as to avoid creating an impression that South Africa was declaring a vote of no confidence on the handling of AUC Chairperson's security.

SECRET



██████████ also thought that it would be necessary to reflect on the issue of last year that was involving his department and the arrest of DMI officer by the Ethiopians. According to him, the Host Service did not want to meet with him during his visit despite the fact that they had shown willingness and commitment to do so.

The Acting Director concurred with the sentiments raised by ██████████ on the aspect of managing the issues and the sensitivities that comes with issue of the obligation the Host country to protect all AU and member states in Addis Ababa, Ethiopia.

The Acting Director further pointed out that the issue at hand was about to receiving briefing and update on how they are proceeding about the issue of an unnamed state alleged to be seeking to cause harm to the Chairperson on 24 October 2012. He also intimated that this issue was then followed by another alert which further pointed out a potential assassination plot that was allegedly hatched to be carried out at a different venue that it been planned earlier.

The Team adopted the following approach to engaging the Ethiopians:

The team agreed that the correct approach to engage the Ethiopians would be to say that South Africa is pleased with manner in which they have provided and elevated security arrangements around the Chairperson despite the fact that the alert provided to them does not add up in some respect.

The expected outcome:

- To develop a security capacity to deal with security challenges as well as to render security service capacity as and when the travels around the continent
- To establish a multi-disciplinary coordinating structure that is not intrusive but that would be perform specific functions for the protection of the AUC Chairperson
- To ensure that the work of the task team is coordinated through NICOC or cluster

Recommendations

- That the VIP protection team capacity be increased from one Officer to a of several officers to be constituted by SAPS and would perform duties on a rotational basis.
- Special Forces to explore ways of strengthening security capacity to cover travels of the Chairperson when she visits hot spot in the continent
- To create a Nodal-point in the Office of the Chairperson to facilitate the flow of information between her office and the Nodal point.
- As a means of ensuring an inclusive nature of the security of the Chair, SADC needs to be influence to participate in providing security to the AUC Chairperson



- The task team would also want to prioritise on building relations with NISS as the latter is the primary provider of security to the Chairperson
- support the idea of utilising the medical capability of the Cubans medical contingent currently stationed in Ethiopia

DAY TWO:

**DRAFT REPORT OF MEETING WITH  
THE FOREIGN SERVICE OF  
NATIONAL INTELLIGENCE AND SECURITY SERVICES  
IN ADDIS ABABA, ETHIOPIA  
ON 25 OCTOBER 2012**

The South African delegation to the above –mentioned meeting was led by Director S. M. NTOMBELA composed of the following members: [REDACTED] Colonel MOLEFE (Attache) and Messrs M. APHANE [REDACTED] and [REDACTED]

The Delegation was warmly welcomed by the Director of Foreign Service of NISS Mr. Hadera ABERA and [REDACTED] (Head of Liaison). He congratulated South Africa for the election of the new Chairperson of the African Union Commission (AUC) Director NTOMBELA thanked the Director of Foreign Service for the warm welcome to him and his delegation. He then indicate the purpose of the visit to Addis Ababa firstly to expressed the gratitude for the manner in which NISS has handled the issue of security of the African Union Commission Chairperson as well as the speedy responds to the request forwarded from SSA to NISS. He further expressed condolences on passing away of the beloved leader, Prime Minister Meles ZENAWI.

The Director of NISS Foreign Service pointed out that he had received the request from SSA FB with names of the person who pose a potential threat to the Chairperson of the AUC. In this regard, gave a brief that upon receipt the Service auctioned the operation to check the names from all entry points especially those bordering Sudan; airports through immigration. He further pointed-out that their investigation could not establish the existence of the names provided. He requested that the information be beefed-up in terms of the details on specifics of the individuals involved. Furthermore he reiterated the point that NISS would do everything possible to ensure the safety of the Chairperson of the AU. He emphasised the



point that there has been never a threat that developed into a situation where a diplomat is killed in Addis Ababa with exception of the former Egyptian President **MUBARAK** whose life was threatened in 1987. However he pointed out that NISS has foiled a number of terrorist activities aimed at Ethiopia. In this regard he requested there be a process of sharing intelligence on continuous basis between the two Services. He further indicated that NISS had had good working relations with the South African Secret Service under the former Director-General Mr T. **DENIS** and that this could form the basis of close cooperation between the two Services. He also made reference to the agreement between the two Services regarding the drafting of the Memorandum of Understanding (MoU).

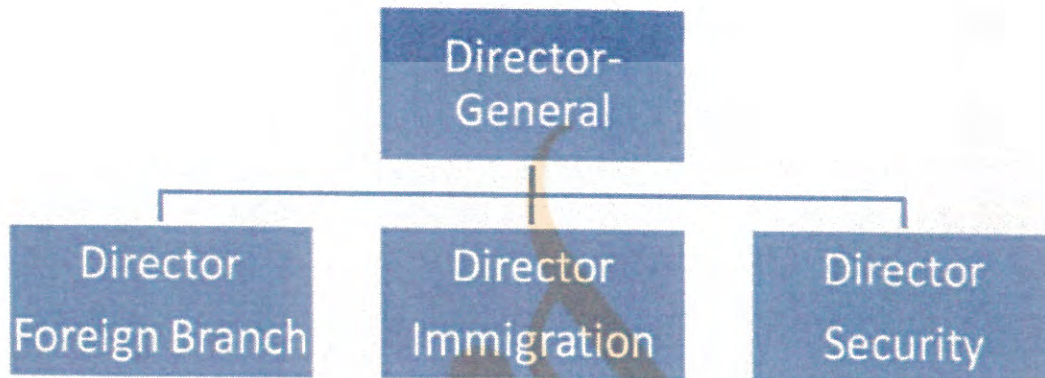
The Acting Director of SSA FB responded by pointing out that the two countries occupy strategic location in the continent and that their respective governments had cooperated on numerous issues. He also intimated that the SSA was looking forward to future cooperation between the two Services on matters of Security, information sharing, assistance to issues that cannot be handled by one service such as Terrorism, Cyber threats especially those that could be directed to the African Union.

The Director SSA requested a briefing on the security assessment of the region as well as the one of the African Union. He further enquired for an indication on the security of the Chairperson when she travels around the continent to hot-spot areas in particular. The Director NISS Foreign Service pointed out that he would not have the details on the assessment due to the short notice to which the meeting arranged. However he would consult with different branches of NISS especially the one dealing with VVIP Protection.

He committed that the assessment could be covered within the context of issues that would be contained in the MoU. However he would arrange an exchange meeting of experts to discuss the regional security situation and that of the security of AU. In his response he pointed out that the VVIP Service does not belong to his portfolio but to that of Security. He then briefed the delegation on how NISS is structured:

**ALJAZEERA**





The Director NISS request the Director SSA-FB to share the details of the threat against the AUC Chairperson as they did not pick anything from their side but would like to find out the background to the threat. This would enable NISS to have a better assessment of the threat. He also requested SSA to share any threat that may be picked-up against or directed against AU and the Federal Democratic Republic of Ethiopia as the issues of terrorism are not confined within the borders of FDRE. The Director SSA- FB responded by outlining the following types of threats that could impinge the success of the AU Chairperson in her work:

- Threats that could arise from those who oppose the principles of the AU Constitutive Act – the coup plotters and those involved in unconstitutional change of governments;
- Those who may not want the Chairperson to visit the hot-spot like Somalia and Mali to address the issues pertaining to peace and stability;
- Threat from the emanating from extremist groups like Alshabaab directed at the AU as vulnerable target
- Threat emanating from forces outside the continent who may not wanting to stall implementation of the AUC programmes
- The Acting Director pointed out that there was no specific threat other than the reported potential threat reported against the life of the AUC Chairperson

further expressed the sentiments of the Director SSA-FB by expressing South Africa's gratitude for the manner NISS in which the security of the AUC Chairperson and the feed-back on the request pertaining the threat. He emphasised the need to liaise at an expert level between the two Services on matters of cyber threat against the AU.



The Director SSA FB requested the facilitation by NISS Director with VIP Security department of NISS so that he can express the same gratitude on the protection of the AUC Chairperson. He further asked if NISS could facilitate the licensing of the additional number of fire-arms for the VIP protection. The NISS Director responded by indicating that he would facilitate the experts meeting with the department of Security to engage on the details.

The Director SSA-FB concluded by extending a wish to meet the Director-General NISS either by the Acting Director-General; himself or both of them as soon as it that meeting could possibly take place.

General Egziabher MEBRAHTU's briefing was in line with issues that were covered by SSA delegation led by [REDACTED]: Refer to paragraphs below :

**Daily update on the State Security Agency (SSA) task team visit to the Headquarters of the African Union Commission (AUC) 10 October 2012**

1. Introduction

1.1 Following the engagements of 09 October 2012, the SSA Task Team proceeded with its programme on 10 October 2012. This programme entailed the following:

- Courtesy call on the South African Ambassador to the Federal Democratic Republic of Ethiopia and Permanent Representative of South Africa to the African Union, General LC PEPANI.
- Meeting with the Head of AUC Security and Safety Division (SSD), General Egziabher MEBRAHTU, Deputy Head of SSD, Colonel Sadeeq Garba SHEHU and the SSD Operations Officer [REDACTED]
- Meeting with the AUC Facilities Manager, Dr Auguste NGOMO.

**2. Courtesy call on the South African Ambassador to the Federal Democratic Republic of Ethiopia and Permanent Representative of South Africa to the African Union, General LC PEPANI**

2.1 During the courtesy call the following points were raised by the Ambassador:

- Since the July Summit of the AU which elected Dr DLAMINI-ZUMA as the AUC Chairperson, a number of countries that had opposed the latter's election had changed their attitude and expressed willingness to cooperate with the South African Embassy.
- Significant developments in this regard took place, chief amongst which was the re-call of the previous French Ambassador<sup>1</sup>, Mr Jean-Christophe BELLIARD and his replacement by Madame Brigitte COLLET. In addition, the United States (US) Embassy in Addis Ababa had also indicated

<sup>1</sup> He had tirelessly campaigned against the candidature of Dr DLAMINI ZUMA



willingness to facilitate a meeting between Secretary of State, Hillary Rodham CLINTON and the newly elected AUC Chairperson Dr DLAMINI-ZUMA. In this regard the Ambassador also recalled that the US, through its Embassy in Addis Ababa, had also played a significant behind the scenes role in campaigning against Dr DLAMINI-ZUMA. Furthermore, the majority of African countries who had campaigned against SADC candidates are beginning to express willingness to co-operate with the newly-elected Chairperson. Countries like Nigeria, Kenya and others have indicated readiness to turn a new leaf for the sake of the African continent.

- On the other hand, developments in the host country including the unfortunate and untimely demise of former Prime Minister Meles ZENAWI have presented an opportunity for both RSA and Ethiopia to repair the damaged relations between the two countries. However, the Ambassador also emphasised the tenuous internal situation in the host country mainly characterised by ongoing tensions between the ruling minority Tigrayans<sup>2</sup> and the rest of the Ethiopian People's Revolutionary Democratic Front (EPRDF). These tensions have recently been exacerbated by what appears to be the tightening of the grip on power by the Tigrayan Peoples' Liberation Front (TPLF) which is the dominant partner in the EPRDF.
- Nonetheless, developments in the host country point towards the emergence of possibilities for a substantive turn around in RSA-Ethiopia relations including the forging of business ventures and an opportunity for both countries to learn from each other's experiences<sup>3</sup>
- With regard to the request of the task team to conduct an inspection at the official residence of the Chairperson, Ambassador PEPANI gave members of the task team an explanation of some of the difficulties the Embassy had experienced in accessing that site. It was only after prolonged persistence that a delegation from the Embassy, DIRCO, AU and the Station led by the Ambassador was finally given permission by Dr Jean PING to visit the official residence on 05 October 2012<sup>4</sup>.
- Ambassador promised to share with the SSA task team a copy of the inspection visit to the official residence.
- In conclusion, the leader of the task team [REDACTED] thanked the Ambassador for the opportunity to make a courtesy call to on the Ambassador and expressed a desire to work closely with the Embassy and the station in ensuring that Dr DLAMINI-ZUMA's tenure at the helm of the AUC was a productive one in furtherance of the objective of securing peace security and sustainable development for the people of Africa

### 3. Meeting with the Head of AUC SSD

<sup>2</sup> Since the death of former Prime Minister ZENAWI, thirty seven (37) new Generals from the Defence Force have been promoted, thirty four (34) of which are Tigrayans.

<sup>3</sup> The Ambassador stated his disappointment with regard to the recent developments at South African Airways (SAA) and pointed to how RSA could tap into the vast experience of Ethiopian Airlines in addressing issues of turnaround strategies and general management of airlines.

<sup>4</sup> Refer to task team report of 09/10/2012 for full details.



After the courtesy call on the Ambassador the team and the Head of Station (HOS) proceeded to the a meeting with the Head of the SSD General Egziabher **MEBRAHTU** who was joined by his deputy and Nigerian national Colonel Sadeeq Garba **SHEHU** and SSD Operations Officer Mr Christopher S **KAYOSHE** from Rwanda.

In his introductory remarks the HOS [REDACTED] thanked the Head of SSD for the opportunity to meet and introduced members of the SSA Task Team He further elaborated that the meeting was a follow up on earlier engagement with the Head of SSD. During the meeting the following points were raised:

- The international security environment; the situation on the African continent and the Horn of Africa in particular had changed thereby meriting a re-assessment of the threats facing the AU. In this regard, the increased involvement in conflict resolution especially in areas like Somalia, Mali and others increase the prospects of attacks on AU personnel and property. Coupled to the above, recognition had to be made of the fact that in the past eighteen (18) months the size of AU personnel had quadrupled.
- It was also felt that the increase in the number of meetings and events hosted by the AU and Ethiopia compounds the security threats and risks.
- The Head of SSD gave the SSA delegation a brief on the personal security deployments level around the Chairperson of the AUC in line with what was mentioned in the report of SSA Task Team dated 09/10/2012.
- He lamented the absence of an approved security policy and standard operating procedures and the fact that their past attempts to access senior AUC management had yielded no tangible results. *He then expressed a feeling that the finalisation of the existing draft policy should be one of the first priorities of the incoming Chairperson.* Furthermore, the Head of the SSD was of the view that the creation of a Security Advisory Board residing in the office of the Chairperson was of paramount importance.
- General **MEBRAHTU** also reiterated the need for RSA assistance in capacity building; enhancement in safety and security and the development of security systems and standards in line with international best practice.
- He further lamented the lack of requisite attention to security by senior management of the AUC and gave the example of the cumbersome chain of command.<sup>5</sup> Consequently, it would be in the best interests of the AU, AUC and in securing the safety of personnel and property for the line of command to be streamlined such that security reports directly to the AUC Chairperson.
- The meeting concluded by an agreement that any further engagement between the AUC Security and RSA in relation to training should take place within the context of all AU protocols including Host Country Agreement.
- All pertinent issues raised by the Head of SSD and his delegation should be duly packaged and presented directly to the incoming Chairperson in a meeting to be facilitated by the HoS.
- The SSD made a promise that he and his staff will provide an efficient service, to protect and support the incoming Chairperson of the AUC.

<sup>5</sup> Currently, the Head of SSD reports to the Head of administration who in turn reports to the Director of Administration who reports to the Commissioner of Human Resource, who reports to the Deputy Chairperson of the AUC



#### 4. Meeting with the AUC Facilities Manager

This meeting discussed the following:

- Mr **NGOMO** ascertained it would take a period of two months to complete the refurbishment and the purchasing of furniture for the official residence. He also added that there are three companies from Spain, RSA and the USA that were short-listed for the installation of the electronic security systems for the Office and the Official Residence.
- The current official vehicle of the Chairperson is five years old.
- The AU is guided by the European Union (EU) blacklisting framework in selecting airlines to be used by the Chairperson. The AUC Chairperson uses the following commercial airlines: Lufthansa, European and other Star Alliance airlines including South African Airways. She would travel first or business class depending on availability.
- The Chairperson's entourage ordinarily travels economy class except in cases where the trip is longer than eight (8) hours.
- Mr **NGOMO** further elaborated the following additional travel arrangements in respect of the additional VIP protector from RSA:
  - the AUC would cover the initial travel costs from RSA and on subsequent trips when travelling with the Principal. In such a case the AUC would also cover the subsistence allowance, travel and accommodation costs.
  - In cases where the accommodation costs exceed the AUC norms, the VIP protected would be required to pay the costs and claim the difference arising therefrom upon return.
- He also shared with the delegation concerns regarding the recent transfers against the letter and spirit of declared staff transfers and appointments. This has led to a situation where tension, anxiety and uncertainties among senior staff<sup>6</sup> are rife. *The team asserts that these developments hold the potential of heightening tensions and suspicions particularly in relation to perceived post-PING movement of senior staff as already elaborated in the SSA POA and IP dated 07/10/2012 (section dealing with assumptions and principles).*

**CONTINUATION OF THE MEETING ON 25 OCTOBER 2012,**

**AT THE SOUTH AFRICAN EMBASSY**

Upon arrival of the Chairperson to Ethiopia, the host country of the AUC, security was provided by NISS against the background that were raised which are poor capacity to provide and protect .

AUC security is unarmed

General Egziabher **MEBRAHTU** lamented on the challenges.

<sup>6</sup> A case in point is the proposed transfer of Dr Abdul-Hakim **ELWAER** the Director of Human Resource and Administration to Human resources Science & Technology



Whilst NISS provided security for the AUC Chairperson, AU did not arrange accommodation and resources for food.

General Egziabher **MEBRAHTU** also mentioned that the protectors slept in corridors for four days without food and water provided.

The current situation is that they are provided with accommodation without food and water. This creates a gap since they have to go out of the hotel to get food and water, leaving the Chairperson unattended, therefore vulnerable.

To this effect a decision was taken at the meeting that on her return from South Africa the accommodation and food costs will be factored as part of the AUC Chairperson's account.

This has been done to avoid creation of a perception that South Africa is taking over the provision of the protection of the Chairperson from NISS and AUC.

#### **SECURITY**

It was agreed in the meeting that SAPS will avail resources and advance team. AUC Head of Security would avail buy-in and programme of the Chairperson when she visits hot spot areas.

There was also a decision that moving forward there must be a clear division of responsibilities to all role players. (**SSA, SAPS, MILITARY**)

A decision was taken that issues relating to VIP Protection will be dealt with by SAPS, that is including:

- Fire arm licensing for additional security personal including future co-operation with NISS and SSD.
- SAPS would provide cover for State Security to access AUC building and official residence to execute its CI and TSCM functions.

End

**ALJAZEERA**



MESSAGE FORM	
1.	2I2L0011.C6D
2.	111330A
3.	11 December 2012
4.	01 of 02 Pages
5.	Routine
6.	Attention: Divisional head NF21 Copy: Liaison Officer A1A
7.	Secret
8.	Operational Report
9.	Liaison Contact Report
10.	EL/LS/LR
11.	HOS NF21/02
12.	Station NF21/02
13.	<b>STATION NF21/02 : CONTACT REPORT</b>

1. Contact report attached.

# ALJAZEERA



**STATE SECURITY AGENCY:  
SOUTH AFRICAN SECRET SERVICE  
LIAISON CONTACT**

---

Name of Liaison Service : DGED , DST  
Country : Morocco  
Name of SSA: members : [REDACTED]  
Name of LS member(s) : [REDACTED] (Head of Liaison DGED),  
[REDACTED] (DGED), Head of Internal Security  
(DST), [REDACTED] (Director of DST)  
Date of meeting : 11/12/2012  
Place of meeting : Rabat  
Type of meeting : Telephonic/personal  
Documents exchanged (yes/no) : No  
Other people/officials involved : No  
Initiator of contact : DGED

---

**1. PURPOSE**

1.1 HoS was contacted telephonically by DGED on 10 December 2012, for a meeting at their HQ.

**2. DISCUSSIONS**

2.1 HoS was welcomed by [REDACTED] and introduced to Head of Internal Security DST and the Director of DST [REDACTED]

2.2 They stated that the purpose of the meeting is to bring under the attention of HoS and discuss an incident which took place in South Africa. Their representative in Pretoria



was high jacked at gunpoint close to the Moroccan Embassy, beaten up and kidnapped for five hours, after which he was dumped in the outskirts of Pretoria. The Director enquired if there could be a political motif behind this incident. The Diplomatic branch of SAPS is handling the case.

2.3 HoS replied by expressing his shock and sadness at what happened, stating that unfortunately, violent high jacking became very common in South Africa and the modus operandi of this incident is in accordance with this criminal activity in South Africa. The Director indicated that they are flying their representative back to Morocco for consultations and recovery, whereby he will be debriefed.

2.4 HoS indicated that if necessary, he is available for further briefing after the arrival of their representative.

3. HoS utilised this opportunity to indicate the good relations between SSA and DGED and offer his availability if any liaison is needed. DGED could be the nodal point to arrange meetings. Member also informed DST that the SSA was recently formed to amalgamate the Domestic and Foreign services, which in fact extend HoS's functions to include liaison with DST. The Director indicated his satisfaction with the suggestion.

#### **4. COMMENTS/IMPLICATIONS FOR RSA**

The seriousness with which DST is regarding this incident is confirmed by the seniority of the officers present. The Moroccans tend to be a bit paranoid, because of the Sahara issue. The meeting took place in an amicable atmosphere.

It is suggested that a response being send to DST as soon as possible, even just a letter expressing our shock and concern would be appreciated.

# ALJAZEERA





# State Security

State Security Agency  
REPUBLIC OF SOUTH AFRICA

**DOMESTIC LIAISON**

2012 -10- 26

TIME: 09:40 SIGN: *[Signature]*

S.A.S.S.

## LIAISON CONTACT REPORT

Liaison Contact	L670	
SASS Member/s Involved	Head of Station	
Unit	NF22/2	
Date of Contact	22 October 2012	
Place of Contact	Sheraton Hotel	
FIS Member/s	NISS Head of Liaison	
FIS Members Positions	NISS Head of Liaison	
Type of Contact	Operational	X
	Social	
	Telephonic	
	Other (Specify)	
SSA Requested Contact	Yes:	No: X
Documents: a. Requested	None	
b. Exchanged	None	

### 1. Background

The Director-General of the State Security Agency (SSA) had sent a letter of condolence to the Director-General of the National Intelligence and Security Service (NISS). In that letter the SSA Director-General raised the issue of the Memorandum of Understanding (MoU) between the Agency and the Service.

### 2. Reply by the Director-General of NISS

Consequent to the letter, the Director-General has replied requested that the Head of Station be consulted on the proposed dates of the meetings, first the experts meeting on the 29 November 2012, followed by the Senior officials meeting on the 5 December 2012. The first round of meetings will take place in Addis Ababa, FDRE. The Head of Station agreed to the proposed dates and has since sent the letter for attention.

On the Analysts' exchange visits to discuss the issue of human trafficking, human smuggling as well as the terrorism, NISS is of the opinion that the Analysts meeting be held back until the draft MoU has been agreed upon in principle as it would guide the way forward on areas of cooperation.

### 3. Conclusion

The Head of Station request the Divisional Head NF23 to consult with the Division on Counter-Terrorism to establish whether it can wait until the meeting on the MoU takes place. If the situation warrants immediate contact with NISS, it is requested that it be indicated.

### 4. Thank you. End.





**State Security**

State Security Agency  
REPUBLIC OF SOUTH AFRICA

**DOMESTIC LIAISON**

2012 -10- 26

TIME: 10:33 SIGN: *[Signature]*

S.A.S.S.

**LIAISON CONTACT REPORT**

Liaison Contact	L670	
SASS Member/s Involved	Head of Station	
Unit	NF22/2	
Date of Contact	23 October 2012	
Place of Contact	South African Embassy	
FIS Member/s	NISS Head of Liaison	
FIS Members Positions	NISS Head of Liaison	
Type of Contact	Operational	X
	Social	
	Telephonic	
	Other (Specify)	
SSA Requested Contact	Yes:	No: X
Documents: a. Requested	None	
b. Exchanged	None	

**1. Background**

The Station received a message J044 from Head Quarters at about 20H30 on 22 October 2012.

**2. The Developments**

a. Meeting with the Ambassador at about 21H15

On receipt of the message, the Head of Station in consultation with the Deputy Head of Station decided that the Ambassador of South Africa to the African Union and the Federal Democratic Republic of Ethiopia be informed for information of the situation. After receiving the briefing from the Head of Station, the Ambassador decided to brief the African Union Commission Chairperson and also informed her that there might be some changes in the protection arrangements and the State Security Agency is handling the matter.

b. The Contact with the NISS Head of Security

The Head of Station attempted at about 20H38 to call the NISS Head of Security but could not get through to him and left a request to call him back. The NISS Head of Security responded to the request by the Head of Station to call him at about 21H47. The head of Station requested a beef-up of security of the AUC Chairperson.

The Head of Station was at Sheraton Hotel at about 06H30 this morning and can confirm that there was a beef-up on the security. A V8 back-up vehicle is provided with four security personnel.

c. Meeting with Head of NISS Liaison

At about 08H30 on 23 October 2012, the Head of Station met with the Head of NISS Liaison. The Head of NISS Liaison requested more details on the development so that appropriate measures can be put in place. The Head of station could not provide further details because message J044 indicated that 'Until further notice no details (names) must be shared with the host Service.



**3. Conclusion**

It is requested by the Station that a determination be made on how soon the names should be shared with the host Service as it wants to avoid any diplomatic embarrassment if anything takes place.

**4. Thank you.  
End.**



**ALJAZEERA**



SECRET

DMS: 10000342728

# ISRAEL



## GEOPOLITICAL COUNTRY AND INTELLIGENCE ASSESSMENT



**ALJAZEERA**  
National Intelligence Agency

SECRET



SECRET

2

This document is subject to the Protection of Information Act (Act 84 of 1982) The distribution of information contained in this document is restricted to official institutions of the Republic of South Africa. Permission for deviation from the authorised distribution list should be obtained from the General Manager Intelligence Management Centre, on behalf of the Director-General of the National Intelligence Agency (NIA). After use, which may not exceed a period of six weeks, this document should be destroyed by either burning or shredding. The Head of NIA should be notified accordingly by means of the Declaration of Destruction form attached to the back of this document.

ALJAMERA

SECRET



**GEOPOLITICAL COUNTRY AND INTELLIGENCE ASSESSMENT  
ISRAEL**

**TABLE OF CONTENTS**

1.	Introduction.....	4
2.	Background.....	5
3.	Leading Members of Parliament.....	5
4.	Domestic Situation.....	6
5.	International Relations.....	7
6.	Role of Israel in Africa.....	7
7.	Bi-lateral Relations between SA and Israel.....	8
7.1	History of Relations between SA and Israel.....	8
7.2	Diplomatic Representation in SA.....	10
8.	Israeli Intelligence Community.....	12
8.1	Organogram.....	12
8.2	History/Background.....	12
8.3	Management.....	18
9.	Israeli Intelligence Activities in SA.....	40
10.	Relations between SA and Israel Intelligence.....	43
11.	Current Intelligence Activities in SA.....	46

**ALJAZEERA**



**GEOPOLITICAL COUNTRY AND INTELLIGENCE ASSESSMENT**  
**ISRAEL**

1. **INTRODUCTION**

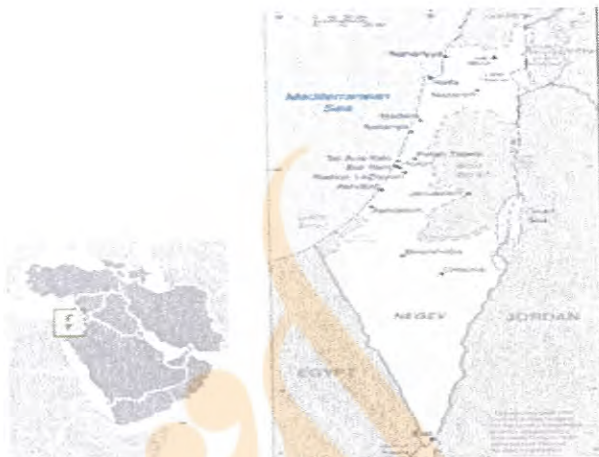
Following World War II, the British withdrew their mandate of Palestine, and the UN partitioned the area into Arab and Jewish states. Rejected by the Arab state, this dispensation led to a succession of wars between the two states and though Israel claimed victory, the deeply rooted tensions between the warring parties are still very much in evidence. The territories that Israel had occupied since the 1967 war are not included in this country profile.

Israel withdrew from Sinai on 25 April 1982, pursuant to the 1979 Israel-Egypt Peace Treaty. In keeping with the framework established at the Madrid Conference in October 1991, bilateral negotiations were conducted between Israeli and Palestinian representatives and Syria to achieve a permanent settlement. Israel and Palestinian officials signed a Declaration of Principles (also known as the "Oslo Accords") on 13 September 1993 guiding an interim period of Palestinian self-rule. The Israel-Jordan Treaty of Peace signed on 26 October 1993 settled unresolved territorial disputes. In addition, on 25 May 2000, Israel withdrew unilaterally from southern Lebanon, which it had occupied since 1982.

Working in conjunction with the EU, UN, and Russia - the "Quartet" -, US President BUSH took the lead in April 2003 in laying the groundwork for a final solution to the conflict by 2005, which would culminate in the establishment of two states, Israel and a democratic Palestine. However, progress toward a permanent status agreement was undermined by Israeli-Palestinian violence between September 2003 and February 2005. An Israeli-Palestinian agreement reached at Sharm al-Sheikh in February 2005 and an internally-brokered Palestinian cease-fire significantly reduced the violence. In the summer of 2005, Israel unilaterally disengaged from the Gaza Strip, evacuating settlers and withdrawing its military while retaining control over most points of entry into the Gaza Strip.

The election of HAMAS in January 2006 to head the Palestinian Legislative Council froze relations between Israel and the Palestinian Authority (PA). Ehud OLMERT became prime minister in March 2006; he shelved plans to unilaterally evacuate from most of the West Bank following an Israeli military operation in Gaza in June-July 2006 and a 34-day conflict with Hezbollah in Lebanon in June-August 2006. OLMERT resumed talks with the PA in June 2007 after HAMAS seized control of the Gaza Strip and PA President Mahmud ABBAS formed a new government without HAMAS. OLMERT resigned in September 2008 in the wake of several corruption allegations, but remained prime minister until the new coalition government under former Prime Minister Binyamin NETANYAHU was formed in late March 2009, after the February general election.





## 2. BACKGROUND

Israel occupied the West Bank, Gaza Strip, Golan Heights, and East Jerusalem as a result of the 1967 War. Pursuant to negotiations between Israel and the Palestinians, the Palestinian Authority (PA) was established in the Gaza Strip and West Bank in 1994. HAMAS, a US-designated terrorist organisation, took control of the Gaza Strip in June 2007 and exercises control in that region. The division of responsibilities and jurisdiction in the West Bank between Israel and the PA is complex and susceptible to change. Palestinian Authority security forces are responsible for maintaining order in areas of the West Bank where the PA exercises a range of civil functions. Definitive information on entry, customs requirements, arrests, and other matters in the West Bank and Gaza is subject to change without prior notice or may not be available.

## 3. LEADING MEMBERS OF GOVERNMENT

	NAME
Prime Minister and Minister of Economic Strategy, of Pensioner Affairs and of Health	Binyamin NETANYAHU ( Likud)
Vice-Prime Minister and Minister for Regional Co-operation and the Development of the Negev and Galilee	Silvan SHALOM (Likud)
Vice-Prime Minister and Minister of Strategic Affairs	Moshe YA'ALON (Likud).
Deputy Prime Minister and Minister of Defence	Ehud BARAK (Labour)
Deputy Prime Minister and Minister of Foreign Affairs	Avigdor LIEBERMAN (Israel Beytenu).
Deputy Prime Minister and Minister of Intelligence and Atomic Energy	Dan MERIDOR (Likud).
Deputy Prime Minister and Minister of the	Eliyahu YISHAI ( Shas)



Interior	
Minister of Finance	Yuval STEINITZ (Likud)
Minister of Communications	Moshe KHLON ( Likud)
Minister of Industry, Trade and Labour	Binyamin BEN-ELIEZER (Labour)
Minister of Religious Services	Yaacov MARGI (Shas)
Minister of Immigrant Absorption	Sofa LANDVER (Israel Beytenu)
Minister of National Infrastructure	Uzi LANDAU (Israel Beytenu)
Minister of Improvement of Government Services	Michael EITAN (Likud)
Minister of Public Safety	Yitzhak AHARONOVITCH (Israel Beytenu)
Minister of Environmental Protection	Gilad ERDAN (Likud)
Minister of Justice	Yaacov NE'EMAN ( Likud)
Minister of Construction and Housing	Ariel ATIAS (Shas)
Minister of Welfare and Social Affairs	Isaac HERZOG (Labour)
Minister of Transport and Road Safety	Yisrael KATZ (Likud)
Minister of Agriculture and Rural Development	Shalom SIMHON (Labour)
Minister of Tourism	Stas MISEZHNIKOV (Israel Beytenu)
Minister of Education	Gideon SA'AR (Likud)
Minister of Science and Technology	Rabbi Daniel HERSHKOWITZ (Jewish Home)
Minister of Culture and Sport	Limor LIVNAT (Likud)
Minister of Minority Affairs	Avishay BRAVERMAN (Labour)
Minister of Public Diplomacy and the Diaspora	Yuli-Yoel EDELSTEIN (Likud).
Ministers without Portfolio	Ze'ev Binyamin BEGIN (Likud), Meshulam NAHARI (Shas), Yossi PELED (Likud)

#### 4. DOMESTIC SITUATION

The State of Israel is a parliamentary democracy with a modern economy. Two main parties hold a similar number of seats in the 120-seat Knesset (parliament), and no single party controls sufficient seats to secure a majority within its own coalition government. The new government headed by the leader of the right-wing Likud party, Binyamin NETANYAHU, is predominantly right-wing but includes the left-wing Labour Party. With 12 parties represented in the Knesset and six in the government, the new coalition will be fragile and unlikely to last its four-year term. This is despite the fact that, in theory, it has a comfortable Knesset majority, controlling 74 seats. The loyalty of some coalition members to the government is weak, with several Labour MPs likely to break away from the party. Moreover, the leader of the second largest coalition party, Yisrael Beiteinu, is facing a possible criminal charge which could affect his party's standing in the coalition. Given internal ideological and personal rivalries, as well as some financial demands from coalition parties, the government will be vulnerable to desertions. The departure of almost any one of Likud's partners could push the coalition below the 60-seat threshold needed for a majority government.



Policymaking is likely to be deadlocked, given the divergent views of coalition members on various issues. This will make it difficult to deal with the most pressing security and economic challenges and may slow efforts to implement measures to counteract the impact of the global economic crisis on Israel's economy. The failure of any one party to gain a significant margin over the others will also impede decision-making, with several politicians vying for influence.

The recent broad consensus on the general direction of economic policy has been tested by the global downturn. Although Mr NETANYAHU was able to introduce policies during his tenure as finance minister in 2003-05 that helped Israel to emerge from recession, the political climate is now more challenging. There is little chance of substantial movement on issues of peace and diplomacy, given the composition of the government, although there is a broader range of views held within the coalition than the election results suggest. International pressure may force even a right-wing government to make modest diplomatic concessions, although this may presage the collapse of the government.

#### 5. INTERNATIONAL RELATIONS

Key foreign policy concerns will be Iran's regional ambitions and the conflict with the Palestinians. Following the incursion into the Gaza Strip, the new Israeli government will seek to improve security by cracking down on Palestinian militants and, reluctantly, by continuing peace talks with Fatah, which governs the West Bank. Despite Mr NETANYAHU's recent concession on Palestinian statehood, substantive progress on peacemaking is unlikely (despite the attempts of the new US administration to re-engage with the issue) given Mr NETANYAHU's right-wing stance, the fragility of his government and the political stalemate within the Palestinian Territories. Both Mr NETANYAHU and his defence minister, Ehud BARAK, will focus increasingly on the strategic threat from a potentially nuclear-armed Iran, but the government is unlikely to agree to an attack on Iran's nuclear installations unless it is certain that weaponisation is imminent and that it has the support of the US. This support is unlikely to be forthcoming, at least in the short term, given the new US administration's greater emphasis on diplomatic engagement with Iran.

The government may make further concessions to the Palestinian president, Mahmoud ABBAS, including prisoner releases, and has removed a few checkpoints and small Jewish settlement outposts in the West Bank. However, much progress beyond these modest steps is unlikely, particularly since Mr NETANYAHU is leaning towards halting settlement expansion completely and keen to push for an "economic peace" rather than the step-by-step process to a two-state solution sought by international mediators. Tensions with Syria could also flare up, although Mr NETANYAHU may seek to reopen indirect peace talks, to try to draw Syria away from Iranian influence and also as a means to deflect attention away from the Palestinian issue. Tensions between Israel and Hizbullah will remain high, but the Lebanese Shia group is unlikely to risk a massive Israeli retaliation by launching an offensive. The US will remain Israel's key strategic ally, despite the increasingly divergent policy stances of both countries.



## 6. ROLE OF ISRAEL IN AFRICA

Israeli foreign minister LIEBERMAN visited 5 African countries in July 2009: the first visit by an Israeli foreign minister in 20 years which was allegedly used, *inter alia*, to lay the groundwork for arms deals. While LIEBERMAN talked with African leaders about hunger, water shortage, malnutrition and plagues afflicting their nations, Tel Aviv's promises to African states could be seen as the gloss on an exercise in cynicism, eg that Israel's military, security, economic and political tentacles have reached every part of Africa behind a philanthropic façade. Africa's 54 nations have rebuffed Israel's diplomatic overtures for decades. Today the NETANYAHU administration believes it stands a chance to breach that wall.

Now, not only are many African nations prepared to thaw their relations with Israel, some have already begun to explore the possibility of strategic cooperation. Tel Aviv fully appreciates the vast potential that Africa offers. In addition to copious natural resources Africa represents strategic depth for the Arab world, for which reason Israel has been allegedly instrumental in arming some African regimes and allegedly aggravating crises among others, including Somalia, Sudan, Eritrea and South Africa.

Israel's concerns in Africa are suspected to be exclusively shaped by its own agenda. LIEBERMAN visiting these countries is thus not only intended to show interest in boosting their economies, enhancing agricultural production, optimising their vast water resources and putting Israeli technological expertise at their disposal. Sudan offers a possible proof of this. Accused by Israeli officials of arming and supporting the Palestinian resistance, Tel Aviv is working assiduously to encircle and isolate Sudan from the outside, and to fuel insurrection inside Sudan.

Israel has long been keen to capitalise on Africa's mineral wealth. It plans to appropriate African diamonds and process them in Israel which is already the world's second largest processor of diamonds. And if the composition of LIEBERMAN's entourage was anything to go by, Israel is also interested in African uranium, thorium and other radioactive elements used to manufacture nuclear fuel. In addition it is looking for new markets for its range of lightweight weapons. It also appears that a few Israeli military pensioners are on the lookout for job opportunities as trainers of African militias, while other members of LIEBERMAN's delegation were facilitating contracts for Israelis to train various militias. The huge oil reserves in a number of African countries are also high on Israel's agenda, with Tel Aviv seeking a share in exploration, extraction and export operations.

Since the 1950s Israel has sought to compromise Egypt's water security by consolidating its influence over countries straddling the sources of the Nile in the central African great lakes and the Ethiopian highlands. By keeping Egypt preoccupied with its water security Israel imagines that it can diminish Cairo's role in the Arab-Israeli conflict. Towards this end Israel's Ministry of Science and Technology conducted extensive experiments and eventually created a type of plant that flourishes on the surface or the banks of the Nile and that absorbs such large quantities of water as to significantly reduce the volume of water that reaches Egypt.



Israeli concerns with Iran also featured high on the agenda of LIEBERMAN's African tour. Israel has been keeping a close eye on the Iranian drive in Africa where Tehran, following Beijing's footsteps, has become involved in a number of major development projects. Tel Aviv is very wary of Tehran's ambitions in a continent so rich in the raw materials for producing nuclear fuel. It hopes to forge a network of strategic relations in order to check the expansion of Iranian influence in Africa. Working to its advantage are its close ties with Washington, which can use its extensive influence in Africa to smooth out many of the bumps that would otherwise hamper Israel's African drive.

## 7. BILATERAL RELATIONS BETWEEN SOUTH AFRICA AND ISRAEL

### 7.1.1 History of Relations

Israel established a Legation in South Africa in 1952 and upgraded it to an Embassy in 1974. In 1972 South Africa established a Consulate General in Tel Aviv which was upgraded to an Embassy in December 1975. Israel continued to enjoy close relations with the Apartheid Government in South Africa. Following the democratic transition in South Africa and the establishment of full diplomatic relations with Palestine, South Africa adopted an approach which favours resolution of the Israeli-Arab conflict through peaceful negotiations, on the basis of the relevant UN Security Council resolutions.

### 7.1.2 Israeli Relations with Apartheid South Africa

In the 1950s and 1960s, Israel prioritised building relations with the newly independent states of sub-Saharan Africa; this, in turn, led it to take a critical stance on the question of apartheid. On 11 October 1961, Israel voted for the General Assembly censure of Eric LOUW's speech defending apartheid. In 1963, Israel informed the United Nations Special Committee on Apartheid that it had taken steps to comply with the military boycott of apartheid South Africa and had recalled its ambassador to South Africa. According to Chris MCGREAL, "Israel was openly critical of apartheid through the 1950s and 60s as it built alliances with post-colonial African governments. In 1971, Israel offered the Organisation of African Unity a gift of \$2,850, which was rejected by the organisation, but not before causing tension between South African Jews and their government.

