UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

OPEN-SOURCE ENVIRONMENTAL SCANNING AND RISK ASSESSMENT IN THE STATUTORY COUNTERESPIONAGE MILIEU

Petrus Carolus Duvenage

Student number	27544614
Study Leader	Prof. M Hough
Programme	DPhil (Political Science)
Document Status	Endorsed (UPeTD dd 2011/02/15)
© 2011 Duvenage	

OPEN SOURCE ENVIRONMENTAL SCANNING AND RISK ASSESSMENT IN THE STATUTORY COUNTERESPIONAGE MILIEU

by

PETRUS CAROLUS DUVENAGE

Thesis submitted in partial fulfilment of the requirements for the degree of

DOCTOR PHILOSOPHIAE (POLITICAL SCIENCE)

in the

DEPARTMENT OF POLITICAL SCIENCES

UNIVERSITY OF PRETORIA

FACULTY OF HUMANITIES

SUPERVISOR: PROF. M. HOUGH

NOVEMBER 2010

ACKNOWLEDGEMENTS

This thesis is, above all, in memory of my late father and mother, Sarel and Jossie Duvenage. They shared the initial stages of the research with parental pride, but passed away in short succession before its completion. Their selfless (*selfopofferende*) love; the *ethos* of inquisitiveness and compassionate respect, all in which we were raised; as well as their personal sacrifices and material provision afforded us (their children and grandchildren) immeasurable opportunities.

I would furthermore like to express my sincere appreciation to the following:

- My sons, Werner and Francois, for their sacrifices and bearing with a preoccupied dad in the study. I am indebted to them for forfeiting quality father-and-son time, taking over dad's chores, tolerating inevitable glitches in the running of the household and, quite significant from a fast-growing teenager's perspective, stomaching the monotonous quick-recipe-dinner menus. This thesis is dedicated to them.
- The Duvenage 'clan' (brothers, sisters and their families) for their encouragement and understanding of the precedence the study took over numerous precious gatherings.
- My employer, the Ministry for State Security, for affording me the unique opportunity to conduct this study. Without the institutional and individual support I received from top management, the study would have remained an unrealised goal. The relevant (current as well as former) members of the Ministry and executive management will be thanked in person for what, career-wise, was simultaneously a most empowering and humbling experience.
- In what is decidedly more than a customary remark, my study leader, Professor Mike Hough, from the University of Pretoria, for his professional guidance. It was a privilege for me as a practitioner – with academic acumen blunted through decades in the 'field' – to conduct the study under the guidance of a widely respected academic at the peak of his career.
- Karen, Madeleine and Gus for their continual encouragement, support and immense effort in the editing of various drafts.
- Willie, the two Jacos, Hermien, Ria, Sarie, Zondiwe, Ida, Corneluis, Ronelle and Nyanisile for not only their assistance, but also their interest in the study. Each of them contributed in a unique way to the completion of the thesis and will be thanked accordingly.

- My friends, several of which are also colleagues, for their continued support and understanding – despite the many invitations to get-togethers I had to decline. To my present and former colleagues in the ‘field’: *Ars contra artem*.

TABLE OF CONTENTS

CHAPTER ONE

INTRODUCTION

CHAPTER TWO

A CONCEPTUAL AND THEORETICAL FRAMEWORK: NATIONAL SECURITY, INTELLIGENCE AND COUNTERINTELLIGENCE

CHAPTER THREE

INTERNATIONAL SECURITY, INTELLIGENCE AND COUNTERINTELLIGENCE IN THE 21ST CENTURY AS THE FOCUS OF COUNTERESPIONAGE ENVIRONMENTAL SCANNING

CHAPTER FOUR

REQUIREMENTS PERTAINING TO AN OPEN-SOURCE RISK IDENTIFICATION AND ASSESSMENT FRAMEWORK WITHIN THE STATUTORY COUNTERESPIONAGE MILIEU

