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?

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

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

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 and 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

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 cheek, 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

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 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.[1] 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?"[2] 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.

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

[2] "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.[3] 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 places 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 and 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.

[redacted]

2009-12-02