7.1.3 Most African states broke ties after the 1973 Yom Kippur war and the government in Jerusalem began to take a more benign view of the isolated regime in Pretoria. Ethan A. NADELMANN has claimed that the relationship developed due to the fact that many African countries broke diplomatic ties with Israel during the 70s following the Arab-Israeli wars, causing Israel to deepen relations with other isolated countries.

7.1.4 By the mid 1970s, Israel's relations with South Africa had warmed. In 1975, increasing economic co-operation between Israel and South Africa was reported, including the construction of a major new railway in Israel, and the building of a desalination plant in South Africa. In April 1976 South African Prime Minister John VORSTER was invited to make a state visit, meeting Israeli Prime Minister Yitzhak RABIN. Later in 1976, the 5th Conference of Non-Aligned Nations in Colombo, Sri Lanka, adopted a resolution calling for an oil embargo against France and Israel because of their arms sales to



South Africa. In 1977, South African Foreign Minister Pik BOTHA visited Israel to discuss South African issues with Israeli Prime Minister Menachem BEGIN and Foreign Minister Moshe DAYAN.

- 7.1.5 In 1981, Israeli Defence Minister Ariel SHARON visited South African forces in Namibia for 10 days, later saying that South Africa needed more weapons to fight Soviet infiltration in the region.
- 7.1.6 In 1984, Pik BOTHA again visited Israel but this time only for an unofficial meeting with Israeli Foreign Minister Yitzhak SHAMIR.
- 7.1.7 By 1987 Israel found itself alone among the developed nations in still maintaining strong, even strategic relations with apartheid South Africa (Among African nations, only Malawi maintained diplomatic relations with South Africa throughout the Apartheid era ). On 18 March 1987 the Inner Cabinet of the Israeli government denounced the Apartheid policy of South Africa and limited Israel's security ties with Pretoria. On 16 September 1987 the Israeli Cabinet approved a series of measures designed to limit trade, sports and cultural ties with South Africa. Among them was a clause in the "measures" package stating that effective immediately, only coloured, Indian and black students would be allowed to attend leadership courses held in Israel.

#### 7.1.8 Nuclear Collaboration

US Intelligence believed that Israel participated in South African nuclear research projects and supplied advanced non-nuclear weapons technology to South Africa during the 1970s, while South Africa was developing its own atomic bombs. According to David ALBRIGHT, "Faced with sanctions, South Africa began to organise clandestine procurement networks in Europe and the United States, and it began a long, secret collaboration with Israel." However, he goes on to say "A common question is whether Israel provided South Africa with weapons design assistance, although available evidence argues against significant cooperation." According to the Nuclear Threat Initiative, in 1977 Israel traded 30 grams of tritium in exchange for 50 tons of South African uranium and in the mid-80s assisted with the development of the RSA-3 ballistic missile. Also in 1977, according to foreign press reports, it was suspected that South Africa signed a pact with Israel that included the transfer of military technology and the manufacture of at least six atom bombs.

Chris McGREAL has claimed that "Israel provided expertise and technology that was central to South Africa's development of its nuclear bombs". In 2000, Dieter GERHARDT, Soviet spy and former commander in the South African Navy, claimed that Israel agreed in 1974 to arm eight Jericho II missiles with "special warheads" for South Africa.

#### 7.1.9 Israel Relations with Post-Apartheid South Africa

Former ANC leader Nelson MANDELA first visited Israel in 1999. MANDELA said: "To the many people who have questioned why I came, I say: Israel worked very closely with the apartheid regime. I say: I've made peace with many men who slaughtered our people like animals. Israel cooperated with the apartheid regime, but it did not participate in any atrocities". Then Israeli



SECRET

11

Deputy Prime Minister Ehud OLMERT visited South Africa in 2004, meeting with South African President Thabo MBEKI, the first visit by an Israeli leader since the end of apartheid.

Some prominent South African figures, such as Desmond TUTU and Ronnie KASRILS have criticised Israel's treatment of the Palestinians, drawing parallels between apartheid South Africa and modern-day Israel.

The Congress of South African Trade Unions, which represents 1.2 million South African workers, has also accused Israel of practising apartheid and supported the boycott of the Canadian Union of Public Employees, as well as all Israeli products.

However, South African ambassador to Israel Major General Fumanekile GQIBA generally did not agree with the analogy, saying about his time in Israel *"Before I came here. I regarded Jews as whites. Purely whites. But when I came here I discovered that, no, these guys are not purely whites. ... You've got Indian Jews, you've got African Jews, and you've got even Chinese Jews, right? I began to say to our comrades, No, Israel is not a white country. ... Perhaps we would say there are those who came from Poland, who happened to be, white- ie Ashkenazi their culture still dominates. It's difficult to say Israel is racist, in a classic sense."*

Malcolm HEDDING, a minister who railed against apartheid during its time, currently Executive Director of the International Christian Embassy Jerusalem, says *"Calling Israel an 'apartheid state' is absolute nonsense. You might have structures that look like apartheid, but they're not. The barrier fence has nothing to do with apartheid and everything to do with Israel's self-defence. There was no such barrier until the second intifada, when people were being murdered on the highways. And the country does not dehumanise its minority in the sense of apartheid. The issues are totally different."* HEDDING believes Israel has more than proven its desire to reach an accommodation with the Palestinians, while granting political rights to its own Arab citizens within a liberal democratic system. Nevertheless, the Palestinians remain committed to Israel's destruction. By contrast, he says, it was a tiny minority in South Africa that held power and once democracy came, the National Party that had dominated the masses disappeared.

South Africa is an advocate of the two-state solution. In 2004 South African Deputy Foreign Minister Aziz PAHAD criticised Israel's building of the Israeli West Bank barrier.

Annual trade between Israel and South Africa totalled \$500 million USD as of 2003.

According to the Pew Global Attitudes Project in 2007 the vast majority of South Africans were indifferent to the Israeli-Palestinian conflict. Of those with opinions on the matter, the majority sympathized more with Israel: 28 per cent of South Africans overall sided with Israel compared to 19 per cent with the Palestinians.

SECRET



SECRET

12

7.2 **Diplomatic Representation**

7.2.1 **South African Representation in Israel**

H E Mr I COOVADIA  
Ambassador Extraordinary and Plenipotentiary

**South African Embassy**

Office hours  
Mon-Thurs: 07:00-16:00  
Friday: 07:00-12:00

7.2.2 **Israeli Representation in South Africa**

H E Mr D SEGEV-STEINBERG  
Ambassador Extraordinary and Plenipotentiary

7.2.3 **Embassy of Israel**

**Israel (State of)**  
*(Embassy of the State of)*

Pretoria  
428 King's Highway cor.  
Elizabeth Grove Street  
Lynwood

Postal Add:  
Private Bag x 50  
Menlo Park  
0102

Tel: 012 470 3500  
Fax: 012 470 3555

**Consular Department**

Tel: 012 470 3511  
Tel: 012 470 3542/3  
Fax: 012 470 3561

E-mail:  
cao-sec@pretoria.mfa.gov.il

Web:  
<http://pretoria.mfa.gov.il>

Ambassador Extraordinary & Plenipotentiary - H  
E Mr D Segev-Steinberg

Second Secretary (Admin & Consular) - S  
Dadon

Second Secretary (Political) - Mr E Inbram  
Second Secretary (Chief Security Officer) - A  
Almog

Attaché - G Sabah  
Attaché - E Maimon

Attaché - R Efodi  
\*Attaché (Police & Public Security) - A L Granit  
(Ms)

Defence & Armed Forces Attache (Non  
Resident) - Col. E Shermeister

Trade Office  
Johannesburg  
Trade Office  
Marsh Building (PTY) Ltd,  
No 4 Sandown Valley Crescent,

First Secretary (Economic Affairs) - O R Pearl

\*non-resident

SECRET



Third Floor,  
Sandton, 2196

Tel : 011 506 5000  
Fax : 011 506 5241  
E-mail : pearl@moital.gov.il  
National Day varies annually

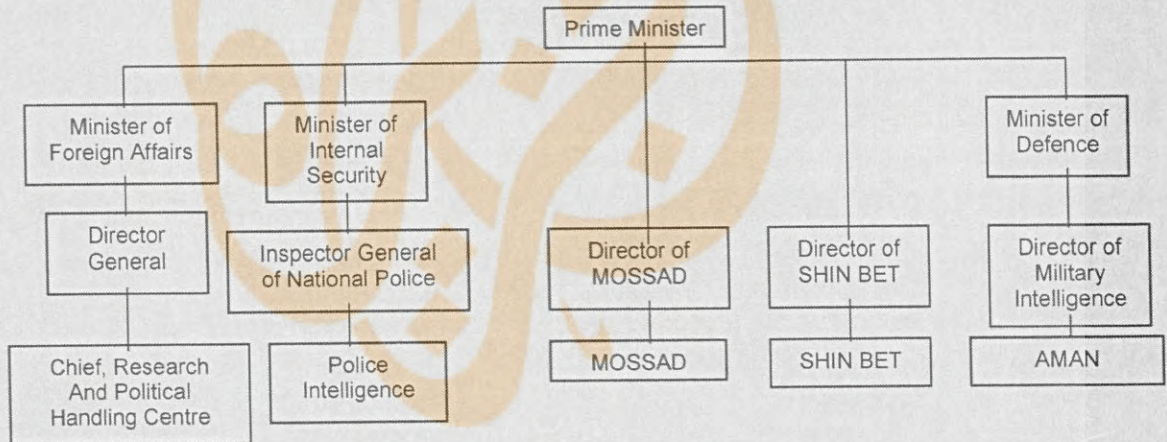
#### 7.2.4 Travel Info

##### Visa Requirements for South Africans

Visas are not required for South African passport holders not intending to stay for more than three months. Persons holding temporary or emergency passports are excluded and it is imperative for persons with such travel documents to obtain visas prior to departure.

### 8. ISRAELI INTELLIGENCE COMMUNITY

#### 8.1 Organogram of Israeli intelligence and security community (1997)



#### 8.2 History/Background of the Mossad

8.2.1 The first Israeli intelligence service was Shai (Information Service), the intelligence arm of the underground, pre-independence army of Palestine's Jews known as the Haganah, which means Defence. Haganah was swallowed up by the Israel Defence Forces with the birth of the state of Israel. A new intelligence community was created consisting of four intelligence agencies: military intelligence (called the Intelligence Department of the army), a domestic secret service (known as Shin Bet), a foreign intelligence service, the foreign ministry's Political Department, Varash, and The Institute for Aliyah B responsible for smuggling Jews to Israel.



The founder of Shai, Reuven SHILOAH, became the special adviser to the Prime Minister on foreign affairs and broad strategy. Israeli intelligence was based on his views: clear identification of enemies, the comprehensive collection of information about them, and the perpetual search for allies. He defined the secret side of Israeli diplomacy and foreign policy:

- "Enemy number one of the Jewish community was the Arab people, and Arab society had to be penetrated by professional agents.
- Israel intelligence also had to think beyond Palestine, as a "Jewish-Zionist" protector of Jews throughout the world.
- Clandestine work should be based on modern technology, keeping up with the latest in espionage methods by maintaining ties with friendly agencies in Europe and the United States."

Overlapping of functions led to restructuring that included the formation of the Mossad that was directly subservient to the Prime Minister. All responsibility for special assignments was transferred to Aman, the military intelligence agency. The agency established a top secret "Unit 131" to plant agents in Arab countries. When Mossad was created it did not have an operations department. All it did was take part in a joint committee with Aman, to oversee the use of Unit 131. Otherwise the Mossad's function was to collect facts.

In late 1950s an Aman agent committed murder in Argentina and lead to restructuring. Responsibility for operations in Arab countries remained in the hands of military intelligence, but Mossad was permitted an operations department with responsibility for the rest of the world. In the initial years it was available to both the Mossad and Shin Bet. His agents began running all over the world: London, Paris, Geneva, Rome, Antwerp, Johannesburg and New York.

The Israeli intelligence community is a synthesis of various traditions that were learned, adopted, inherited or copied from other countries, especially Britain, France, United States and the former Soviet Union.

The current Israeli Intelligence Community includes the following organisations:

- Aman: the supreme military intelligence branch of the Israeli Defence Forces
- Mossad: the agency responsible primarily for overseas intelligence work
- Shabak (Shin Bet): the organisation responsible for internal security, including in the Israeli-occupied territories
- The intelligence branch of the Israeli Police
- The Centre for Political Research: the intelligence branch of the Ministry of Foreign Affairs

#### **Former Foreign Intel Agencies**

- Aliyah B was disbanded in March 1952. During its time Aliyah B was a huge organisation involved in the global conveyance of its people. Built around a massive undercover travel agency, Aliyah B owned over sixty ships and airplanes and countless cars and trucks. Their movements were well coordinated by a world-wide network of quasi-legal radio transmitters. The agency helped hundreds of thousands of Jews make their way to Israel. Aliyah B's budget was in the tens of millions of dollars, a sum so impressive that it had genuine economic impact in some of the



SECRET

15

port areas of war-ravaged Europe, so extensive was the system of bribes paid to policemen, port officials, government functionaries, and ship owners. Israel's agents distinguished themselves in the black markets of France, Greece, Italy, Austria and other countries. Some of its planes became the first El Al airliners. Its vessels helped form the core of Israel's national shipping company, Zim. Aliyah B also had some of Israel's finest forgers and field agents, whom the Mossad put to good use.

- Nativ: the organisation responsible for bringing Jews from Soviet Bloc countries, a later manifestation of the Mossad Le'aliyah Bet. Following the dissolution of the Soviet Union, it was moved out of the intelligence community and became a department within the Prime Minister's office.

Lekem @ Lakam @ Lakem: the technological agency responsible for the security of Israel's nuclear project as well as locating and purchasing parts and materials for Israel's nuclear reactor at Dimona. It was also responsible for open and covert collection of scientific and technical information. The agency's personnel were sent abroad as science attachés in Israeli embassies in Europe and the United States. It was disbanded after the American Jonathan POLLARD, who was run by Lakam, was convicted of spying. Some sources assert that open and covert collection of scientific and technical information formerly conducted by Lekem is now conducted by a unit of the Ministry of Foreign Affairs.

For years various committees tried to resolve disputes about the division of responsibilities and jurisdictions between Aman, Shabak, and Mossad. In a document known as the "Magna Carta," the heads of the three services continue their attempt to arrive at agreements regarding these. According to Magna Carta the directors of Aman and Shin Bet agreed to transfer internal security tasks within the West Bank and Gaza, now under the administrative control of Palestinian Authority, from Shin Bet to Aman officials. Shin Bet had dealt with internal security functions in these areas for over thirty years. Further, Aman reportedly agreed to transfer its Unit 504 that controls its covert agents to Mossad, while Mossad acknowledged the control over signals intelligence collection by Aman's Unit 8200. These changes in responsibilities are intended to avoid duplication in effort.

Shabak (Shin Bet) conducts counterintelligence and internal security operations for the Israeli intelligence community. Shabak is regulated by the Law on General Security Service of February 2002. The agency focuses on domestic and regional intelligence operations, but maintains a network of personnel worldwide.

Three internal departments aid Shabak operations. The Arab Affairs Department maintains information on Arab terrorist networks, and conducts anti-terrorism operations. The Non-Arab Affairs department concerns itself with other nations, with special attention paid to Russia and Eastern Europe. Both agencies operate within Israel and abroad. The third Shabak department, Protective Security, is responsible for the protection of Israeli diplomatic missions abroad, as well as internal security at military, government, industrial, and scientific installations within Israel's borders.

Shabak is also a political espionage agency. The agency monitors extremist political groups. Scrutiny and surveillance of the political associations of

SECRET



foreigners living within Israel is an additional routine Shabak activity. The agency also possesses the authority to arrest and detain persons suspected of anti-government activity.

#### 8.2.2 Aman

The Directorate of Military Intelligence (Aman) is Israel's central, overarching military intelligence in the Israel Defence Forces. Aman collates, processes, and disseminates military intelligence information, as well as coordinates interagency operations. The agency produces reports for military and government use. Aman, produces comprehensive national intelligence estimates for the prime minister and cabinet, daily intelligence reports, risk of war estimates, target studies on nearby Arab countries, and communications intercepts. Aman acts as liaison between the military and government, coordinates the flow of information between civilian and military intelligence agencies, conducts cross-border agent operations and assesses the threat of war.

##### Staff units

- The Intelligence Corps
- The Collection Department (responsible for the humint running of agents and informers just over the borders, for sigint radio interceptions and often for plugging into the telephone systems of Arab countries to eavesdrop and record landline conversations.

##### Collection units

- Unit 8200
- The Hatzav Unit
- The Visual Intelligence Branch
- The Mapping Unit
- The HUMINT Branch

##### Research

- The Research Department
- Information security
- The Information Security Department
- The Military Censor *[Part of Aman, but an entirely independent unit, not subordinate to any military or political level, only to parliamentary and judicial oversight]*

##### Other units

- The Supervision Department
- The External Relations Department is the agency liaison with foreign military commanders and military intelligence services.

The Sayeret Maktal, or Deep Reconnaissance Unit, conducts counter-terrorism operations.

##### Professionally subordinate units

- Air Intelligence Directorate: the intelligence unit of the Israeli Air Force



- Naval Intelligence Department: the intelligence unit of the Israeli Sea Corps
- Field Intelligence Corps: the intelligence unit of GOC Army Headquarters
- The intelligence units of the Regional Commands: Central, Northern, Southern and Home Front Commands

Production Department: largest with the task to receive and analyse the information that has been collected. They are organised into desks and are divided along geographical and functional lines: the Western area for Egypt, Sudan and Libya, the Eastern for Iraq, Syria and Lebanon; a separate desk for Jordan and Arabic Peninsula; a Palestinian desk to track guerilla groups; analysts of inter-Arab relations and a desk for Middle East economic. There is a tiny Research and Development Department that devises hardware and software to help in the collection of intelligence. Aman is also responsible for sending military attaches to Israel's overseas embassies.

A number of electronic intelligence collection and observation facilities are located on the Golan Heights, including a facility at Har Avital which monitors Syria, and another at Mount Hermon which monitors both Lebanon and Syria.

### 8.2.3 MOSSAD

The Institute for Intelligence and Special Operations), often referred to as The Mossad (meaning The Institute), is Israel's foreign intelligence agency. Mossad was created by instruction of Prime Minister David BEN-GURION placing it under the Foreign Ministry. Besides the above instruction there is no legislation to regulate the activities of the Mossad.

Reuven SHILOHA made certain to establish working relationships with foreign intelligence agencies, especially the CIA. He set up an economic intelligence unit, which looked for loopholes around and poked holes through the Arab embargo against trade with Israel. He also emphasized the need for Israel to have close and trusting relationship with Jews around the world.

Over the years, the Mossad has expanded into many fields, the most prominent of which are:

- Covert intelligence collection beyond Israel's borders.
- Preventing the development and procurement of non-conventional weapons by hostile countries.
- Preventing terrorist acts against Israeli targets abroad.
- Developing and maintaining special diplomatic and other covert relations.
- Bringing Jews home from countries where official Aliya agencies are not allowed to operate.
- Producing strategic, political and operational intelligence.
- Planning and carrying out special operations beyond Israel's borders.

Mossad's original motto: "For by wise counsel thou shalt make thy war" (Proverbs XXIV: 6) The less accurate but more recognised translation "By way of deception thou shalt make war" was changed recently as part of the Mossad's public 'coming out' to another Proverbs passage: "Where no counsel is, the people fall, but in the multitude of counsellors there is safety." (Proverbs XI: 14).



## Departments:

In addition to numerous specialised forces, the Mossad maintains eight operational divisions.

- Collections Department is the largest, with responsibility for espionage operations, with offices abroad under both diplomatic and unofficial cover. The Mossad has a virtual monopoly on the collection of intelligence outside Israel, with the exception of certain military targets – usually not far from Israel's borders on which Aman may spy. The department consists of a number of desks organised on both regional and functional bases, and they are highly specialised, directing case officers based at "stations" around the world, and the agents they control. Their field intelligence officers, called katsas, are similar to case officers of the CIA. Thirty to forty operate at a time. The katsas are organised in a division known as Tsomet (intersection) or Melucha (kingdom). The katsas are responsible for recruiting human intelligence (moles and snitches) in foreign countries.

They are further split into three geographic branches:

- Isarelis Branch: Includes the Middle East, North Africa, Spain, and the 'jumper' katsas who move between operations.
  - Branch B: Covers Germany, Austria, and Italy.
  - Branch C: Covers England, France, Low Countries, and Scandinavia.
- Political Action and Liaison Department called Tevel, conducts political activities and liaison with friendly foreign intelligence services and with nations with which Israel does not have normal diplomatic relations. In larger stations, such as Paris, Mossad customarily has under embassy cover two regional controllers: one to serve the Collections Department and the other the Political Action and Liaison Department. It coordinates Mossad activities and shares information with allied nations.

Apart from intelligence sharing with friendly foreign services, the division's most important jobs are to develop joint projects targeting terrorist groups and rogue regimes, and to provide a karit-raka, or "soft landing", should any of Mossad's operatives get in trouble while on unilateral operations in a friendly country. Tevel also acts as a sort of 'shadow' foreign ministry by maintaining covert quasi-diplomatic relations with the governments of nations normally considered hostile to Israel, such as Indonesia and the Arab Gulf countries. It also maintains relations with stateless groups, such as the Kurds in northern Iraq. Tevel also arranges training courses and seminars to allied services on subjects of Israeli expertise, such as dealing with Islamic terror. India, in particular, has benefitted enormously from the counterterrorism training it has received through Tevel.

The desks are organised on both regional and functional bases, and they are highly specialised. The various departments include Far East, Western Europe, "A" (northern Europe, including Germany, France and the UK), Western Europe "B" (southern Europe including Italy, Spain and Greece), Eastern Europe, North America, Africa, Americas and another department that maintains covert intelligence ties with Muslim countries. Tevel brings in about 70% of intelligence Mossad receives; the head of the Tevel foreign liaison department is Itzik Barzilai.



- Special Operations Division, also known as Metsada or Caesarea (also called Kesaria and Komemiute) conducts highly sensitive assassination, sabotage, paramilitary, and psychological warfare projects. Metsada is responsible for running Mossad's most secret agents, known as "combatants" (Lohamim in Hebrew). These are Jewish people, usually of Arab origins and Arabic speaking, who are sent under "borrowed identities" to conduct special operations in "target countries" - "the most hostile Arab countries". Jews with European features and accents are also placed under deep cover usually in Europe from where they operate into Arab countries. Kidon (Hebrew: "bayonet") is the name of a department that is responsible for assassination and kidnapping. The Massada unit, "together with Kidon are regarded as the 'holy of the holies'" in the Mossad. [Aaron Klein.Politiek in Israel Plaats van misdaad 28-09-2007
- LAP (Lohamah Psichlogit) Department is responsible for psychological warfare, propaganda and deception operations. The department had built up a global network of media contacts and used them with great skills giving info to give stories the spin LAP wanted. The unit also created information for press attaches at Israeli embassies to pass on to a journalist.
- Research Department is responsible for intelligence production, including daily situation reports, weekly summaries and detailed monthly reports. The Department has 15 sections or desks targeting Arab states. The US, Canada, Latin America, Britain, Europe and Russia all had separate desks expanding over years to include China, South Africa, and the Vatican.[ Gideon's Spies. The secret history of the Mossad. Gordon Thomas. New York: St Martins.1999] it also includes the Maghreb (Morocco, Algeria, Tunisia), Libya, Iraq, Jordan, Syria, Saudi Arabia, the United Arab Emirates and Iran. A "nuclear" desk which specialises solely in nuclear developments around the world.
- Technology Department is responsible for development of advanced technologies for support of Mossad operations. Agents trained in computers and engineering staff the Technology Department. The department extracts data from stolen, damaged, or foreign information systems, while ensuring the security of Mossad systems. In April 2001, the Mossad published a "help wanted" ad in the Israeli press seeking electronics engineers and computer scientists for this department.

Later publications also mention other units within Mossad such as:

Bitsur was involved in counterterrorism operations in Southeast Asia and Africa. Bitsur was mandated with recruiting locally based assets (helpers who are either recruited or inherited by predecessors) to provide intelligence, background information, and logistical support, conducting covert operations and helping out other overstretched operational divisions. One of its primary missions was helping Jews in countries where they faced persecution. It is for example Bitsur that helped secretly ex-filtrate Israel's immigrants from North Africa, Syria, Lebanon, Iraq, Iran, Yemen and Ethiopia. This unit made use of jumpers.

A counterproliferation unit that was responsible for operations to counter the proliferation of weapons of mass destruction to countries and organisations of concern to Israel.



#### 8.2.4 Neviot

The Neviot department is the specialist surveillance unit in the agency which collects intelligence for Mossad through the medium of break-ins, street surveillance, installation of listening devices and other covert methods.

The latest director has since restructured Mossad into two halves, an operational directorate and headquarters directorate ("H") responsible for non-operational units and long-term planning). The division of the above old directorates within the new structure is not clear.

Mossad was established in 1951 by the then Prime Minister, BEN-GURION. The Mossad was established as a result of the Jews' dire struggle for an own homeland/ state of Israel. The predecessor of the current organisation was already established in 1937 by Haganah (the Jewish liberation organisation). It was known as the Mossad Le Aliya Beth (Institution for Intelligence and Special Services). The name MOSSAD (Institution) was retained.

Initially the Mossad was responsible for aiding and facilitating the large-scale illegal immigration to Palestine. The Mossad's task was later extended to include espionage activities abroad, the obtaining of armaments and related technologies and counter-espionage.

Up until 1942, the Mossad resorted under the leadership of first Eliahu GOLOMB and after that, Shaul AVIGUR, but David BEN-GURION, leader of Haganah and later Prime Minister of Israel, still had a leading role to play in the Mossad.

Other organisations were, however also involved in intelligence, namely:

REKESH was established by Haganah in order to obtain weaponry and other supplies for the organisation. This effort required the launch of clandestine operations on an international scale.

Shin Bet - especially after 1948 - BEN-GURION paid special attention to this organisation and the development thereof.

In 1951 after Israel's war of independence, BEN-GURION united the above-mentioned three organisations under the command of a single head - Isser HAREL.

With the passage of time and due to personality clashes as well as enmity and clashes among the organisations themselves (due inter alia to each one's individual and specific needs), three intelligence services came into being, namely the Mossad (foreign intelligence service), the Shin-Beth (domestic security service) and the Aman (military intelligence service). These services form the current Israeli intelligence community of Israel.

Due to clashes between the Mossad and AMAN, Prime Minister BEN-GURION established a joint intelligence committee with the head of the Mossad as the ex-officio chairman. The head of the Mossad then became known as the "father figure" of the intelligence community, a title which has ever since been "awarded" to every head of the Mossad.



A former head of the Mossad, Mr Nahum ADMONI, made history with his 1982 appointment in the intelligence community. He is the first member of the Mossad to be appointed head of the Mossad from within the ranks of the organisation itself. Prior to the appointment of Mr ADMONI it was considered an unwritten rule that the Head of the Mossad would be appointed from outside the ranks of the intelligence community.

### 8.3 Management

- 8.3.1 **Director:** The head of Mossad is the Director. The current director is Meir DAGAN. He was appointed in 2002 and his term was extended in 2007.

Meir Dagan unexpectedly broke with Israel's official line in mid-June 2009 by announcing that Iran would have a nuclear bomb in 2014 rather than in 2010 as numerous Israeli government officials have claimed up until now. Dagan's statement, which came as supporters of Mir Hossein MOUSSAVI demonstrated in Tehran, weakened the position of prime minister Binyamin NETANYAHU vis a vis the United States. Claiming the threat to be imminent, NETANYAHU wants to persuade the US to attack Iran before any resumption of the Middle East peace process. In making common cause with CIA analysts on Iran's nuclear bomb, DAGAN pulled the rug from under NETANYAHU's feet. NETANYAHU plans to replace Dagan at the end of 2010.



### 8.3.2 Personnel

From its headquarters on the Gelliloth intersection, on Highway 1, between Tel Aviv and Hertzlia, the Mossad oversees a staff estimated at between 1200 to 1 500 personnel, although it may have numbered up to 2 000 in the late 1980s. The Mossad is a civilian service, and does not use military ranks, although most of its staff have served in the Israel Defence Forces as part of Israel's compulsory draft system, and many of them are officers.

Meir DAGAN, nicknamed *the gun*, was born in Russia. He is a retired general and expert in counterterrorism. He was adviser on terrorism to the prime ministers Ehud BARAK and Binyamin NETANYAHU. He has also undertaken extremely sensitive diplomatic missions for them. During his 32-year military career he commanded intelligence units in southern Lebanon and directed infiltration operations on the West Bank. DAGAN was for some time engaged in private business activity. He specialised in security consulting and provided intermediary services in the arms and special technical equipment market. He was successful in several countries of Southeast Asia, Russia and Africa.

*Intelligence Online no 437, 26 September 2002.*

### 8.3.3 Recruitment

In the past, the Mossad recruited almost exclusively through word of mouth and front companies that screened potential applicants at generic offices set up around Israel and the world. Moreover, the Mossad even set up false foreign intelligence agencies – staffed by men and women from Denmark, Turkey or Spain for instance – to recruit and give assignments to newly "hired" Israeli agents taken in from the cold. Agents who refused to carry out fake "spying assignments" against their own nation were quickly promoted by the Mossad, having passed the test of loyalty.



SECRET

22

The Mossad has substantially opened up the recruitment process since 2001. The agency features ads on government websites and in various national newspapers.

In July 2007, Mossad published a job vacancy ad in several Israeli newspapers: "A governmental institution is recruiting people who speak Persian for an interesting and highly challenging job. The applicants will speak Persian as their mother tongue and be ready to make a long-term engagement. In recruiting Persian speakers, Mossad is intent on keeping on top of the Iranian issue.

#### 8.3.4 HUMINT

During 1963-1968 Mossad Director Meir AMIT turned HUMINT into an art form. He resisted attempts to turn Mossad into a version of CIA or KGB who employ thousands. He insisted on permanent appointing a staff of 1200 handpicked and multiple skill staff. A scientist must be able to work in the field if the need arises, a katsa must be able to use his specialist skills to train others.

Salaries paid to employees were in line with those paid to ordinary civil servants in Israel, but approximately doubled for operatives on foreign assignments. Those who worked in Support division were also eligible to enjoy benefit of overseas trips. From time to time, technicians, mechanics or secretaries were sent abroad on missions that did not require special skill, such as acting as couriers or for guard duty. In return, Harel demanded total loyalty and commitment.

#### 8.3.5 Katsas

A katsa is a field intelligence officer of the Mossad. He collects information and runs agents, similar to the case officer of the CIA. Katsas are organised under the Mossad Head of Operations, in a division known as Tsomet (intersection) or Melucha (kingdom). There are typically 30-40 katsas at a time, operating mainly in Europe and somewhat in the Middle East. They have operated to a lesser degree in Africa and Asia. Some sources also suggest that they have had a presence in the United States. Most of the information being gathered for Israel is on the Arab world. Because it is more difficult to operate in Arab countries, Mossad recruits many of its agents in Europe. While some katsas are stationed permanently in foreign countries, others are moved among operations, hence their nickname 'jumpers'. The jumpers (or hoppers) work from the Israel Station, or local station, which handles countries it considers dangerous to operate in including Cyprus, Egypt, Greece and Turkey. They travel back and forth for a few days at a time, to recruit, operate the agents and the sayanim and run operations.

Attack case officer: A case officer who has the ability to make fast contact with a target and proceed quickly with recruiting him to work as an agent for the Mossad. Once the person has been recruited, the attack case officer will transfer the everyday running of the agent to a regular case officer and start a new recruiting operation elsewhere. Attack case officers within Mossad number about five men at the most, and are usually stationed in The Mossad European headquarters in Brussels.

SECRET



AMIT's rules for selecting katsas were:

- No katsa is accepted who is primarily motivated by money.
- The overly zealous Zionist has no place in this work.
- The job calls for calm, clear, farsighted judgement and a balanced outlook.
- Unacceptable reasons for joining were: glamour, idea of adventure, enhancement of one's status or belief that being in the Mossad would give them secret powers.

Traits of katsas:

Aptitude for languages

Good at filling gaps in case study drawing fact out of speculation and know limits of informed conjecture. Natural manipulator of people, can persuade, cajole, and if all else fail, threaten.

Female katsas (Bat laveyha):

For many years women have worked in the Mossad, in military intelligence and on special missions. Alone she usually provokes less suspicion. If she works with a male colleague, it is believed that an apparently married or courting couple attracts less attention than single men in a surveillance operation. The Mossad does send women into action for purposes of sexual entrapment, but reluctantly. First, intelligence chiefs prefer to use single women for entrapment. Secondly, they are almost always used in this way only once. While there is no pressure on female agents to exploit their gender, it is expected of them to use sex as one of many weapons in their field. If sexual blackmail or entrapment is an integral part of the mission, however, Mossad often employs actual prostitutes. It is said to be common practice when debriefing Arab informants run by either Mossad or Aman to reward them with prostitutes afterwards. Their activities are occasionally photographed for potential blackmail leverage to ensure the Arab agents' loyalty in the future.

There is less hesitation in sending Mossad men abroad to befriend and usually to become intimate with an international array of embassy secretaries and airline stewardesses, for they can provide much valuable information about the diplomats, airports and cities of the Arab world.

### Combatants

Kememiute (Metsada) operates almost like a Mossad within the Mossad, a highly secretive department that handles the combatants, regarded as the real spies working under deep cover.

The combatants work closely together in pairs. One is a target-country combatant, his partner a base-country combatant. They do not spy inside friendly countries like England, but may operate a business together there. When needed, the target-country combatant operates using the company as cover, while the partner combatant acts as his lifeline and gives whatever support is needed.

Combatants' role has changed over the years as Israel itself has evolved. At one time the Mossad had people working for long periods of time in Arab countries, but often they were too long there and got burned. In the early days many Jews came from Arab countries and there were no shortage of people



SECRET

24

who could pass as Arabs. This is no longer true, and Arabic learned in school is not considered suitable for deep cover.

Now most combatants pose as Europeans. They usually sign up for a four-year stint. It is crucial for cover that they have an actual business that will allow them to travel at any time on short notice. The business usually deals in export import sales. About 70% of the base-country businesses are in Canada.

The combatants' only contact with the office is through their case officer/controller. Controllers are the unit's representatives who operate under diplomatic cover overseas and act as intermediaries between the Office and the combatant in the field. They are usually on official Israeli documents and have access to diplomatic missions. Controllers convey the details of missions, bring funds, provide directions as per HQ commands, and are the combatant's only contact with the 'real' world outside of cover. Each controller usually operates four or five sets of combatants.

An example of a combatant is the case of Michael ROSS a Canadian who operated as a combatant in Europe. The Mossad created for him a new identity which had to be developed into a "three-dimensional persona". He devised plans to live undercover in a European nation for an extended period and had to study history, culture, literature, language and regional idioms of the area.

When he was ready for deployment, the Mossad drew up an operational order for deployment, known as a pakam. It contains all relevant details about timing, codes, and itinerary documents to be used. There is also a section called Mikrim v'Tguvot (occurrences and reactions) designed to set out expected responses to contingencies that may arise.

When he arrived in Europe, he met his Caesarea controller at a café where they discussed his pakam. He gave ROSS money and took his travelling Israeli passport (an alias) in exchange for ROSS's foreign operational papers.

ROSS established himself as a respectable commodities broker. He kept office in Switzerland as his business address, and even hired someone to answer the phone in the name of the cover company he devised. He received a clothing budget as his clothing had to match the social standing of a successful businessman.

He rented a suitable apartment. Combatants select their apartments with care. Multiunit buildings in upscale areas, far from prying eyes, are preferred. So are buildings with plenty of exits and a secure main entrance equipped with a camera and coded entry. Such precautions are aimed as much at thwarting common criminals as rival intelligence agents. Combatants often find themselves carrying large amounts of cash (Credit cards are eschewed where possible because they leave a paper trail).

He opened a bank account, joined a gym and followed the local sports team. He also had to form opinions about the country's politics and become a regular at bars and restaurants. He had to make sure that all relationships would be superficial. He had to become known without being known about. After establishing his cover in Europe in just two months, ROSS went back to Israel to receive his next assignment.

SECRET



Back in Europe he met his combatant partner, Charles. Combatants do not know the real names of those with whom they work, where they live, or if they are married or have children. The idea is that the more a Mossad agent knows, the more he will tell Israel's enemies under interrogation. ROSS and Charles both had their own companies in Europe. It was not mentioned whether it was in the same country or not. They carried out operations in various places like Tunisia, Casablanca, Iran, Khartoum and Turkey.

#### **Kidon**

There is a small internal unit within Metsada called Kidon or "bayonet". They are the assassins, called "the long arm of Israeli justice". Their average age is in mid twenties. Normally there are two such teams training in Israel and one out on an operation abroad. They know nothing about the rest of the Mossad and do not know each other's real names. They are divided into three teams of about 12 men each.

According to Thomas (2007: 468) DAGAN increased the kidon number from 48 to 60, eight of them women. Kidon are fluent in Arabic and major European languages, eg English, Spanish and French. Some are even proficient in Chinese.

They are able to use any type of weapon and have access to an arsenal of guns: short-barrel pistols, sniper rifles with a mile killing range, long and short-blade knives, piano wire to strangle, explosives no bigger than a throat lozenge capable of blowing off a person's head and a laboratory of poisons, sealed in vials.

#### **Bodels**

Bodels act as couriers between the Mossad headquarters and Israeli embassies from where katsas operate under diplomatic cover. They carry documents in diplomatic pouches and deliver packages from the Mossad station in the embassy to the safe houses and back. Bodels are usually fresh out of an elite military unit where they receive special anti-surveillance training.

#### **Sayanim**

Meir AMMIT realised that katsas would need support in the field. He created the sayanim, volunteer Jewish helpers. Sayanim are Jews living outside Israel as foreign citizens that volunteer to provide assistance to the Mossad or are often recruited by relatives living in Israel.

Sayanim fulfil many functions. This assistance includes facilitating medical care, money, logistics, and even overt intelligence collection. Station Katsas are in charge of the sayanim, and most active sayanim will be visited by a katsa once every three months or so, which for the katsa usually means between two and four face-to-face meetings a day with sayanim, along with numerous telephone conversations. Sayanim also collect technical data and all kinds of overt intelligence: a rumour at a cocktail party, an item on the radio, paragraph in newspaper, and provide leads for katsas.

The idea is to have a pool of people available when needed who can provide services but will keep quiet about them out of loyalty to the cause. Suppose



SECRET

26

during an operation a katsa suddenly had to come up with an electronics store as a cover. A call to a sayan in that business could bring 50 television sets, 200 VCRs, whatever was needed, from his warehouse for the cover business. There are also address and telephone sayanim. If a katsa has to give out an address or a phone number, he can use the sayan's. And if the sayan gets a letter or a phone call, he will know immediately how to proceed. Sayanim only receive expenses for their services. They are never put at risk nor are they privy to classified information. No official number is known, but estimates put the number of sayanim in the thousands. In 1998 there were over 4 000 sayanim in the United Kingdom (UK).

### Agents

The Mossad likes to recruit personnel who serve in foreign embassies around the world, especially Europe, students studying abroad and military people. Since the Mossad has no time to develop talent in the hope that people will get into a position where they can provide information, but rather want people already in that situation, the targets are fairly easy to identify.

White agents: non-Arabs recruited, either by covert or direct means who may or may not know they are working for Israel.

Black agents: Arabs.

White agents are usually less risky to deal with than black agents. Arabs working abroad are very likely to be subjected to security by Arab intelligence and if they catch a katsa working with one as a black agent, they will want to kill him. The worst thing of a katsa being caught working with a white agent in France for example is deportation, while the white agent himself could be charged with treason.

According to overt information people make the mistake of thinking the Mossad is at a disadvantage for not having stations in obvious target countries. The Mossad however obtains information about them and recruits agents in other areas like Europe. Most Arab countries do not manufacture their own weapons. Most lack high-level military colleges, for example. If the Mossad wants to recruit a Syrian diplomat, katsas do not have to do that in Damascus. They can do it in Paris. If they want data on an Arab missile, they get that in Paris or London or the United States where it is made. And if they want to get to the senior officers, they recruit or collect on them while they are studying in England or the United States. Their pilots train in England, France, and the United States. Their commandos train in Italy and France. The Mossad attempts to recruit them there because it is easier and less dangerous.

The LAP department assists in the recruiting of agents with psycho profiling of the targets that will assist in discovering vulnerability and advice what is the best way to recruit a person. A favourite opening gambit for Mossad recruiters on a cold-approach operation is that they work for a company that was forever looking for ways to update its database and would pay good money to those who could help do so. A cold approach requires a real finesse. Move too quickly and the fish is off the hook. Take too long and suspicion is soon coupled with fear. Recruiting is an art all by itself and a European is different from hooking an Arab on the West Bank or Gaza Strip.

SECRET



The Mossad also uses false-flag recruiting. They used that method for example to recruit Jack Leon THOMAS, an Armenian who grew up in Cairo and worked for Israeli intelligence in Egypt without at first realising it. He was recruited by the Mossad in 1958 under the ruse of working for one of the NATO countries. It was only later revealed to him that he had been working for the Israeli intelligence.

The Mossad likes to have a hold on an agent. A paid agent feels obligated to deliver and the threat of blackmail lies in the background. The recruiters could always get the agent in trouble with documentary proof of money handed over. Lakam gave for example Pollard cash and a diamond ring for his fiancé.

### Training

Similar training was mentioned by both a former katsa and a former combatant. Training took place in stages. They had to create a convincing cover story. Then they were taken on streets of Tel Aviv. They had to appear on a randomly chosen apartment balcony after convincing the tenant to allow them access; get the first three names from a hotel register; start a conversation with a complete stranger and hold his attention for twenty minutes; put a device in a public phone mouthpiece in the heart of the Hilton Hotel foyer without being noticed; and a whole host of other odd but challenging tasks. In each case, they had to rely not only on an invented identity — a legend, or "status cover" — but also on what they later learned to refer to as his operational cover, that is, a fictional motive for being in a particular place and doing a particular thing at a particular time. A legend stays with them for years, but an operational cover is often invented on the spot. The tests varied, but they all had the same goal: to see how far one could be pushed before one broke cover.