CHAPTER FIVE

STATUTORY INTELLIGENCE PROCESSES AS THE FUNCTIONAL CONTEXT FOR OPEN-SOURCE, COUNTERESPIONAGE ENVIRONMENTAL SCANNING

CHAPTER SIX

AN INTEGRATED PROCESS FOR OPEN-SOURCE, COUNTERESPIONAGE ENVIRONMENTAL SCANNING AND RISK ASSESSMENT: METHODICAL APPROACH, DESIGN AND THE DEMARCATION OF THE REFERENT OBJECTS

CHAPTER SEVEN

AN INTEGRATED PROCESS FOR OPEN-SOURCE, COUNTERESPIONAGE ENVIRONMENTAL SCANNING AND RISK ASSESSMENT: ESPIONAGE ADVERSARIES, OWN STATE VULNERABILITIES AND COUNTERESPIONAGE ASSESSMENT

CHAPTER EIGHT

EVALUATION

LIST OF FIGURES

CHAPTER TWO

CHAPTER THREE

CHAPTER FOUR

CHAPTER FIVE

CHAPTER SIX

CHAPTER SEVEN

CHAPTER ONE

INTRODUCTION

1. RESEARCH THEME

This study was conducted within the context of the challenge posed to statutory intelligence services internationally to meet the demands of governments for the delivery of high quality, unique intelligence in an accelerating globalising world that rides on the crest of exponential growth in both the availability of information and information technology. On the one hand, the information overload and the globalisation-driven diffusion of threats against the transmuting nation state, emphasise the pivotal role of intelligence services in the prosperity and stability of countries. On the other hand, the information age has eroded statutory intelligence services' predominance in the provision of information required by governments. The centrality intelligence services afford to the analysis function is proving to be a critical factor in meeting the expectations of their sponsor governments. It is currently accepted that analysis and excellence in the delivery of valuable intelligence, also presuppose effective utilisation of overt information. Despite this realisation and attempts, especially since the 1980s, to adapt to the changing environment organisationally, statutory intelligence services have "slipped behind the sharply rising curve of modern information management" (Johnson, 1996: 657). Consequently, the quest is intensifying for theoretical and conceptual frameworks that not only delineate the analysis process, but also enable the focused scanning, synthesising and assessing of overt information relevant to national security.

Surprisingly, academic discourse on the efficient utilisation of overt information is predominantly restricted to the field of positive intelligence. The use of overt information for purposes of counterintelligence, and even more so for counterespionage, is treated with scant attention. This can in part be ascribed to perceptions of counterespionage being a secretive function almost exclusively reliant on (classified) information derived from sources such as human intelligence (HUMINT) and technical intelligence (TECHINT) collection, or sources that are otherwise deemed to be of sensitive origin and content (such as information exchanged between intelligence services). As will subsequently be elaborated upon, such perceptions have as consequence a myopic approach that divests statutory counterespionage of significant advantages to be gained from effectively scanning and utilising overt information.

2. LITERATURE OVERVIEW

The concepts 'environmental scanning' and 'risk', with denotations applicable to this study, emerged during the 1960s within the Business Management discipline. Subsequently, they gained wide application in a variety of other disciplines and fields that included Political Science, Information Management and Future Studies. General works found useful for purposes of the study were for instance those authored by Choo (1998, 2001), Knip (2003), Lapstra & Knip (2005), as well as Daft & Weick (1984). These authors explored two interrelated themes of importance. Firstly, the modes of environmental scanning an organisation would employ were in relation to its perceptions of the environment. An example of relevance to the research theme is the assertion of a causal relationship between an organisation's perceptions regarding the hostility of its environment, and the intensity of scanning it would employ. Secondly, perspectives pertaining to the structuring, process and methods of effective environmental scanning were informative to the design of a framework suitable to the counterespionage domain.

It is also within the Business Management sphere that Competitive Business Intelligence (CBI) has since the 1980s crystallised as a specialisation field with a strong multi-disciplinary character. In addition to its contribution to environmental scanning and risk assessment, applications in certain categories within Competitive Business Intelligence (such as Market Intelligence, Partner Intelligence, Competitor Intelligence and Defensive Competitive Intelligence) proved useful in expounding on the relationship between a government and its espionage adversaries. Relevant sources in this regard included those of Fleisher & Bensoussan (2003), Fleisher & Blenkhorn (2003), Nolan (1997) as well as Brouard (2004). Fleisher & Bensoussan (2003) provide a comprehensive contemporary exploration of Competitive Business Intelligence practice. A compilation of views on controversies within Competitive Business Intelligence, under the editorship of Fleisher & Blenkhorn (2003), afforded perspectives pertinent to the evaluation of concepts and practices useful for adaptation to the statutory environment. Works by Nolan (1997) and Brouard (2004) explore the conceptual structuring of corporate counterintelligence and the integration of the latter with positive business intelligence. These works were instructive in this study's propositions on the statutory counterintelligence and counterespionage processes as well as the process of open-source, counterespionage environmental scanning.

Environmental scanning and risk assessment, although not necessarily phrased as such, have over decades been an integral part of, *inter alia*, disciplines that concerned themselves with the study of national security. The most comprehensive South African academic work in this field was authored by Bernhardt (2003). While this study contests certain assertions in Bernhardt's thesis, aspects thereof are regarded as fundamental to, and are espoused in the design of a counterespionage framework. Bernhardt's study, however, focuses on domestic (positive) intelligence and does not purport to address environmental scanning in the counterintelligence domain and therefore the counterespionage sphere.

A substantial volume of literature exists on espionage and counterespionage relating to national and international security. Although this literature is selectively reviewed from a conceptual and theoretical perspective in Chapter Two, some introductory remarks are necessary.

On a theoretical level, ample literature has been produced on the inter-related themes of international and national security, international relations and statutory intelligence. Works of note include: Buzan (1991), Buzan, Wæver & De Wilde (1998), Lowenthal (2003), Booth (1991), Hough (2003), Buzan & Wæver (2005), Snow (2004), Gill & Phythian (2006), and Sterling-Folker (2006). Literature dealing with statutory counterintelligence and counterespionage predominantly focuses on the manifestation of espionage ('spy cases') and/or concentrates on one or more statutory intelligence services. Notable exceptions that address counterintelligence more holistically, and to which the study frequently refers are works by Wettering (2000), Godson (2001) and Taylor (2007).

A growing body of literature exists on the use of overt information in statutory intelligence or, as it is referred to in short, open-source intelligence (OSINT). Some works on this theme cited in the study include Burke (2007), Steele (2007), a report compiled on OSINT for the United States of America's (US) Congress (US, 2007*e*), the *Open source intelligence: interim field manual* of the US Department of Defense (2006*b*), Mercardo (2005), Clift (2003), Jardines (2002) and the North Atlantic Treaty Organisation's (NATO, 2001) *Open source intelligence handbook*. Literature with regard to the use of overt information in the statutory counterespionage sphere is, however, markedly more limited. The scant attention afforded to this topic can firstly be ascribed to, as identified by Godson (2001: 203), a perception that counterintelligence stands to derive limited benefit from overt sources. Secondly, in comparison to other specialisation fields, analysis is assigned a much more restricted role in counterintelligence. Counterintelligence analysis is projected as a nearly subservient, tactical support to the array of secret operational activities within the counterintelligence field such as secret collection and defensive/offensive measures. Shulsky & Schmitt (2002: 126-127), for example, devote a section to counterintelligence analysis, but restrict a ‘’special counterintelligence office’’ to perform its ‘’overall task’’ through serving as ‘‘an institutional memory’’ and analysing ‘‘connections’’ between counterintelligence ‘‘cases’’. As overt environmental scanning largely forms part of the analysis function, the assigning to analysis of a narrow tactical role would inevitably be at the expense of such scanning.