They were also taught report writing. There is a saying in the Mossad: "If you complete a mission and don't report it, the mission never happened."

Katsas: If selected, a candidate must go through and pass the Mossad training academy, the Midrasha, located near the town of Herzliya. There they are taught the tradecraft of intelligence gathering for approximately three years. The main priority of training is to teach katsas how to find, recruit, and cultivate agents, including how to clandestinely communicate with them. They also learn how to avoid being the subject of foreign counter-intelligence, by avoiding car and foot surveillance, how to run SDRs (surveillance detection routes), and preventing foreign agents from creating 'traps' at meetings. Although katsas do not always carry a weapon, each is trained in the use of the .22 Beretta pistol. Even once training is completed, trainees will spend an apprenticeship period working on various projects before becoming full fledged katsas.

Female katsas are also trained to:

- draw a gun while sitting in a chair
- pack a Beretta inside her pants on the hip or to cut a concealed opening in skirt for easy access to the handgun
- use sex to coerce, seduce and dominate
- disguise herself by inserting cotton wool in the cheeks to subtly alter shape of face



- steal cars
- pose as a drunk
- chat up men
- create a mishlachim (a dead letter box)
- read a floater (a strip of microfilm attached to the inside of an envelope).

They are sent on practice missions: breaking into occupied hotel room, stealing documents from an office, picking up tourists in a nightclub, and disengaging outside their hotel.

Combatants are also taught finance to be able to discuss stocks and bonds and appear to be able to make investment and business decisions.

Training for katsas going on special missions is extensive. Training for operations in the desert is described as:

A katsa underwent training in Negev Desert, mastering "memory training", how to recognize the target even in a sandstorm, and "self-image protection", how to blend in with his surroundings. The only weapon he had with him was a hunting knife which he could use to kill in a number of ways. A pharmacist taught him how to use his emergency medicine in the desert. A morning devoted to memorising the maps that would lead him across the sands. Part of each day was given over to testing his sheer physical stamina with a forced march in the fierce noon heat, carrying a rucksack weighted with rocks. He only ate the food he would live on in the desert. He had attended a one-day class with a Mossad psychiatrist on handling stress and how to relax. Aptitude tests determined his present emotional stability and his self-confidence. A dialect coach sat with him for hours listening to him repeating the correct dialect. Every night he was driven to a different part of Negev to sleep. Burrowing into the ground, he would rest for a short while, never more than dozing, then move to another place to avoid instructors he knew were hunting him. Discovery would almost certainly mean his mission would either be postponed for further training or assigned to another katsa.

**Kidon:** Kidon members must pass a two-year course at the Mossad training school at Henzelia, near Tel Aviv. They also go to a special camp in the Negev desert. The facility could be adapted to approximate a street or a building where an assassination was to take place. There are getaway cars and an obstacle course to negotiate. The instructors include former unit members who supervise practice with a variety of guns, and teach how to conceal bombs, administer a lethal injection in a crowd, and make a killing appear accidental. They are taught to use the weapon appropriate for the target. Kidons review videos of successful assassinations and study the faces and habits of scores of potential targets stored on their own highly restricted computer and memorize the constantly changing street plans of major cities as well as air and seaport layouts.

After graduation they regularly undergo the same physical checks as a front-line-pilot in the Israeli Air Force. To perfect their skill they watch some of Israel's leading forensic pathologists in Tel Aviv's Institute of Forensic Medical Research at work so as to better understand how to make an assassination appear to be an accident.

The agents used by katsas also receive training.



For example Jack Leon THOMAS who was recruited to spy for Israel in Egypt received training in the basics of espionage: photographing documents and developing film, hiding negatives in toothpaste tubes, shoe boxes or books; writing with invisible ink; and passing coded messages by leaving them in "dead letter boxes" for unknown accomplices. His wife who acted as courier received training in how to use a radio transmitter. The chosen code book was Pearl Buck's *The Good Earth*.

### **Cover**

Katsas work sometimes out of Israeli embassies. Katsas, combatants and kidon members all use covers to work in foreign countries. They use different guises like salesman, businessman, travel writer, journalist etc. They make use of a number of names and biographies drawn from library of aliases maintained by the Mossad. The list of aliases is kept on file in the Operations Division. Rafi EITAN had introduced the idea of a list after the Eichmann operation. They like to use British aliases as "no one would think a Jew would have a name like that."

All officers like katsas and combatants are trained to perfect their cover including that the personality portrayed match the supposed identity. That means getting the vocabulary and diction right, as well as the clothing, food preferences, mannerisms and grooming. They learned how to refine a cover to the point where they can fool true experts.

The Mossad has garments from all over the world and regularly updates it. It is given to katsas for operations to suite their specific covers. Most of the clothes are obtained by sayanim and delivered to local Israeli embassies and sent on to Tel Aviv in diplomatic bags. Other clothes are brought out of hostile Arab countries by pro-Israeli visitors. A few are actually made by the wardrobe mistress who presides over the storeroom who had developed a reputation for detail.

To assist in disguises especially for deep cover agents, the Mossad also has appearances changed. For example, the appearance of one of their officers working in Africa, Yaakov COHEN, who had distinguished himself in undercover missions in Egypt and elsewhere, was changed. As part of his disguise, Mossad had changed Cohen's physical appearance by arranging for a plastic surgeon to alter his distinctive ethnic feature – his nose.

### **Documentation**

The Mossad uses forgers to compile documentation for operations overseas. Three different "qualities" of passports are used by the agency: top, second, field operation and throwaway. Top-quality passports are real passports with a real person's name that can withstand official checks in the country of origin.

Mossad was several times in trouble for using or trying to obtain passports of other countries. The Mossad provided its agents with forged British passports to carry out attacks on PLO officials abroad. The tactic was discovered when eight forged British passports were found in a Frankfurt telephone booth in 1986. Similar discoveries took place in 1973 and 1979, Mossad agents also were found to be carrying forged British identification while on anti-PLO missions in Beirut.

Canadian passports are also a favourite with Mossad as Canadians are regarded as the good guys and Canada is a nation of immigrants, populated by people of



SECRET

30

virtually every race and creed. Canadian passports were used during a bungled assassination attempt in Jordan and in 1973 Israeli agents travelling on doctored Canadian passports botched another execution attempt in Lillehammer, Norway. One member of that hit squad, arrested by Norwegian police, was found to be using the identity of Canadian Patricia ROXBOROUGH, a legal secretary whose passport had been stolen months earlier from the desk of her Montreal office.

In 1973 fifty blank passports were stolen from the vault of the Canadian Embassy in Vienna. One of those documents, traced by the registration number, turned up a year later in Nicosia, Cyprus. It was left behind by a member of a Mossad team that had detonated explosives under the hotel bed of a sleeping Palestinian guerrilla leader, killing him instantly.

In 1997, Canada recalled its ambassador to Israel after undercover Mossad agents were caught using falsified Canadian passports during an assassination attempt on a Palestinian militant leader.

In addition to creating false passports or theft, Israel's clandestine services have other means to obtain Canadian documents. New immigrants to the Jewish state, especially from Canada, are sometimes encouraged to donate passports, both valid and expired, to unidentified bureaucrats in the interests of what is euphemistically known as "the security of the state."

The Mossad also tried to illegally obtain a real New Zealand passport by applying for a passport in the name of an Auckland man with cerebral palsy. Urie Zoshe KELMAN and Eli CARA were caught and sentenced to six months in prison, while Zev William BARKAN for whom the passport was meant and the sayan David Tony RESNICK, an Auckland paramedic who provided the name for the passport, escaped New Zealand. Kelman also had a Canadian passport with him.

The Mossad used Jordanian, French and Italian documents.

#### **Communicating with Agents/ Case Officer:**

Mossad katsas use dead letter boxes at locations such as hotel corridors or restaurant rest rooms where a small envelope could be left to be picked up later by an unseen courier. They used to transmit urgent information to Israel on a tiny radio set.

A special method of communication was through a floater, a little microfilm attached to the inside of an envelope. The agent would rip the envelope and tip the microfilm into a glass of water. He'd then stick it on the outside of the glass and by using a magnifying glass read the message.

According to ROSS (2007) Mossad officers still use shortwave radios to receive messages from HQ when out in the field during operations. He stated: "Why use old-fashioned laborious method in era of instantaneous digital communication? Wouldn't it be simpler to use devices like cellphones, text messaging, e-mail or Internet chat room?" He said that "unlike all of these rival methods, shortwave radio broadcasts provide an eavesdropper with no means of identifying the person receiving the message, or of determining if anyone is receiving a message. Moreover the communication leaves no electronic residue and requires no specially configured gadgets; all you need is shortwave radio. E-mail and telephone lines are an open book to counterintelligence services. With other

SECRET



SECRET

31

gadgets government snoopers can use voice recognition, calling patterns, and signal tracking to zero in on a suspect user. Need a one-time pad to decode. Each combatant is assigned his own one-time pad, which means you can't hack an entire network merely by seizing a single code."

One incident reported was of case in France where a case officer working out of the Israeli embassy set up meetings with his agent. They had regular meeting points in cafes and on the metro. The agent would carry a copy of that day's newspaper in which he had inserted his information. The case officer would have a similar copy in which was concealed the agent's instructions and his monthly salary. In a technique both had perfected at the Mossad training school, one would bump into the other and offer profuse apologies and they would go their separate ways, having exchanged newspapers.

#### Technological Aids

When YATOM was head of the Mossad he ordered Mossad programmers to develop new software to hack into PLO computers and create electronic microbes to destroy, should the need arise, its communication systems. He had asked scientists in research and development to focus on "infowar" weapons that could insert black propaganda into enemy broadcasting systems. He wanted the Mossad to be part of the brave new world where the weapons of the future would be in keyboards that shut down an enemy's ability to mobilise its military forces. Mossad technicians were researching ways to infect enemy computer systems with a variety of virulent strains of software viruses. They would include the 'logic bomb' designed to remain dormant in an enemy system until a predetermined time when it would be activated and begin to destroy stored data. Such a bomb could destroy an enemy's air defence system or central bank. The technicians had already created a program that could insert booby-trapped computer chips into weapons a foreign arms manufacturer planned to sell to a hostile country like Iran or Syria. Mossad katsas in key Eastern European arms manufacturing countries had also been briefed to find independent software contractors who wrote programs for such weapon systems. They would be offered substantial sums to slip viruses into the systems. Mossad agents were also equipped with a briefcase-size device that generated a high-powered electromagnetic pulse. Placed near a building the pulse can burn out all electronic components in the building. The device had its own self-destruct mechanism that ensured its innards remain a secret.

It is also claimed that the Mossad prepared a bug capable of monitoring all calls in and out of a suspected PLO member's apartment. The bug would be linked to a miniature recorder capable of storing hours of phone calls. The recorder had a built-in capacity to be electronically emptied by a pre-arranged signal from the safe house. There the recordings would be transcribed and sent by secure fax to Israel. Agent would carry laptop that had been wired to provide the link between the concealed recorder to be installed in the apartment basement and the safe house.

In 1999 then Palestinian leader Yasser ARAFAT received information that Israel was able to eavesdrop on most of the mobile telephones used by the Palestinians, particularly the Leader telephone manufactured by the Israeli Miritz Telecommunications Company. Even when turned off, the telephones were able to record the voices around them. The signals were allegedly retransmitted and picked up by an antenna in Israel which transmitted them to a centre that

SECRET



SECRET

32

eavesdropped (still does) on the Palestinians. ARAFAT then issued an order to keep the mobile telephones of all of his visitors in the main room of the guards which is situated 150 meters away from the presidential headquarters.

A Mossad scientist developed a microchip to plant under the skin. Using natural body energy, the bleep could be linked to one of Israel's new space satellites, enabling a person who wore it to be swiftly tracked to his or her hiding place.

It is being mentioned in overt sources that the Mossad had the best capability for cracking locks. He claims that various lock manufacturers in Great Britain send new mechanisms to British intelligence for security testing; they in turn send them on to the Mossad for analysis. The procedure was for the Mossad to analyse it, figure out how to open it, and report back that it was "impregnable."

Mossad's technological unit was involved in wireless communications and developed various communications systems to support Mossad operations abroad. There are very sophisticated systems. For example, there are departments involved in electronics -- from VLSI to embed and RF systems, while other are more involved in computers or physics. The Mossad keeps a yaholomin unit in New York to spy on Arab and other missions.

The Mossad was one of first intelligence services to monitor the Internet. As militants recognised that their mosques were almost certainly under surveillance, websites offered a new and relatively safe way to communicate with their followers. The Mossad had created a large number of its own websites on which it posted carefully constructed disinformation in all the languages of the Middle East.

#### **Safe Houses**

The Mossad has many safe houses all over world. There were scores of such department in all major cities all over the world, either purchased or rented on long leases. Many were left unoccupied for lengthy periods, ready for the time they would be needed for an operation.

The safe houses are also manned by Israeli students who make sure the houses are well stocked with food and other essentials, so that when they are activated they are ready. They live in some of the houses and visit the others to collect the mail, turn the lights on and off, and make phone calls, so the place is in use and does not raise suspicions when it is used by the case officers. They are usually the same age as the bodel and will meet with him socially.

A bodel takes packages from the Mossad station in the embassy to the safe houses and back. He makes most of the trips to the safe houses during the day and most of the pickups during the night. He rarely uses embassy vehicles and does not have any specific pattern of work.

The station does not use the safe houses for their sayanim. They meet them in their houses and under regular everyday circumstances. Rarely will they meet clandestinely, unless of course the sayan is in the process of bringing vital info form his place of work.

The safe houses are used purely for debriefing or field planning sessions with katsas or combatants who do not enter the embassy. Safe houses are also used

SECRET



as meeting places for an informer or to interrogate a suspect who had the potential to be recruited as a mole. In that case they will almost always discard it right after that. Sometimes safe houses are rented for specific operations. During Eichmann abduction at least half a dozen safe houses were rented in Buenos Aires.

### Covert Action

### Kidnappings

On several occasions suspects were kidnapped and taken back to Israel to stand trial. Mossad also assisted other countries in kidnapping operations. Some of the known cases were:

- In 1960, the Mossad kidnapped Nazi war criminal Adolph Eichmann from Argentina.
- Nuclear technician, Mordechai VANUNU, who had revealed details of the Israeli nuclear weapons programme to a London newspaper, was kidnapped in 1986. (A bat leveyha enticed him to leave from Britain to Rome. When they arrived at the apartment in Rome, Mossad katsa overpowered him and injected him with a paralysing drug. Late that night an ambulance arrived and he was carried on a stretcher out of the building. The ambulance sped out of Rome and down the coast. At a pre-arranged point a speedboat was waiting, on which Vanunu was transferred back to Israel. (p190-194: Gideon's spies)
- In 1986 an Israeli naval patrol boat with Mossad agents on board stopped a ship called Opportunity on its regular shuttle between Beirut and Larnaca. From the bilges they dragged out Faisal Abu SHARAH, a terrorist wanted in Israel. He was trailed in Israel and received a long jail term.
- In 1984 the Mossad assisted the Nigerian military cabal led by Major General Muhammad BUHARI in a botched attempt to kidnap Umaro DIKKO, ousted transport minister. Dr Levi-Arie SHAPIRO who worked at Hasharon hospital in Tel Aviv was recruited by Mossad katsa Alexander BARAK. The kidnapping group consisted of two Mossad officers BARAK and Felix ABITHOL, Dr SHAPIRO and members of the Nigerian security service headed by Major YUSUFU. DIKKO was kidnapped on 04 July 1984 when he left his home, put in a van, anaesthetized into unconsciousness by Dr SHAPIRO, locked into a crate and taken to Stansted airport. A customs officer noticed an unusual medical smell and a noise emanating from one of two crates labelled "diplomatic baggage" and addressed to the Nigerian Ministry of External Affairs in Lagos as they were being loaded onto the Nigerian Airways and ordered the crates to be opened. DIKKO was found unconscious in the one crate with Dr SHAPIRO with him, while ABITHOL and BARAK were found in the second crate. The Nigerian and Israeli governments never acknowledged the role of the Mossad in this incident. The Israelis claimed they were mercenaries acting on behalf of Nigerian businessmen. All received heavy prison sentences and were deported after serving their time.
- In 1999 Mossad assisted Turkey to capture Abdullah OCALAN, the Kurdish leader that waged a guerrilla war against Turkey. The Mossad located OCALAN in the Greek embassy compound in Nairobi. Mossad was able to intercept radio traffic from the Greek Foreign Ministry to the compound. A Mossad agent influenced one of his Kurdish bodyguards to persuade OCALAN to get out of embassy and go to Iraq to regroup. He went on an aircraft that left for Athens but he ended up in a Turkey jail.



### Assassinations

Israel accepted the legitimacy of assassination as a tactic to deal with terrorists. Assassinations procedures were clearly defined by Meir AMMIT when he was Mossad DG:

There would be no killing of political leaders. They needed to be dealt with politically. There would be no killing of a terrorist's family unless they are also proven to be implicated in terrorism. Each execution had to be sanctioned by the Prime Minister of the day. And everything must be done by the book. Minutes kept of the decisions taken. Actions must not be seen as state-sponsored murder but the ultimate judicial sanction the state could bring. "We would be no different from the hangman or any other lawfully appointed executioner." Since the successful hunting down of the nine terrorists responsible for killing of Israeli athletes at Olympic Games in Germany in 1972, all subsequent assassinations had broadly observed these conditions.

Executions were for vengeance, the biblical "eye for an eye" principle Israelis believe justified such killings. But sometimes Mossad killed a person when he stubbornly refused to provide his skills to support Israel's aspirations. Then, rather than risk those talents falling in the hands of the enemy, he too was ruthlessly terminated. For example Dr Gerald BULL, a Canadian scientist, the world's greatest expert on barrel ballistics, had a distaste for Israel and offered Saddam HUSSEIN to build a super-gun capable of launching shells containing nuclear, chemical, or biological warheads from Iraq directly into Israel. He was killed in his apartment in Brussels in March 1990.

Rafi EITAN responsible for capturing Adolf EICHMANN told how he travelled across Europe to find and execute Arab terrorists. To do so he used remote-controlled bombs; the Beretta; and where silence was essential, his own bare hands to either garrote a victim with steel wire or deliver a lethal rabbit punch. For each journey, he used a different nationality and identity, built around the vast number of stolen or perfectly forged passports Mossad had patiently acquired.

The usual composition of a hit team is four. One is the "target locator". His task is to keep tabs on the victim's movements. Another is the "transporter", to get the team safely away from the killing area. The remaining two men perform the execution. Preparation for an assassination can take weeks, even months.

Since DAGAN's appointment as Mossad DG he increased the number of kidons. He had sent kidon to seek out all those who had been condemned in a meeting he had chaired in his office. The assassins had done so in countries across the Middle East, in Iran, Pakistan, Afghanistan; in each case the killing had been swift and unexpected, using anything from a single bullet to the nape of the neck, to garrotting with a cheese-cutting wire or a knife thrust into the larynx. They had also used nerve agents and a poison arsenal of substances specially prepared for them.

In Mossad's eye the need for kidon had increased with the spread of Islamic fundamentalism in all its guises: Hamas, Hezbollah, Islamic Jihad, Solidarity Front, PLO, the terrorists of the Philippines; all were pledged to destroy Israel. The kidon had killed in all those places regarded as Israel's enemies: Saudi Arabia, North Korea, Iran and numerous Islamic republics of the former Soviet Bloc.



## KENYA

The Mossad through its station in Nairobi has long maintained excellent ties with the Kenyan security service. The special interest for Israel is that Nairobi is not far from the Horn of Africa and is one of most important capitals on the continent, with diplomats and spies of all nationalities and allegiances at offices of the UN and OAU. Together with DRC in Central Africa and Nigeria in the west, Kenya became one of three strategic centres for Israeli intelligence activity in Africa.

Kenya and Israel had developed over the years a close 'understanding' on intelligence matters. As part of Mossad's safari in Central Africa it had exposed to the Kenyans the activities of other foreign spy networks. In return, Kenya continued to grant Mossad "special status", allowing it to maintain a safe house in the city and providing ready access to Kenya's intelligence service. Kenya for example allowed Mossad to operate from the country to free hostages at airport in Entebbe in Uganda.

The Director of Mossad Meir DAGAN and CIA DG Porter GOSS worked together in the early 2000s. They sent agents into the badlands of Kazakhstan, to the mountains of Kashmir, to the seaports of the Horn of Africa, into the highlands of Kenya and Ethiopia, and reinforced their presence in Saudi Arabia. While the CIA worked closely with the Saudi secret service to locate Islamic fundamentalists, Mossad's role was different. Mossad agents were concerned with tracking jihadists coming out of the country and heading toward Israel. All too often before reaching its borders, they met their deaths at the hands of Mossad's kidon unit.

DAGAN is also sending his agents to the jungles of Venezuela, the mountains of Colombia, the back streets of Mexico, the Amazon and down into Chile and Argentina where Al Qaeda was fermenting hatred against Israel.

Several known assassinations are:

- Nazi war criminal Herberts CUKURS hiding in Brazil in 1965.
- Ghassan KANAFANI, PFLP spokesperson and accused of planning Lord massacre was killed by letter bomb in Beirut in 1972
- The assassination of members of Black September, which was responsible for the Munich massacre at the 1972 Olympic Games, called "Operation Wrath of God". The first to die was shot eleven times at close range – a bullet for each murdered athlete. The next was killed by a bomb planted in the receiver of his telephone; another was pushed under a bus in London. The next was asleep in a hotel room in Nicosia when it was wrecked by a similar bomb that was placed in a bedside lamp. Their leader Ali Hassan SALAMEH was killed in 1979 on a Beirut street by a remote-controlled car bomb. To create panic among the remaining members, Mossad Arab sayanim arranged for their obituaries to appear in local Arab newspapers. Their families received flowers and condolence cards shortly before each was killed. While the kidon carried out the executions it had required a team backup of some eight units. One group was responsible for tracking down each killer. Technicians form yaholomin set up eavesdropping equipment to monitor each terrorist as he was located. Another team organised dead letter boxes in a dozen European capitals to receive messages from informers. Safe houses were rented for secret meetings in London, Paris and Madrid. LAP was responsible for sending cards flowers and publishing of notices in newspapers. All paperwork was produced by Mossad's forgery department. Explosives were created in Tel Aviv and brought to the team.
- The assassination of PFLP and PFLP-EO leader Wadie HADDAD in 1978.



- The assassination of As-Sa'iqa leader Zuhayr MUHSIN in 1979.
- The assassination of Abu JIHAD from the Fatah in 1988 in Tunis. He was shot in his study and several of his guards killed in the process.
- Mohammed TAMIMI, one of PLO leaders of Intifada against Israel and two senior PLO officers were killed in motorbomb at Cypriot port of Limassol on 14 February 1988
- Gerald BULL, a Canadian scientist who developed the famed "Super Gun" for Iraq was killed by the Mossad at his Brussels apartment in March 1990. He was first visited by Israeli friends, both from the Israeli intelligence community to persuade him to stop, but he did not want to listen. Thereafter a kidon team was sent to eliminate him.
- In 1992 Hezbollah guerrilla leader Abbas MUSAWI is ambushed and killed in south Lebanon.
- In 1994 Islamic Jihad activist and journalist Hani ABED dies when his car explodes in the Gaza Strip.
- In 1995 Dr Fathi al-SHIQAQI, the leader of a small Islamic Jihad organisation dies on a busy street in Sliema, Malta, when he is shot five times in the head by two assailants on a passing motorcycle and who fled to an unknown destination in a ship that was positioned near the site of the incident.
- In 1996 Yahya AYYASH, known in the Hamas movement as "the engineer" for his skill in bomb-making, is decapitated when 50g of explosives planted in his cellular telephone detonates as he makes a call.
- Hamas leader Izz El-Deen Sheikh KHALIL in Damascus on 26 September 2004 was killed when a bomb exploded under the driver's seat of his SUV.

#### **Alleged but Unproven Assassinations/ Deaths:**

- Mossad is accused of the murders of Iraqi nuclear scientists. In 1980, Yahya al-MESHAD, a physicist working for the Iraqi government, was stabbed to death in a hotel room in Paris. The purpose of his visit to France was to examine the characteristics of uranium materials intended for nuclear reactors. In a period of a few months, two more nuclear physicists who worked for the Iraqi government were murdered. In their cases, they were poisoned. A number of workers at Osirak began receiving threatening letters from a shadowy organisation called the Committee to Safeguard the Islamic Revolution.
- Dr Majid Husayn ALI, an Iraqi nuclear scientist and a professor at the College of Science in Baghdad University was assassinated in Baghdad. This assassination incident is the ninth within four months to target distinguished Iraqi scientists.
- Dr Ardeshir HOSSEINPOUR, a scientist involved in the Iranian nuclear program, was according to Stratfor killed by the Mossad on 15 January 2007. He was killed by gas poisoning.
- Mossad is also suspected of murdering media tycoon Robert MAXWELL, their British sayan who was in financial trouble and insisted Mossad pay him back and threatened to reveal Mossad secrets. He disappeared overboard at sea in November 1991 off the Canary Islands. It is alleged that Maxwell Mossad agents boarded his private yacht under cover of darkness and plunged a needle filled with a lethal nerve agent into his neck, where after they lowered his body into the sea.
- Mossad is suspected of involvement in the death of Yasser ARAFAT, the Palestinian leader in October 2004. He complained of severe stomach pains after a meal and after drinking a homeopathic drink he made himself. The real



cause of his death on 12 November 2004 was not revealed and there was no autopsy. Many speculated he was poisoned.

- The assassination of Hamas military leader Izzedine Sheikh KHALIL in Damascus on 26 September was widely seen as a Mossad operation.
- Alan KIDGER in South Africa. He had been supplying high-tech equipment to Iran and Iraq that could be used to manufacture biochemical weapons. KIDGER had been found with his arms and legs amputated in Johannesburg.
- South African police also suspected Mossad involvement in the strange deaths of several people in South Africa in the 1990s: Seven South Africans, including a British immigrant, are believed to have been assassinated over three years. In some cases they were gassed in an attempt to fake a suicide, while in others they were executed and their bodies dismembered. The murders are being linked to similar investigations in Europe. They were chemical engineer Wynand VAN WYK who died in Cape Town in April 1993, two apparent suicides, one of former arms dealer Don LANGE (was found gassed in his home in July 1994) and chemical engineer John SCOTT. Another two young chemical engineers, Scott AYTON and Felix COETZEE were found bound and gagged at AYTON's parent's home with a single bullet wound in the head also in 1994. KIDGER and VAN WYK were all acquainted with each other and KIDGER knew SCOTT. LANGE apparently knew of Israeli involvement in KIDGER's death before police did. A business associate quoted him as saying several months later he feared he would be "eliminated". Connected to this is the alleged suicide of Dirk STOFFBERG and his wife at his home at Hartebeespoortdam, near Pretoria.
- Mossad is also suspected to be responsible for the assassination of Hezbollah's external security chief Imad MUGHNIYEH, nicknamed the "ghost," in Damascus on 12 February 2008. Just as he was climbing into his black Mercedes, a Mitsubishi Pajero parked just beside it exploded, killing him instantly.

#### Failed assassinations or wrong targets:

- In Damascus Nazi war criminal Alois BRUNNER lost an eye and several fingers from letter bombs sent to him by Mossad during the Operation Wrath of God campaign.
- In 1972 PFLP Basam Abu SHERIF lost an eye and several fingers with a letter bomb sent by Israel to his Beirut office.
- In Lillehammer Norway on 07 January 1974 Mossad agents mistakenly killed Ahmad BOUSHIKI, an Algerian waiter whom they mistook for PLO security head Ali Ahmad SALAMEH, believed to have masterminded the Olympics massacre. Two of those involved in his murder had rented cars under their own names, Dan ERT and Marianne GLADNIKOFF. They were arrested at Oslo airport. Once they had provided the address of a flat used by Mossad, six other agents were arrested. Five of the 15 agents involved in the operation serve sentences in Norwegian jails. **Remark:** *Salameh was killed in a 1979 car-bomb explosion in Lebanon.*
- On 24 September 1997 Mossad operatives attempted to assassinate Khalid MESHAAAL, a top leader of Hamas, in Jordan. The assassins injected MESHAAAL with poison. Two were caught; four other agents involved in the operation fled to the Israeli embassy. Israel was forced to provide the antidote to the poison and to release around 70 Palestinian prisoners.



### Counterproliferation Activities

As noted above Mossad also uses assassinations were to prevent nuclear material to reach enemies, eg Gerald BULL who developed the super-gun for Iraq, Alan KIDGER who sold high-tech equipment to Iran and Iraq, several South Africans who were chemical engineers or involved in arms deals. They also targeted Iraqi and Iranian nuclear scientists.

### Intimidation

In early 1960s Mossad was concerned about the German rocket scientists in Egypt. Mossad Director Isser HAREL believed the Germans were involved in an effort to exterminate Jews. He responded with *Operation Damocles*, a sword hanging over the head of every German scientist working for the Egyptians. Israeli agents sent booby-trapped letters to German scientists involved in the missile project and their families in Egypt. Similar intimidation was being carried out throughout Europe. In the campaign there were a few injuries and much intimidation. Mossad used the 'false flag' game of posing as representatives of a NATO intelligence service, to meet with ex-Nazi officer Otto SKORZENY, who was friendly with some of the Germans in Cairo. They persuaded him to urge his friends to get out of Egypt for the sake of Western interests. Mossad also recruited an Austrian Dr Otto JOKLIK who had been one of the rocket scientists working for NASSER in Egypt. He was not an expert as he indicated to NASSER and worked on his project to build a high-energy cobalt bomb with no real success. HAREL sent JOKLIK later with Israeli agent Yosef Ben-Gal on a secret mission to Switzerland to frighten the daughter of Paul GÖRKA about the dire consequences if her father did not leave Egypt. She informed the Swiss police who arrested the two on 15 March 1963. Just a few weeks' earlier two Israeli agents had been arrested in West Germany near the home of one another rocket scientists. The Mossad had been lucky that its warm relations with BND persuaded them to release the Israelis. But in Switzerland they were not lucky and a public trial embarrassed Israel and the two were sent to prison, although only for short terms.

Mossad agents were also sent on briefing missions to journalists in various European countries and three leading Israeli newsmen – persuaded by HAREL – undertook a special assignment, partly for their newspapers and partly as an espionage mission to learn more about the German scientists. It was one of first times Mossad used Israeli journalists as agents. The articles they published caused panic among the Israeli public about the ballistic dangers from Egypt. But the Israeli president was not happy with Mossad head as he spoiled developing ties between Israel and West Germany and HAREL resigned.

### Africa

In mid 1950s Israel's policies in Africa were implemented through three major channels – The Histadrut, Israel's Federation of Trade Unions; the Mossad, and Mashav, the Foreign Ministry's Department of Technical Cooperation which was responsible for organizing the dispatch of hundreds of experts to Africa and the holding of a large number of courses for Africans in Israel. Israel opened embassies in many African countries after establishing diplomatic relations and provided various aid programs. Israel had Mossad agents working in the embassies under diplomatic cover. Where official relations were not established or were later cut owing to overt political disputes, the Mossad's alternative diplomats performed functions that are not customarily handled by intelligence services.



SECRET

39

Specifically in Africa Amit persuaded CIA to provide millions of dollars to underwrite Israel's clandestine activities. They were judged to be in the general interest of the West. Newly independent black African states of the 1960s saw Israel as an example to copy. Over a dozen African states welcomed Israeli technicians and instructors in agriculture, industry, commerce and defence. The number of Israeli advisors grew and naturally quite a few of them were Mossad agents. Israel developed excellent intelligence cooperation with Kenya, DRC, Liberia and Ghana. In each country, espionage agencies or security services were trained or assisted by the Israelis.

Israel also assisted African liberation movements in fighting colonialism and fascism in the African countries that were not independent. Contacts were established with African national movements. In Dar es Salaam Israeli Mossad agents established an Intelligence School which served the various Liberation Movements of Central and Southern Africa.

When the KGB became involved and brought with them Arab activists, the Israeli involvement changed. Meir AMIT reinforced his katsas with kidons. His new orders were to disrupt by all means possible relations between the Russians and their African hosts and between the KGB and Chinese intelligence; to kill Arab activists when the opportunity arose. Mossad operatives ambushed some victims driving on dirt roads; others were killed in their beds. One day it would be a KGB agent, the next a CSIS (Chinese intelligence) spy. Each side blamed the other for what Mossad had done.

Mossad was involved in a war against Chinese agents in Africa during the 1950s. Mossad wrecked a Chinese plot to overthrow the pro-West Hastings Banda regime in Malawi. Next it informed Kenya about the full extent of Chinese network in its midst. The Chinese network was kicked out of the country. Several Chinese intelligence operatives were killed by Mossad katsas. Kidons stalked Chinese intelligence operatives wherever they set up shop. In Ghana a Chinese intelligence agent was shot dead, another died in Mali in a car bomb, in Zanzibar a fire consumed an apartment block where Chinese intelligence staff lived. The Chinese intelligence local commander narrowly escaped when a car he travelled in Brazaville in the Congo exploded. In Zambia a Chinese intelligence agent was left bound to a tree for lions to consume. When Kwame NKRUMAH, the pro-Chinese ruler of Ghana, was on state visit to Beijing, Mossad orchestrated the uprising that led to his overthrow and destruction of Chinese intelligence infrastructure in Ghana.

For three years Mossad waged its war of attrition against the Chinese intelligence over the length and breadth of Africa. There was no mercy on either side. When Chin Intel hit team ambushed a Mossad katsa in Congo, they fed him to crocodiles, filmed it and sent footage to local Mossad station chief who retaliated by firing a rocket into the building from where Chin Intel operated. Three Chinese were killed.

Through an intermediary, President MOBUTO of Zaire (DRC), the Chinese intelligence led Mossad know it no longer wished to fight rather. They shared a common interest on the continent. The offer was accepted and the Chinese began to provide details about Arab movements in and out of Africa. Some Arabs were killed by usual Mossad method of car bombs or explosives placed in hotel rooms. Mossad on its part assisted China. It tipped off that Moscow intended to offer a massive financial aid package to Somalia and China doubled it. Next Mossad helped China in Sudan where KGB planned a coup. Mossad informed China who told President Nimeri and he expelled all Russian diplomats and suspended Soviet bloc aid schemes.

SECRET



SECRET

40

African countries turned their back on Israel after the Six-Day War in 1967. By the end of 1973, only four African countries: Malawi, Lesotho, Swaziland and Mauritius – continued to maintain diplomatic relations with Israel. Despite the break in diplomatic ties, some countries still continued with bilateral relations.

At the same time, economic contacts continued unabated, especially in Nigeria where a large number of Israeli businessmen set up base, but also in Kenya, Ethiopia, Zaire (DRC) and elsewhere. African trainees continued to attend courses in Israel, especially at the Histadrut Afro-Asian Institute.

Mossad activities continued in Ethiopia, Southern Sudan, Kenya and elsewhere. The Horn of Africa and Ethiopia in particular, had always held a special interest for Israel, as that region was considered to be of strategic importance, bordering on the Red Sea.

In 1980 Israel's Foreign Minister, Yitzhak SHAMIR, and David KIMCHE, as his Director-General, decided to launch a concerted effort to renew diplomatic relations with the countries of Africa. Although there was no immediate rush to resume formal relations, the new dialogue which Jerusalem had initiated with African leaders bore fruit: instead of automatically supporting Arab or Soviet moves against Israel in international bodies as they had done previously, African delegates were now preventing initiatives against Israel.

During the 80s, Mossad was involved widely in Africa. As well as playing off the Chinese against Russians, it made matters difficult for CIA, MI6 and other European intelligence agencies operating on continent. Whenever one threatened Mossad's own position, Mossad exposed its activities. In Kenya an MI6 agent was blown. In Zaire (DRC), a French network was wrecked. In Tanzania a German intelligence operation was hurriedly aborted after being uncovered by Mossad through a tip to a local reporter.

Mossad policy was to work with anyone who would work with Israel. That enabled them to know everything that was happening in a country. The slightest mood change that could affect Israel was reported back.

### **Ethiopia**

Ethiopia is of strategic importance to Israel. Israel had good relations with Emperor Haile SELASSIE who had proclaimed himself a descendant of the ancient Hebrew tribe of Judah. The Israelis helped the emperor train his security forces and Israel was permitted to build a powerful listening post, which monitored Arab radio traffic. The Mossad ran a large "station" of operatives in the Ethiopian capital. After SELASSIE was overthrown in 1974, Colonel Mengistu Haile MARIAM, the new Marxist president of Ethiopia in 1977 wanted to renew Israeli arms sales to Ethiopia. Israel requested a letter from the president to permit Jews of Ethiopia to move to Israel. He agreed but when the covert relations were revealed he stopped the departure of more Jews. Mossad established an alternative plan and obtained permission from Sudan to move Ethiopians through that country across the border to Kenya and then from there to Israel. But after an airplane incident the clandestine plan was published in newspaper and Kenya withdrew permission. Thereafter Mossad received help from CIA and established a dummy corporation named Navco, which leased land by the Red Sea in Sudan with the stated intention of constructing a holiday village for undersea divers. The divers that arrived were not the amateur variety but from the naval commando force. Under cover of darkness the frogmen took the refugees in small boats to Israeli vessels anchored offshore. Sudanese

SECRET



SECRET

41

president then became concerned about the flow of Jews through his country and wanted Israel to stop. US promised economic aid of \$200million in exchange for the use of Khartoum airport to fly them out as part of Operation Moses. When it was leaked the Sudanese stopped it.

Israel also helped Ethiopia against the Somalis.

#### Ivory Coast

In 1997 Mossad stumbled upon a CIA operation in Abidjan while they were targeting a local Hezbollah operative who had been identified as a possible recruit. The CIA accused Mossad of spying on them.

#### Nigeria

Mossad assisted the Nigeria security service in 1984 in the botched kidnapping of Umaro DIKKO from London. (See kidnappings)

#### Morocco

Israel had good relations with the Arab state, Morocco. In the 1960s Morocco felt threatened by Algeria and Egypt. Mossad experts helped King HASSAN II to establish a secret service.

In 1965 Mossad assisted Morocco intelligence service to help them kidnap dissident Ben-BARKA who was sentenced to death in absentia. (See kidnappings)

In 1976 clandestine cooperation between Israel and Morocco was reaffirmed. Mossad and CIA were free to roam Morocco, making contacts with potential useful Arabs, running listening posts to keep an electronic ear on North Africa and advising the king and top officials on internal security.

An Israeli general of Moroccan descent represented Mossad for a long time with King HASSAN II but the relationship had cooled. Relations increased later again and Mossad reportedly was allowed to set up a permanent station in Casablanca in 1993, injecting fresh impetus into security cooperation between Israel and Morocco.

#### Tunisia

When Tunisia arrested some Jews in 1961, Mossad feared for Tunisia's Jews and arranged for French warships to pick up 1000 Jews from the coast of Bizerte and transport them first to France and then on to Israel.

In 1988, Israeli commandos, led by future Prime Minister Ehud BARAK, slipped into the home of Palestine Liberation Organisation leader Khalil al-Wazir Abu Jihad in Tunis, Tunisia. Abu Jihad was killed in his sleep in a well-planned tactical military assault.

#### Sudan

Sudan was of great interest to the Mossad because the country was just to the south of Israel's nemesis, Egypt. During its transition to independence Sudan was afraid Egypt might intervene and Sudan turned to Israel in 1956 where various schemes for anti-Nasser cooperation were discussed. The contacts ended in 1958 when Prime Minister Agdallah KHALIL was overthrown by his army.

SECRET



SECRET

42

In 1985 Sudanese intelligence lent a helping hand to Mossad and the CIA in carrying out Operation Moses, the transfer of Ethiopian Falashas to Israel via Sudan.

It was reported in 1995 that between 20 and 30 Israeli advisers headed by a former head of Aman operated in Khartoum. Some of them were responsible for the protection of the Sudanese president Gen. Omar Hassal al-BACHIR, while the others have set up a communications system which serves to both eavesdrop on and secure the security of presidential telecommunications.

### Algeria

Said SAHNOUN, an Algerian journalist, was found guilty of spying for Israel and jailed for 10 years on 04 July 2007. A police officer, accused of giving him information, was acquitted. SAHNOUN was accused of collecting and supplying military information on Algeria and other Arab countries for Mossad. SAHNOUN was arrested at the borders between Morocco and Algeria in possession of several documents containing secret information about the Algerian army plans and lists of wanted terrorists. He provided information about Algerian army's military capabilities and an Islamist rebel group known as the Salafist Group for Preaching and Combat (GSPC). He was said to have been in contact with the Israeli embassy in Abidjan since 1992 and went on a journalism and communications course in Israel. He was recruited there and started working for Mossad. He sent them detailed reports about economic and security situation in Algeria and the Kabylia area for \$1500 per month. At the same time, he allegedly also worked for Spain's intelligence and sent them the same reports.

In his confession SAHNOUN cited that Mossad was interested in information regarding Algeria's domestic crises, the thinking and positions of Algeria's top political figures, confidential Algerian financial information and the country's general morale, prosecutors said.