Although not termed ‘overt counterespionage environmental scanning’, the importance of this notion, in a sense wider than merely supporting secret (counterintelligence) operational activities, is recognised by authors such as Godson (2001: 203-211) and Steele (2007: 109-111). The latter draws the distinction between ‘‘tactical counterintelligence’’, aimed at the penetration of specific targets, and ‘‘strategic counterintelligence’’, focused on scanning for ‘‘emerging threats’’. It is on the strategic level, Steele (2007: 109) asserts, where “OSINT should, but does not shine”. While agreeing on the critical importance of the role of overt information on a strategic level, Godson also points to definite advantages to be derived at a tactical level. Neither Godson nor Steele, however, deliberates on a framework for overt environmental scanning in the counterintelligence field.

As far as could be ascertained, a study presenting a coherent framework for open-source environmental scanning and risk assessment within the statutory, counterespionage domain has not previously been undertaken. Consequently, it is postulated that the thesis is relevant to the indicated quest by statutory intelligence services for frameworks to delineate the analysis process as well as to address voids in the research field.

3. RESEARCH OBJECTIVES

The research posed as its primary objective to design, contextualise and elucidate a conceptual, qualitative framework for open-source environmental scanning within the statutory counterespionage milieu, specifically relating to the civilian counterintelligence sphere. The conceptual framework is presented as the principal instrument by means of which environmental scanning is executed. Therefore it is advanced as part of a broader process which includes the framework’s design and the planning of scanning activities. It is contended that the study will contribute to the academic discourse on a subject largely yet unexplored.

The stated primary objective was concretised in the following sub-objectives:

- To propose a systematic conceptualisation incorporating the two key dimensions of environmental scanning namely, the 'looking for' (that is procurement of) and the 'looking at' (that is assessment of) information. Given the complexity of scanning associated with the increasing volume of overt information, the study endeavoured to construct a premise that can serve to direct the environmental scanning process to those areas of the highest counterespionage concern. The research further aimed to provide a theoretical foundation enabling the following:
  - Identification of espionage risks to national security, on a strategic as well as tactical level, not necessarily detectable through the assessment of classified information;
  - description of these risks in respect of aspects such as espionage role players (adversarial to the state), areas towards which espionage activities are likely to be directed, as well as the expected nature of adversarial espionage activities;
  - prioritisation and categorisation of identified risks; and
  - the structuring of the outcome of the environmental scanning process in accordance with demands particular to the statutory counterespionage domain.
- To construct a counterintelligence cycle, germane to requirements that the counterespionage discipline poses, and to contextualise the environmental scanning framework as part of this cycle.
- To elucidate the study's theoretical dimensions, through an eclectic examination of the manifestation of 21st century espionage threats and those confronting the national state, as well as the practice of statutory counterintelligence.

4. IDENTIFICATION AND DEMARCATION OF THE RESEARCH PROBLEM

4.1 PROBLEM STATEMENT

At its core espionage is deceptive, secretive and designed to avoid detection. Similarly, counterespionage has an intrinsic element of secretive countermeasures and classified information. An over-reliance on classified information, however, is likely to degenerate into institutional atrophy when it comes to the identification and countering of the espionage threat. The self-feeding cycle of prioritisation and collection endemic to statutory counterespionage is a case in point. A practical illustration is where classified information on the activities of foreign intelligence service X exists and the latter is prioritised for counterespionage collection. In most instances, the collection produces more information on service X, leading to the continued or higher prioritisation of this service. Since resources are limited, this self-feeding cycle results in the operational and analysis effort, as well as other resources, being converged to certain areas while the espionage risks posed by other espionage adversaries go undetected. Counterespionage is, in other words, rigidly directed to areas that are not necessarily of the highest counterintelligence and notably counterespionage priorities.

Against this background the first dimension of the central research problem was to determine to what extent, and in which manner, scanning of overt information would benefit the statutory counterespionage function, specifically insofar as the identification, description and prioritisation of undetected risks were concerned. While the expansion in overt information at the avail of an intelligence service presents the opportunity for enhancing the execution of the counterespionage function, its sheer volume poses a near overwhelming challenge. In remarking on the information overload which intelligence assessment agencies are struggling to overcome, Dupont (2003: 15, 22, 29) rightly points out that this overload threatens gains from the "technical improvements in intelligence collection and dissemination", and may in future be at the root of major intelligence failures. This challenge embodied the second dimension of the central research problem that has a bearing on the two main composites of environmental scanning, namely, what information should be 'looked for' and how the information should be 'looked at' to be of value?

Flowing from the two-pronged research problem, the following salient and inter-related research questions arose:

- Considering the voluminous extent of overt information, how could environmental scanning be methodically focused and structured?
- Given the contemporary views, as well as the current manifestations and expected developments regarding national security in general and counterespionage in particular, with which requirements should such a framework comply?
- Since the concept 'risk' profoundly influences both the 'looking for' and the 'looking at' of information:

  - What definition could be assigned to an espionage *risk* and in what respect is a *risk* distinguishable from a *threat*? Do current notions of 'threat' and 'risk' provide a definition that could be feasibly employed within an overt counterespionage environmental scanning framework or are specifically tailored conceptualisations required?
  - How could overt information be assessed to 'reveal' espionage risks and what would construe the principal indicator(s) thereof?
- Since multiple risks would emerge, what criteria could be employed to categorise and prioritise risks?
- Would such a counterespionage framework be in synergy with existing conceptualisations of the intelligence process and, if not, what modification or alternative could be postulated?
- How could the outcome of counterespionage overt scanning be structured to be of optimal utility in the counterintelligence cycle?

4.2 ASSUMPTIONS

The study has as its central assumption that environmental scanning and the contextual analysis of overt information enable the identification, description and prioritisation of espionage risks that would not necessarily have emerged through statutory counterespionage processes that rely on classified information. While complementary to the latter, the environmental scanning framework was presumed to offer a theoretical foundation to surmount an over-reliance on classified information and to enrich the counterespionage process on a tactical as well as strategic level.

This assertion was based on the following underlying assumptions which were explored in the research:

(1) A methodically demarcated referent premise enables the focusing and structuring of the counterespionage environmental scanning process amid the exponential proliferation of overt information.

The referent premise was postulated to rest on two pillars. Firstly, the convergence between a sponsor government's objectives and the legislative counterespionage mandate of a particular intelligence service demarcates and prioritises the spectrum ('terrain') of overt information to be scanned and assessed. Secondly, the aim of the environmental scanning (namely the identification, assessment and prioritisation of espionage risks) constitutes the specific focal points of scanning within the demarcated terrain.

(2) Effective environmental scanning of overt information for counterespionage necessitates a distinctive definition of 'risk' and 'threat', as these are interlinked yet different concepts. It is therefore asserted that current notions of 'threat' and 'risk' are inadequate for feasible employment within an overt counterespionage environmental scanning framework.

An espionage risk was postulated as a plausibility statement of a situation, resulting from the activities of an opposing intelligence entity, which exists or may develop in a manner impeding a sponsor government optimally in pursuing its strategy and realising its objectives. This is distinguishable from an espionage threat which is a probabilistic statement (with a high degree of certainty) regarding such a situation. It was thus contended that a risk is distinguishable from a threat primarily on the basis of the inherent quality of uncertainty.

(3) A framework for overt counterespionage environmental scanning has as its primary requirement the ability to identify diverse risks, descriptively and predicatively, on a strategic as well as a tactical level.

It is required of the framework to detect the espionage risks posed by diverse adversarial role-players which are in competition or conflict with the interests of a particular nation state. Whereas the description of espionage risks posed by current activities of adversaries is of self-evident importance, it is not sufficient. It is also demanded of the framework to alert on future developments that could have counterespionage implications.