### Uganda

On 27 June 1976 PLO terrorists hijacked Air France plane filled with Jewish passengers en route to Paris from Tel Aviv and landed at Entebbe airport in Uganda. They announced the aircraft would be blown up along with the Jewish passengers unless their demands were met. Israel decided to free them. Half a dozen katsas went to Nairobi and were installed in a Kenyan intelligence service safe house. Kenya provided approval for a fuel stop at Nairobi. Israeli paratroopers waited close to Ugandan shore ready to storm the airport. Six Mossad katsas surrounded the airport; each carried a high-frequency radio and an electronic device that jammed the radar in the control tower. A force of C-130 Hercules transporters swept down on Entebbe Airport and commandos raced into the building where the hostages were held and freed all killing all terrorists and 16 Ugandan soldiers. The attack force lost one man and three hostages died.

Three suicide bombers attacked an Israeli-owned hotel in Mombasa, Kenya on 28 November 2002 and killed 16 people, including three Israelis. Minutes later, unknown assailants launched two shoulder-fired missiles that barely missed a chartered flight filled with Israeli tourists as it took off from Mombasa's airport. The previously unknown Army of Palestine claimed responsibility for the dual attacks. Israeli Prime Minister Ariel SHARON has pledged to avenge the killings of the Israelis in Kenya and has deployed agents from Mossad to Kenya. Mossad agents in Nigeria have provided important details on al-Qaeda in that country. Katsas in South Africa have

SECRET



joined colleagues in Mombasa, Rome, Malta and Cyprus went to Kenya to assist in the investigation. DAGAN also sent kidon to find and kill the men behind the three suicide bombers. He said that no one knows for certain what success the Mossad team had. But sources in a number of intelligence services say it did kill several suspected terrorists and dumped their bodies in crocodile-infested swamps.

### Egypt

In early 1960s Mossad was concerned about the German rocket scientists in Egypt. It was been alleged that the Germans were involved in an effort to exterminate Jews. Response was given with Operation Damocles, a sword hanging over the head of every German scientist working for the Egyptians. Israeli agents sent booby-trapped letters to German scientists involved in the missile project and their families. Similar intimidation was being carried out throughout Europe. In the campaign there were a few injuries and much intimidation.

During time as Mossad chief Meir AMIT he had placed spies everywhere including in Egypt. In the run-up to the Six Day War in 1967, there was either a Mossad katsa or an informer inside every Egyptian air base and military headquarters. There were three in the General High Command headquarters in Cairo. To each katsa and informer he gave the same instruction: as well as the big picture he wanted the small details. That helped to determine when to strike.

Some in Israel think the end of Israel would come at the hands of the Egyptians. That is why Israel has been continuously recruiting spies and sending them to Egypt. Mossad activity in Egypt is also extensive. Mossad used Egypt both as a source of information and as a jumping-off point to the rest of the Arab world. Mossad reasons that it would be much easier and much less suspicious to have an Egyptian who was recruited under a false flag in Cairo and had never set foot outside the Middle East to carry out intelligence gathering in other Arab countries than Arabs who had been to Europe and therefore might be suspected.

Ever since signing peace treaty with Egypt at Camp David in 1978, Israel has been trying to measure Egypt's military and economic power. Egyptian security authorities said since that time until 2000 it have managed to expose and apprehend at least 24 Israeli espionage networks operating against Egypt.

Various espionage operations and agents have been uncovered in Egypt over the years.

- Wolfgang LOTZ, a German Jew, was sent on a spying mission to Egypt from 1957-1965; he operated first under Aman and then Mossad. His cover was a riding instructor, an East German refugee who had served in Africa Corps in WW11 and had returned to Egypt to open an equestrian academy. It gave him access to Cairo's high society, but also meant his bills we high leading to Mossad accounting department dubbing him "the champagne spy". He also married a woman in Egypt, while he also had a wife in Israel.

LOTZ had developed a circle of clients that included the deputy head Egyptian military intelligence, and chief of security of Suez Canal zone. LOTZ was shown Egypt's formidable defences, the rocket launch pads in Sinai and on THE Negev frontier, the complete list of Nazi scientists living in Cairo working in Egypt's rocket and arms programs. LOTS and his wife were arrested by Egyptian Mukhabarat on 22 February 1965. The radio transmitter



hidden in his bathroom scale was detected by direction-finding equipment, just as Syrian intelligence and the Soviet GRU assisted to help plug security leaks affecting Syria and Egypt. LOTZ was sentenced to life imprisonment, but after a lot of lobbying and pressure from the UN LOTZ and wife were released in an Israeli-Egyptian swap of Six-Day War prisoners.

- Shaaltiel BEN-YAIR was a successful spy for the Mossad who lived in Egypt under deep cover from 1958-1962. He was in charge of mapping Egyptian airfields and providing details of military installations. It was dangerous, but he was one of the Israeli agents who completed their missions and returned home without being caught. He could pose as an Arab, talk English like the Scots, French like the Belgians.
- Jack Leon THOMAS, an Armenian who grew up in Cairo and hated NASSER was recruited via the false-flag method in 1958. Mossad recruited him under the ruse of working for one of the NATO countries. It was only later revealed to him that he work for Israeli intelligence. He ran a large network until May 1960 when he was caught. When he discovered that he was in trouble he obtained false passports for himself and his wife who was part of his network. She managed to escape together with another member of the network, a Jewish dancer. THOMAS was hanged in 1962. During his trial prosecutors revealed that the network offered pilots of Egyptian air force a US\$1 million to defect to Israel or Cyprus with a Soviet-made MIG jet.
- Aman recruited Ibrahim and Inshirah SHAHEEN, Palestinians living in Cairo. They provided good information re Egypt's preparations for the 1973 war. However they and their handlers became careless and Ibrahim was arrested in 1974 and hanged three years later. His wife and three children were imprisoned. After peace negotiations started they were released and slipped over the border to Israel. The intelligence community helped them create and start new lives.
- Max BINNOT and Moshe MARZUK, who ran Mossad's most successful network in Egypt, were caught and died a painful, lingering death in a Cairo prison.
- In 1996 Arab Assam AZZAM, who worked for a textile company, was sentenced to 15 years in prison for espionage for Israel, partly carried out by writing messages in invisible ink on lingerie. According to Egypt AZZAM was recruited by Mossad and sent to Egypt to work for an Israeli textile company. He then allegedly recruited an Egyptian to help him collect information. He was released after eight years as part of a prisoner exchange for Egyptian students who had allegedly crossed into Israel to carry out attacks.
- Egyptian engineer Sherif El-FILALI was sentenced in 2002 to 15 years in prison with hard labour for spying on behalf of Israel. He was convicted of trying to collect military information and data on Egyptian tourism and an agricultural project for Israel. Court sources said that a Russian man, who was convicted of espionage in absentia, recruited El-FILALI in Spain to obtain secret information about Egypt for Mossad. He died in jail in 2007.
- Mohammed Essam Ghoneium al-ATTAR was arrested on espionage charges at Cairo Airport on 01 January 2007 while on a visit to Egypt. He studied



science at Al-Azhar University in Cairo but dropped out of the Islamic institution in 2001 after becoming involved in a civil dispute because he refused to pay for damaging a rental car. He fled to Turkey before serving his three-year sentence. Once in Ankara, ATTAR sought asylum at the United Nations High Commissioner on Refugees (UNHCR) on the basis that he was homosexual. He sought employment at the Israeli embassy there and was introduced to Daniel LEVI, a Mossad agent who allegedly became his handler in Turkey. According to the case file, Mossad agents tempted him with US\$56 000 and a new Mercedes. ATTAR was then trained to collect information from Arabs living in Turkey - an activity he later continued when he moved to Canada, where he obtained citizenship.

ATTAR left for Canada near the end of 2002 and moved to Vancouver, where he met Kemal KOSBA, a second Mossad agent who landed him a job at a restaurant. He then moved to Toronto and met up with another agent, Tuncay BUBAY. In 2005, Bubay landed him a job with CIBC in the customers' service sector. According to Egyptian reports, he spied on financial dealings of local Egyptians and Arabs to determine who would be suitable to work with the Mossad. He allegedly recruited several new agents in Canada, targeting gays and those he knew were in financial trouble within Arab communities. He also sought to recruit Egyptians for operations with the Mossad and has recruited Egyptians, Syrians, and Iraqis in Canada. The Egyptian intelligence service was monitoring him for five years since his travel to Turkey and Canada and his relations with the Israeli officers who recruited him. He was sentenced to 15 years in jail and his handlers in absentia.

- Mohammed Sayed SABER @ Muhammad Sayyid SABIR ALI, an engineer at the Nuclear Energy Agency, was arrested for espionage on 18 February 2007 after returning to Egypt from Hong Kong. The prosecution said he used to meet his Mossad handlers namely Japanese Shiro IZO and Irishman Brian PETER. SABER first met the two foreigners in Hong Kong between 2004 and 2006. He allegedly passed on classified documents relating to the work of the AEA (Egypt's Atomic Agency), including information on experiments and International Atomic Energy Agency (IAEA) inspections at Inshas (Egypt's atomic reactor); the reactors' capabilities and hours of operation; and technological problems. He also purportedly used computer software provided by IZO and PETER to hack into the AEA computer system. According to the charges, he received US\$17 000 in return for confidential information. They gave him a laptop equipped with coded software and communicated with him in secret coded e-mails.

Ali ISLAM, head of Egypt's atomic agency, said the engineer stole confidential reports from the agency and gave them to the Israeli Mossad. SABER illegally obtained the documents from his department, kept them for 10 years although they were confidential and classified documents. During his trial SABER praised Israel for its advanced technology and claimed the documents he passed on were so outdated they posed no threat to Egyptian security.

He aroused the suspicions of Egyptian authorities when he went to the Israeli embassy in Cairo in 1999 to ask for a grant to study nuclear engineering at Tel Aviv University. He claimed that he did not know it was for Mossad but was under the impression it was a Japanese multinational firm, but that he did



report his suspicions to the Egyptian Embassy in Riyadh, Saudi Arabia. He was sentenced to life imprisonment.

*Remark: It is said that Israel has a clear interest in determining the nature and scope of the experiments carried out at Inshas, which could give indications as to Egypt's readiness for nuclear expansion following the Hosni MUBARAK government's decision to restart its shelved nuclear energy program in September 2006. Alleged covert Egyptian nuclear experiments, uncovered in 2005, have also raised fears that Egypt may be seeking a weapons option, should regional tensions worsen over time.*

## 9. ISRAEL INTELLIGENCE ACTIVITIES IN SOUTH AFRICA

- 9.1 During the Apartheid era there were good relations between South Africa and Israel. Israel intelligence had friendly relations with South Africa's BOSS. Israel also bought uranium directly from South Africa. South Africa became Israel's partner in clandestine projects including nuclear and missile research. OSTROVSKY mentioned a certain URI from AL department. He came back from an assignment in South Africa. OSTROVSKY helped him prepare a large shipment of medication to South Africa to accompany several Israeli doctors who were headed for some humanitarian work in Soweto. The doctors were to assist in treating patients at an outpatient clinic for the Baragwanath hospital in Soweto. The hospital and clinic were supported by a hospital in Baltimore, which served as a cut-out for the Mossad. It has been alleged that Mossad was testing new infectious diseases and new medication that can't be tested on humans in Israel, for several of the Israeli medicine manufacturers.

After Apartheid Mossad was involved in various counter proliferation operations in the country including intimidation of Iranians and is suspect of the assassinations of a number of South African chemical engineers and arms dealers.

It is known that there are katsas working in South Africa. For example it was reported that during the bomb investigation in Kenya, Katsas in South Africa have joined colleagues in Mombasa to assist in investigations.

An SA Municipal Workers' Union (Samwu) official has claimed that Israeli security strip-searched him at OR TAMBO International Airport in Kempton Park. Samwu first vice-president Xolile NXU claimed he was detained and interrogated in June 2007 on his departure for the second annual conference on Popular Non-Violent Resistance in the West Bank village of Bil'in, in occupied Palestine. He further alleged that Israeli security escorted him directly to the aircraft a minute before take-off after covering his luggage and hand-luggage with red stamps.

However, the Airports Company South Africa (ACSA) said it knew nothing of the incident. No security police from foreign countries had offices at OR TAMBO.

### 9.2 Modus operandi in SA:

A former declared MOSSAD member in South Africa utilised the following modus operandi:



- 9.2.1 By means of detail billing it was determined that [REDACTED] had regular contact with members of the South African Jewish community. *It is known modus operandi of the MOSSAD to utilise the Jewish community around the world to assist the MOSSAD in its intelligence activities. The contact between [REDACTED] and these members of the South Africa Jewish community might have been an indication that the MOSSAD utilised them in its covert collection activities.*

[REDACTED] head of the Africa and Latin American Division of the Foreign Relations and Special Political Operations Directorate of the MOSSAD and supervisor of [REDACTED] was in South Africa on a liaison visit. During [REDACTED] visit to South Africa he and [REDACTED] visited Cape Town. During this visit to Cape Town [REDACTED] had a possible "brush" meeting with two persons in a public toilet, one of them of Muslim origin. *Radical Islam had been identified as one of the most important collection priorities of the MOSSAD in South Africa. In this regard the MOSSAD is interested in the activities of inter alia PAGAD and QIBLA. In light of the fact that one of the persons met by [REDACTED] was of Muslim origin, the possibility existed that this person might have had access to information with regard to PAGAD, QIBLA or other radical Islamic activities in South Africa and that this person operated as a source/agent for [REDACTED]. The possibility further existed that the information was urgently needed by the MOSSAD from its source and had to be provided to [REDACTED] while he was in South Africa.*

It has also been determined that [REDACTED] utilised rental vehicles on some occasions to attend meetings. In this regard it was established that [REDACTED] was in regular contact with a member of the South African Police Service (SAPS). It was determined that [REDACTED] and the SAPS member's contact revolved around Islamic Militancy issues in South Africa. As mentioned earlier, the MOSSAD possesses good information on this topic and therefore the possibility existed that [REDACTED] would have endeavoured to verify his own information and also to glean more information from his SAPS contact. It was established that the liaison relationship between [REDACTED] and the SAPS member had been carrying on since 1996 without NIA (CDE) being informed about it. It has further been established that [REDACTED] also had contact with two other members of the same Division of the SAPS. *Although the SAPS has indicated that this liaison with [REDACTED] was official, the fact that NIA (CE) had not been informed in this regard, should have been be addressed on a higher level as this situation could have led to possible espionage opportunities.*

It was also established that [REDACTED] had constant contact with the South African Jewish Board of Deputies, a very well organised body in the country with their offices spread around the country. This body has a direct influence over the Jewish community in South Africa, with strong emotional bonds with the State of Israel.

[REDACTED] also had contacts within government departments which included the Agriculture, Trade and Industry, Health and other institutions that deal with research. Most of his contacts within these departments were contacting him on his cellular phone precisely because he might have been aware that it was not easy to monitor a cellular phone. The most serious of the contacts he had, were within the Crime Intelligence of the SAPS.



SECRET

48

After [redacted] family had returned to Israel, [redacted] stayed at the Protea Lodge for almost three weeks. During this time he never utilised the room's telephone, neither did he receive any messages or visitors via the reception. On the last day of his stay at the Lodge, [redacted] requested that his account being divided in two parts, respectively in the names of EL AL Airlines and Tiger Wheel and Tyre. Through the analysing of the account it has come to light that [redacted] was also settling the account of a certain [redacted] an American. *The reason behind [redacted] request to change the account to EL AL and Tiger Wheel and Tyre was unknown. EL AL made sense, but the link with Tiger Wheel and Tyre was unexplainable. The relation between [redacted] and [redacted] was yet another point of concern.*

*All the abovementioned information indicated that the Israeli Intelligence Services, through its declared member, were involved in the collection of intelligence by means of covert activities.*

It was also known modus operandi of the Israeli intelligence services to utilise EL AL as cover for intelligence members. As mentioned above, 45 people are employed by EL AL as their security personnel at the JHB International Airport and 8 are employed at the Cargo and Passenger side. According to the Airports Company of South Africa (ACSA), EL AL has the privilege of not being searched at the restricted areas. EL AL officials are also allowed to travel freely with their weapons amongst the EL AL passengers. When a flight from Tel Aviv arrives, the EL AL personnel, carrying hidden handset two-way radios, disguise themselves as passengers. At check points they simply flash their EL AL cards and are allowed to go through any restricted area in the airport as been agreed to by ACSA.

EL AL cars are also allocated permits without specifying the make and model of each car. The reason for this is because EL AL does not have permanent cars, but utilises rental vehicles.

Because of the situation in Israel (terrorists attacks etc), EL AL is of the opinion that they are responsible for the security/guarding of Israeli planes and passengers at the airport, and therefore all the abovementioned privileges are afforded to them by ACSA.

*Because of abovementioned privileges the possibility exists that an Israeli intelligence officer can enter South Africa and under the disguise as an EL AL member go through all the checkpoints at the airport without presenting any documentation. As mentioned earlier, one of the members of EL AL has also been identified as a courier for the MOSSAD. Although this still needs to be investigated, his status as an EL AL member provides him with freedom of movement that will make it easy for him to act as a courier.*

#### 9.2.2 Counter surveillance

When attending liaison meetings [redacted] varied his driving speed between 30km/h and 90km/h. He would also pull over and waited next to the road for approximately 4 minutes for no specific reason.

- When leaving the embassy building for the Hatfield shopping centre on foot, [redacted] would first walk around the block instead of walking directly to the shopping centre.

SECRET



- [REDACTED] also changed his access routes to his house every time he used his vehicle.

### 9.2.3 Communication

[REDACTED] had two cellular phones. One phone was registered in his name and the other phone was a rental phone. According to MTN no records were kept of calls made from a rental phone.

### 9.2.4 Passports

[REDACTED] had two passports, an official passport and a private passport. He used his diplomatic passport to travel to Israel, Botswana and Mozambique.

### 9.2.5 Cutting of rubbish bags

[REDACTED] cut his rubbish bags in such a manner that it could not be lifted from the dustbin without spilling the content.

### 9.2.6 Utilisation of rental vehicles

Despite having two official vehicles, [REDACTED] had on ten occasions, rented vehicles from *Budget Rent a Car* for the period 1 January 1998 to 7 September 1998, for utilisation in the Gauteng.

### 9.2.7 Front Companies

It is an internationally known practise of the Israeli intelligence services to utilise the following organisations as cover structures for its members:

- EL AL Airlines.
- Armament industries e.g., EL BIT and the Israeli Aircraft Industry (IAI).
- Jewish Community organisations; e.g.: South African Jewish Board of Deputies (SAJBD) and individuals in the Jewish Community with legitimate business.

*Note: No members attached to these organisations in South Africa have to date been identified as intelligence officers.*

### 9.2.8 Recruitment Methods

The possibility existed that some of [REDACTED] contacts were recruited unwittingly. The contacts were under the impression that the meetings with [REDACTED] were "above board" whilst [REDACTED] acted in a covert manner by not informing NIA about his meetings.

It is also possible that some of these contacts had been recruited wittingly, and that they were aware of exactly what they were doing, that is, providing information to a foreign intelligence service.



### 9.2.9 Communication with agents

It was determined that [REDACTED] utilised cellular phones for communication with his contacts.

Personal meetings also took place between [REDACTED] and his contacts.

### 9.2.10 Agent Handling Procedures

It seemed as if some of [REDACTED] contacts might have been handled unwittingly by him.

### 9.2.11 Collection Methods

It seemed as if [REDACTED] made use of personal meetings (interviews) with contacts. It was possible that during some of these meetings information was provided unwittingly to [REDACTED]

## 10. RELATIONS BETWEEN MOSSAD AND NIA

### 10.1 Background

The Mossad was handled by [REDACTED] from 1996 to 2004. At that stage it was the only country in the Middle East that was represented and declared to NIA. Relations were always more tense with the Mossad than with any other country, solely because of the history between the two countries.

The representative initially met [REDACTED] was [REDACTED] he was succeeded by [REDACTED] [REDACTED] During the time of [REDACTED] relations were standard and regular exchange took place. Exchanges regularly took place, mostly on individuals and organisations suspected of terrorism involvement. A counter terrorism expert visit took place in 1996. Background on terrorism modus operandi was shared by them, even before the first PAGAD related bombs exploded in the Western Cape. Meaningful exchanges became less at the end of [REDACTED] term. The Mossad at that stage also indicated they were thinking of a part time representative responsible for handling the whole of Africa. NIA discarded the idea and [REDACTED] subsequently was placed in South Africa, although he regularly travelled to West and East Africa where he also was the declared member. Reasonable relations existed with [REDACTED] until he was handed over to [REDACTED]

Examples of exchanges are attached as Annexure A, during the above-mentioned period.

During February 2005, [REDACTED] the Mossad Director for Foreign Relations, led a Mossad delegation that visited NIA Head Quarters in Musanda Liaison Centre. The objective of the Mossad visit was to create a space for dialogue on how cooperation between Mossad and NIA can be improved. Mr NJENJE, former NIA DDG led the NIA delegation

[REDACTED] mentioned that non-conventional threats are more worrying to the Mossad and the Israeli government. He also mentioned that was priority threat for Israel because it Iran possessed nuclear capability that could be used against Israel and for funding Hezbollah and HAMAS.



SECRET

51

Mr. NJENJE welcomed the sentiments expressed by [REDACTED] regarding the need for Intelligence Services to cooperate and work together to avert terrorist threats. He assured Mossad that NIA was a willing partner in the fight to combat international terrorism and proliferation of weapons of mass destruction. He emphasised the importance of that meeting as having brought to the fore bases for productive cooperation between NIA and Mossad in the area of Counter Terrorism and Counter Proliferation.

There was improvement of information exchange soon after the Mossad delegation visit. In May 2006 NIA Counter Proliferation experts delegation visited Israel. MOSSAD was pushing to hard to included information request on Counter Intelligence area such as [REDACTED] the Iranian national staying in Cape Town. He alleged that [REDACTED] was in contact with [REDACTED] a Hezbollah member based in Lebanon. NIA did not provide feedback to MOSSAD on this request.

In 2007 Mossad provided information on [REDACTED] to NIA with the hope that the information would benefit South Africa. They expected that NIA would share information with them on what are finding of their monitoring and investigation. However, [REDACTED] bluntly told [REDACTED] the Local Representative of Mossad that he was prevented by NIA Management to share information on [REDACTED] could not understand [REDACTED] because Mossad provided to NIA information on [REDACTED]. He stormed out of the meeting.

[REDACTED] former Head FIS Liaison Mossad grievance on NIA's action to refuse to share information on [REDACTED] activities after his return from Somalia to NLC to get guidance. He was confused by the actions of [REDACTED] and [REDACTED] and sought NIA's position on cooperation with Mossad. The NLC reversed [REDACTED] decision to refuse IM to share information on [REDACTED] with Mossad. However, [REDACTED] took over from IM Analysts.

[REDACTED] the former DDG instructed [REDACTED] to confine cooperation between NIA and Mossad to Counter Proliferation and Counter Terrorism.

The political stance from Minister KASRILS contributed to the perception that NIA was not willing to cooperate with MOSSAD because the adversaries of Israel are allies of South Africa. Of course Mr KARSILS has openly demonstrated political differences with Israel and supported the cause of the Palestinian. He also favoured Iran's material support to Palestinians Resistance Movement. He ordered audit of information NIA liaised with MOSSAD.

[REDACTED] the former DG paid unofficial visit to Mossad HQ in March 2009. Mossad complained to him about lack of concrete cooperation with NIA. According to Mossad the situation has not changed. Instead it has deteriorated to the levels which have compelled MOSSAD to withdraw their Representative from South Africa. Hence they have withdrawn their Representative but have not severed the relations from residing in South Africa.

SECRET



## 10.2 Current status of relations between Mossad and NIA

During February 2005, [REDACTED] the Mossad Director for Foreign Relations, led a Mossad delegation that visited NIA Head Quarters in Musanda Liaison Centre. The objective of the Mossad visit was to create a space for dialogue on how cooperation between Mossad and NIA can be improved. Mr NJENJE, former NIA DDG led the NIA delegation

[REDACTED] mentioned that non-conventional threats are more worrying to the Mossad and the Israeli government. He also mentioned that was priority threat for Israel because it Iran possessed nuclear capability that could be used against Israel and for funding Hezbollah and HAMAS.

Mr NJENJE welcomed the sentiments expressed by [REDACTED] regarding the need for Intelligence Services to cooperate and work together to avert terrorist threats. He assured Mossad that NIA was a willing partner in the fight to combat international terrorism and proliferation of weapons of mass destruction. He emphasised the importance of that meeting as having brought to the fore bases for productive cooperation between NIA and Mossad in the area of Counter Terrorism and Counter Proliferation.

There was improvement of information exchange soon after the Mossad delegation visit. In May 2006 NIA Counter Proliferation experts delegation visited Israel. Mossad was pushing to hard to included information request on Counter Intelligence area such as [REDACTED] the Iranian national staying in Cape Town. He alleged that [REDACTED] was in contact with [REDACTED] a Hezbollah member based in Lebanon. NIA did not provide feedback to Mossad on this request.

In 2007 Mossad provided information on [REDACTED] to NIA with the hope that the information would benefit South Africa. They expected that NIA would share information with them on what are finding of their monitoring and investigation. However, [REDACTED] bluntly told [REDACTED] the Local Representative of Mossad that he was prevented by NIA Management to share information on [REDACTED] could not understand [REDACTED] because Mossad provided to NIA information on [REDACTED] He stormed out of the meeting.

[REDACTED] former Head FIS Liaison Mossad grievance on NIA's action to refuse to share information on [REDACTED] activities after his return from Somalia to NLC to get guidance. He was confused by the actions of [REDACTED] and [REDACTED] and sought NIA's position on cooperation with Mossad. The NLC reversed [REDACTED] decision to refuse IM to share information on [REDACTED] with Mossad. However, [REDACTED] took over from IM Analysts.

[REDACTED] the former DDG instructed [REDACTED] to confine cooperation between NIA and Mossad to Counter Proliferation and Counter Terrorism.

The political stance of from Minister KASRILS contributed to the perception that NIA was not willing to cooperate with Mossad because the adversaries of Israel are allies of South Africa. Of course Mr KARSILS has openly demonstrated political differences with Israel and supported the cause of the Palestinian. He also favoured Iran's material support to Palestinians



Resistance Movement. He ordered audit of information NIA liaised with Mossad.

██████████ the former DG paid unofficial visit to Mossad HQ in March 2009. Mossad complained to him about lack of concrete cooperation with NIA. According to Mossad the situation has not changed. Instead it has deteriorated to the levels which have compelled Mossad to withdraw their Representative from South Africa. Hence they have withdrawn their Representative but have not severed the relations from residing in South Africa.

## 11. CURRENT INTELLIGENCE ACTIVITIES IN SA

### 11.1 Intelligence Representation:

██████████ has been the declared MOSSAD member in SA and suspected of being involved in espionage activities. He has indicated through liaison that the Mossad give priority attention to CP and CT issues. He left South Africa in August 2009 and has been replaced by ██████████ who will only visit SA approximately once a month.

Surname	:	██████████
Name	:	██████████
Cell phone	:	██████████
Fax	:	██████████
Date of Birth	:	██████████
Dip Passport	:	██████████
Diplomatic Id number	:	Currently based in Israel
Date of arrival	:	██████████
Nationality	:	Israeli
Position in embassy	:	██████████
Intelligence status	:	██████████
Date of assumption of duty	:	██████████
End period stipulated	:	Based in Israel, so no period was stipulated
Marital status	:	Not known

### 11.2 Current activities indicating threat

The Mossad perceives SA to be close to the Iranians regarding Iran's nuclear development program and thus show interest in SA. MOSSAD is suspected of collecting CT-related information, for example financial information on the Al-Aqsa Foundation and the African Muslim Agency (AMA) and it is alleged that these organisations are responsible for the channelling of funds to terrorist organisations.

### 11.3 Interests

- Foreign involvement in/with Radical Islamic groups in South Africa.
- Proliferation of Weapons of Mass Destruction.
- Activities of Iran and other Middle Eastern countries in South Africa.

The Iranian nuclear programme is seen as posing real and immediate danger to the MOSSAD / Israelis. MOSSAD in SA has the objective to persuade NIA



to cooperation at the level of having joint operations against threats posed by the Iranian Intelligence Service to South Africa and Israel.

It is known that the MOSSAD is interested in Zimbabwe.

#### 11.4 Current modus operandi

11.4.1 The usage of front companies and placement of suspected Intelligence operator at OR TAMBO International Airport still needs to be investigated, as a former member of EL AL security and a suspected Israeli intelligence operative, was appointed as Security officer at OR TAMBO International Airport (ACSA). **Remark:** *It is known modus operandi of the MOSSAD to make use of EL AL as cover for intelligence collection activities.*

11.4.2 It is furthermore suspected that the MOSSAD might be using the company AMDOCS who also operates in South Africa as AMDOCS South Africa Joint Enterprises (ASAJE). According to the ASAJE website, TELKOM SA and Cell-C are currently their two main customers in South Africa. **Remark:** *The Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI) and the National Security Agency (NSA), as well as other US Federal Law Enforcement agencies in the past had investigated AMDOCS in the USA and have raised their concern regarding the protection of identity information of US telephone customers. The implications are serious and speak for itself, since the same concerns, as in the USA, can be raised with regard to Telkom SA and Cell-C in South Africa.*

11.4.3 An Israeli procurement agent in the RSA, [REDACTED] acts as the Israeli link for the supply of Israeli armaments to selected countries inter alia India. The initial investigation into Indian procurement identified a shopping list to procure inter alia nuclear, chemical, laser and conventional warfare technologies and hardware in the RSA market. India has an excellent trade relationship with the RSA, however, according to the source India accepted the fact that the RSA would not necessarily sell them sensitive technology or equipment. India has therefore set up a parallel procurement system to obtain goods or technology covertly. This system is also used to verify prices on equipment or technology. On their attempt to acquire early warning and trigger systems for their rockets, India has made contact with an Israeli procurement agent [REDACTED] based in the RSA. It was established through operations that [REDACTED] has also strong links with MOSSAD. [REDACTED] has a company, [REDACTED] is operated by Ex-Mossad members and if compromised, would not create a possible embarrassment for the Israeli government.

11.4.4 It has been determined that the previous Mossad member in SA, [REDACTED] was covertly active in South Africa, including agent handling and the coordination and running of Mossad operations in South Africa. He was additionally suspected that he runs Mossad operations directed against targets in Africa using South Africa as a base of operation. Information obtained that [REDACTED] utilised South African and Israel citizens as co-workers/cut-outs for these operations in order to protect the involvement of the MOSSAD. [REDACTED] had contact with several Government Departments, including the presidency. Investigations are currently underway to determine the activities, contacts and modus operandi of [REDACTED]



SECRET  
55

Compiled by [REDACTED] in cooperation with [REDACTED] (Overt information)  
and EM41 (NIA Liaison), including covert information received from CI20.

IM23 October 2009



**ALJAZEERA**

SECRET



SECRET

DMS: 10000585948

Copy 01 of 02 copies

# INTELLIGENCE

## BRIEF

SEPTEMBER 2012

GROWING ANTI-  
ISRAEL  
LOBBYING:  
SECURITY  
IMPLICATIONS  
FOR SOUTH  
AFRICA



state security

State Security Agency  
REPUBLIC OF SOUTH AFRICA

SECRET



## SECURITY AND ADMINISTRATION

**This document is subject to the  
Protection of Information Act  
(Act 84 of 1982)**

The distribution of information contained in this document is restricted to official institutions of the Republic of South Africa. Permission for deviation from the authorised distribution list should be obtained from the General Manager Intelligence Management Centre, on behalf of the Director of the Domestic Branch of the State Security Agency (SSA).

After use, which may not exceed a period of six weeks, this document should be destroyed by either burning or shredding. The Director of the Domestic Branch of the SSA should be notified accordingly by means of the Declaration of Destruction form attached to the back of this document.

# ALJAZEERA



**SSA DOMESTIC BRANCH  
INTELLIGENCE BRIEF  
GROWING ANTI-ISRAEL LOBBYING:  
SECURITY IMPLICATIONS FOR SOUTH AFRICA**

**SEPTEMBER 2012**

## 1. BACKGROUND

The purpose of this Intelligence Brief is to encapsulate local developments and initiatives against Israel and to assess the security impact that these will bear on the stability of South Africa.

Tension between the pro-Palestinian lobby<sup>1</sup> and Jewish communities over Israel's "apartheid policies" and human rights abuses against Palestinians in the occupied territories has been prevalent in South Africa. Several protest actions, aimed at expressing growing opposition against Israel, have mostly been driven by organisations sympathetic to the Palestinian cause. Displaying a commonality of calls for the boycott of Israeli goods and the cancellation of official visits to Israel, they have exerted pressure on the South African government to sever ties with Israel. Repeated anti-Israel statements pronounced by representatives of the South African government, in line with the official South African foreign policy on Israel, have further contributed to the passive resentment denoted by the Jewish communities in the face of such actions.

Incidents with an explicit anti-Israel slant have occurred since the beginning of 2012 but failed to elicit a significant reaction from Jewish organisations in South Africa. Their frustration and anger were instead manifested in concerns raised within the Jewish community with the South African Jewish Board of Deputies (SAJBD) over intimidation and the possible targeting of Jewish interests in South Africa.

## 2. RECENT DEVELOPMENTS

### 2.1 Cancellation of Hibiscus Coast Delegation to Israel

The South African branch of the Boycott, Divestment and Sanctions (BDS)<sup>2</sup> movement against Israel expressed its satisfaction in August 2012 over the cancellation of a planned trip to Israel by a delegation of mayors and other members of several KwaZulu-Natal (KZN) municipalities.

<sup>1</sup> The pro-Palestinian lobby in South Africa is represented by, among others, Al-Quds Foundation, Muslim Judicial Council (MJC), Media Review Network (MRN), Open Shuhada Street, Palestinian Solidarity Committee (PSC), and Congress of South African Trade Unions (COSATU).

<sup>2</sup> The BDS campaign was launched internationally in July 2005 in support of the Palestinian call for international sanctions against Israel by 171 Palestinian NGOs. BDS South Africa is based in Johannesburg, Gauteng.



The visit, organised by the SA-Israel Forum<sup>3</sup> and scheduled to have taken place in early August 2012, was aimed at facilitating contact with Israeli experts on agriculture, science and technology. The BDS further qualified the cancellation of the visit as a major setback for the Israeli lobby and particularly the SA-Israel Forum, and called on all other provinces, municipalities and government structures to follow the lead of KZN. **Remark:** *This was the first time that a visit to Israel organised by the SA-Israel Forum was cancelled.*

## 2.2 National Israeli Apartheid Week

The Eighth International Israeli Apartheid Week (IAW)<sup>4</sup> was held across South Africa on 05 – 11 March 2012, and included lectures, rallies, film screenings and multimedia displays. The purpose of the IAW was to raise awareness about Israel's "apartheid policies"<sup>5</sup> towards the Palestinians and to mobilise support for the BDS campaign against Israel. This event ran simultaneously with worldwide IAW programmes. IAW renewed calls on the South African government to boycott Israeli investment and products. In its reaction to the IAW, the SAJBD branded the event as an attempt to "delegitimise Israel in the eyes of the international community and to undermine its sovereignty".



Dr Abdul Aziz UMAR, one of the guest speakers invited to address perceived human rights abuses perpetrated by Israel, was hosted during his stay in South Africa by the Muslim Judicial Council (MJC) and the Al-Quds Foundation. Dr UMAR has been branded by the Israeli intelligence services as a terrorist for his involvement in the 2003 Café Hillel bombing that killed six Israelis and one Palestinian.

In an attempt to counter the anti-Israel rhetoric, the SAJBD invited several Israeli role players to attend the IAW events, including Benjamin POGROUND and Bassem EID, an Israeli and Palestinian respectively who, according to the SAJBD, "strive for peace and understanding between the two peoples".

## 2.3 Re-labelling of Products from Israel

Adding impetus to the BDS campaign, the South African Minister of Trade and Industry, Rob DAVIES, announced on 10 May 2012 that, in terms of section 26 of the Consumer Protection Act (2008), products from the West Bank would no longer be permitted to carry the "Product of Israel" label. In his response to criticism that followed this announcement from Jewish groups in South Africa and accusations of racism, Minister DAVIES rejected suggestions that there was a racial motivation

<sup>3</sup> The SA-Israel Forum has been coordinating its operations in close conjunction with the Israeli government for several years and has been taking individuals from the academic, cultural, sports, business and local government sectors to Israel with the objective of forging lasting relations with their counterparts in Israel.

<sup>4</sup> The IAW is an international series of events held in cities and campuses across the world. In 2011, 90 cities worldwide and 9 universities in South Africa participated in the IAW.

<sup>5</sup> The pro-Palestinian lobby has consistently equated Israel's policy against the Palestinians to the South African pre-1994 apartheid policy of the previous regime, hence on-going references to apartheid policies.



behind this step and indicated that his department sought to neither promote a boycott of Israeli goods, nor prevent the entry of such products into South Africa.

In an attempt to have this notice overturned, the South African Zionist Federation (SAZF) and the SABJD sent a delegation to meet with Minister DAVIES on 24 May 2012 to discuss the perceived inflammatory language used in the notice, the Minister's failure to meet with Jewish community representatives despite frequent approaches in that regard and his acquiescence to the request of Open Shuhada Street<sup>6</sup> to adopt that course of action. The Minister was further requested to address the matter with Israel at a bilateral diplomatic forum.

Following the Minister's dismissal of their appeal, the SAJBD and the SAZF announced that they would challenge "this flawed, tainted and politically biased" process. David HERSCH, from the Cape Town-based South Africa Israel Public Affairs Committee, said "we will be calling for this law, should it be promulgated, to be legally challenged in the South African Constitutional Court and we will pursue the possibility of doing so ourselves".

The MJC and the Media Review Network (MRN) circulated a petition of support for Minister DAVIES within the greater Muslim communities in South Africa, especially in Masjids in Western Cape and Gauteng.



In a demonstration of support for Israel's opposition to the re-labelling of products from the occupied territories, the Inkatha Freedom Party (IFP) and the African Christian Democratic Party (ACDP) joined the SAZF in a march on 28 June 2012 to the offices of the Department of Trade and Industry where a memorandum was handed over. According to the ACDP, South Africa should not take sides on the Middle East crisis and should rather position itself as a credible mediator. In the aftermath of this march, COSATU accused the ACDP and IFP of legitimising apartheid in Israel "by marching against the proper labelling of products made in the illegal Israeli settlements in the occupied Palestinian territories" and Israel of meddling in South Africa's democratic process.

#### **2.4 University of KwaZulu-Natal Cancels Lecture by Israeli Deputy Ambassador to South Africa**

The University of KwaZulu-Natal (UKZN) announced on 20 May 2012 that it had cancelled a lecture on 21 May 2012 to be delivered by Israeli Deputy Ambassador to South Africa, Yaakov Finkelstein. The decision was reached after the university came under pressure from student organisations and academic staff to cancel the lecture, as it would have violated the "academic boycott" of Israel. In reaction, a spokesperson for the Embassy of Israel in Pretoria conceded that the pro-Palestinian campaign of "intimidation and threats" had reached a level where "there was a genuine threat to the diplomat's well-being". This cancellation came in the wake of the University of Johannesburg (UJ)'s decision in 2011 to impose an academic boycott on Israel and bring an end to its institutional relationship with Israel's Ben-

<sup>6</sup> Open Shuhada Street is a pro-Palestinian organisation campaigning for boycotts and sanctions against Israel.



Gurion University, thereby becoming the world's first university to enforce an academic boycott on Israel. Several student movements, including the South African Students Congress (SASCO), have publicly supported this academic boycott.

## 2.5 Calls for Boycott of Israeli Goods

During the June 2012 ANC Policy Conference held in Midrand, Gauteng, delegates reaffirmed their intention to "increase" support for the Palestinians, and called for the boycott of Israeli goods. In this regard, presidential advisor on international relations, Lindiwe ZULU, echoed participants' belief that there had to "be an increase in the boycott of products imported from Israel to South Africa" and that "an increase in visibility" had to be evidenced on



Palestine. These comments came in the wake of statements by Minister of Arts and Culture, Paul MASHATILE in February 2012 that South Africa was considering imposing economic and cultural sanctions on Israel as part of the worldwide BDS campaign and in reaction to Israel's "destruction of the Palestine society and denial of basic Palestinian rights".

In a related development, students and representatives of Palestinian civil society youth organisations appealed to the Student Council of the University of the Witwatersrand (Wits) in August 2012 to adopt at its annual meeting a resolution to boycott Israel. A number of pro-Palestinian student organisations, such as the Palestinian Student Campaign for the Academic Boycott of Israel, had successfully approached like-minded student groups in South Africa, which resulted in that request. These organisations hope that their initiatives will contribute to efforts to force Israel to respect international laws and conventions on human rights.

## 2.6 Anti-Israel Statements by Representatives of the South African Government

On 12 August 2012, the South African Deputy Minister of International Relations (DIRCO), Ebrahim EBRAHIM called on South Africans to avoid visiting Israel because of Jerusalem's treatment of Palestinians and urged South Africa to "scale down" its economic ties with Israel. In response, the SABJD called these remarks "grossly discriminatory, counter-productive and wholly inconsistent with how South Africa normally conducts its international relations". Earlier on 14 July 2012, Deputy Minister of DIRCO, Marius FRANSMAN, had suggested in a speech in Cape Town that "economic diplomacy could be one of the most effective weapons of change in the Palestinian situation".