(4) The degree of adversity in the relationship between a government and an adversary constitutes the principal indicator and determinant of an espionage risk.

The stratification of the adversity in three tiers (cooperation, competition and conflict) was presumed not only to serve as a barometer for the presence of espionage risks, but also inform the description and categorisation of such risks. Cooperation between a government and an opponent on a specific issue denotes a limited espionage risk, with the opposite applying should there be intense conflict. A consequential assumption was that in instances of intense conflict an opponent will resort almost exclusively to target-specific clandestine espionage activities, while cooperation will be accompanied by low-risk overt information gathering. The employment of this stratification thus 'uncovers' espionage risks through the assessment of overt information and is also central to the categorisation and prioritisation of risks.

(5) The logical accommodation of a framework for overt counterespionage environmental scanning necessitates a distinctive counterintelligence cycle, as existing conceptualisations of the intelligence cycle are inadequate. In addition to collection and analysis, the counterintelligence cycle incorporates both defensive and offensive dimensions (of counterintelligence).

4.3 DEMARCATION

Employing the distinction made between risks and threats, the study addressed the identification and assessment of 'risks' and not 'threats'. Classified information, in stating the obvious, is a defining characteristic of statutory intelligence practice. A precondition to authorisation for the study was that the thesis should not in any manner compromise secret information or insights directly derived from classified information. Although the research centred on the design of an open-source based process and framework, this precondition presented a challenge. Whether based on open or secret sources, statutory counterespionage takes as a premise assumptions on a nation state's national security context and its secrets. In meeting this challenge, the study employed the construct of a hypothetical 'own state'. While mostly applied in respect of espionage adversaries, hypothetical nation states have been used in counterespionage literature for decades (Kent, 1949, 1966: 40-61; US 2007*b*: 42-47; US 2007*i:* 1-7). For illustration purposes, this study posited the People's Republic of China (PRC) as one of the own state's primary espionage adversaries. Such elucidations by means of examples should not be construed as purporting to present a case study. A credible case study would have required specialised knowledge and extensive research of several nation states, non-state actors and societal sectors. A case study of such magnitude was not realistically achievable within the confines of an exploratory study.

In accordance with the noted precondition, the thesis is thus generic in its approach regarding the conceptualisation and design of the environmental scanning process. The research should not be seen as being informed by, or geared towards a particular statutory intelligence structure. In extending the generic approach, the research was conducted at a micro-theoretical and not at a praxis level. The thesis did not purport to advance a 'practical manual', but was posed as a methodological ‘skeleton’ around which the praxis of open-source CE environmental scanning and risk assessment can be refined.

5. METHODOLOGY AND SOURCES

Both description and analysis were used in the research which is primarily of a qualitative nature. In its positivistic aim of developing a framework that enables the identification and description of ‘real’ espionage risks, the study is located within the realist paradigm. Posited as the primary referent object of analysis, the state is seen as rationally pursuing its primary objectives of survival, sovereignty as well as the protection and expansion of its vital interests. It strives to achieve these objectives through exerting its relative power in an environment of anarchy and insecurity where other entities covetously pursue their own interests.

In this context, national security is defined as a condition favourable to the state realising its objectives of survival, sovereignty and prosperity (in other words the promotion of its vital interests). However, national security is not viewed as having military matters as a single determinant. The state, and thus intelligence services, can also be directed to security concerns arising from the economic, social and environmental spheres. Likewise, the general wellbeing and prosperity of the individual falls within the mandate of the state and are relevant to security. As rightly pointed out by Snow (2004: 157-159) such a broadening of the concept ‘national security’ is not necessarily incongruent with a realist/traditional approach. The broader concept of national security and associated concepts, such as risk and threat perception, as well as strategic intelligence and counterintelligence, therefore form the basis of the theoretical approach to the study.