## 3. SECURITY IMPLICATIONS

Despite growing levels of frustration experienced by the Jewish community in South Africa, no violent retaliatory threats have thus far been evidenced. The following



illustrates, however, what the diplomatic and security implications would represent for South Africa, if the status quo were to worsen:

- ***Increased Pressure by the pro-Palestinian Lobby on the South African Government:*** The South African Government can expect to come under renewed pressure from organisations in South Africa sympathetic to the Palestinian cause to harden its stance and impose economic and cultural sanctions against Israeli. This pressure is expected to increase exponentially as more successes, such as the cancellation of official visits to Israel, are achieved.
- ***Deteriorating Diplomatic Relations between South Africa and Israel:*** Although diplomatic relations between South Africa and Israel are strained, they are likely to deteriorate if the South African government intensifies its anti-Israel stance and implements a measure of cultural and economic sanctions. Following the announcement by Minister DAVIES in May 2012, some Israeli politicians called for Israel to lower South Africa's diplomatic ranking and even mooted the possibility of expelling the South African ambassador to Israel. It should be considered too that Israel is currently involved in several development projects in Africa and that it could use its influence to jeopardise South African interests, including diplomatic efforts, on the continent.
- ***Relations between the SSA and MOSSAD:*** Although the current relationship between the SSA and MOSSAD is strained, the SSA believes that it would be in the MOSSAD's interest to uphold the status quo with the SSA. It is expected that the MOSSAD will continue to aggressively approach the SSA on issues critical to Israel's national security interests, such as planned terror attacks by Hezbollah against Israeli interests in South Africa. However, should any response by the SSA not meet with its approval, the MOSSAD is likely to expand its existing cooperation with local security institutions and foreign intelligence services. Depending on the nature of this cooperation, this could prove detrimental to the SSA.
- ***Relations with the US:*** Given the global geopolitical landscape and the fact that the US is a major ally of Israel, deteriorating diplomatic relations with Israel and the possible introduction by South Africa of economic sanctions against Israel could put strain on existing US/South Africa relations and jeopardise South Africa's future participation in various global economic and development forums. The possibility exists that the US could adopt a tougher attitude against South Africa in multi-lateral forums such as the UN.
- ***Possible Incidents of violence against Jewish Institutions in South Africa:*** The risk exists that an escalation in current anti-Israel initiatives in South Africa may significantly increase polarisation between the Jewish community and pro-Palestinian support groups in South Africa, resulting in isolated incidents of violence against Jewish interests.
- ***Increased Concerns over safety of Jewish Interests in South Africa:*** Although it is to be expected that the Jewish community will continue to voice its disapproval through accepted constitutional means, there is a growing feeling



within the local Jewish community that the anti-Israel sentiment in South Africa is gaining momentum and that Jewish interests could in future be targeted.

In an article published in the *Jewish Report* in August 2012, the SAJBD in Johannesburg urged its members to report anti-Israel or anti-Semitic graffiti in public places and described these graffiti as a "way of intimidating the Jewish people for their support to the Israeli government". This call was made after yet another anti-Semitic graffiti was spray-painted on a wall in Louis Botha Avenue in Johannesburg, Gauteng. During previous periods (2009 – 2011) of intensified anti-Israel protest actions and rhetoric, often ferocious in nature, concerns were raised by the Jewish community in South Africa over the safety of its members and were instructed by the SAJBD to be vigilant in relation to the safety of Jewish schools and religious institutions.

In a related matter, the activities of the Community Security Organisation (CSO)<sup>7</sup> came under the attention of the SSA during the World Summit on Sustainable Development during 2002, when concerns regarding the security of visiting Israeli delegation were raised by the SAJBD. Being closely aligned to the SAJBD, the CSO, with the assistance of private security companies, took ownership of securing the safety of the Israeli delegation in anticipation of possible pro-Palestinian protest action. The CSO came under intelligence attention in 2007 when security concerns were expressed by the Jewish community following threatening pamphlets being distributed, allegedly targeting local Jewish institutions and communities. Even though the CSO in South Africa has not been linked to any violent actions in recent years, it is likely that the CSO will respond to any direct threat to Jewish interest in South Africa.

- **Attacks on South African IT and Telecommunications Infrastructure:** It is possible that Israeli nationals active in the IT and telecommunications environments can penetrate and deliberately compromise South Africa's IT and telecommunications infrastructure. This suspicion was strengthened after the SSA was notified in July 2012 that the Minister of Finance had received a hand-delivered letter from unknown sources on 28 June 2012 threatening to launch an internet-based cyberattack against South Africa's banking and financial sectors if certain demands were not met within 30 days. These demands, in response to South Africa's support for the BDS campaign, called for the discontinuation of the BDS campaign and the removal and prosecution of some unidentified individuals linked to the BDS.

The authors of this letter claimed to be former MOSSAD members with access to various technologies and resources of the MOSSAD's Electronic assault and Defence Division. They further claimed to have assisted with the development of the malicious Stuxnet and Flame viruses<sup>8</sup>. Although the authenticity of the letter and credibility of the threat are currently being investigated by the Directorate of Priority Crime Investigation (DPCI), they are nonetheless indicative of the growing dissatisfaction within the Jewish community over the perceived anti-

<sup>7</sup> Concern exists within the SSA over the links between the CSO and Israeli intelligence/security structures and the role being played by the CSO to safeguard Israeli interests abroad.

<sup>8</sup> Highly sophisticated and malicious computer viruses believed to have been developed by Israel and the US to attack entities in several countries in the Middle East.



Israel stance in South Africa and the extent to which some individuals and groups are prepared to retaliate. **Remark:** *The outcome of the DPCI investigation is not known.* It remains another strong possibility that Israeli businesses in South Africa, especially those suspected in some cases of being linked to the Israeli intelligence/security community, could increase their offensive espionage activities.

- **Implementation of Stricter Travel Measures to Israel and Palestine:** Israel could impose stricter travel measures on South African nationals wanting to travel from South Africa to Israel and Palestine. Numerous examples exist of Israeli authorities refusing entry into Gaza to South African humanitarian organisations. Likewise, the screening and profiling of travellers to Israel by EL AL personnel at the O R Tambo International Airport (ORTIA) could be intensified.

#### 4. CONCLUSION

Although it is expected that any counteroffensive by the Jewish community in South Africa and even Israel will be subtle and calculated in nature, rather than violent or disruptive, the rising levels of frustration and anger within the Jewish community in South Africa should be noted.

Current information does not indicate the likelihood of any incidents of violence against Jewish interests in South Africa in the short term but the situation will be closely monitored.



# ALJAZEERA



**SSA DOMESTIC BRANCH  
INTELLIGENCE BRIEF  
GROWING ANTI-ISRAEL LOBBYING:  
SECURITY IMPLICATIONS FOR SOUTH AFRICA**

**SEPTEMBER 2012**

**HARD-COPY DISTRIBUTION**

**EXTERNAL CLIENTS**

1. Minister of State Security
2. Director-General: State Security Agency

**INTERNAL CLIENTS**

1. Director: State Security Agency: Domestic Branch (DB01)
2. Deputy Director: Counterintelligence (DB03)
3. Deputy Director: Domestic Intelligence (DB02)
4. General Manager: Counterintelligence (CI10)
5. General Manager: Counterterrorism (CT10)
6. General Manager: Domestic Intelligence (OC10)
7. General Manager: Intelligence Management (IM10)
8. General Manager: Operational Support (OS10)
9. Manager: Counterintelligence Analysis (IM20)
10. Manager: Counterintelligence Centre (DB30)

**ALJAZEERA**



**FEEDBACK TO THE DOMESTIC BRANCH OF THE STATE SECURITY AGENCY**

Clients are kindly requested to complete this form by ticking in the relevant block and returning it to the Domestic Branch of the State Security Agency.  
Product Particulars: Intelligence Brief: Growing Anti-Israel Lobbying: Implications for South Africa

Client: \_\_\_\_\_

FEEDBACK ON PRODUCT RECEIVED	
QUALITY – RATING AND GRADING SCALES	RATING
<b>Value</b>	
3: Product had <i>strategic value</i>	
2: Product had <i>tactical value</i>	
1: Product was of <i>no use</i>	
<b>Quality</b>	
3: <i>Excellent</i> product	
2: <i>Good</i> product	
1: <i>Poor</i> product	
<b>Timeliness</b>	
2: Product was received timely	
1: Product not received timely	
<b>Contribution</b>	
3: Product <i>contributed significantly</i> and enabled client to make informed decisions	
2: Product <i>contributed</i> to client's need for background information	
1: Product <i>did not contribute</i> – irrelevant to the client	
<b>CLIENT'S COMMENT</b>	

ALJAZEERA



**DECLARATION OF DESTRUCTION**

FROM:

TO: State Security Agency: Domestic Branch  
Divisional Head: Records Management (IM42)  
Private Bag X87  
PRETORIA  
0001

We, the undersigned, declare that the following document has been destroyed in our presence and according to the relevant security instructions:

INTELLIGENCE BRIEF: GROWING ANTI-ISRAEL LOBBYING: IMPLICATIONS  
FOR SOUTH AFRICA  
DMS:10000585948  
COPY ..... OF ..... COPIES

We have verified by means of a physical check that the document was complete when destroyed.

WITNESS

SIGNATURE: .....

SIGNATURE: .....

NAME: .....

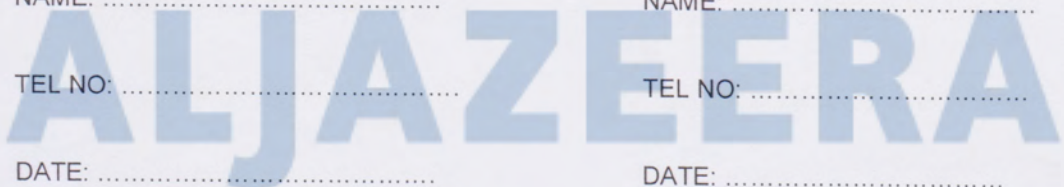
NAME: .....

TEL NO: .....

TEL NO: .....

DATE: .....

DATE: .....





SECRET



**STATE SECURITY COMMITTEE**

**JOINT ACTION PLAN**

**ZIMBABWE-REPUBLIC OF SOUTH AFRICA**

**2011/2012**

---

**ALJAZEERA**

SECRET



SECRET

**OBJECTIVE: 1: TO EXCHANGE INFORMATION AND INTELLIGENCE**

ACTION STEP	TARGET DATE	RESPONSIBILITY	COMMENT/S
<p><b>1. Cooperate and exchange information on Border Intelligence.</b></p> <ul style="list-style-type: none"><li>• Illegal Migration (including information on informal border-crossings);</li><li>• Human Smuggling and Trafficking, Drug Trafficking and goods smuggling;</li><li>• Corruption at border posts (identify corrupt officials and counter their activities);</li><li>• Identity cards theft and forgery of travel documents;</li><li>• Counterfeit drugs and medicines;</li><li>• To share approaches on the conduct of Threat and Risk Assessments.</li></ul>	<p>30 April 2012 31 October 2012</p>	<p><b>CIO and SSA: Internal/Domestic</b></p>	<p>Meetings to be held bi-annually</p>
<p><b>2. Conduct experts meetings to share information, perspectives and expertise</b></p>	<p>29 February 2012 31 October 2012</p>	<p><b>CIO and SSA: Internal/Domestic</b></p>	<p>Meetings to be held bi-annually</p>

ALJAZEERA

SECRET



ACTION STEP	TARGET DATE	RESPONSIBILITY	COMMENT/S
<p>on the two countries' legal frameworks governing migration, human trafficking and smuggling.</p> <p><b>3. Conduct analysis exchange meetings on issues relating to bilateral, regional and international developments.</b></p>	<p>30 April 2012</p> <p>31 October 2012</p>	<p><b>CIO and SSA: External/Foreign</b></p>	<p>Meetings to be held bi-annually. SSA to host the first meeting</p>
<p><b>4. Cooperate and exchange information on International Terrorism &amp; Proliferation of WMD:</b></p> <ul style="list-style-type: none"> <li>• Monitor and share information (perspective and expertise) on counter terrorism; <ul style="list-style-type: none"> <li>▪ terror financing</li> <li>▪ émigré communities and entities; extremist individuals</li> </ul> </li> <li>• Conduct experts meetings to share information (perspectives and expertise)</li> </ul>	<p>31 March 2012</p> <p>31 August 2012</p>	<p><b>CIO and SSA: CI</b></p>	<p>Engage in information sharing on regional and continental perspectives on activities of suspected terrorists, suspected networks and movement of terror cells.</p> <p>First workshop to be held in Pretoria.</p>



ACTION STEP	TARGET DATE	RESPONSIBILITY	COMMENT/S
<p>on terrorism;</p> <ul style="list-style-type: none"> <li>• Monitor issues pertaining to proliferation of WMD.</li> </ul> <p><b>5. Exchange information and cooperate on issues pertaining to Economic Intelligence</b></p> <ul style="list-style-type: none"> <li>• Sharing of information on threats facing the two economies; <ul style="list-style-type: none"> <li>▪ Precious metals and rare earth minerals</li> <li>▪ Financing systems,</li> <li>▪ Money laundering</li> <li>▪ Economic sabotage/under invoicing</li> <li>▪ Agriculture</li> <li>▪ Illicit Textile industry</li> <li>▪ Illicit tobacco industry</li> </ul> </li> <li>• Best practice visit by SSA to CIO on Economic Intelligence</li> </ul>	<p>31 March 2012</p> <p>31 August 2012</p> <p>Ongoing</p> <p>31 March 2012</p>	<p><b>CIO and Economic Intelligence</b></p> <p><b>SSA:</b></p>	<p>Continue to engage and share information</p> <p>Possible training needs to be identified during both visits</p>



ACTION STEP	TARGET DATE	RESPONSIBILITY	COMMENT/S
<ul style="list-style-type: none"> <li>Best practice visit by CIO to the Financial Intelligence Centre (FIC)</li> </ul>	30 April 2012		

**OBJECTIVE 2: TO MONITOR ACTIVITIES AIMED AT SUBVERTING CONSTITUTIONAL ORDER**

ACTION STEP	TARGET DATE	RESPONSIBILITY	COMMENT/S
<p><b>1. Monitor and exchange information on rogue NGOs and other Institutions<sup>1</sup>.</b></p> <ul style="list-style-type: none"> <li>The identification, profiling and assessment of NGOs engaged in subversive activities taking into account the following:</li> </ul>	<p>31 March 2012 31 August 2012</p>	<p><b>CIO and SSA: Internal/Domestic</b></p>	<p>CISSA definition of rogue NGOs to apply</p> <p>Further engage and share information.</p>

<sup>1</sup> These include other non-state actors like Think Tanks, Non Profit Trusts etc.



ACTION STEP	TARGET DATE	RESPONSIBILITY	COMMENT/S
<ul style="list-style-type: none"> <li>▪ Financing;</li> <li>▪ Regulation;</li> <li>▪ Nature of the pressure exerted;</li> <li>▪ Political agenda; and</li> <li>▪ Undue influencing of policy.</li> </ul> <ul style="list-style-type: none"> <li>• Continuous sharing of experiences using case studies</li> </ul> <p>2. <b>Cooperate and exchange intelligence on Private Security/Intelligence Organisations (involved in Military and Intelligence activities)</b></p> <ul style="list-style-type: none"> <li>• Individuals and companies involved in mercenary activities, illicit weapons supply and military training;</li> </ul> <p>3. <b>To identify and neutralise activities of information</b></p>	<p>31 March 2012</p> <p>31 August 2012</p> <p>31 March 2012</p>	<p><b>CIO and SSA: CI</b></p> <p><b>CIO and SSA: CI</b></p>	<p>Further engage and share information.</p> <p>Further engage and share information.</p>



ACTION STEP	TARGET DATE	RESPONSIBILITY	COMMENT/S
<p><b>peddlers taking into account the following:</b></p> <ul style="list-style-type: none"> <li>• Create a database on information peddlers; and</li> <li>• Development of a common approach on profiling</li> </ul>	31 August 2012		
<p>4. <b>Monitor and exchange information on Media, including social networks</b></p> <ul style="list-style-type: none"> <li>• Identify and profile subversive media.</li> </ul>	<p>31 March 2012</p> <p>31 August 2012</p>	<b>CIO and SSA: CI</b>	Further engage and share information.



SECRET

**OBJECTIVE: 3: TO CONDUCT JOINT OPERATIONS**

ACTION STEP	TARGET DATE	RESPONSIBILITY	COMMENT/S
1. Ratify and sign the Joint Operational Guidelines.	31 January 2012	CIO and SSA : Directors General	
2. Implement Operational Plans (Project Hippo) for the following:- <ul style="list-style-type: none"><li>• Human Smuggling and Trafficking</li><li>• Cigarette Smuggling</li></ul>	Continuous	CIO and SSA : Internal/Domestic	
• Develop and Implement Operational Plans to counter Poaching	31 March 2012	Internal/Domestic	



**OBJECTIVE 4: TO ENHANCE COOPERATION ON SPECIAL EVENTS**

ACTION STEP	TARGET DATE	RESPONSIBILITY	COMMENT/S
<p>1. <b>Exchange Intelligence and information regarding COP17</b></p> <p>Assessments to be conducted in terms of:</p> <ul style="list-style-type: none"> <li>• Specific focus on border security at Ports of Entry and border lines;</li> <li>• Terror-related risks;</li> <li>• Monitoring of pressure groups and social media networks.</li> </ul>	<p>Ongoing until February 2012 (COP17)</p>	<p><b>CIO and SSA: Internal/Domestic</b></p>	<p>Identification of risks needs to be based on threat and risk assessment</p>



## OBJECTIVE 5: TO ENHANCE COOPERATION THROUGH TRAINING AND DEVELOPMENT

ACTION STEP	TARGET DATE	RESPONSIBILITY	COMMENT/S
1. <b>Implementation of mutual training needs.</b>			
1.1 <b>SSA Needs</b>			
• Training in Counter-intelligence Management	16-27 April 2012	<b>CIO Academy</b>	Training will take place in Harare
• Border Intelligence	13-24 February 2012	<b>CIO Academy</b>	Harare
• Economic Intelligence Collection	26 March-6 April 2012	<b>CIO Academy and SSA IA</b>	Harare
1.2 <b>CIO Needs</b>			
• Advanced Investigations in Intelligence	9-20 July 2012	<b>SSA IA</b>	Training will take place in Pretoria
• Management Development Studies (Advanced Supervisory Effectiveness)	16-27 January 2012	<b>SSA IA</b>	SSA IA will facilitate training with relevant academic institutions in RSA.



<ul style="list-style-type: none"> <li>• Train the Trainer programme             <ul style="list-style-type: none"> <li>▪ Facilitation</li> <li>▪ Assessment and Moderation</li> </ul> </li> </ul>	16-27 2012	January	<b>SSA IA</b>	Pretoria
<ul style="list-style-type: none"> <li>• Evaluation and Analysis (Threat Perception and forecasting)</li> </ul>	19-30 2012	March	<b>CIO Academy and SSA IA</b>	Pretoria
<ul style="list-style-type: none"> <li>• Management on the Counter-Proliferation of Weapons of Mass Destruction (WMD)</li> </ul>	20-24 2012	August	<b>SSA IA</b>	Pretoria
<ul style="list-style-type: none"> <li>• Border Intelligence</li> </ul>	12-22 2012	March	<b>SSA IA</b>	Pretoria
<ul style="list-style-type: none"> <li>• Financial Intelligence</li> </ul>	11-22	June 2012	<b>SSA IA</b>	Pretoria
<ul style="list-style-type: none"> <li>• Illicit Mining             <ul style="list-style-type: none"> <li>▪ The identification and evaluation of minerals and precious stones.</li> <li>▪ Trends and methods used by smugglers to conceal special stones and minerals.</li> <li>▪ Fingerprinting of precious metals and stones such as diamonds, gold and platinum.</li> <li>▪ Training in the use of gold and diamond testers/detectors.</li> </ul> </li> </ul>	31	March 2012	<b>SSA NC SSA DB SSA IA</b>	CIO to liaise with NICOC/IA (any other institution considered appropriate) on cost cutting measures, focus areas and course content. CIO to unpack the training needs.
<ul style="list-style-type: none"> <li>• Illicit Mining (Intelligence Perspectives)</li> </ul>				Training will focus on the role of intelligence pending allocation of resources to the full course.



## OBJECTIVE: 6 TO ENHANCE TECHNOLOGICAL COOPERATION

ACTION STEP	TARGET DATE	RESPONSIBILITY	COMMENT/S
<p><b>1. Identification of areas of technological cooperation.</b></p> <ul style="list-style-type: none"> <li>• Counterfeit document detection</li> <li>• Basic Technical Surveillance Counter Measures (TSCM)</li> <li>• Advance TSCM</li> <li>• Night Vision Surveillance Counter Measures</li> <li>• Tactical Operational Equipment</li> </ul>	<p>June 2012</p> <p>6- 9 February 2012</p> <p>26 – 31 March 2012</p> <p>28 May – 1 June 2012.</p> <p>23 – 31 July 2012</p>	<p><b>CIO and SSA NC: Technical</b></p> <p><b>SSA NC SSA IA</b></p> <p><b>SSA IA</b></p> <p><b>SSA IA</b></p>	<p>SSA already prepared two Courses in Harare (SSA will facilitate all training to be conducted by NC and DB)</p> <p>Harare</p> <p>Pretoria</p> <p>Basic Induction Course for detection and concealment of clandestine devices.</p> <p>Visit to Suppliers SA Joint Training on Tactical Detection to be presented at OSL Pretoria</p>



SECRET

ACTION STEP	TARGET DATE	RESPONSIBILITY	COMMENT/S
<b>2. Secure Communications:</b> Secure Communication link between the two Services; <ul style="list-style-type: none"><li>• Provision of secure room</li><li>• Installations</li></ul>	26-31 March 2012	<b>CIO SSA NC (Technological)</b>	Equipment ready and CIO to prepare room for the installations
<b>3.</b> Conducting of research into Threats and Opportunities presented by social media networks	August 2012	<b>CIO and SSA NC</b>	To convene a Workshop to share assessments



SECRET

**JOINT ACTION PLAN:**

**ZIMBABWE – REPUBLIC OF SOUTH AFRICA**

**2011/2012**

---

SIGNED BY: \_\_\_\_\_

DEPUTY DIRECTOR GENERAL  
CENTRAL INTELLIGENCE ORGANISATION

Date: \_\_\_\_\_

SIGNED BY: \_\_\_\_\_

DIRECTOR  
STATE SECURITY AGENCY

Date: \_\_\_\_\_

**ALJAZEERA**

SECRET



CONFIDENTIAL

(This document is the property of the Governments of the  
Republics of Zimbabwe and South Africa)



REPORT OF THE 3<sup>RD</sup> MEETING OF THE JOINT INTELLIGENCE  
TASK TEAM OF THE STATE SECURITY COMMITTEE OF THE 6<sup>TH</sup>  
SESSION OF THE ZIMBABWE-SOUTH AFRICA JOINT  
PERMANENT COMMISSION ON DEFENCE AND SECURITY,  
ELEPHANT HILLS HOTEL, VICTORIA FALLS, ZIMBABWE

29-30 OCTOBER 2011

ALJAZEERA



CONFIDENTIAL

REPORT OF THE 3<sup>RD</sup> MEETING OF THE JOINT INTELLIGENCE TASK TEAM (JITT) OF THE STATE SECURITY COMMITTEE OF THE 6<sup>TH</sup> SESSION OF THE ZIMBABWE-SOUTH AFRICA JOINT PERMANENT COMMISSION ON DEFENCE AND SECURITY, ELEPHANT HILLS HOTEL, VICTORIA FALLS, ZIMBABWE

1. INTRODUCTION

1.1 The third meeting of the Joint Intelligence Task Team (JITT) of the Zimbabwe-South Africa Joint Permanent Commission on Defence and Security (JPCDS), was held at Elephant Hills Hotel, Victoria Falls, Zimbabwe from 29 to 30 October 2011. The Zimbabwean delegation was led by [REDACTED] Director External of the Central Intelligence Organisation (CIO), who chaired the meeting. The South African delegation was led by [REDACTED] the General Manager at the State Security Agency (SSA), who co-chaired the meeting.

2. OPENING REMARKS

2.1 In his opening remarks, the Chairperson, [REDACTED], welcomed the South African delegation to Zimbabwe and particularly, to Victoria Falls. He highlighted that JITT provides the two sister Services with the opportunity to review progress on the implementation of the Joint Action Plan adopted at the last meeting held in November 2010 in Durban, South Africa. The Chairperson then underscored the role played by the Southern African Development Community (SADC) at continental gatherings, such as the African Union (AU) related meetings, where SADC, made meaningful and significant contributions.

2.2 In his reciprocal remarks, the Co-Chairperson, [REDACTED] expressed appreciation over the warm hospitality accorded his delegation. He urged the

ALJAZZEERA



CONFIDENTIAL

4.2 The meeting noted the need for the exchange of information on risks and threats associated with hosting a global event of such magnitude. These include, *inter alia*, possible terror attacks, border management challenges, transnational organised crimes and disruptive acts by non state actors.

4.3 The committee emphasized the need to monitor the activities of pressure groups stationed in either country or those that might want to use regional countries as transit to South Africa. The report cited the three African caravans as having the potential for disruptive behaviour thus meriting the attention of intelligence Services.

4.4 The meeting then expressed hope that South Africa will host a successful COP17 and that the conference will yield positive views on issues of climate change that would benefit Africa.

5. **REVIEW OF THE 2010/2011 JOINT ACTION PLAN**

5.1 The meeting noted, with appreciation, considerable progress made in the implementation of the 2010/2011 Joint Action Plan. These included:

- Enhancing cooperation through training and development
- Cooperation in respect to combating international terrorism and proliferation of Weapons of Mass Destruction
- Monitoring activities aimed at subverting constitutional order
- Cooperating and exchanging information on border intelligence
- Enhancing cooperation on the hosting of COP17



CONFIDENTIAL

- Exchanging intelligence on bilateral, regional and international developments through analysis exchange meetings
- Enhancing technological cooperation.

5.2 The meeting noted the challenges faced in the implementation of the Joint Action Plan, such as the adoption of the Joint Operational Guidelines and the financial constraints in fulfilling some of the agreed objectives. The meeting resolved to address the challenges in the new Joint Action Plan.

5.3 The meeting recommended some changes to the Joint Action Plan. These included the realigning of objectives and the provision of specific dates, wherever possible. The committee then agreed that, for purposes of clarity, the timeline of the Joint Action Plan should be the JITT calendar.

**6. JITT SUB-COMMITTEES**

- 6.1 A new sub-committee namely, Domestic Intelligence, was established. The meeting broke into the following sub-committees
- a) Counter Intelligence;
  - b) Training;
  - c) Technical;
  - d) Domestic Intelligence; and
  - e) Economic Intelligence

**7. THE 2011/2012 JOINT ACTION PLAN**

- 7.1 The JITT reviewed the 2010/2011 Joint Action Plan, developed and adopted the 2011/2012 Plan. These included new training requirements and enhanced co-operation in the exchange of information on threats and opportunities of social media networks, illicit textile and



CONFIDENTIAL

tobacco industries as well as best practice visits. The committee noted the need to develop and implement operational plans to counter poaching.

7.2 The meeting further agreed that respective Heads of branches should meet regularly to discuss matters at their level. Hitherto, meetings were being held at lower levels without much participation at the level of Heads of branches.

**8. CONSIDERATION OF THE DRAFT AGENDA FOR THE STATE SECURITY COMMITTEE**

8.1 The JITT proposed the following agenda items for the State Security Committee:

- 1) Opening Remarks;
- 2) Adoption of the Agenda;
- 3) Presentation of Security Situation Briefs;
  - a) Zimbabwe
  - b) South Africa
- 4) Presentation and Adoption of the 2010-2011 JITT Report
- 5) Presentation and Adoption of the 2011-2012 Joint Action Plan;
- 6) Any Other Business;
- 7) Closing Remarks

**9. CLOSING REMARKS**

9.1 The co-Chairperson, [REDACTED] expressed satisfaction that the meeting had deliberated on key issues pertaining to the Joint Action Plan. He underscored the need for continued engagement on issues of mutual cooperation and reiterated the challenges the region was facing. He thanked the Chairperson for successfully steering deliberations of the JITT meeting.



CONFIDENTIAL

9.2 In his concluding remarks, the Chairperson, [REDACTED] [REDACTED] thanked the South African delegation for the fruitful engagement and expressed hope that the two Services will work to implement the agreed work plans. He thanked both teams for displaying commitment to JITT deliberations.



ALJAZEERA



CONFIDENTIAL

Document Number: 10000384717



## state security

State Security Agency  
REPUBLIC OF SOUTH AFRICA

### *FIS Feedback*

---

File reference: 1/5/2  
Compilation Date: 9 June 2010  
Originating structure: CT Analysis Desk (IM22)

---

**FROM:** *General Manager: Intelligence Management Centre (IMC)*

**TO:** *Head Foreign Liaison*

**CC:** *See recipient list*

#### *LS 867 (Sri Lanka): Feedback*

1. It would be appreciated if the appended document could be liaised with the representative of LS 867.
2. Thank you for your attention.

*As signed*

General Manager: Intelligence Management Centre (IMC)

# ALJAZEERA

CONFIDENTIAL



CONFIDENTIAL

Reference: 10000384717

**Feedback: LTTE Training Camp**

1. Your request (Ref no: S1424/10)
2. Our Service could not confirm information from your Service suggesting that a Liberation Tigers of Talim Ealam (LTTE) military training camp was held in South Africa in May 2010 and that individuals from Australia, Canada and the United Kingdom (UK) may have attended.
3. Our Service would like to note that a number of Tamil organizations do exist in South Africa. Although previous estimates suggested that the membership/supporters of these Tamil organizations in South Africa could be around 700 000, this remains an estimated figure.
4. Tamil organizations in South Africa are actively involved in promoting the Tamil culture and heritage and are continuously involved in organising various cultural and other events. They are involved in various fundraising initiatives such as concerts, to raise funds to provide relief to the under-privileged, homeless, disabled, orphans and refugees both in South Africa and Sri Lanka. In this regard, some Tamil organizations are also financially supported by prominent businessmen in South Africa. Tamil organisations also continue to voice their criticism against issues of morality such as pornography and blasphemy specifically relating to their religion and culture.
5. Over the past year, Tamil organizations from time to time staged peaceful protest marches, including at major sporting events, to voice their opposition at perceived human rights abuses against the Tamil people by the Sri Lankan Government. However, their focus was not solely on Sri Lanka, but also against perceived human rights abuses in other countries.
6. Tamil organizations in South Africa have previously played host to several foreign delegations from Sri Lanka and had been involved in discussions with various government structures and politicians on the issue of the Tamil people in Sri Lanka. Members of Tamil organizations in South Africa, for example the Tamil Federation of KwaZulu/Natal, have previously formed part of official South African government delegations (for example to India) to sign agreements in respect of trade and industry, science and technology, agriculture, as well as cultural exchange programmes.
7. Tamil organizations from Sri Lanka have also previously visited South Africa on invitation of the South African Government and had discussions with senior South African government officials as well as with representatives of Tamil organizations in South Africa. The primary aim of these visits was to convey the concerns of the Tamils for a negotiated settlement, to strengthen the peace process and to promote the political aspirations of the Tamil-speaking people. Throughout these engagements, the South African Government gave assurances that South Africa will not be used as a base for terrorist activities, with specific reference to the LTTE, and

CONFIDENTIAL



CONFIDENTIAL

emphasized that South Africa would only support efforts for a political solution in Sri Lanka through negotiation.

8. Although contact between local Tamil organizations in South Africa and similar organizations in other countries, including the LTTE has been confirmed in the past, the exact nature and extent of these links and to what extent cooperation is currently taking place remains largely unclear. Available information does not indicate which of these Tamil organizations are *actively* and *directly* supporting the LTTE. Most of these organizations, if not all, are supporting a peaceful settlement in Sri Lanka and are, as stated before, voicing their support through peaceful and constitutional means.
9. Despite being committed to promoting the Tamil culture and heritage, several Tamil organizations in South Africa have experienced some level of discontent over issues of who is best suited to promote the cause of the Tamil people in South Africa. However, these differences are low key and have not disrupted the activities and objectives of these organizations in any way.
10. As for the LTTE in particular, the LTTE does not have any offices or known representatives in South Africa. Ongoing allegations have been made since 1998 by amongst others Sri Lankan government officials and some Sri Lankan academics that Tamil organizations in South Africa are providing the LTTE and some of their supporters with weapons, as well as providing members of the LTTE and Tamil organizations in South Africa with para-military training. It has also been alleged that current contact exists between the LTTE and some former members of the South African Defense Force (SADF). However, available information does not confirm these allegations.
11. Allegations were made in the past that Tamil organizations in South Africa are making donations to charitable and relief organizations abroad and that these donations are used to purchase weapons and other ammunition for the LTTE. Some Tamil organisations in South Africa have even been accused to be a possible terrorist front for the LTTE and of possible involvement in channelling funds to the LTTE. Even though it is known (confirmed through the media) that some Tamil organizations in South Africa did in the past donated funds to the LTTE and acknowledged by the LTTE, no current information exists indicating the amounts involved, the frequency of donations as well as the methods utilised for channelling funds to the LTTE by local Tamil organizations.
12. While the LTTE is a listed terrorist organization in many countries, current risk assessments do not indicate the LTTE to be a direct threat to South Africa's national security. Furthermore, available information currently does not indicate any planning by Tamil organisations in South Africa to stage any protest action or to engage in any unconstitutional activity.
13. Notwithstanding, any activities of the LTTE internationally continues to be monitored with the aim of identifying the possible involvement of the LTTE and local Tamil organizations in possible unconstitutional activities.

CONFIDENTIAL



CONFIDENTIAL

14. Our Service remains committed to close cooperation with your Service in exchanging information relevant to the effective countering of international terrorism.
15. Thanking you for your attention, and our apologies for the late reply.



**ALJAZEERA**

CONFIDENTIAL



SECRET

***Counter Espionage Input to the State Security Project***

1. ***Background on function/theme***

- 1.1 Despite the name change of the former Ministry of Intelligence to the Ministry of State and Security, and the consequent formation of the State Security Agency (SSA), the mission of the latter should stay to collate intelligence on the integrity of the state and to inform government on matters that could impact on national security. The SSA should function as a civilian intelligence service that strives for objectivity and political neutrality which, should not be compromised by giving the new structure executive powers. However, members of the SSA should be empowered to have access to places and information that allows them to fulfil the mandate of the SSA.
- 1.2 Counter Espionage is a component of Counter Intelligence which, traditionally resorts within a domestic civilian intelligence service as one of its primary focuses.

2. ***Conceptualisation of function/theme***

- 2.1 Most readers of intelligence literature, and many counterintelligence practitioners, believe that the essence of counterintelligence is investigation - the collection of information needed to hunt down spies and moles who have infiltrated one's own government and society. This is a restricted view of the defensive investigative aspect of counterintelligence. Perhaps the queen of the counterintelligence chessboard is counterintelligence analysis, both offensive and defensive.

The problems start at the beginning. Where to concentrate energy and resources? Sometimes circumstances point counterintelligence in a particular direction. The defection of an officer of an adversary service, such as the KGB's Anatoliy Golitsyn in the 1960s or Oleg Gordievsky in the 1980s, provides "leads." Or an agent is "turned in," as was the American spy John Walker. Counterintelligence runs down the implications of such cases and conducts a damage assessment.

Most of the time, however, determining the precise focus of counterintelligence, what resources should be deployed where to accomplish the mission, is anything but obvious. What does a counterintelligence analyst zero in on when, for example, at any one time Russia or China alone may have as many as several thousand government employees abroad? Then there is the additional problem of many thousands of émigrés from the former Soviet Union. A tiny percentage of these individuals are, despite the changes in those countries, Russian and Commonwealth of Independent States (CIS) intelligence officers seeking to enter into a clandestine relationship with U.S. citizens. But which ones?

SECRET



SECRET

2

And those are just the foreign agents. At any one time in the United States itself, several million people have access to classified information. Some are generals in the military or senior managers of intelligence agencies. Many more work in data banks, administration, and communications. Only a handful might ever be tempted to pass sensitive information to foreign intelligence services. But it takes only one Wilker-Whitworth ring or one Aldrich Ames to do a country massive damage. Even in a dictatorship, but certainly in a democracy, it is impractical to watch over millions of people, much less to secure their communications and their telephone calls from monitoring by foreign intelligence services. Moreover, each major industry, each sensitive weapons or communications system, each command and control system each sensitive installation such as an Embassy abroad is a potential target of hostile intelligence personnel or technical collection. But which ones are targeted, and what techniques are being used to target them. U.S. satellite systems play an important role. What can foreign governments be reasonably expected to know about them-how they look, how they orbit, how and where they were built? How could they use this information for deception or to conceal their activities from collection?

Day in and day out, intelligence services receive a flood of information about foreign governments' attempts to influence events in other countries. Some of these reported activities reveal the hands of hostile intelligence. Which ones? The answers to such questions are far from obvious. If a government deploys its security agents and its counterspies without first determining the priorities of foreign intelligence operatives, it will likely miss many of the threats and opportunities it ought to be targeting. At best, and with luck, it may stumble on a few. But if a government answers these questions well, if, that is, it has good analysis-it will be well positioned to use its counterintelligence resources effectively.

#### **Triage of Targets.**

Ascertaining what really needs protection is the place to begin, especially given the limited and diminishing resources available to counterintelligence. As former White House director of intelligence programs has pointed out, although democracies have far fewer secrets than authoritarian regimes (where most official actions machinations are secret), the ones they have may be more precious. Thus in a democracy, each secret is an inviting target.

What secrets need top protection in a powerful technologically advanced country? They include strategic command and control systems, locations and characteristics of strategic

SECRET



SECRET

3

weapons; the information-processing circuits that such weapons depend on; and specific plans for the use of these weapons and for the defence of leaders and retaliatory forces.

Next on the list of priorities come the details of the government's relations with scores of other regimes around the world. In the absence of immediate common threat, relations among states can be particularly strained. Adversary governments or groups may use both overt diplomacy and propaganda and covert action to split up allies and isolate and discredit certain states.

Consider the US effort to limit the flow of narcotics into America from the Andean regions through Mexico. While many Mexican leaders have goals complementary to those of the United States concerning narcotics – that is, the Mexican leaders do not want their country to become another Colombia – some Mexican also benefit from producing or exporting drugs to the United States. And some Mexican officials have benefited financially or otherwise from narcotic trafficking. Fighting local growers and traffickers and their private armies can be extremely costly to Mexican political and military officials – sometimes even deadly. In these circumstances, US anger at what may appear as Mexican indifference to, or even at times cooperation with, narco-trafficking can be counterproductive. Drug traffickers could inflame US-Mexican tension by, for instance, planting stories in Mexican Newspapers and elsewhere non real or alleged high-level Mexican government involvement with narco-trafficking. Exposing or otherwise neutralising those who use clandestine means to exacerbate strains between states is-or should be- a priority of counterintelligence.

Another essential element to keep under wraps in the plan one state uses in negotiations with another – for instance, where the state is prepared to make concessions, where it will draw the line. Using clandestine means to learn the negotiating position of another state is a longstanding intelligence technique. In French example, a former French intelligence officer, has described how in the 1960s the French foreign intelligence service photographed documents belonging to, the then under-secretary of state George Ball in Ball's hotel room. This operation was conducted to assist then French finance minister Giscard d'Estaing, who was negotiating trade tariffs with the United States. When President de Gaulle was told about this intelligence coup he at first refused to believe it, and then was very grateful. Apparently the French were still using this sort of technique in the late 1980s. Clearly such inside information is a great advantage in difficult negotiations.

A state's military and economic capabilities depend to some extent on technological superiority; in a democracy, this is likely to be in the more vulnerable private sector. Hence, there is a need for government protection of proprietary technology, especially

SECRET



when it is targeted by foreign intelligence. States also need to protect their own clandestine operations-the collection of intelligence, and influencing events abroad. In the United States this is called operational security (opsec). For example, identifying hostile agents is relatively easy if dates of meetings and subject matter to be discussed are discovered, even if specific locations are not disclosed in intercepted message traffic. It was just such a cryptological break, known as Venona, that largely enabled Western services to identify Soviet networks operating in the 1940s and 1950s.

Few states, especially democratic ones, centrally identify which key secrets need the most protection. Counterintelligence resources, rather than being deployed after logical consideration of what it is most important to protect, on the contrary tend to be rationed out in response to bureaucratic pressure and other less calculated factors. Counterintelligence officers on their own cannot assign priority to their country's secrets. They need to work with substantive specialists to determine what areas most need protection, what particular counterintelligence resources and interagency efforts will provide it, and whether these programs are working.

#### **Assessing Vulnerability**

Once the secrets to be protected are identified and policymakers agree, the role for counterintelligence analysis is to ascertain the peculiar vulnerabilities of those secrets. Vulnerability needs to be assessed at the beginning of a major project. A good illustration of this principle is the contrast between the U.S. and Soviet planning for new embassies in the late 1970s and 1980s.

During this time, the United States and the Soviet Union each broke ground on the sites of their respective new embassy complexes in Moscow and Washington. Gaining access to the other's building would have a decided diplomatic, intelligence, and perhaps military advantage, because embassies usually house a government's central diplomatic and Intelligence secrets and sometimes key military secrets. Unlike the Soviet counterintelligence assessment, the American assessment was poor to non-existent, and it showed in the results. Moscow picked an excellent hilltop site in Washington that had many potential benefits for Soviet intelligence activities. The United States fared less well. Moreover, the Soviets took advantage of the construction stage of the US Embassy to enhance their eavesdropping capabilities.

Counterintelligence vulnerability should also be assessed details of proposed treaties and other agreements. As the director of the FBI belatedly pointed out in 1989, the INF treaty and the START agreement allowed the Soviet intelligence service to gain access to numerous sensitive areas and individuals in the United States which, until then, were



SECRET

5

accessible only on a most limited basis. Until 1988, Moscow had only three legal residencies or bases in the United States from which to conduct signals and human intelligence operations: Washington, New York, and San Francisco. As a result of the INF agreement and verification protocol, the Russians acquired a thirteen-year permanent site for twenty personnel in Magna, Utah-known as a "portal site." According to the FBI director, this was in a location uniquely situated for the collection of sigint and humint. Other nuclear, biological, and chemical weapons and other treaties multiply such opportunities.

Changing patterns of emigration may also pose problems. In the mid-1980s, less than one thousand Soviet immigrants entered the United States in a given year. By 1989 the number had risen to approximately twenty-four thousand." Many more thousands of East Europeans, Chinese, and Middle Easterners are now entering Western Europe and Israel, and there is every indication their numbers will increase in future years. In the United States, after five years of residence, an immigrant is eligible for citizenship and a security clearance. If no compromising information turns up in a background check, the immigrant may be eligible for employment even in sensitive installations. This is not to suggest that immigrants are not loyal Americans; to the contrary, those who have gained the liberties and opportunities America grants its citizens may value and protect them more vigorously. Some, however, may be subject to coercion, for example, through pressure on family members at home. And some may be moles, trained intelligence operatives masquerading as immigrants, but in fact already in the employ of a foreign intelligence service. Obviously, this immigration trend subjects the secrets of the United States and other Western countries to increased threat of exposure through the efforts of agents of foreign intelligence services. Determining the nature and degree of this and other threats is one of the first and foremost tasks of counterintelligence analysis.

#### **Adversaries: Targets and Competence**

After defining the defensive perimeter, as it were, the next job of counterintelligence is to analyse what areas foreign intelligence is targeting and assess its ability to reach those targets. On occasion, governments receive windfalls in such matters. A recruited agent or intelligence defector such as the KGB officer code-named Farewell who exposed the extensive Soviet theft of Western technology will produce internal documents evaluating the performance of his or her service. One of the clearest indications of an intelligence service's true interest is what it chooses to target, that is, what its human and technical sources are being tasked to collect or influence. For example, in the 1980s the KGB and

SECRET



GRU did indeed start to target Magna, Utah, as a useful spot from which to intercept U.S. telecommunications.

**Remark: This is an extract from a book written by a CIA analyst about 10 years ago. I felt it made sense.** [REDACTED]

- 2.2 Counter Espionage theory suggests that espionage is traditionally exposed in two ways, namely:
- By scrutinising the communication of a FIS' representative (declared/undeclared) with those who might be his/hers contacts/agents. The main methods to be utilised are interception of communication and surveillance of the representative to identify personal meetings with contacts/agents.
  - By looking at the place where espionage might be taking place. In order to be able to do this it is necessary first to establish national interest by scrutinizing threats and opportunities. This is not being done at present within NIA's Counter Espionage capability (CI20) and if some of it is done by the Chief Directorate Vetting and Advising, the results do not filter through to CI20.
- 2.3 The strategic objectives included in both the national counter intelligence and the NIA counter espionage strategy documents to be included as proposals for the CI function within the SSA.
- 2.4 There is a very strong feeling that the very nature of a civilian intelligence service negates the opportunity for it to have executive powers, as this would tarnish its objectivity in a major way. Having said that there is also members that say we need executive powers as we are not able to enforce anything within the public sector that we need, such as access to information, the arresting and interviewing of espionage suspects and access to restricted areas (for example at airports). The majority of members still felt that executive powers should not be considered for the SSA put that the legitimate problems with access to information and restricted areas should be addressed in such a way that:
- Government departments and its employees, parastatals and its employees, as well as policy makers would be obliged to channel all relevant information automatically and all requested information willingly to the SSA.
  - Membership cards of applicable SSA personnel (operational members and certain researchers and analysts) should afford such a member the ability to say "Please give me that information" (with the necessary checks and balances" in place) and "Please open for me here" in terms of restricted areas.



- The members (especially Operational and Research & Analyses) should be re-trained in order for them to have a different attitude and effectively plug into the community and public sector to obtain relevant information regarding early warning on threats and opportunities in terms of national security.
- 2.5 Another basic element that impacts heavily on an intelligence service's objectivity, public image and effectiveness is the way in which it manages to be apolitical in terms of domestic party politics. The history of NIA and SASS made it almost impossible to achieve this in its forming years but it is necessary that the SSA should follow a new direction and set new standards.
- 2.6 Analyses should inform intelligence collection.
- 2.7 The mapping of national interest through the scrutinising of the different sectors of society for threats, opportunities and needs, should inform the operational priorities of the SSA. This is not an internal process within the SSA only, but should be preceded by a similar annual exercise from the top down within the national government and also within provincial governments. This should be a compulsory and enforceable exercise driven by NICOC and the results should filter down to line functional level.
- 2.8 Another enforceable function of NICOC should be the reporting by all government and parastatal employees of contact with foreigner diplomats.
- 2.9 The SSA should be at the centre of government, but this cannot be achieved through institutionalisation, but will have to be achieved through our intelligence product that should render us indispensable. The SSA should provide government daily with a unique and relevant *intelligence* product which will then put it apart from other consultants.
3. ***Threats/Opportunities on theme (if applicable) - Current as defined in existing NIA documents such as NIE, DIE, 2010, etc***
- 3.1 See Counter Espionage Strategy of NIA as approved in 2007.
- 3.2 Sectors targeted by FIS
- It has been positively established through investigations that FIS have targeted several industrial sectors. They are the following:
- 3.2.1 Defence & Aerospace Sector
- SA experienced the theft of Rooivalk Helicopter Blueprints by a known FIS



- Missile Systems stolen by a known FIS
- Several FIS played an active role influencing decision makers during the tendering process for the Multibillion Defence Procurement Programme, "so called arms deal".
- Theft of Intellectual Property (IP) Rights at several State Owned Enterprises.

### 3.2.2 Bio-Chemical Sector

Most Western services have shown interest in technological development at the Onderstepoort Biological Products (OBP) and Agriculture Research Council (ARC). Those services raise the concern about SA's ability to regulate, protect and control technology used from falling into the hands of terrorist groups such as Al Qaida. Their concerns are that the same technology can be switched in the production of Biological Weapons.

### 3.2.3 Government Security Sector

FIS are interested in knowing locations of NIA's Counter Espionage Units. They are interested in influencing NIA to prioritise and focus its resources towards combating International Terrorism (CT) and Counter Proliferation (CP).

### 3.2.4 Energy sector

FIS have been working frantically to influence the Nuclear Expansion Programme bidding Process. Two main services were identified, namely services from France and the USA. Due to sophistication of their covert operations and lack of CE capacity, it has not been able to neutralise their activities.

Several FIS have shown interests in the progress of the SA's Pebble Bed Modular Reactor (PBMR) research and development. It is suspected that the thefts and break-ins that took place at PBMR were to advance China's rival project called chinergy. As is currently, China has developed and are now one year ahead of PBMR project though they started several years after PBMR launch.

### 3.2.5 Policy Makers & Senior Government officials

Some FIS use their covert members to interact, profile government officials with the sole purpose of accessing first hand, SA's policy position around the world. Departments that are known to have been targeted by FIS are the following:

#### 3.2.6 The Presidency

#### 3.2.7 Department of International Relations and Cooperation

#### 3.2.8 Department of Home Affairs (DHA)

#### 3.2.9 Department of minerals and Energy (DME)

#### 3.2.10 Department of Agriculture (DoA)

#### 3.2.11 Department of Environmental Affairs and Tourism (DEAT)

## 4. *New non-traditional threats*



- National interest should be defined by real threats and opportunities within the different sectors of the economy. It should be established what expert technologies in South Africa should be protected.
- Theft of intellectual property
- Internet warfare/Cyber attacks (Electronic espionage)
  - Attacks on government computer systems
  - Electronic hacking
- Collection of trade, scientific, military and industrial secrets in order to bridge technological gaps as soon as possible (especially China).
- Coercion of government employees in obtaining these secrets
- Targeting of the industrial business cycle
  - Contract details
  - Supplier lists
  - Planning documents
  - Research and development data
  - Technical drawings
  - Databases
- Utilisation of tourists for economic and industrial espionage (especially China)
- Trade secrets theft
- Intelligence collection on technologies in terms of civilian and military projects
- Intelligence collection on policy attitudes of regional political structures (such as the EU, AU, SADC, etc), economic entities (such as the G8) as well as on countries' foreign policies.
- Intelligence collection on countries' economic strategic advantages
- International terrorism
- Intelligence collection on nuclear, biological and chemical research
- The "foreign national" threat (foreign national-employees stealing secrets)
- The "insider" threat (insiders stealing secrets)
- Acquisition risk (When you don't know the origin of components that can undermine the integrity of your product)
- Product manipulation

**Source: Nation States' Espionage and Counterespionage**

*An overview of the 2007 Global Economic Espionage Landscape*

By Christopher Burgess

April 21, 2008

**5. Counter measures**

**5.1 Existing strategies (current functions of NIA)**

- Fulfil national counter intelligence responsibility
- Conduct and coordinate counter intelligence
- Defensive
  - Physical security
  - Personnel security
    - Vetting
    - Advising
    - Auditing
  - Document security
  - Information and Communication Technology security
  - Security investigations (Defensive - reactive)
  - All aspects as informed by MISS



- Offensive
- Counter espionage
- Counter subversion/sabotage
- Counter terrorism
  - International
  - Domestic
- CI Investigations (Offensive - proactive)
- WMD/Proliferation – All Chemical, Biological, Radioactive and Nuclear (CBRN)
- Countering measures
  - Security audits
  - Security awareness
  - Technical Surveillance Counter Measures (TSCM)

#### 5.1.1 *Knowledge and understanding*

### **Theory and Design in Assessing Political Risk: An Assessment of “Countries in Trouble”: The *Economist* Method**

Llewellyn D. Howell

Thunderbird School of Global Management

Glendale, Arizona

Paper prepared for presentation at the 2008 Annual Meeting of the International Studies

Association, San Francisco, CA

#### **Introduction**

In the late 1980s, in the waning days of the Cold War, a surge of international investment occurred with young developing countries as the targets. Both sides—investors and host countries—found difficulties in getting to know each other and in making investments work for both parties. Investors often thought they knew the country where they intended to invest but this knowledge—like that of the U.S. government when it invaded Iraq in 2003—frequently turned out to be superficial and inadequate.

For both the investors and the host countries alike, there were existing frameworks and data available for use in examining investment environments in a constructive way. Business Environment Risk Information (BERI—later to become Business Environment Risk Intelligence) provided a model beginning in the middle 1970s that laid out in a simple and clear 10 point index (their PRI—Political Risk Index) the origins of potential dangers for foreign investors.<sup>1</sup> The BERI PRI covered 50 countries, including some that we would regard as developed, such as the United States.

In separate indices and with alternative sets of variables, BERI also examined economic and financial variables that could negatively affect foreign investors. Beginning in 1979, Political Risk Services (later to become The PRS Group) provided an alternative political risk model that intertwined government actions and economic consequences for investors. PRS still covers 100 countries. Other approaches existed as well in the 1970s and early 1980s, such as an early format of today's International Country Risk Guide (ICRG) that provided separate



political, economic, and financial risk advisories, with accompanying indices for 160 countries.

Each of these was theoretically based and time tested. Each was a for-profit business and neither academic nor journalistic exercises.

Independently, in 1986 the editors of *The Economist* magazine developed their own country risk model and presented it in a four page article titled "Countries in Trouble: Who's on the Skids?"<sup>2</sup> This new and internally (with the staff of the *Economist*) devised model, including political, social, and economic factors, provided a risk assessment and well stated method that had world wide distribution, had global reactions, and raised some critical questions about both the nature of country risk and the nature of the world in which foreign investors operate.

<sup>1</sup> The BERI, ICRG, and PRS models are all described in Llewellyn D. Howell, Author/Editor, *The Handbook of Country and Political Risk Analysis*, 4<sup>th</sup> Edition, East Syracuse, NY: The PRS Group, 2007.

<sup>2</sup> "Countries in Trouble: Who's on the Skids?" *The Economist*, December 20, 1986, pp. 25-28.

### 1

Importantly, while the article tries to underplay its likely impact and its scientific foundations, as a prototype it has been very helpful in academic and executive education classrooms.<sup>3</sup> Maybe even in boardrooms and government offices. For reasons that will be discussed below, the *Economist* model is useful in provoking both theoretical and substantive policy discussion. Some of the analyses that stemmed from the "Countries in Trouble" article in December of 1986 have implications well beyond the turn of the century and into the ongoing Middle East and other regional conflicts and instability. Indeed, Iraq's place in the ratings over the last two decades provides a jumping off place in examining the *Economist* method.

#### 5.1.2 *Prevention/deterrence*

Cooperation with relevant businesses by CI and CE.

#### 5.1.3 *Mitigation*

#### 5.1.4 *Damage control*

#### 5.2 *New issues for consideration:*

- Implement NIA CE Strategy which has been adopted by NIA Top Management in 2007.
- National and Provincial CE Capacity be created.
  - CE needs to have decentralised offices in identified provinces reporting directly to CE HQ, as we effectively operated in the past.
  - Create capacity in all Provinces whose primary function will be to identify, investigate and neutralize **Non State Actors** : That is,
    - Non Governmental (NGO) and Non Profit Organizations (NPO) officials (such as Peace Corps).
    - Members of Private Intelligence Organisations (PIO).
    - Journalists and Media Personalities (hiding in the open).
    - Members of Foundations and Cultural Institutes.



- Political, Economic, Social Commentators who are intent on influencing public opinions and set the national agenda on behalf of foreign powers.
- Academics (Lecturers, Students, Exchange Programs) etc.
- Screen for Espionage risks, Joint Ventures and be part of negotiations (IP).
- Screen for espionage risks Twinning Agreements.
- Identify and Monitor activities of FIS members during visits by Foreign Delegations and/or Foreign visits by RSA delegations from Municipal and Provincial Governments, including state entities.
- Update register and monitor Foreign Nationals in Government Departments.
- Provinces that have **consulates**, to identify and monitor activities of declared, undeclared and suspected FIS members operating from the mission, and lastly
- Assist the province in screening and monitoring of identified or suspected FIS members during **Special Events**.
- Proposed CE capacity in provinces.
  - Unit Heads: 13
  - Agent Handlers: 35
  - Investigators: 69
  - CE Analysts: 33
  - Admin officers: 13
  - Cleaners: 22
  - Offices: 13
- Foreign Language Capacity/Expertise be created.
  - Create and fill posts with persons who can speak the following languages:

China	Mandarin	2
India	Hindi	2
Pakistan	Urdu	2
North Africa & Middle East	Arabic	2
Israel	Hebrew	2
Russia	Russian	2
Germany	German	2
France	French	2
Mozambique, Angola, Portugal	Portuguese	2
South Africa	Multi language Expert of SA Languages including English	6

- Locate such a capacity at NIA HQ due to its sensitivity, need for use by other structures such as CT and the fact that CE is a high mobility outfit.
- Nodal Point at the Department of International Relations and Cooperation (DIRC) be created and properly staffed as well as a capacity at the OR TAMBO International Airport (ORTIA).

Unit Head	P3	1
DFA Head	P2	8



Office		
Admin Officer	G2-G3	1
General Assistant	G1-G2	2
OR Tambo DFA Permit Office	P2	2
OR Tambo DFA as well as Ministry of Intelligence Executive Lounge suites	P2	2
OR Tambo ACSA Permit Office	P2	2
Total		18

- DFA has offered to avail office space at its new HQ
- Be responsible for accreditation of diplomats in RSA
- Nodal point, recipient and processors of CICF initiated Government officials - Diplomats contact reports.
- Run and manage DFA –Foreign missions liaison office.
- Screen all incoming foreign delegations for possible FIS actors.
- Draft MOU has been compiled for scrutiny and approval
- Be responsible to monitor violations by diplomats of their immunities and privileges. In order to this effectively in co-operation with an "Embassy"- unit within CE Investigations, the following issues will have to be addressed.
  - The new registration system for diplomatic vehicles in South Africa (DBBB ...D) that was implemented after missions have claimed that the old system left them vulnerable to criminal actions, makes it impossible to immediately identify a vehicle as belonging to a specific foreign Mission versus the old system where a specific number at the beginning provided an indication of the Mission (eg 174D...D – British High Commission and 175D...D – Embassy of the USA). The latter system had its restrictions – only 1 000 vehicles could be registered per country. According to regulations a specific number was only allocated once, after which the plates had to be returned upon de-registration and destroyed. Both systems allow for a vehicle to only be registered in the name of the particular Mission, without providing the name of an allocated driver. It is necessary that all vehicles other than pool vehicles should be registered in the name of the diplomat to whom it has been allocated and some sort of Mission-identification has to be incorporated in a new registration system which criminals would not be able to utilise to their advantage.
  - Diplomats frequently hand old and/or poor quality photos of themselves/family members to the Department of International Relations and Cooperation, which hampers NIA's counter intelligence actions. It is suggested that such photographs should be taken by the Department of International Relations and Cooperation.
  - A declared member of a FIS is per definition someone who has been declared by his/her service to the host intelligence service as a member of the former service (FIS) that is being placed in the host country for a stipulated period of time. SSA Liaison should diligently keep record in hard



copy of all FIS members officially declared to it and forward copies of such documentation timely to CE.

- The violations by diplomats of their immunities and privileges is being monitored and reported on during the course of CE investigations. Any member of the SSA should, in the event of observing such actions inform CE about it. The information should then be sent to Liaison to deal with the matter. The question here should in actual fact be: "What is the appropriate actions against the violation of immunities and privileges by diplomats"? Members regularly report on such violations but the issue is hardly ever raised with the countries concerned. Examples exist of FIS members contacting NIA members directly (when, for some reason they have their names and numbers), instead of working through liaison.
- Create a SSA nodal point within the Department of Home Affairs with dedicated representatives for CE, Economic Intelligence and Border Intelligence.
- Create a Polygraph and Psychological Capacity within CE.
- Create a dedicated and capacitated CE Technical Interception and Monitoring capacity with 24 hour access to the OIC.
- CE operational members need cover for action which includes operational documentation such as vehicle registration, identity documents and passports. Operational members have to handle sensitive agents (including double agents) whilst driving in cars registered in their own names. When a hotel room has to be booked (for operational purposes), it is necessary to produce an identity document, even if payment is done in advance by means of cash.
- CE operational members need an "operational toolbox" which each member should have at his/her disposal all the time, including a laptop with 3G connectivity, biometric memory sticks, GPS, camera, binoculars, etc.
- CE operational members need standing operational advances.
- CE needs a dedicated editor to be part of the Analyses capacity dedicated to it.
- Create CE Specific Surveillance Capacity
  - CE targets are unique and it often include the investigation of colleagues. Thus it is important to have a dedicated CE surveillance team which is highly trained and motivated. This team should also be screened off. There have been examples of the team not being able to work on a target because they have all been exposed to the individual. Another issue to consider is that when a team is not dedicated to CE, CE has no input when it comes to prioritisation of operations. It may happen that an investigator has put in a request for surveillance and another investigator requests surveillance after the first one but the latter's request is more urgent than the first. In such a case the management of CE should determine the priority. If surveillance is under CE management it simplifies matters. Currently the process of requesting surveillance is too cumbersome. Too many signatures are needed. The whole idea of the investigator first having to compile a complete budget is ridiculous. The insistence of a powerpoint presentation during briefing is adding a burden on the time of the requesting investigator. At present surveillance is not rendering a support function at all. Again, if the team is part of CE, it would eliminate some of the above steps.
  - Create and fill posts listed below.
  - Apply same surveillance dispensation as in the provinces where administratively the unit is accountable to CDCI but operationally to CDOS

Unit Head	P3	2
Physical Surveillance	P1-P2	15
Electronic Surveillance	P1-P2	5
Cleaner	G1	2



Admin	G3	2
TOTAL		26
Office		1

- Economic/Industrial Espionage
  - In order to keep up with new developments in the area of international espionage, especially with regard to the application of new tradecraft, it is important to create a dedicated **cyber espionage capacity** within counter espionage. The envisaged structure can be divided into an **offensive** and **defensive** component. Over the past few years there has been a drastic increase in espionage cases involving the cyber space (hacking/viruses/illegal access to sensitive computer systems/damage and sabotage of systems).
  - **Industrial and economic espionage** involving foreign countries and companies surely remains the focus and responsibility of the Agency's CE capacity. This is a further area in which a dedicated structure or capacity will have to be established as part of the State Security Agency (SSA)'s counter intelligence/counter espionage responsibility. Interaction and cooperation with a Chief Directorate Economic Intelligence to be clarified in order to prevent confusion and duplication.
- SSA offices at South African diplomatic missions abroad
  - The deployment of counter espionage at SSA offices at South African diplomatic missions abroad with a counter espionage function need to be considered in order to increase awareness and effective countering in this area.
  - Also deployment of members with counter espionage experience in other posts at these offices. It was mentioned that CE should be the feeding ground for filling foreign postings.

5.2.1 **Identify and define the positioning of the theme/function within the SSA (centralisation, decentralisation, etc)**

The national responsibility for Counter Intelligence should be centralised within the SSA. Since Counter Intelligence is foremost a domestic function, it should be part of NIA if not directly under the DG of the SSA.

A continuous division between NIA and SASS within the SSA will undermine the very purpose of the formation of the SSA to unite civilian intelligence.

There is also a feeling amongst members that it is useless to discuss such issues since a political decision has already been made through which structures have been established in order to give jobs to friends.

5.2.2 **Mechanisms for effective liaison and coordination with external role-players**

**Inter-departmental CI coordination:**

CI coordination between the Agency and SASS has over the past decade been problematic. Problem areas identified is the transgression of NIA's domestic CI mandate by SASS (conducting of investigations/operations on domestic territory) and the lack of informing NIA on CI related incidents occurring at SA missions abroad. The participation of SASS in both the CICF and the different inter-departmental CI functional committees to enhance coordination and cooperation could not resolve the matter mainly due to the lack of a legislative framework to comply SASS and other relevant departments to cooperate



with NIA on counter intelligence. The main stumbling block is the fact that the draft Regulations on counter intelligence coordination is still not approved at higher level, which could be utilized as a tool to enforce coordination and cooperation in this regard.

Inter-departmental CI coordination is being conducted on the following three dimensions/levels:

- Information coordination
- Operational coordination
- Integrated counter measures

The proposed establishment of an integrated/centralized analysis structure/capacity (including both the domestic and foreign intelligence focus areas) is regarded as a workable solution to also address coordination of CI related information between NIA and SASS.

The conducting of joint CI operations, projects and investigations is to be handled within the envisaged Multi Lateral CI Project Coordinating Centre (MCIPCC) as part of the new NIA NOC. This is not only restricted to joint operations between NIA and SASS, but will include joint CI operations with the SAPS, SANDF (DI), NCC, COMSEC and other structures that can make a contribution.

It is furthermore foreseen that the different departmental data basis relevant to the counter intelligence field will be link up / centralized within the MCIPCC. The MCIPCC will be run on a project basis.

Effective CI liaison with other members of the South African intelligence community should enhance the SSA's CI and CE capacities. A clause should be written in the new SSA Act which would read something like, "SAPS CI in consultation with the SSA ....", in order to ensure that the SSA is effectively in control of CI/CE within these departments, although the SSA would obviously delegate certain functions to these departments for practical reasons.

#### **Effective Utilisation of Intelligence Derived from Double Agent Operations**

Double agent operations offer CE the opportunity to have "contact with the enemy" in the same way in which an army commander would send out a foot patrol near enemy lines with the purpose of engaging the enemy in order to obtain certain intelligence from it.

The intelligence that is obtained in this way from an opposing FIS, often contains information on that FIS or its home country that could afford the South African government the opportunity to change its policies and actions so that it could be to the advantage of the country and its people. When a FIS indicates for example to a double agent that its home country / a company from that country wants to obtain a certain contract or concession and they are willing to pay what South Africa wants for it, it is necessary that there is a direct and effective way of getting intelligence derived from it through analysis, to the correct department / parastatal and policy makers as soon as possible and to obtain coordinated feedback (again as soon as possible - if applicable) to be fed back into the double agent operation. Another example is when indications have been obtained that a FIS plans to target a specific individual or structure within government.

Currently such information is not optimally fed into government and this is one of the most effective tools in the hand of CE to help establishing the SSA in the centre of government.



It seems that the above-mentioned scenario necessitates the formation of a mean and lean capacity within Analyses which have because of its CICC responsibilities already access to other government departments / parastatals. To do this extra task effectively, it should muster immediate direct access to departments, parastatals and policy makers at the highest level.

### 5.2.3 *Capacitating of function/theme with regard to skills requirements*

The CE capacity of the SSA should be boosted significantly. Obvious investigations, agent and technical operations are not being initiated almost on a weekly basis as the capacity of CI20 does not allow it. The Manager CI20 has an updated input that can be used here, if an extra capacity of at least 25% is added to it in terms of the national CE operational capacity.

Counter Espionage function within the SSA

- CE should be restructured in such a way that CE Pretoria is the Head Office with CE regional offices. The CE Head Office should have its own administration and financial capacity, a CE data base where raw information and intelligence is available and a lone standing CE Document Management System (DMS). At the moment it is virtually impossible to do record checks on any individual. The DMS is a document management system and not a database.
- In practice this would mean that the regions would give attention to CE targets. Currently the regional offices do not give attention to CE matters when they have more important issues (according to their priorities) in their regions. Moreover, often the personnel in the regions lack the insight and knowledge to conduct CE investigations. Members of CE should be screened off and as such should not use the DMS which is accessible by all SSA members. In cases where CE reports should be disseminated to other Directorates, other means of communication should be used. CE agent handlers should be screened-off from the CE head office as it would limit chances of compromising members and operations. It must be kept in mind that they sometimes handle sources in sensitive positions and should be in a covert office.
- CE Investigations (Investigation of FIS's, Private Intelligence Organisations (PIO's), front companies, contacts and sources) must be distinguished from CI Investigations.
- CE Investigations, Agent Operations, Double Agent Operations, Technical Operations, Surveillance, Records Centre and Analysis - Tactical and Strategic, should be integrated into one Directorate/Chief Directorate.
- A FIS Desk (with an operational and an analysis capacity) approach should be implemented within CE.
- The FIS Desk must have one operational coordinator and one analysis coordinator. A combined approach will assist immensely regarding the direction that needs to be taken and in tracking progress.
- A CE clearance panel needs to be established. This panel needs to make decisions based on inputs from members regarding important issues and tasking which needs to be implemented or terminated or redirected to other responsible CI Directorates pertaining investigations and agent operations.
- CE should have priority access to all information in the SSA. Any CE related information obtained in any other investigation should be channelled to the CE Analysts who would then deal with it according to the need. In practice this would mean that members of CE should not have to beg IS for photographs of declared FIS members who visited the liaison centre at Musanda. Such photographs and information should automatically be passed on to CE.
- The view as been raised that there is a need for a structure within CE whose function is solely to recruitment agents and then hand the agents over to the agent handlers. **(BOTH JOBS ARE VERY IMPORTANT, AND NOT ALL RECRUITMENT**



**PERSONEL ARE ABLE TO BE AN AGENT HANDLER AND NOT ALL AGENT HANDLERS CAN BE RECRUITERS – BOTH ARE VERY SPECIALISED JOBS.)**

This structure will carry out all pre-recruitment requirements and will also approach the target and do the actual recruitment. They will run the agent for a period of time before handing the agent over to the professional agent handler. It is very important that the agent handler is not identified during the recruitment of an agent, as should the recruitment not be successful, the handler is compromised and this will effect other operations. It would be ideal if both the recruitment structure and the agent handlers are completely separate and housed in different buildings/offices.

**5.2.4 Integration of function between domestic branch and foreign branch of SSA.**

There need to be complete integration and restructuring in those areas where integration are proposed.

This is very important in terms of the Counter Intelligence (CI) and Counter Espionage (CE) functions within the SSA. The feeling is overwhelming that there must be a total integration of the function, either under NIA or directly under the DG of the SSA. NIA and SASS CE and CI should integrate. For all intents and purposes NIA and SASS forms one service – the SSA. In practice it would mean that SASS members serving abroad would send all CE related information to one CE and it would be placed on the CE database. This would also prevent cases where known FIS members who were declared in other countries come to SA as ordinary diplomats and work undetected.

In terms of other functions of the SSA it is suggested that:

- Information should be centralised, which has been made out as an extremely important issue.
- Operational functions of the domestic and foreign branches should stay apart.
- Analysis should be integrated. The fragmented manner in which the analysts work at the moment is not contributing to a good CE product. All information is not being sent through to the strategic analysts and they do not have a complete picture of what is going on. Similarly the tactical analysts also give tactical guidance on fragments of information as they also do not receive all the information from all the sources.
  - The CE-specific capacity must be situated close to CE investigations.
  - Analyses should have a class-leading overt capacity.
  - Analyses capacity to inform intelligence gathering should be transformed to world class levels as it is currently not up to standard.
- Management should be integrated.
- Coordination should be integrated.
- Training
  - SANAI should establish a shielded CE training capacity that should be deployed in Pretoria. There is a need for the resurrection of a CE Training Campus.
  - Training must take place!!! The problem with the current training is that it is non-existent in terms of CE.
  - There are also concerns about the CE training that is now being devised in-house as its basis is dated and it has not kept up with new international trends.
  - In the interim, identify cordial Foreign Services and engage in discussions to assist in providing "CE Training".
  - Exchange programmes with FIS' must be a common phenomenon.
- Surveillance should be integrated.
  - CE should have access to a dedicated surveillance unit.
  - The current red tape concerning the application and deployment of surveillance should be avoided, as well as problems with prioritisation.



- CE must be able to tap into the central surveillance unit, its access' and capabilities.
- An Economic Intelligence Analyses capacity should be integrated within the integrated Analyses capacity.
  - This Economic Intelligence Analyses should play a leading role in directing Counter Espionage operations with a distinct economic / industrial espionage inclination.
- Border Intelligence should be an integrated function of Counter Intelligence.
  - Internal and external targets should be monitored in an integrated way.
  - Border Intelligence in conjunction with NICOC should establish an effective Watchlisting system which should be available to CE.
- Counter Terrorism should be an integrated function of Counter Intelligence.
- Counter Espionage (CE) need to have a bigger emphasis on infiltration/penetration of active hostile and foreign intelligence services, in order to build in our current state of knowledge. We need to target the target country HQ. We also need to focus on the interception of communications between SA and the HQ country. In addition we must review our CE/CI cooperation within SADC in terms of common interest.

#### 5.2.5 *Enablers, for eg. technological requirements*

One member felt that the SSA cannot continue to use the DMS system because it is foreign owned and there is the possibility that it can therefore compromise the integrity of the SSA's document security. The input on Cyber threats show that it is not impossible for the developers of such systems to build in back doors and Trojan horses that can afford the developer / intelligence service of the developer's choice access to information.

#### 5.2.6 *Implication on processes level*

#### 6. Conclusion

The compilation of the input was extremely difficult as the scope has been so broad and everyone's input had to be considered. The compiler does not want to claim that the input is either exhaustive or a correct reflection of the thinking within CI20 and other current CE role players / stakeholders within NIA. It is suggested that some line functional experts as well as Management within CI20, the Chief Directorate Counter Intelligence and IM should be co-opted on the task team when the function of CE is discussed and the final document is compiled.

2009-12-02

# ALJAZEERA



## CURRENT STATUS OF RELATIONS BETWEEN MOSSAD AND NIA

### 1. BACKGROUND

- 1.1 The MOSSAD was handled by [REDACTED] from 1996 to 2004. At that stage it was the only country in the Middle East that was represented and declared to NIA. Relations were always more tense with the MOSSAD than with any other country, solely because of the history between the two countries.
- 1.2 The representative initially met, was [REDACTED] he was succeeded by [REDACTED]. During the time of [REDACTED] relations were standard and regular exchange took place. Exchanges regularly took place, mostly on individuals and organizations suspected of terrorism involvement. A counter terrorism expert visit took place in 1996. Background on terrorism modus operandi was shared by them, even before the first PAGAD related bombs exploded in the Western Cape. Meaningful exchanges became less at the end of [REDACTED] term. The MOSSAD at that stage also indicated they were thinking of a part time representative responsible for handling the whole of Africa. NIA discarded the idea and [REDACTED] subsequently was placed in South Africa, although he regularly traveled to West and East Africa where he also was the declared member. Reasonable relations existed with [REDACTED] until he was handed over to [REDACTED].
- Examples of exchanges are attached as Annexure A, during the above-mentioned period.
- 1.3 During February 2005, [REDACTED] the MOSSAD Director for Foreign Relations, led a MOSSAD delegation that visited NIA Head Quarters in Musanda Liaison Centre. The objective of the MOSSAD visit was to create a space for dialogue on how cooperation between MOSSAD and NIA can be improved. Mr NJENJE, former NIA DDG led the NIA delegation.
- 1.4 [REDACTED] mentioned that non-conventional threats are more worrying to the MOSSAD and the Israeli government. He also mentioned that was priority threat for Israel because it Iran possessed nuclear capability that could be used against Israel and for funding Hezbollah and HAMAS.
- 1.5 Mr. NJENJE welcomed the sentiments expressed by [REDACTED] regarding the need for Intelligence Services to cooperate and work together to avert terrorist threats. He assured MOASSAD that NIA was a willing partner in the fight to combat international terrorism and proliferation of weapons of mass destruction. He emphasised the importance of that meeting as having brought to the fore bases for productive cooperation between NIA and MOSSAD in the area of Counter Terrorism and Counter Proliferation.
- 1.6 There was improvement of information exchange soon after the MOSSAD delegation visit. In May 2006 NIA Counter Proliferation experts delegation visited Israel. MOSSAD was pushing to hard to included information request on Counter Intelligence area such as [REDACTED] the Iranian national staying in Cape Town. He alleged that [REDACTED] was in contact with [REDACTED] a Hezbollah member based in Lebanon. NIA did not provide feedback to MOSSAD on this request.
- 1.7 In 2007 MOSSAD provided information on [REDACTED] to NIA with the hope that the information would benefit South Africa. They expected that NIA would share information with them on what are finding of their monitoring and investigation. However, [REDACTED] bluntly told [REDACTED] the Local Representative of MOSSAD that he was prevented by NIA Management to share information on [REDACTED] could not understand [REDACTED] because MOSSAD provided to NIA information on [REDACTED]. He stormed out of the meeting.



- 1.8 [REDACTED] former Head FIS Liaison MOSSAD grievance on NIA's action to refuse to share information on [REDACTED] activities after his return from Somalia to NLC to get guidance. He was confused by the actions of [REDACTED] and [REDACTED] and sought NIA's position on cooperation with MOSSAD. The NLC reversed Mr [REDACTED] decision to refuse IM to share information on [REDACTED] with MOSSAD. However, [REDACTED] took over from IM Analysts.
- 1.9 [REDACTED] the former DDG instructed [REDACTED] to confine cooperation between NIA and MOSSAD to Counter Proliferation and Counter Terrorism.
- 1.10 The political stance of from Minister KARSILS contributed to the perception that NIA was not willing to cooperate with MOSSAD because the adversaries of Israel are allies of South Africa. Of course Mr KARSILS has openly demonstrated political differences with Israel and supported the cause of the Palestinian. He also favoured Iran's material support to Palestinians Resistance Movement. He ordered audit of information NIA liaised with MOSSAD.
- 1.11 Mr. MANZINI the former DG paid unofficial visit to MOSSAD HQ in March 2009. MOSSAD complaint to him about lack of concrete cooperation with NIA. According to MOSSAD the situation has not changed. Instead it has deteriorated to the levels which have compelled MOSSAD to withdraw their Representative from South Africa. Hence they have withdrawn their Representative but have not severed the relations from residing in South Africa.

#### Annexure A

#### FEEDBACK

We would like to express our appreciation for providing leads on [REDACTED]. It is, however, at this stage only possible to provide preliminary feedback. In this regard the following:

Information that is currently available on [REDACTED] also known as [REDACTED] neither confirms nor refutes suspected links to terrorism in general and al-Qaeda in particular. An accurate assessment of the real or potential threat posed by [REDACTED] and his followers is thus not viable at this stage.

[REDACTED] is associated with an organisation called Majlis Ul Ulama and a newspaper called the Majlis. The current status of the organisation and the newspaper is being investigated.

He is furthermore involved in a project to establish and fund madrassas locally and abroad. Funding of this project has previously been done through two organisations, namely Mujlisul Ulama of South Africa and Servants of Suffering Humanity. The current status of this project, as well as details about the organisations involved, still need to be determined.



Details about possible followers are sketchy at this stage, which could be attributed to [REDACTED] unpopularity within the broader Muslim community and the animosity between him and his family.

There is at this stage no information available pertaining to suspicious money collection, as well as transfers to and from South Africa involving [REDACTED].

Although the existence of "The Centre Director Islamic Information Charitable Trust" could not be confirmed, the banking details provided are being followed up.

It is suspected that [REDACTED] travels abroad are linked to the above-mentioned project. He is said to have connections in India, Pakistan and Afghanistan. Details and confirmation of his trips, however, are still outstanding.

Investigations into the matter continue and any relevant information that may become available would be liased.

Thank you for your attention.

#### EVENTS THAT FOLLOWED THE 'WALK-IN' SITUATION AT THE ISRAELI EMBASSY.

1. Liaison report NIA/A32/13/2/5(LS825) dated 5 June 2001 refers.
2. Information regarding the 'walk-in' was conveyed to NIA on 4 June 2001 as was stated in the report. All the relevant chief directorates were tasked for information on [REDACTED] through J62. It was already established by the liaison officer that he used a false passport number and that he was not Algerian as he stated.
3. [REDACTED] apparently called the Embassy twice and threatened to blow-up the Embassy if they did not give him money as he requested. As far as could be established he never personally came to the Embassy again. [REDACTED] wife reported to the liaison officer while he was in Paris to visit his parents. He did call from Paris on 15 June 2001 to ask about the situation regarding [REDACTED]. He then indicated that [REDACTED] contacted the embassy again and threatened them if they did not pay him.
4. The events that happened resulted in the liaison officer of NIA and [REDACTED] SAPS member in the protection unit assigned to the Israeli Embassy, making contact on a daily basis. New facts came to light and other Embassies became involved.
  - The Canadians reported that they received information from Montreal that the Israeli Embassy in Canada could be a target. They reported the info to NIA. They did however not indicate that they also got the information from the Israeli Embassy in Pretoria. They also said that the same person might have walked-in at their Embassy. This



information was confusing and was followed up by CDCE. The SAPS showed a photo of [REDACTED] to them. Only then did they realise that it was the same person. The photo was received by NIA from the Mossad and given to the SAPS.

-The Americans requested to see [REDACTED] on 18 June 2001 who met with [REDACTED] and gave him the following information:

On 25 April 2001, one [REDACTED] (Given name) [REDACTED] (Muslim name) walked into the US Embassy in Pretoria offering information on individuals allegedly involved in the US Embassy bombings in Nairobi. [REDACTED] provided his date and place of birth as [REDACTED]. He indicated that he was a resident of [REDACTED]. He appeared to be East African, was of medium height and built, had a dark complexion and a small amount of facial hair. He provided some information of potential interest concerning a former employer in [REDACTED] who [REDACTED] claimed was involved in the US Embassy bombings and is now threatening his life. This information dated to December 1998. He also claimed to have attended Jama'at Al-Tabligh meetings in Cape Town. He maintained that he destroyed his [REDACTED] passport and left his [REDACTED] residency permit in [REDACTED] he could not provide any identification.

[REDACTED] was accompanied by a Belgian/Congolese national [REDACTED] with date and place of birth [REDACTED]. [REDACTED] was of medium height, very slight built and dark complexioned. It was assessed by the Embassy that [REDACTED] sought to benefit financially from his role in assisting [REDACTED] and [REDACTED] convincing him to approach the US Embassy. [REDACTED] and [REDACTED] initially were unwilling to provide an address or telephone number, where they could be contacted. They eventually provided the name of the [REDACTED]

[REDACTED] claimed that he shared the room with three other males. [REDACTED] also indicated that he had a sister who resided just outside [REDACTED]

[REDACTED] admitted to having previously approached the Canadian Embassy and possibly the Swedish Embassy. Although [REDACTED] story initially appeared reasonably credible, he later admitted lying on certain aspects. It was clear that he tried to give information on an ongoing manner to receive money in return. He claimed on several occasions that his life was in danger



from his former employer in [REDACTED] one [REDACTED]  
[REDACTED] He was referred to  
the SAPS on these occasions.

[REDACTED] indicated to [REDACTED] that they have worked with  
[REDACTED] since October 2000. They indicated to the SAPS that they  
would assist them in locating him and to lure him to the American  
Embassy for an interview. The SAPS contacted the liaison officer to  
ask if NIA would be interested in being involved in the interview. This  
was relayed to CDCE who indicated that they were interested.

5. On Friday, 8 June 2001 the SAPS in Rosebank disabled a pipe bomb that was found at a company named Polaris in Waverly, Johannesburg. On Saturday, 9 June 2001 at 5:00 in the morning a petrol bomb was thrown into the building housing the Polaris Shipping Company and extensive fire damage was reported. The local representative contacted the liaison officer on 9 June 2001, giving the details of the incident and stating that the Polaris Company was connected to a big company in Israel named the Zintek Company. It was however not common knowledge that the Polaris Company was an affiliate of the Zintek Company. The MOSSAD expressed their concern on this issue, seeing that some kind of investigation had to be done by the person who attacked the company, in order to know that it was an Israeli company. This information was given through to the Alert Centre on 9 June 2001. It was later established through the SAPS that the Polaris Company was involved in shipping navigational systems. There is also no South African working at the Company. The SAPS are investigating possible internal personnel problems as well as an insurance fraud scheme.

6. The following counter intelligence information was gathered through liaising with the Police, after the two events and weighing it against information received from the MOSSAD:

-The Shin Beth member working with the security at the embassy is [REDACTED]

[REDACTED] The EL AL manager at JIA is also very involved in the gathering of intelligence. He is the individual that handled the whole issue of the pipe bomb at the Polaris Company. He took a video of the demonstration that took place outside the Israel Trade Centre on 8 June 2001, as well as video footage of the pipe bomb. The video was received by NIA and distributed to the relevant CD's. The head of Africa desk at the Shin Beth arrived in South Africa on 11 June 2001 to oversee the situation concerning the security of the Embassy after the two events. (Polaris and 'walk-in'). NIA was not informed of the arrival of the Shin Beth member.



-Through liasing with the SAPS it came to the attention that a security committee consisting of the Americans, British, Canadians and the Israelis comes together once a month to discuss any threat or terrorist activity. Previously the SAPS were invited to these meetings. It was on a meeting like this that the first information on the 'walk-in' was liased with one another.

#### COMMENTS BY LIAISON OFFICER

1. Investigators and analysts of CDCE and analysts in J5 were already given all the information as the situation evolved.
2. A lot of questions can be asked:
  - Was the CIA handling the walk-in as a source?
  - Did he actually walk-in at the Israeli Embassy or was this staged to ensure more protection by the SAPS?
  - Was the bombing incident also staged to attract more attention to safety at the Israeli Embassy and other Israeli Companies?
  - Why did the CIA not inform the SA authorities immediately after the first approach by the walk-in, and why did they not inform NIA at all about the incident?

**ALJAZEERA**



3. The Americans, Israelis and the Canadians compromised their relationship in the different information that was given to NIA and the SAPS. This was a good exercise for NIA and the SAPS and their co-operation in using all the information to our advantage.

[REDACTED]

LIAISON OFFICER

NIA/CI13/1/5/2 (LS 825)  
Copy..... of ..... Copies

LIAISON AND PROTOCOL

2002  
September

DIRECTOR GENERAL EM 10  
DEPUTY DIRECTOR GENERAL EM 30  
SENIOR GENERAL MANAGER CI 10  
MANAGER IM 20  
MANAGER IM 30

LIAISON MEETING: LS 825(MOSSAD): 2002 SEPTEMBER 10 AND 12

ALJAZEERA

TIME:	19:00	11:30
VENUE:	Giovanni's	Café
PERSONS INVOLVED:	[REDACTED]	local representative for LS 825 liaison officer NIA



**1. DETAILS OF CONTACT:**

- 1.1 An urgent meeting was requested by [REDACTED] on 2002 September 10. He supplied the following information:

A Saudi Arabia travel agent in South Africa issued six plane tickets arriving September 11 at JIA on flight AT 402 (Airlines and time unknown) to the following persons from Arabic descent:



ALIQEILI SAUDI INTERNATIONAL TRAVEL AGENCY issued the tickets as 'collect tickets' in South Africa. Two of the individuals will travel from Morocco and the other four from Benin.

- 1.2 The local representative mentioned that the information was received late September 10. The information is not confirmed. The reason why this issue raises suspicion is the way in which the tickets were purchased and the fact that they travel together from different locations.
- 1.3 A follow-up meeting was requested by [REDACTED] on 2002 September 12. The following additional information was received from LS 825 as a follow-up on the previous information regarding the suspicious travellers from Benin and Morocco:

[REDACTED] is a Moroccan citizen.  
Passport number [REDACTED]  
Born in [REDACTED]  
Currently living in Marrakech  
Moroccan ID [REDACTED]

The flight plan for the above-mentioned individual is as follows:  
Departed Agadir, September 11 to Casablanca on Royal Air Moroc, flight AT 402.  
Departed Casablanca, September 11 to Paris on Air France, flight 2497.  
Depart Paris, September 18 to Johannesburg on Air France, flight 990.  
Depart Johannesburg, September 19 or 20 to Paris.  
Depart Paris, September 20 to Casablanca on Air France, flight 2195  
Depart Casablanca, September 20 to Agadir on Inter Air, flight AT 423.

**2. REQUESTS**



- 2.1 Thirty individuals of the AL AQSA FOUNDATION will leave for Tel Aviv on 2002 September 20. They will be meeting the PLO in GAZA. Additional information is requested on the visit and specifically on [REDACTED] a member of the SOUTH AFRICAN HUMAN RIGHTS ORGANISATION. He attracts attention because he has contact with [REDACTED] in the West Bank in Palestine. NIA was requested to indicate if this group should be allowed to enter Israel and to indicate if this group will enhance the possibility of a peace process or hamper the possibility in the region.
- 2.2 The local representative requested a courtesy call with the DG, NIA. The reason is that he has a message from his Service regarding the WSSD to convey to the DG, NIA. He also wants to use the opportunity to shortly give a briefing on the situation in the Middle East.

### 3. DOCUMENTS EXCHANGED

- 3.1 The following documents were exchanged:
- SIGNIFICANT DATES IN SEPTEMBER-OCTOBER 2002
  
  - GULF TENSION
  
  - TERRORISM THREAT TO VESSELS

### 4. COMMENT BY LIAISON OFFICER

- 4.1 The initial information was received on September 10 and was forwarded to the National Operational Centre and to the JIA office for follow-up on the same day. Although the information is unconfirmed and not a specific threat, one could not ignore the information of this nature especially on the 11<sup>th</sup> of September.
- 4.2 The flight plan of [REDACTED] raises suspicion in the sense that he travels from very far and with a lot of effort to get to Johannesburg to stay only one day.  
It also needs to be highlighted again that the reason why the group of suspicious travellers attracted attention was that their tickets were bought in South Africa and were collected at their places of departure.
- 4.3 It was indicated to the local representative that the DG, NIA is very busy, but that the request for a courtesy call will be forwarded to his office.

**ALJAZEERA**

[REDACTED]  
LIAISON OFFICER

### 5 COMMENT BY CI 13



- 5.1 Even though the information was not confirmed, it could not be ignored especially that the travelling arrangements casts some suspicion.
- 5.2 It is a protocol procedure to allow a local representative to convey a message from his Service to the Director General.

  
**HEAD FIS LIAISON CI 13**

**Copy 1 of 2 copies**

NIA/IM20/1/5/2

DZ: IM20/2002/1653

3

4

Office of the Manager

National Analysis (IM20)

2002 October 04

Head Foreign Intelligence Service Liaison (CI13)

**FEEDBACK TO REQUEST BY LS 825: AL AQSA FOUNDATION  
MEETING WITH PLO IN GAZA**

1. Your letter NIA/CI13/1/5/2 (LS 825) dated 2002 September 19 (entitled LIAISON MEETING: LS 825 (MOSSAD): 2002 SEPTEMBER 10 AND 12) refers.
2. Directorate IM20 would like to respond as follows to the request for information regarding a meeting between the Al Aqsa Foundation (AAF) and the Palestinian Liberation Organisation (PLO) in Gaza, with specific reference



to one [REDACTED] member of the South African Human Rights Organisation (SAHRO), who would be part of the South African delegation:

2.1 Meeting between AAF and PLO

The above-mentioned meeting between the AAF and the PLO in Gaza could not be confirmed. As to the question of whether the AAF group would enhance or hamper the possibility of a peace process in the Middle East, there is no information at this stage to support either likelihood.

2.2

[REDACTED] is possibly identical to [REDACTED] (see Annexure for photo), who is a [REDACTED]. He is closely associated with the organisation People Against Gangsterism and Drugs (PAGAD), a staunch anti-American and involved in Muslim organisations, including SAHRO. He was involved in demonstrations in front of the USA Consulate in Durban from 5 to 19 April 2002. It is not known at this stage if [REDACTED] has links to individuals in other countries.

3. It would be appreciated if LS 825 could indicate whether [REDACTED] is indeed identical to [REDACTED]. If so, information on his contact with [REDACTED] the West Bank, Palestine, would be appreciated.

4. Kindly place the above information in a format that is suitable for liaison purposes.

5. Thank you for your cooperation.

As signed: [REDACTED]

[REDACTED]  
MANAGER NATIONAL ANALYSIS

Distribution:



Copy no 1: CI13 (*via GroupWise*)

Copy no 2: NIA/IM20/1/5/2



**ALJAZEERA**





**ALJAZEERA**



## **RECORD CHECKS:**

Information was obtained on [REDACTED] and [REDACTED]. Their travel records confirm that both persons exited South Africa onboard the same flight on 2001/07/07 and returned to South Africa onboard the same flight on 2001/07/21. This period coincides with the information supplied regarding their alleged activities in Jordan, Syria and Lebanon.

[REDACTED] and [REDACTED] are both linked to the Central Islamic School in Pretoria and the Media Review Network. Attached herewith the personal particulars, company links and detailed travel records of the two mentioned individuals.

Attempts are still being made to positively identify [REDACTED]. The first mentioned may be identical to a [REDACTED] but according to the available information the latter is a South African citizen and not a Palestinian as indicated.

Thank you.



# ALJAZEERA



## RECORD CHECKS

1. [REDACTED]

### 1.1 PERSONAL PARTICULARS

Date of Birth: [REDACTED]

Passport: [REDACTED] prior to 2001 utilised SA passport

Identity number: [REDACTED]

Physical address: [REDACTED]

### 1.2 COMPANY LINKS

- [REDACTED]  
Private company registered as a Financial Intermediation, Insurance, Real Estate Business company.  
Appointed as Director on 2000/08/31.  
Address: [REDACTED]
- [REDACTED]  
Registered as Article 21 company involved in Health and Social Work.  
Appointed as Director on 2000/11/21.  
Address: [REDACTED]
- [REDACTED]  
Registered as Article 21 company involved in Community, Social and Personal Services.  
Appointed as Director on 1990/10/15.  
Address: [REDACTED]

### 1.3 TRAVEL RECORD

- Departed from Johannesburg International Airport onboard Emirates Airline flight EK464 on 1998/07/06 and arrived back from Dubai onboard South African Airways flight SA151 on 1998/07/17.
- Departed with British Airways flight BA6265 on 1999/10/30 from Johannesburg International Airport and arrived back onboard flight BA6266 on 1999/11/01.
- Departed from Johannesburg International Airport onboard Emirates Airline flight EK464 on 2001/01/26 and arrived back onboard flight EK463 on 2001/02/09.



- Departed from Johannesburg International Airport onboard Emirates Airline flight EK464 on 2001/04/21 and arrived back onboard flight EK463 on 2001/04/28.
- Departed from Johannesburg International Airport onboard Egypt Air flight MS878 on 2001/07/07 and arrived back onboard flight MS879 on 2001/07/21.

2. [REDACTED]

### 2.1 PERSONAL PARTICULARS

Date of Birth: [REDACTED]  
Passport: [REDACTED] prior to 1994 utilised SA passport  
[REDACTED] No PA [REDACTED]  
Identity number: [REDACTED]  
Physical address: [REDACTED]  
Postal address: [REDACTED]

### 2.2 COMPANY LINKS

- [REDACTED]  
Registered as Article 21 company involved in Community, Social and Personal Services.  
Appointed as Director on 1990/10/15  
Address: [REDACTED]

### 2.3 TRAVEL RECORD

- Departed through the Beitbridge border post between South Africa and Zimbabwe on 1993/12/04 in a vehicle registered as [REDACTED]
- Departed from Johannesburg International Airport onboard South African Airways flight SA276 to Mumbai on 1999/02/01 and arrived back onboard flight SA277 on 1999/03/01.
- Departed from Johannesburg International Airport onboard Egypt Air flight MS878 on 2000/06/08 and arrived back onboard flight MS877 on 2000/06/29.
- Departed from Johannesburg International Airport onboard Egypt Air flight MS878 on 2001/07/07 and arrived back onboard flight MS879 on 2001/07/21.

ALJAZEERA





## Intelligence

National Intelligence Agency  
REPUBLIC OF SOUTH AFRICA

NIA/EM41/1/5/1

FOREIGN INTELLIGENCE LIAISON

17 February - 5 March 2010

### LIAISON ACTIVITY REVIEW: WEEK

COUNTRY	CONTACT DATE	DMS NO.	PURPOSE/DISCUSSION	ACTION BY IMM
SOUTH KOREA (LS843)	18/2/2010	100003359775	<p>-LS843 reported that the following two Pakistan nationals were arrested in South Korea. The persons were travelling with South African passports, as follows:</p> <p>[REDACTED]</p> <p>LS843 explained that the above persons previously worked in South Korea for three years, after which their visas expired and they were expelled from South Korea. Recently, the same persons tried to enter South Korea with South African passports and were arrested.</p> <p>Copy of the passport is included (Annexure A)</p>	LS843 requested NIA to verify the above information and would appreciate any further information that NIA may have on the above individuals.

ALJAZEERA  
CONFIDENTIAL



	4/3/2010	<p>-NIA was further requested to indicate any possible security threat against the President of South Africa during the G20-Summit to be held in South Korea from 11 – 12 November 2010.</p> <p>-Specific security assessments were requested on the following SA nationals:  The Director of Green Peace, Mr. Kimi NAIDOO  Mr. Feeroz Abubaker GANCHI (DOB: 28/01/1971)  Mr. ZUBAIR Ismail (DOB: 06/12/1984)</p> <p>Mr. GANCHI and Mr. ZUBAIR are listed in South Korea as "dangerous persons" that may travel to South Korea during the G20 summit. LS843 was aware that the mentioned persons are South African Nationals and that they travelled to Pakistan.</p> <p>-LS843 reported that during November 2009, the Durban harbour authorities confiscated a shipment from North Korea that was en route to the Congo. LS843 said that it is reported that there were parts of combat Tanks: T55 and T54 found on the shipment.</p> <p>- LS843 requested the Liaison Officer to facilitate an invitation to the Head Domestic, the DDG Domestic and the Head FIS Liaison, to play golf or attend a lunch at their convenience with himself and the Ambassador of South Korea</p>	<p>Threat assessment to NIS</p> <p>Threat assessment to NIS</p> <p>LS843 requested if NIA could indicate what the current status of the investigation is.</p> <p>Invitation to Head Domestic, DDG Domestic and Head FIS Liaison – approval to go ahead with arrangements is hereby requested.</p>
LESOTHO (LS635)	5/3/2010	<p>4 Bangladesh nationals were briefly questioned at ORTIA where they were in transit to Lesotho. They had a clearance letter from Lesotho immigration.  However on questioning it became clear that their final destination was Ladybrand in South Africa</p>	



			<p>orchestrated and facilitated their travel from Lesotho. AMOT is carrying a South African ID: 64062950044088 and he apparently has a house in Ladybrand, Eastern Free State and a house in Escourt KZN. (Annexure B)</p>	
ISRAEL (LS825)	17/2/2010	10000359072	<p>MOSSAD has extended an open invitation to the Head Domestic, Mr NJENJE to visit Israel. The invitation letter has been provided to the Office of Mr NJENJE. It should be expected that Israel would intensify on all fronts, efforts to get South Africa under their sphere of influence. The South African Jewish Community has a huge contribution to the Israeli economy and that places South Africa top of the Israeli Government's priority countries. The NIA Management to have clear objectives when Mr NJENJE leads a NIA delegation to Israel. MOSSAD has done its homework and hope to exploit the visit by putting forward their objectives. It is noted that MOSSAD has not demonstrated the same kind of interest in SASS.</p> <p>The MOSSAD information request to NIA on Counter Proliferation is long overdue. It was provided to NIA in September 2009. (See Annexure B).</p>	IMM to decide
ISRAEL (LS825)	15/2/2010	10000358324	<p>MOSSAD formally proposal a secured communication system between Tel Aviv and Musanda. The absence of a permanent local representative of MOSSAD in South Africa has prompted this proposal. It was further suggested that the secured communication could be utilised to conduct record checks of suspicious names for the 2010 FIFA World Cup and contribute to information exchange volume.</p>	<p>IMM to decide.</p> <ul style="list-style-type: none"> <li>• Please note that this is the 2<sup>nd</sup> request in this regard: <ul style="list-style-type: none"> <li>- CIA</li> <li>- MOSSAD</li> </ul> </li> </ul>
ALGERIA (LS674)	26/2/ 2010	10000362168	<p>the Local Representative of LS674 discussed the confusion regarding parking in front of the Algerian Ambassador's residence in Waterkloof. Embassy security prohibited parking in front of the Ambassador residence regarding security concerns and has put up no parking signs. DIRCO has responded in a letter ordering the Embassy to take down the signs.</p> <p>Letters to DIRCO and the Tswane metro are attached as Annexure C.</p>	IMM/EXCO to advise.



			██████████ was advised to address the security concerns with DIRCO and the Diplomatic Security (SAPS).
ZAMBIA (LS630)	26/1/2010	10000361588	List of suspected AL-QAIDA terrorists operating between RSA, Zambia, DRC, Rwanda and Somalia with intention to carry out terrorists attacks during 2010 FIFA World Cup Tournament.  Request for information on asylum seeker ██████████ who claims that he lived in RSA between March and December 2009.
ZAMBIA (LS630)	6/3/2010		-Information requested on travel record of Rajan MAHTAN who is wanted in Zambia for massive fraud which include state's funds. According to the representative, MAHTAN is a very bitter man and could do anything in a third country to embarrass the Zambian government. - MAHTAN was spotted at the intercontinental hotel at ORTIA on 06/03/2010, on the same day the President of Zambia and the Director General of the Zambian Intelligence Service were at the hotel whilst in transit to China. His passport no is ██████████
RUSSIA (LS 848)	26/2/2010	10000362166	██████████ indicated that he will request more documents from Moscow on terrorism as a priority seeing the RSA is hosting the 2010 FIFA World Cup. He indicated that it was important to receive feedback on the information that the SVR shared with NIA.  ██████████ mentioned that the Iranian has a new missile called SIMORGH. A meeting with the NIA Counter Proliferation members is



			requested to share information with the SVR on the technical characteristics of the missile. The Russians are concerned because the range of this missile is longer than previous ones and could be utilised as a carrier of nuclear war heads.	
MALAWI(LS 626)	24/ 11/ 2009	10000343843	<p>A reminder that in November 2009 the Malawi Service forwarded a request to NIA on two diplomats who were going to be station in Malawi.</p> <p>HE LADISLAY STRAKA - SLOVAK Ambassador to Republic of South Africa since September 2008.</p> <p>HE MOHSIN MOVAHLEDI GHOMI - former Islamic Republic of Iran Ambassador to Republic of South Africa from 1996 - 2000.</p> <p>(Annexure D)</p>	IMM to give direction and decision
CANADA (LS 827) (CSIS)	4/3/2010	10000363535	<p>-NIA was requested by LS827 to attend the upcoming annual bilateral discussions between the South African and Canadian governments on "Sixth Annual Bilateral Consultation" that will be held in Ottawa, Canada on 20-21 April 2010.</p> <p>The Canadian High Commissioner invited the HOS of LS827 to be part of the visit to Canada. This could however only materialize if there is a representative from the South African security and intelligence community who also take part in the visit. (See Annexure E for ease of reference)</p> <p>-Information is requested regarding media reports on allegations by a former employee of EL AL Airlines that the airline was a front for Israel clandestine operations in South Africa. (See Annexure E for ease of reference)</p>	



REQUESTS RECEIVED FROM SASS

COUNTRY	CONTACT DATE	DMS NO.	PURPOSE/DISCUSSION	ACTION BY IMM
NETHERLANDS (LS733)	12/02/2010	10000357881	-Trace Request number 2944 from the Netherlands, was received from the Directorate Domestic Liaison (SASS). SASS would like to have the response on or before 01/03/2010	IMM to give feedback on the matter.
	3/3/2010	10000364008	- The following Trace Requests: Numbers 1606 and 3269 from Netherlands were received via SASS: <ul style="list-style-type: none"> <li>• [REDACTED]</li> <li>• [REDACTED]</li> </ul> (Annexure F)	
LESOTHO (LS635)			-Request for information of [REDACTED] who was involved in the plot to assassinate the Prime Minister of Lesotho. According to their information [REDACTED] is currently living in Johannesburg.	IMM to give feedback



			-Request for facilitation of the NCIS member to be part of the intelligence team that works on the FIFA World Cup Tournament as agreed during the Namibia/RSA Joint Commission of 2009.	IMM to initiate
LS831 (SIS):	2/03/2010	10000362939	<p>-An outstanding response by NIA to information requests contained in a liaison report under reference 10000341930 of November 17, 2009 was again brought under attention.</p> <p>-The following two documents were exchanged to alert the NIA (Annexure G):</p> <ul style="list-style-type: none"> <li>• ██████████ Walk-In Claims Knowledge of AL-QAIDA, ref, CI/NIA 10/001, 19 February 2010</li> <li>• Pakistan/South Africa/Terrorism: Huji Commande ██████████ ██████████ wants Huji Facilitator to Meet Extremists in South Africa, Rels/09/1391 of 31 November 2009.</li> </ul>	

PLANNED VISITS

COUNTRIES INVOLVED	LEVEL	INBOUND/OUTBOUND	DATE	PURPOSE
RSA / BOTSWANA	Experts DG/Ministers	Outbound	Postponed, date will be forwarded as soon as fixed Possibly postponed to March 2010 (Not confirmed, will give feedback as soon as finalised)	JITT JPC

ALJAZEERA  
CONFIDENTIAL



RSA / ZIMBABWE	Experts	Outbound	No date	IMM to guide and give time frames
RSA / ZAMBIA	Experts	Outbound	After the SADC Organ meeting. Proposed date 11–12 March 2010.	Outstanding 2010 briefing to the Zambian Service.
RSA / NAMIBIA	Experts	Outbound	Not confirmed. Consult SASS for arrangements.	Implementation of the action plan. IMM to guide (EM41 following up)
RSA / NAMIBIA	Experts / CP	Outbound	No date. Consult SASS for arrangements.	Briefing on CP to NCIS and other relevant Namibian role players
RSA / ALGERIA	Experts	Outbound	Awaiting confirmation from representative	Implementation of the MOU (Need to revisit how the MOU's will be influenced by new SSA structure)  * Please note that the Minister has been invited to Algeria.
RSA / EGYPT	Experts	Outbound	Postponed, new dates to be decided upon (after 2010 FWC)	Annual expert information exchange. NIA is reciprocating GIS visit to RSA December 08.
RSA/PALESTINE	DG/Top Management	Outbound	EXCO to guide.	Invited by LS879 to familiarize and demonstrate what is happening on the ground.
RSA/SWAZILAND/MOZAMBIQUE	Experts	Inbound	To decide	Reminder: To operationalise the MOU signed by 3 DG's after CISSA
RSA/TANZANIA	DDG EM20 Experts	Outbound	Postponed	Benchmarking on retirement model/Appointment officer
SOUTH KOREA/RSA	Experts	Outbound	After 2010 FIFA world Cup.	Discussions / workshop or further training in the area of CT
ZAMBIA/RSA	Experts	Outbound	Proposed 11- 12 March 2010	Briefing on 2010

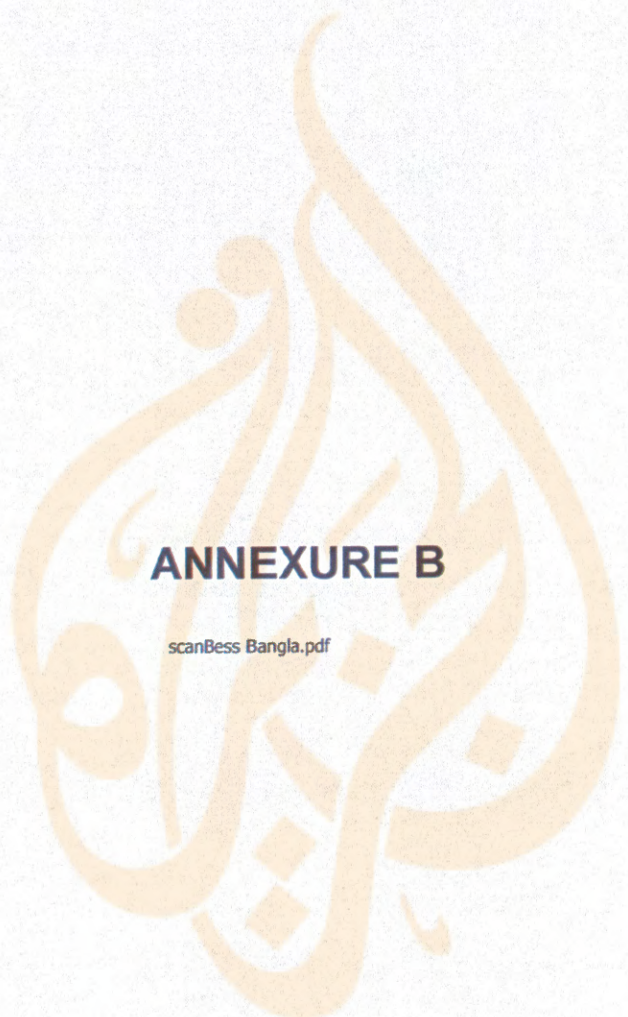


New visits are shown in bold

## ANNEXURE A

**ALJAZEERA**  
CONFIDENTIAL





**ANNEXURE B**

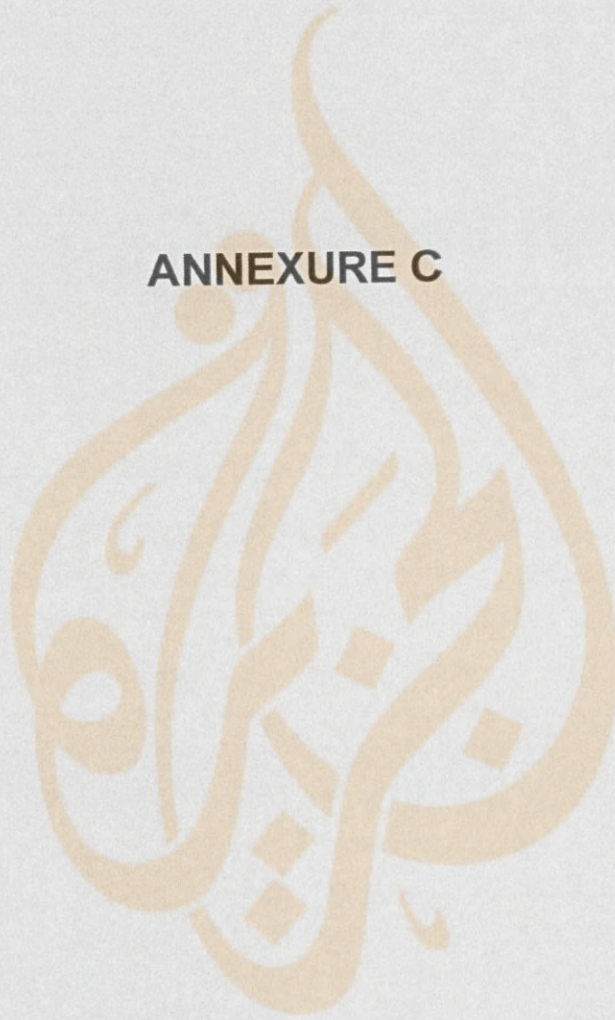
scanBess Bangla.pdf

**ALJAZEERA**

CONFIDENTIAL



**ANNEXURE C**



**ALJAZEERA**

CONFIDENTIAL



SECRET

4. PROCUREMENT ORGANIZATIONS ARE CHARACTERIZED BY BEING DYNAMIC AND ASSERTIVE, AND THEY QUICKLY ADAPT THEMSELVES TO THE CONSTRAINTS ON THEIR ACTIVITY IMPOSED BY TIGHTENING EXPORT CONTROL IN MANY COUNTRIES.
5. DUE TO THE CHARACTERISTICS OF THE PROCUREMENT ORGANIZATIONS' ACTIVITY, THEY IN FACT CAUSE COMMERCIAL ORGANIZATIONS AND SUPPLIERS IN PRODUCING COUNTRIES TO VIOLATE THE LAW, SOMETIMES UNKNOWINGLY.
6. FOLLOWING ARE SEVERAL BASIC QUESTIONS FOR WHICH WE WOULD APPRECIATE RECEIVING YOUR ANSWERS IN ORDER TO EXAMINE POSSIBLE FUTURE COOPERATION:

REQUIREMENT

7. IS THERE ANY IRANIAN OR SYRIAN PROCUREMENT ACTIVITY IN SOUTH AFRICA? IF SO, WHAT IS ITS VOLUME AND WHAT ARE ITS CHARACTERISTICS?
8. WHAT EQUIPMENT AND/OR RAW MATERIAL ARE ELEMENTS OF THESE COUNTRIES INTERESTED IN PROCURING? WHAT IS THE DESIGNATION OF THE PRODUCTS?
9. FOR WHOM DO THE IRANIAN AND SYRIAN ORGANIZATIONS PROCURE THE PRODUCTS, IN OTHER WORDS, WHO ARE THE DECLARED END-USERS OF THE PRODUCTS?
10. WHAT ARE THE CHARACTERISTICS OF THE ACTIVE PROCUREMENT ORGANIZATIONS (PRIVATE COMPANIES, MEDIATORS, EMBASSY

ALJAZEERA



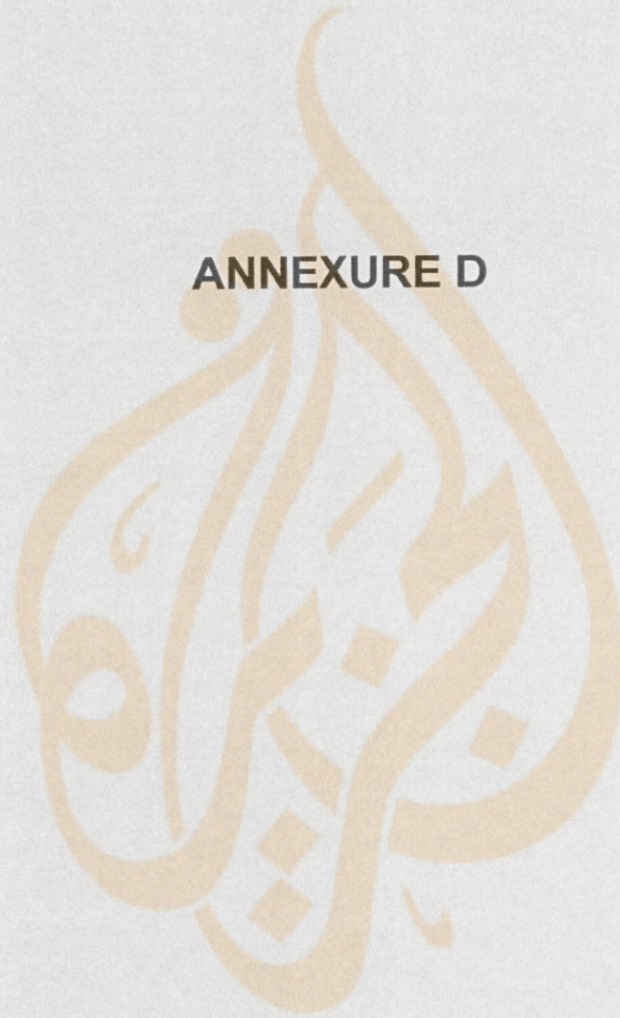
~~SECRET~~

11. DO IRANIAN SHIPS CALL AT SOUTH AFRICAN PORTS? IF SO, HOW OFTEN AND FOR WHAT PURPOSE? IS THE MERCHANDIZE LOADED ON THESE SHIPS MONITORED?
12. IS MERCHANDIZE DISPATCHED OR TRANSSHIPPED FROM PORTS IN SOUTH AFRICA OR IN OTHER AFRICAN COUNTRIES TO IRAN? IF SO, WHAT KIND OF MONITORING IS THERE ON THESE DELIVERIES?
13. IS THERE AN EXPORT MONITORING MECHANISM IN SOUTH AFRICA THAT OPERATES ACCORDING TO PROLIFERATION TREATIES SUCH AS MTCR, NSG, ETC.?
14. IF SUCH A MECHANISM EXISTS, WHAT IS THE MONITORING STRUCTURE? WHICH BODIES ARE INVOLVED? WHICH NATIONAL AUTHORITY IS IN CHARGE OF IT? WHAT ARE THE PRINCIPLES OF THE MECHANISM'S ACTIVITY?
15. WE WOULD APPRECIATE RECEIVING A LIST OF PROCUREMENT REQUESTS BY IRAN AND SYRIA, ESPECIALLY THE SUPERVISION MECHANISM'S LIST OF REFUSALS (WHAT THE COMMITTEE REFUSED TO EXPORT TO IRAN AND SYRIA).
16. THANK YOU FOR YOUR COOPERATION. BEST REGARDS.

ALJAZEERA



**ANNEXURE D**



**ALJAZEERA**

CONFIDENTIAL



Embassy  
of the People's Democratic  
Republic of Algeria  
Pretoria



سفارة  
الجمهورية الجزائرية الديمقراطية الشعبية  
بريتوريا

NV/N° 53 /10/ MINISTRY OF INTERNATIONAL RELATIONS AND  
COOPERATION, REPUBLIC OF SOUTH AFRICA

The Embassy of the People's Democratic Republic of Algeria presents its compliments to the Ministry of International Relations and Cooperation of the Republic of South Africa and has the honour to acknowledge the receipt of note verbale Prot/5/ALG/B2 dated 23 February 2010. This Embassy wishes to inform the latter that the necessary authorisation was definitely given by the Municipality of Tshwane. The Municipality did not yet put its own "No parking" signs in spite of its promise to do so six months ago. The Embassy reminds the honourable Ministry that most of the Embassies and residences, including Great Britain's and USA's, forbid any parking in front and around their premises. Consequently the Algerian Embassy can only be surprised by the unfriendly warning of its note verbale, a copy of which will be sent immediately to the Ministry of Foreign Affairs of the Republic of Algeria in order to examine the question in a reciprocity context, in case the Metropolitan police is asked to remove the signs in place.

The Embassy should like to advise the Ministry of International Relations and Cooperation of the Republic of South Africa not to give any instructions to the Metropolitan Police pending the moment when the Municipality of Tshwane will hang its own signs.

The Embassy of the People's Democratic Republic of Algeria avails itself of this opportunity to renew to the Ministry of International Relations and Cooperation of the Republic of South Africa the assurances of its highest consideration.

Pretoria, 26 February 2010

Ministry of International Relations and Cooperation  
Republic of South Africa



AJAZEERA





PROT/5/ALG/B2

The Department of International Relations and Cooperation of the Republic of South Africa presents its compliments to the Embassy of the Democratic People's Republic of Algeria and has the honour to refer to the Department's Notes Verbales dated 21 August and 16 October 2009 requesting the Embassy for the removal of the "No Parking" signs on the road in front of the residence of the Ambassador at 230 Antares Street, Waterkloof.

The Embassy is informed that the Department will request the Metropolitan Police Department to remove the signs until such time as the Mission has obtained an authorisation letter issued by the City of Tshwane, Division Works and Infrastructure in terms of domestic law.

The Department of International Relations and Cooperation of the Republic of South Africa avails itself of this opportunity to renew to the Embassy of the Democratic People's Republic of Algeria the assurances of its highest consideration.



PRETORIA  
23 February 2010

Embassy of the Democratic People's  
Republic of Algeria  
PRETORIA

ALJAZEERA





**City Planning, Development and Regional Services  
Department**

**Building Control**

Room 108 | 1st Floor | Murodora Building | Vermeulen Street | Pretoria | 0002  
PO Box 5242 | Pretoria | 0001  
Tel: 012 358 7998 | Fax: 012 321 3618  
Email: [pb@tshwane.gov.za](mailto:pb@tshwane.gov.za) | [www.tshwane.gov.za](http://www.tshwane.gov.za)

---

**OFFICE OF THE BUILDING CONTROL OFFICER**

---

Your ref:  
My ref:

Enquiries: M P Phala  
Date: 3 June 2009

Embassy of the People's Democratic Republic of Algeria  
950 Arcadia Street  
Pretoria  
0083  
South Africa

Siz/Madam

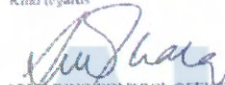
After an inspection which was conducted on the 29th February 2008, our respond was send to Department of Foreign Affairs on the 6<sup>th</sup> of March 2008 for them to communicate it to you. But be that as it may as Building Control, we don't have any objection to your request to put obstruction chain or concrete cones in front of your offices situated in 950 Arcadia street Arcadia, for the problems you experience during rugby and soccer matches at Loftus stadium.

Note: The position of this chain or cones mustn't obstruct the movement of pedestrians through the walkway/pavement.

I recommend an inspection after you finished putting them up.

Regards

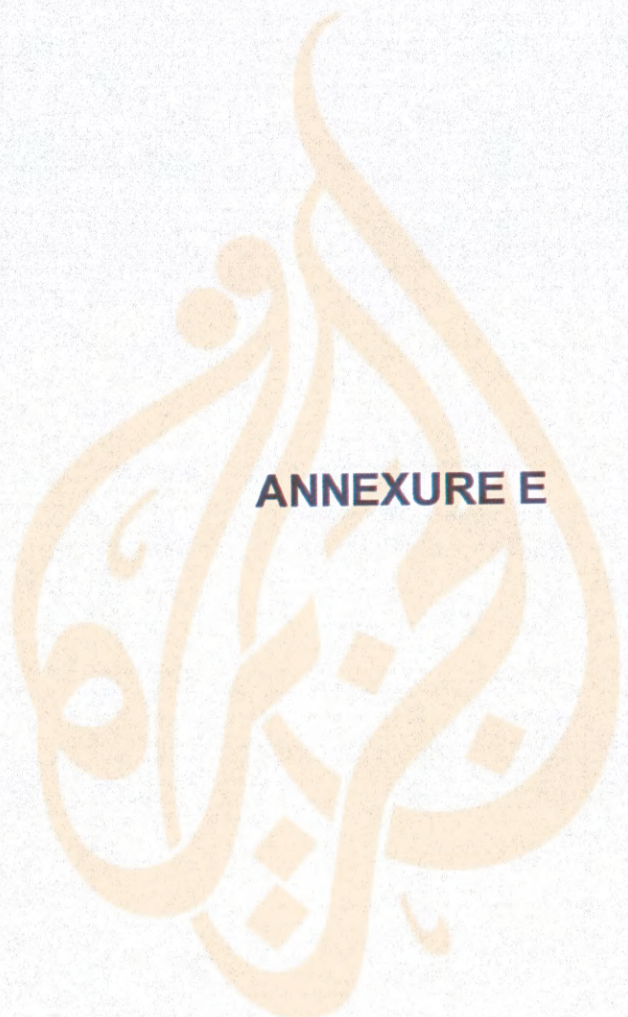
Kind regards

  
BUILDING CONTROL OFFICER  
Peter Phala  
Office of the Building Control Officer  
Murodora

On request, this document can be provided in another official language.







**ANNEXURE E**

**ALJAZEERA**

**CONFIDENTIAL**



TRACE REQUEST

SECRET

December 29, 2009

TO: SOUTH AFRICAN NATIONAL INTELLIGENCE AGENCY (NIA)  
FROM: CANADIAN SECURITY INTELLIGENCE SERVICE (CSIS)  
OUR FILE: 77-09-01290

---

The Canadian Security Intelligence Service (CSIS) presents its compliments to your Service, and would appreciate any information your Service might be able to share on the trace request below.

On 2009 10 23, open media reported that Jonathan GARB, a former employee of EL AL AIRLINES, claimed that EL AL AIRLINES was a front for Israeli clandestine operations in your country. According to reporting, the allegations have been investigated by a private security company which has released its findings in support of GARB's claims. On 2009 11 25, media reporting indicated that the South African government deported an airline official holding a diplomatic passport.

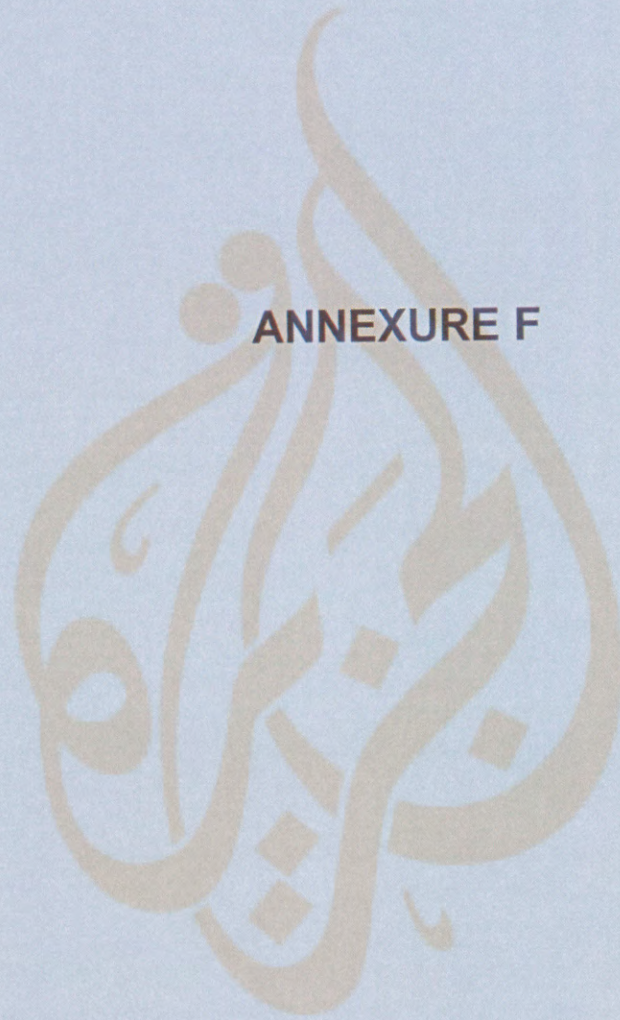
Our Service would appreciate any findings or information regarding the use / potential use of EL AL AIRLINES by the ISRAELI INTELLIGENCE SERVICES that your Agency may be able to share. As EL AL AIRLINES also operates in Canada, our Service is interested in the results of both your conclusions and those of the private security firm referenced above. Specifically:

- i. What evidence was used as the basis for the deportation of the Israeli diplomatic representative? Why was this particular representative chosen for deportation? What position was held by this individual?
- ii. Has your agency uncovered a link between other Israeli diplomatic personnel and Israeli intelligence elements?
- iii. Was your government able to confirm which of the Israeli Intelligence Agencies was involved with EL AL AIRLINES?
- iv. In what position(s) within EL AL AIRLINES were the suspected/confirmed Israeli intelligence operatives employed?
- v. Has your agency been able to confirm/refute media allegations that the alleged Israeli intelligence operatives has surreptitiously and/or illegally acquired firearms for use in their duties with EL AL AIRLINES?

Our Service appreciates the sensitivity of such a matter, and as such will treat any shared information in strict confidence. We look forward to engaging your Agency further.



**ANNEXURE F**

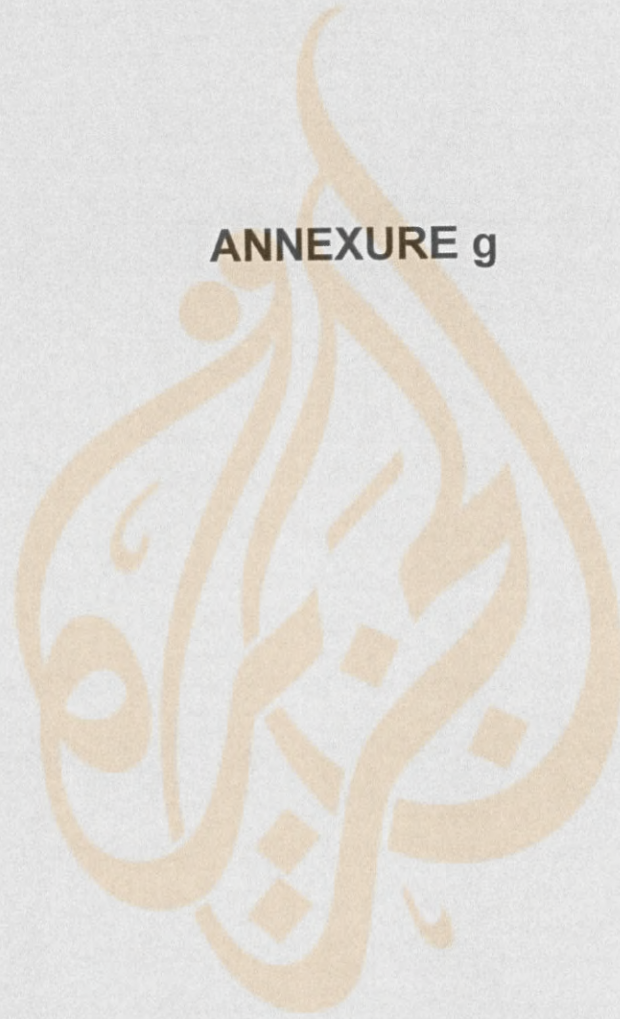


**ALJAZEERA**

CONFIDENTIAL



ANNEXURE g



**ALJAZEERA**  
CONFIDENTIAL



Ministerie van Binnenlandse Zaken en Koninkrijksrelaties



CONFIDENTIAL

Date  
February 1, 2010

Our reference number  
4281065/01

Department  
National Security

Information

T (070) 320 44 00  
F (070) 320 07 33

Your reference number

Page  
1 of 2

Number of enclosures

Postal address  
POB 20010  
2500 EA The Hague

To : SASS  
From : AVD

Subject  
Vetting enquiry

WON/2944-2009  
VETTING ENQUIRY

**URGENT**

**Please answer before: 15 February 2010**

With reference to our vetting enquiries of April 22, 2009, no. 4066583/01, May 27, 2009, no. 4090028/01, June 24, 2009, no. 4109867/01 and July 8, 2009, no. 4123285/01, we inform you that we have not received your reply so far.

Please signal traces of subject and partner as soon as possible.

Subject:

Name [REDACTED]  
Date of birth [REDACTED]  
Place of birth : Amstelveen (The Netherlands)  
Nationality : Dutch  
Present address [REDACTED]  
Passport-number [REDACTED]

Partner :

ALJAZEERA



CONFIDENTIAL

Date  
February 1, 2010

Our reference number  
4281065/01

Page  
2 of 2

Present address



Passport-number

Without your reply subject cannot fill the position involving confidentially. For that reason we urgently need your information and we would therefore ask you to send us your reply as soon as possible.

Please note that we only require an administrative check. No field investigation is needed.

We have subject's written consent for this vetting enquiry.

Please state the above WVON number in your correspondence relating to this vetting enquiry.

Yours sincerely,

THE MINISTER OF THE INTERIOR AND KINGDOM RELATIONS,  
p.p.  
The Director General of the General Intelligence and Security Service (AIVD),  
p.p.  
Head of Team, Unit Security Screening,

F. Uiterweerd

The above information is meant for intelligence use and may be used for this purpose only. The information may not be passed outside your service without prior consent of the AIVD. The AIVD reserves the right to inquire as to how the information has been used.

ALJAZEERA





## intelligence

South African Secret Service  
REPUBLIC OF SOUTH AFRICA

SASS Head Quarters, Musanda, Delmas Road, PRETORIA  
Private Bag X5, Elardus Park, 0047  
Tel: +27 12 427 5500, Fax: +27 12 427 6428

03 March 2010  
EL/LS/RE

Directorate Domestic Liaison

[REDACTED]  
HEAD: FOREIGN INTELLIGENCE LIAISON  
NATIONAL INTELLIGENCE AGENCY (NIA)

Trace Request: number 1606 from Netherlands.

1. Kindly receive the following correspondence from the Netherlands.
2. Kindly forward response to this office on or before 23/03/2010.
3. Thank you.

[REDACTED] ALJAZEERA



CONFIDENTIAL

Algemene Inlichtingen- en Veiligheidsdienst  
General Intelligence and Security Service

AIVD The Hague

Our reference number  
1606

Department  
Unit Security Screening

Page  
1 of 2

With reference to our earlier correspondence of December 31, 2009, we inform you that we have not received your reply so far.

Precedence : ROUTINE  
Classification : CONFIDENTIAL  
Group Name : GENERAL PURPOSE  
To : SASS  
From (Desk) : VO – Team D, VO4HIE  
To (Desk) :  
Date : February 15, 2010  
Message ID : 1606  
Reference nr. : 1606

VETTING ENQUIRY (Urgent)  
Please answer as soon as possible

Please signal traces of:

Subject:  
Name  
Date of birth  
Place of birth  
Nationality  
Passport nr

Address

From  
Until



ALJAZEERA





**ALJAZEERA**

CONFIDENTIAL



CONFIDENTIAL

We would ask you to check subject's criminal records and political background. Please let us know if you have any derogatory information on the subject. We would also like to know during what period of time subject stayed in your country.

Date  
15 February 2010

Our reference number  
1606

Please only carry out an administrative check, do not carry out a field investigation. We have subject's written consent for this vetting enquiry.

Page  
2 of 2

In view of the fact that according to Article 6 of the Security Investigations Act the vetting procedure has to be completed within a limited period of time, we would ask you either to provide the requested information to the AIVD not later than twenty eight days after the date of this request, or to let us know that the requested information cannot be provided or cannot be provided within the aforementioned term.

Please state our above mentioned reference number in your correspondence relating to this enquiry.

The above information is meant for intelligence use and may be used for this purpose only. The information may not be passed outside your service without prior consent of the AIVD. The AIVD reserves the right to inquire as to how the information has been used.

END OF MESSAGE

ALJAZEERA





intelligence

South African Secret Service  
REPUBLIC OF SOUTH AFRICA

SASS Head Quarters, Musanda, Delmas Road, PRETORIA  
Private Bag X5, Elardus Park, 0047  
Tel: +27 12 427 5500, Fax: +27 12 427 6428

03 March 2010  
EL/LS/RE

Directorate Domestic Liaison

[REDACTED]  
HEAD: FOREIGN INTELLIGENCE LIAISON  
NATIONAL INTELLIGENCE AGENCY (NIA)

Trace Request: number 3269 from Netherlands.

1. Kindly receive the following correspondence from the Netherlands.
2. Kindly forward response to this office on or before 23/03/2010.
3. Thank you.

ALJAZEERA

[REDACTED]  
MANAGER: DOMESTIC LIAISON



Ministarie van Binnenlandse Zaken en Koninkrijksrelaties



**CONFIDENTIAL**

Date  
23 February 2010

Our reference number  
3269  
Department  
Unit Security Screening

Information  
T +31 79 320 52 27  
F +31 79 320 54 33

Your reference number

Page  
1 of 2

Number of enclosures

Postal address  
POB 20010  
2500 EA The Hague  
The Netherlands

To: SASS  
From: AIVD

Subject  
Enquiry no.: 3269  
Please answer before: 23 March 2010

Dear Sir,

Please signal traces of subject:

Subject:

Name  
Date of birth  
Place of birth  
Nationality  
Address

Passport nr

From  
Until

Subject has applied for a position involving confidentiality, relevant to national security. In this position subject has access to classified information.

We would ask you to check subject's criminal records and political background. Please let us know if you have any derogatory information on the subject. We would also like to know during what period of time subject stayed in your country.

ALIAZERA



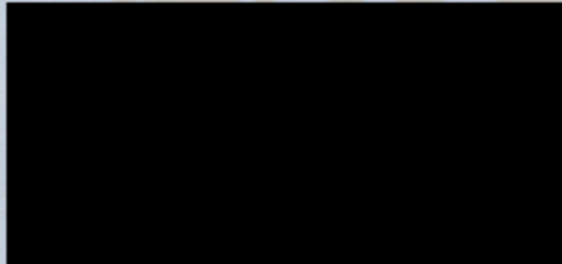
information cannot be provided or cannot be provided within the aforementioned term.

Please state our above mentioned reference number in your correspondence relating to this vetting enquiry.

The above information is meant for intelligence use and may be used for this purpose only. The information may not be passed outside your service without prior consent of the AIVD. The AIVD reserves the right to inquire as to how the information has been used.

Yours sincerely,

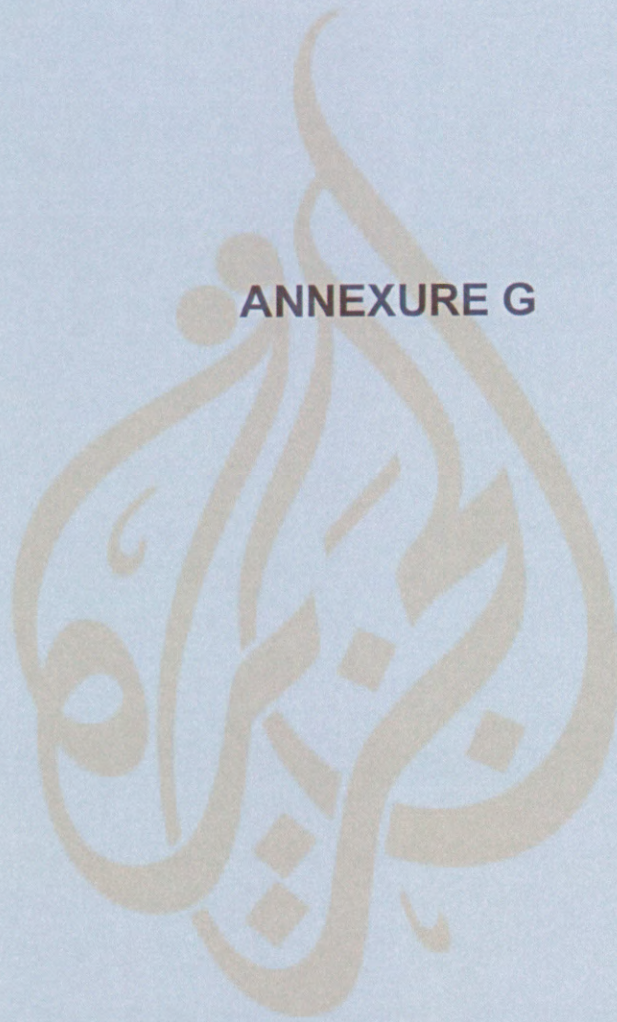
The minister of the Interior and Kingdom Relations  
p.p.,  
the director general of the General Intelligence and Security Service  
p.p.,  
the head of the Team of the Unit Security Screening



ALJAZEERA



**ANNEXURE G**



**ALJAZEERA**

CONFIDENTIAL



1000362939

Ref: CI/NIA 10/001

19 February 2010

WALK-IN CLAIMS KNOWLEDGE OF AL-QA'IDA

1. In February 2010 a walk-in to the British High Commission offered to provide information on Al-Qa'ida. The individual was interviewed by one of our security officers and provided the following bio-details:

Name: [REDACTED]

DPoB: [REDACTED]

Nationality: [REDACTED]

Telephone: [REDACTED]

2. [REDACTED] told our Security Officer that he was born in [REDACTED] but due to the political tensions he moved to Nigeria where he converted to Islam. From Nigeria he claimed to have travelled around Africa (Chad, Egypt, Sudan, Kenya, Zambia, and Botswana) before finally arriving in South Africa in November 2004.
3. [REDACTED] said he was a trained bomb maker and received his training in Egypt. [REDACTED] also said he joined an extremist cell in Zambia.
4. On arrival in South Africa in 200 [REDACTED] said he gave up his religion and tried to claim political asylum. This was not granted so to gain attention he threatened to [REDACTED]
5. We would be grateful for any further information/traces you are able to provide on [REDACTED]

ALJAZEERA



This information has been communicated in confidence to the recipient government.  
Action may not be taken on this information without prior reference to the originator.

**PAKISTAN/SOUTH AFRICA/TERRORISM: HUJI COMMANDER  
MAULANA MUHAMMAD AHMED WANTS HUJI FACILITATOR TO  
MEET EXTREMISTS IN SOUTH AFRICA**

**Source Description: Regular and reliable**

**Detail**

1. Intelligence from mid-September 2009 suggested that HUJI Commander Maulana Muhammad Ahmed wanted an associate, a Harakat-ul Jihad Islami (HUJI) facilitator, and a further associate, to travel to South Africa in order to establish extremist contacts there for training and fundraising purposes.
2. Ahmed envisaged that the HUJI facilitator would identify someone to facilitate his and the associate's travel into South Africa. They would enter and live in South Africa illegally.

**Source Comment**

- A. South Africa is widely viewed in Pakistani extremist circles as a good place from which to enter the UK and Europe undetected.
- B. The idea of the HUJI facilitator and other associate going to South Africa was new. No plans had been made and it would take a long time to arrange. It was possible that the HUJI facilitator would not go at all, or that someone else would go in his place.

**Service Comment**

Maulana Muhammad Ahmed is assessed to be identical with senior HUJI Commander Muhammad Ahmad Choota also known as Maulana Umar, a veteran of the Soviet jihad who has established training camps in North Waziristan with Ilyas Kashmiri.

ALJAZEERA



Document Number: 10000362939

Document Status: In Work

## 2. DOCUMENTS EXCHANGED

2.1 The following documents were exchanged:

- [REDACTED] Walk-In Claims Knowledge of al-Qa'ida, ref: CI/NIA 10/001 of 19 February 2010
- Pakistan/South Africa/Terrorism: Huji Commander Maulana Muhammad Ahmed Wants Huji Facilitator to Meet Extremists in South Africa, Rels/09/1391 dated 31 November 2009

2.2 In addition to the above documents exchanged the following batch of information documents on CT matters were directly exchanged with members of Directorate OC20

- The Terrorist Threat to Major Sporting Events, J-Rels 197/09, dated 10 December 2009
- UK Overall Threat Level Raised from Substantial to Severe, J-Rels 013/10 of 25 January 2010
- Yemeni Country Assessment, J-Rels 011/10 of 20 January 2010
- Terrorist Travel – The Methodology of Umar Farouk Abdulmutallab, J-Rels 005/10 of 12 January 2010
- The Thoughts of Umar Farouk Abdulmutallab, J-Rels 020/10 of 1 February 2010
- Details of the Device Used by Umar Farouk Abdulmutallab in his Attack on Northwest Airlines Flight 253, J-Rels 016/10 26 January 2010
- Terrorism Assessment: UK Based Fighters Associated with Somalia, J-Rels 184/09A, 4 November 2009
- Islamism and Islamist Groups: Are they a Threat? J-Rels 148/09, 1 September 2009
- AQ Core – The Current Status, J-Rels 168/09B, 27 November 2009

## 3. COMMENTS BY LIAISON OFFICER

3.1 The meeting resolved that the next liaison meeting would take place on Tuesday 16

# ALJAZEERA





**ALJAZEERA**

CONFIDENTIAL



## ***Liaison Information Report***

---

File reference: 6/1  
Compilation Date: 2011/09/02  
Originating structure: EM41  
Restriction: DOMESTIC BRANCH ONLY

---

GENERAL MANAGER CI10: Attention  
GENERAL MANAGER IM10: Attention

### **LS672: LIAISON CONTACT 2011 SEPTEMBER 02**

PERSONS INVOLVED: [REDACTED] Local Representative  
Liaison Officer

VENUE: THE PLACE RESTAURANT

TIME: 09:30 – 10:30

#### **1. THE DETAILS OF THE MEETING**

- 1.1 [REDACTED] the Local Representative of the Cameroonian Intelligence Service requested the meeting with the Liaison Officer to discuss and forward information request on a Cameroonian national suspected to have visited South Africa (S A).
- 1.2 [REDACTED] mentioned that Mr Pierre Mila ASSOUTE a Cameroonian national once belonged to the governing party in Cameroon. He broke-away from the governing party and formed his own political party. According to sources of the Cameroonian Intelligence Service Mr ASSOUTE is thought to have travelled to S A.
- 1.3 [REDACTED] mentioned that the Authorities in Cameroon were requesting SSA to confirm or refute if Mr ASSOUTE ever came to S A recently and the purpose thereof if it could be established.
- 1.4 The Liaison Officer indicated that he foresaw difficulty for knowing why and who he visited while in S A. He requested Cameroon to provide more information that would make investigating structures with a clue to conduct their task effectively.

#### **2. DOCUMENT/S EXCHANGED**

- 2.1 Information request: trace check of Mr ASSOUTE

#### **3. COMMENT/S BY THE LIAISON OFFICER**

- 3.1 The Cameroonian Authorities are concerned about events that could blemish or disrupt the Presidential elections in October 2011. The unity of the Cameroonian nation is fragile since most political parties are ethnic/tribal based. It's clear that ASSOUTE is under the radar of



the Cameroonian Intelligence Services and his movements and of other opposition leaders are being monitored.

[REDACTED]  
LIAISON OFFICER

**3. COMMENT/S BY EM41**

3.1 I do not think Mr Pierre Mila ASSOUTE has committed any offence which will warrant SSA to provide information

[REDACTED]  
GENERAL MANAGER LIAISON AND PROTOCOL SERVICES



**ALJAZEERA**



SECRET

2

Document Number:

Document Status: Released



intelligence

National Intelligence Agency  
REPUBLIC OF SOUTH AFRICA

### *Liaison Information Report*

---

File reference: 6/1  
Compilation Date:  
Originating structure: Foreign Intelligence Liaison(EM41)  
Restriction: NIA ONLY

---

HEAD EM10  
GENERAL MANAGER CI10  
MANAGER CI20  
MANAGER IM20

#### **ISRAELI MEETING WITH DIRCO: NEW DIRCO BUILDING: 23 NOVEMBER 2009**

The information was obtained during a discussion with Ambassador Johan MARX, the Director for Middle East at DIRCO.

#### **1. BACKGROUND**

- 1.1 A disgruntled South African employee at the EL-AL security offices in ORTIA, has contacted CARTE BLANCHE to disclose information regarding the supposedly illegal conduct of the Israeli members, working at the offices of EL-AL in ORTIA.

-They did carry firearms and had according to them diplomatic protection if they would have to use it. They even had all access(unrestricted) at the airport. This gave them the advantage to gather information with regards to arrivals and departures to and from South Africa.

This was amongst other matters the main discussion between the two groups on Monday, 23 November 2009.

- 1.2 According to Ambassador MARX the meeting took place at the new offices of DIRCO in Riviera. The Israeli delegation arrived in the morning of 23 November 2009 and departed the evening of the same day.

ALIAZEERA



SECRET

3

Document Number:

Document Status: Released

The Israeli delegation consisted of a legal expert, the head of EL-AL in South Africa and the security head at ORTIA amongst others. (Names unknown at this stage, but will be received on 26 November 2009 from Ambassador MARX)

Ambassador K. MAKHUBELA, the Head of State Protocol at DIRCO handled the meeting. A member of SASS [REDACTED] was also present IN the meeting.

## 2. CONTENTS OF MEETING

- 2.1 After the CARTE BLANCH affair, where it was exposed that the security personnel at EL-AL was accredited as diplomats as well as had diplomatic certificates to carry weapons. It was subsequently withdrawn immediately by DIRCO.
- 2.2 The ISRAELI's came to South Africa to request DIRCO to still give diplomatic immunity to the EL-AL security members. It was explained in the meeting that this was not possible and that according to South African law, no private citizens qualify for diplomatic immunity. It is the preserve of members of declared diplomatic communities.
- 2.3 If they would like to continue at ORTIA they will have to get work permits through the Department of Home Affairs and if they want to carry arms it will have to follow the SAPS processes as stipulated by law in South Africa.

## 3. COMMENT

It is of great concern that neither SASS nor DIRCO informed NIA (the internal branch) wrt the delegation and the actual meeting on Monday.

It is important to note that line functionally, government departments such as the DOT, DIRCO and SASS were obliged to communicate this information/engagement to NIA immediately.

- 3.3 Neither the MOSSAD representative or Israeli Embassy has sensitised EM41 on the matter.

Follow-up on the matter will be conducted by EM41 and other structures as required.

## 5. COMMENTS BY EM41

### 5.1

[REDACTED]  
HEAD FIS LIAISON

ALJAZEERA



## IM25: THEMATIC ASSESSMENT

### SECURITY VULNERABILITIES IN GOVERNMENT

October 2009

#### 1. INTRODUCTION

- 1.1 *Persistent concerns around information security risks in the government are assessed as a **major risk of long-term duration**.*
- 1.2 Foreign governments and their intelligence services strive to weaken the State and undermine South Africa's sovereignty. Continuing lack of an acceptable standard of security at client institutions (government departments, parastatals and national key points) increases the risk. With the formation of the new government and its electoral mandate carried out in key priorities and programmes, particular ministries and their respective departments are becoming targets of foreign intelligence services (FIS) for opportunities and influence.
- 1.3 Previous and current investigations by NIA indicate that the human factor remains the primary cause of security vulnerabilities at client institutions. This resulted in an array of security-related incidents, such as security breaches, the theft of personal and laptop computers and other information and communication technology-related equipment at client institutions over the past few months. The aforementioned demonstrates the extent of non-compliance with information security policies and non-implementation of the Minimum Information Security Standards (MISS), which continue to represent a major risk to the integrity of sensitive/classified information.
- 1.4 Similarly, investigations concluded by the National Intelligence Agency (NIA) have exposed serious deficiencies in the security integrity of the information and communication technological systems (ICTS) at a number of client institutions. Investigations revealed the extent to which these weaknesses were exploited for fraudulent purposes and financial gain. Whilst fraud and concurrent financial losses to the government raises concern, deficiencies exposed by these incidents have far-reaching strategic implications. Such deficiencies render statutory institutions vulnerable to fraud and corruption, and worst to espionage and malicious infrastructural disruption.



## 2. TRENDS ASSOCIATED WITH SECURITY DEFICIENCIES IN GOVERNMENT

- 2.1 Security deficiencies at client institutions remain a standing challenge. Personnel, physical, document and information communication technology security remain prevalent deficiencies.
- 2.2 NIA has established the following trends that underline security vulnerabilities
- Non-adherence to the MISS regarding the criteria for classification of documents and control of information (the aforementioned has been reported nationally);
  - Non-issuing of security clearances /record checks on external courier services transporting classified documents;
  - Insufficient lock-up facilities to store classified information and the lack of control over copies and/or the removal of sensitive information from Client Institutions (the aforementioned has been reported specifically in Mpumalanga, Limpopo, North West and KwaZulu Natal);
  - Non existence of control measures and/or procedures for the destruction of sensitive/classified documents.
  - Limited vetting of senior officials employed at sensitive institutions. ICT personnel in particular are often not being vetted;
  - Inadequate protection of the storage and retrieval of information (sensitive and classified);
  - Recommendations made during security audits at Departments are often not being implemented;
  - No approved encryption facilities on landlines and/or cellular phones;
  - No records with regard to the transmission and receipt of all sensitive information via facsimile and no effective control over open facsimile machines;
  - Virtually uncontrolled access to ICT and communication equipment;
  - Non-adherence to MISS in terms of using encryption for computerised transmission of sensitive/classified data;
  - The lack of proper ICT emergency plans and procedures and disaster recovery plans in terms of information stored on networks;
  - A general lack of skilled personnel to implement and maintain effective ICT security;
  - No institution responsible for performing formal back-up/ restoring procedures or to test the functionality of ICT systems. Institutions that do have own measures in place are making use of un-vetted contractors with facilities which are non-compliant with minimum security standards;
  - Most Client Institutions outsource their ICT functions to private companies of which only a few undergo record checks;



- No password protection of laptop computers. Inadequate control over the issuing of laptop computers and the removal/storage of such computers away from Client Institutions;
- The appointment of Security Managers remains a concern. It should be noted that the Security Managers Forum (SMF) is a sub-committee of the Counter Intelligence Coordinating Forum (CICF), and as such report to the CICF. In many instances the criteria set for filling these positions are not met. In some instances Security Managers have not been appointed as yet. Another challenge that remains is that, in some instances, Security Managers are not appointed at the level of a Director, as stipulated in NIA's position paper on the issue, which result in the lack of adequate communication between Security Managers and their senior management, ultimately negatively impacting on security in that Department;
- Closely linked to the aforementioned is the fact that Security Manager's Forums in some provinces are not functioning (such as in the Northern Cape, The Forum in the Eastern Cape was only reactivated in 2009, after being dormant for two years);
- It has been determined that coordination on provincial level with the SMF remains insufficient;
- A trend has been established that Security Managers do not report incidents of security breaches to NIA as they fear that the incident would negatively reflect on them personally and/or their Department;
- A questionnaire, developed by the Counter Intelligence Coordinating Committee (CICC), to report security breaches, has not been implemented by the SMF.
- Finally, Security Managers are not being held accountable for the implementation of the MISS in their Departments.

### 3. THE CURRENT THREAT POSED TO CLIENT INSTITUTIONS ITO SECURITY VULNERABILITIES

3.1 In addition to the aforementioned, the following section provides a somewhat more detailed exposition of vulnerabilities that have been identified at Client Institutions, which could be exploited by foreign and private intelligence services/structures as part of their espionage efforts:

- **Inadequate awareness among government officials of the threat of espionage posed by foreign intelligence services.**

Although certain Government institutions have been reached through the implementation of the MISS, security consciousness remains deficient. In this regard the problem of naivety among employees at sensitive installations, government departments and even private institutions and businesses mainly stems from a lack of knowledge regarding the threat posed to South Africa in



general. The aforementioned results in South African citizens assisting/co-operating with foreign intelligence services, whether by unwittingly providing them with classified information or by allowing them access to restricted areas.

NIA, from a defensive perspective, frequently provided security awareness interventions at government departments. In this regard, specific programmes were presented to the SANDF, SAPS, NCC, COMSEC, SASS and others. The security awareness programme included an awareness of the espionage threat as well as focussed on security deficiencies and the impact it has in terms of security in Client Institutions in general. A similar awareness intervention was presented to provincial clients, such as the Treasury in Limpopo (Polokwane). However, from a provincial perspective, many provinces reported that security awareness in their provinces are either not being conducted or that it is inadequate.

- **Exploitation of protocol privileges for intelligence purposes inter alia, the lack of control of diplomats placed in South Africa and non adherence of accreditation protocols by foreign diplomatic missions in the country. In addition, foreign intelligence service members utilise diplomatic cover to obtain access to sensitive information through their contact with government officials.**

The activities of some FIS members are characterised by a total disregard for the regulations and protocols governing the conduct of diplomats and their staff. Diplomatic cover is also frequently being used to obtain access to certain individuals and institutions, particularly Departments such as the Department of International Relations and Cooperation (DICO). FIS members also use their diplomatic status to gain access to critical information and/or infrastructure, where they can freely establish contacts in various sectors of the South African government and economy. An example of the former is the free access to the Oliver Tambo International Airport (ORTIA) by the Security Manager of the Israeli airliner, EL AL.

Interestingly, vetting statistics confirmed the fact that DICO remains specifically problematic. DICO had the highest number of security clearances being denied, followed by the then Directorate for Special Operations, the Department of Trade and Industry and then the Department of Home Affairs. Security clearances were denied due to the following: dual citizenship, drug/substance abuse, contact with FIS, poor financial management of personal finances and a lack of cooperation to the vetting investigation process.

- **Limited measures and lines of communication exist whereby South African Government Departments could inform NIA on agreements and arrangements with foreign countries. No information on various**



**Committees and sub-Committees operating in government is being liaised with NIA.**

This holds specific threats to national security since FIS members and/or their countries of origin regularly enter into agreements with South African Government Departments, without the knowledge of NIA, which could negatively impact on government programmes and/or interests. Consideration should be made to involve individuals (government officials) with specific skills to be involved in scrutinising potential agreements between government entities and foreign entities, especially those dealing with complicated and specialised issues such as science and technology.

The fact that many inter-departmental and governmental Committees and sub-Committees are operating without NIA having knowledge of and/or advising on possible inherent risks in this regard is currently being addressed by the Counter Intelligence Coordinating Committee (CICF). This situation is regarded as being pivotal since the functioning of many of these Committees directly impacts on national security. Committees that would be scrutinised include those dealing with weapons control and export procedures as well as those dealing with the coordination of terrorism issues.

- **Inadequate control and regulation over the activities of FIS members and/or liaison officers placed in South Africa.**

FIS members regularly liaise with different components of the SA intelligence community. The aforementioned is to a large extent not co-ordinated within the South African intelligence community, which could be exploited by foreign services.

Another factor which poses a threat to South African national security, is the lack of control of access to the offices of government employees and those employed at strategic institutions in the country. In this regard, it is evident that FIS members continue to enjoy uncontrolled access to the Departments of International Relations and cooperation (DICO) and Trade and Industry in particular, especially when utilising their diplomatic cover as indicated earlier. Foreign embassy staff almost have total freedom of access to especially DICO. FIS members also have access to parliament as well as the offices of provincial governments. FIS operatives not only have access to government departments, but are frequently visiting security installations. Visiting delegations (including delegations from Iran and China) to strategic installations such as DENEL, KOEBERG and Mossgas utilise official access, usually on invitation of these institutions, to demand access to sensitive plants where advanced technology is being developed.



The access of FIS is not restricted to officials of Departments such as DICO, but also includes their interest in obtaining access to specific Ministers. In this regard some FIS showed an interest in the Ministers of Energy, Defence and Military Veterans, Minister in the Presidency on Performance Management and Evaluation, DICO and also focused on the office of the President in particular.

Diplomats and FIS are not the only ones exploiting the inadequate security (lack of control of access in particular) at government offices and installations. Private security companies are of specific concern in this regard.

- ***Prospective job applicants in the public sector are not properly screened and foreigners are appointed in sensitive positions without the required security clearances. In addition, current personnel are not frequently enough being re-vetted.***

The non adherence of pre-employment screening, screening of companies and screening of immigrants remains a challenge in client institutions. On the other hand, infrequent vetting of personnel continues to be a noticeable trend.

In terms of conducting Personnel Suitability Checks (PSC), the former had been identified by Cabinet in order to screen individuals prior to employment, as the vetting process fails to yield timeous information on which the decision should be based in terms of employing individuals. The Minister of Public Service and Administration instructed departments to commence with the PSC as from 1 January 2008.

NIA is to, according to an instruction by Cabinet; improve its vetting capacity to 365 vetting functionaries by 2011. The instruction by Cabinet also prescribed the establishment of Vetting Fieldwork Units (VFU) in specific government departments. Out of the 17 priority Departments, only nine had been established successfully, one is semi-functional, five are in the process of being established and two are not functioning.

It is evident that foreigners (who meanwhile naturalised as South African citizens) employed in South African government departments could also pose a threat to national security. The appointment of technical advisors, under the guise of providing aid, also creates vulnerabilities in government departments. The technical advisors, who are responsible for the practical administering of projects, are placed on a national, provincial and local level across South Africa. The uncontrolled access provided by the formal bilateral aid agreements and placement of technical advisors across South Africa is being exploited for intelligence collection purposes. The possibility exists that some of these technical advisors could be employed in potentially sensitive positions in national departments and provincial legislatures where they might



have access to classified information. No regulatory measures are in place to regulate or monitor such activities.

The appointment of foreigners at sensitive installations (National Key Points) remains problematic. Examples include the employment of individuals with scarce skills such as scientists, which are employed in laboratories and research facilities, thereby having access to classified information and/or the process of developing specialised technology. The risk in terms of skills transfer and technology-transfer is enhanced by this practise. Adding to the concern is the fact that the majority of these individuals are employed on a contract basis, which could have an affect in terms of their loyalty to the Institution. However, foreigners are not only employed in these fields only, cases have been reported of foreigners being employed at the State Information and Technology Agency (SITA), the Department of Trade and Industry, Treasury, etc.

The involvement of foreigners, mainly as consultants to the 2010 FIFA World Cup Tournament to provincial clients (host cities), is also posing a risk in terms of sharing classified information with such entities. It is known that foreigners, in many instances, form part of Provincial and other government meetings, where they have access to privileged information. It is also believed that the risk could be extended well beyond the closing of the Tournament. The aforementioned is not limited to the 2010 Tournament, but is valid for all major special events being hosted by South Africa.

It is evident that the screening of foreign nationals remains a grey area and that there is little control over the process. During a recent CICF meeting it has been suggested that the uniform vetting standards be reviewed in order to address this issue. The problem seems to be the lack of guidance to institutions in conducting such screening. Subsequently departments are not adhering to the prescribed annual reporting of the security competency of foreigners in their employment.

- ***Private security companies, many of whom have connections with foreign intelligence services, are recruiting former intelligence members.***

There is a proliferation of private security and intelligence companies who provide services to and thereby have access to sensitive government, parastatals and private institutions. Clients of Private Intelligence Organisations include foreign embassies, government departments, the private sector, parastatals and foreign-based clients. At present these private intelligence organisations and groups sell their services to whoever is willing to buy them. Apart from possible access to sensitive information, those involved in physical security has access to CCTV footage, which could also



be of interest/value to FIS and an array of other actors. The problem with private security companies is that they are not operating under the same accountability procedures as statutory intelligence structures.

Former and serving members of the government security establishment are recruited by private security companies in order to utilise their expertise, skills, and contacts or to make use of their access within the said institutions. It is known that the American Embassy in Pretoria particularly recruits former SAPS members as security officers, who then maintain and utilise their contacts within the SDAPS and other government departments. It is suspected that these companies still utilize their old contacts in the NIA, SASS, SANDF, SAPS and other government structures wittingly/unwittingly to obtain information.

Private Intelligence Organisations thus potentially provide a perfect conduit for foreign intelligence services (FIS) and organisations hostile to the State who are seeking access to sensitive / classified information from South Africa.

- ***Inadequate security to protect tender documentation***

The lack of adequate security measures, and access control in particular, resulted in serious incidents which have the potential to directly impact on national security. In one such instance sensitive documentation relating to a prominent tender process was being tampered with, which could ultimately result in litigation by those involved.

- ***Security breaches of Technical Information Systems***

It was recommended in the previous NIE that the state should improve the management and coordination of its ICT resources as well as protective strategies and systems. It was stated that the lack of uniform policies, ICT systems and common platforms creates vulnerabilities. When assessing the current status of ICT security in government, it remains evident that the situation has not improved significantly since then.

The improper control over and/or use of laptop computers in particular continue to pose a threat to information security. Numerous investigations have been conducted on the theft/loss of these computers, which in most instances occurred as a result of negligence. In many instances such laptop computers contained official documentation and were not password protected. The majority of these cases proved that it remains to be difficult to prosecute officials found guilty and that at most, such individuals are being charged with internal disciplinary action. The inadequate control over such computers therefore remains a concern.



The outcome of NIA investigations in the past year signalled a disconcerting trend of breaches in the security integrity of ICTS. The following serve as illustration:

- **The former Department of Foreign Affairs (DFA).** Since 2006 NIA has been involved in investigating, under operation Phantom, a series of incidents at the then DFA, involving a scam (involving unauthorised access to and fraudulent usage of ICT systems) to register ghost workers on the DFA system, whereby the state was defrauded of millions of rand. Since then, numerous similar cases have been reported, including the latest at the Department of Health, which is currently being investigated.
- **Gauteng Shared Services Centre (GSSC).** In June 2009 a security breach occurred at the GSSC with the intention to defraud of GSSC. Fifteen individuals intended to defraud the GSSC. Of these fifteen, five were GSSC employees – two of whom were part of the GSSC Technology Support Services SAP Unit. The plot entailed the unobtrusive, remote accessing of the Basic Accounting System (BAS). This system processes all payments in the Gauteng Province as part of GSSC's core function of providing government internal support to Audit-, Human Resource-, Procurement-, Finance- and Technology Support Services.
- **Department of Public Enterprises (DPE) in April 2009.** In April 2009, a forensic analysis conducted by NIA on a laptop of a DPE official revealed the presence of eight malicious software applications downloaded which constituted a threat not only to optimal functioning of DPE's ICTS and its business processes but also to the Intellectual Property (IP) residing in the department as it related to parastatals, eg ESKOM, Denel, South African Airways and Transnet.
- **Department of Sport and Recreation.** An employee of the DSR attempted to fraudulently transfer R13 million from the DSR to his personal bank account. The system's time-delay default prevented the transmission of the full amount, resulting in only R955 000 successfully transferred.
- **Companies and Intellectual Property Registration Office (CIPRO).** A two-year investigation, jointly by the Receiver of Revenue and the South African Police Service, into the activities of the Companies and Intellectual Property Registration Office (CIPRO) has revealed widespread corruption in CIPRO. The latest incident involves the fraudulent utilisation of CIPRO's website by unidentified syndicates, assisted by CIPRO employees, who set up and/or registering duplicate or counterfeit companies. In some instances, directors of companies are



fraudulently replaced by individuals using stolen identities. The duplicate companies or fake directors are then used to re-route money intended for the legitimate company by informing clients that bank details have been changed and advise them to send payments to the new account.

In this regard 114 duplicate companies, including duplicates of Nampak Tissue, Avusa Media, Adcock Ingram Housecare and BJ Engineering, have been set up using the CIPRO website. The investigation so far revealed that, over the past two years, corrupt officials at CIPRO have facilitated hundreds of scams which have impacted on revenue income of government, a number of prominent companies, and hundreds of smaller private businesses.

It was carried in the media on 28 October 2009 that the Head of CIPRO, Michael Twum Darko (a foreigner) does not have a security clearance. A request for a security clearance was submitted to NIA in January 2009.

- **Civil Aviation Authority.** The recent (August 2009) theft of pilot examination papers at the Civil Aviation Authority, through obtaining electronic (unauthorised) access, is a further example of the risk associated with ICT fraud/corruption.

In addition to the investigations conducted, further trends established include the following:

- **Intrusive Software Agents** (programmes/applications) as both the vital instrumentality in, and key indicator of, ICTS breaches. Software agents facilitate unauthorised, unobtrusive and remote access to network data, user profiles and passwords. Such access in turn provides a platform for data manipulation (eg fraudulent funds transfers) and the disruption of ICTS. The high prevalence of such software agents was illustrated by the result of a sampled audit at former DFA. All Personal Computers (PCs) sampled were found to contain spyware and remote access software. Similar software was also identified as part of the investigation at DPE.
- The verified and/ or suspected role of '**insiders**' in the breaching of ICTS security integrity at COMSEC and the GSSC serve as examples.
- The involvement of **organised crime** as in some cases criminal syndicates were directly implicated, while in others they were more indirectly instrumental in providing and 'planting' malicious software agents.



- A general tendency of insecure intra-organisational ICTS links to the **Internet**, thus increasing the risk of contamination with intrusive software agents.
- Low level of ICTS security awareness and insufficient adherence to applicable **standards and procedures**.

The NIA investigations cited were prompted by the breaches of ICTS' security integrity for criminal purposes. The deficiencies identified in the course of these investigations raise information security concerns wider than the criminal exploitation thereof for financial gain. These broader concerns should be seen within the context of the twofold interconnectivity of ICTS. Firstly, and similar to most (if not all) other states, the ICTS of government departments and parastatals are part of an interlinked network. The latter in turn is interlinked with the national infrastructural functioning. Secondly, the national ICTS are, to varying degrees, interconnected with the global cyber sphere. Consequently, national and other ICTS could serve as a conduit for espionage, fraud, corruption and related criminal activities and malicious infrastructural disruption.

COMSEC introduced a number of initiatives to address the risks associated with ICT security including the Computer Security Incidence Response Team through which security breaches could be reported electronically. COMSEC also distributed a security needs analysis questionnaire but it has been noted that the response from client institutions are poor.

### 3. CONCLUSION

It is clear that there are many challenges in improving security in government departments and other client institutions. There remains a need to revisit and evaluate security in prioritised strategic government institutions. One of the initiatives to remedy the situation is the envisaged replacement of the MISS with the National Information Security Regulations (NISR), a crucial development in terms of improving security in the government. The NISR is underpinned by a proper legislative foundation, in terms of the Protection of Information Act, and is intended to address specific deficiencies in the MISS. The NISR will make security measures legally enforceable and set uniform standards to ensure consistency in the government's approach to security matters.

The Protective Security Functional Committee (PSFC) of the CICC recently held a workshop where the mentioned risks and trends have been discussed. All role players agreed to further unpack the aforementioned during the next two meetings of the PSFC meeting. Specific recommendations as to mitigate the risks have also been presented in the annual Departmental Intelligence Estimate.