The framework for overt counterespionage scanning is embedded in the theoretical premise that the state’s survival and prosperity rely on its ability to sufficiently ‘sense’ its environment (Taylor, 2007: 3). The execution of such ‘sensing’ is posed as the core function of statutory intelligence. In substantiation, and for the purpose of further delineating the theoretical approach to the study, the highlighting of four defining aspects of the concept ‘statutory intelligence’ is required. Statutory intelligence is deemed to denote firstly the range of activities performed by an organ(s) of government in relation to the collection and analysis of information on the environment with the aim of informing the state on threats and risks as well as opportunities with a bearing on national security and strategy. To this end, and as was noted previously, information on the environment is gathered principally in two complementary ways; through environmental scanning that employs overt information available in the public domain and through “more aggressive techniques penetrating the secrecy and privacy of others” (Gill & Phythian, 2006: 31). ’Aggressive techniques’ include espionage, which is commonly typified as encompassing the use of secret human sources.

Whatever method used, information procured is subjected to analysis. In essence, intelligence analysis involves the transformation of collected information into descriptions, explanations, assessments, predictions and conclusions. The definition of ‘statutory intelligence’ is, secondly, commonly deemed also to subsume the meaning of ‘intelligence’ as ‘analysed information’.

From the theoretical supposition that a state’s adversaries will as part of their competitive pursuit endeavour to procure classified intelligence, statutory intelligence is thirdly defined as having counterintelligence as a key composite. Counterintelligence, the study asserts, is essentially centred on safeguarding and ensuring the integrity of statutory intelligence on different levels. On the one hand, this involves the physical integrity of intelligence that pertains to preventing the compromising of intelligence to adversaries of the state. On the other hand, it also encompasses the inherent integrity of intelligence that entails ensuring such intelligence is ‘true’ and not distorted by adversarial deception and disinformation. In the latter sense counterintelligence, in certain respects, also subsumes the safeguarding of the state against covert action (which entails adversarial activities designed to secretly influence developments in the targeted state). Conversely, the state can reciprocally or proactively direct an array of covert actions against its opponents. For the purpose of this study, the informational aspects of covert action are considered as embodying the fourth defining element of statutory intelligence.

As reflected in the delineation of its constitutive elements, statutory intelligence therefore has a critical role in enabling the state to pursue its objectives and thus national security. Deemed as the ‘informational’ category of state power, this role is multifaceted (Snow, 2004: 58-59). In its connotation as ‘positive intelligence’, statutory intelligence acts as an ‘environmental sensor’ that provides knowledge and foreknowledge on existential risks and threats to national security. In providing such knowledge, statutory intelligence serves as a magnifier of other instruments of power in the political, economic and military spheres simultaneously. In its counterintelligence dimension, statutory intelligence is charged with not only bolstering national security through the safeguarding of vital secret information, but also through the disruption of the 'informational power' of adversaries.

This multifaceted purpose of statutory intelligence is poignantly epitomised in the execution of the counterintelligence function. Although counterintelligence denotes the defensive part of statutory intelligence, it relies in its execution on protective (personnel and information security measures) as well as offensive (counterespionage) actions. Complementary to a spectrum of neutralisation ('countering') actions that include disinformation and deception, counterespionage also entails the scrutiny of the environment from the perspective of a specific category of risks and threats, namely those with a bearing on the espionage activities of adversaries. In this instance the scrutiny of the environment is also executed through the complementary collection methods of overt scanning and target-specific, intrusive techniques of a secret nature. The significance of the symbiotic relationship in counterintelligence between collection and analysis as well as the increasing importance of overt environmental scanning can hardly be over-emphasised. It furthermore underscores the desirability of research into the design of a framework for overt environmental scanning that examines collection ('looking for') and analysis ('looking at') within the statutory counterespionage field.

The substance of statutory intelligence analysis is predominately of a qualitative nature and the study, as was mentioned, followed such an approach. It endeavoured to provide a logical representation and description of sequential and interrelated steps to arrive at the set aims and objectives.

An extensive body of literature relevant to the focus of this study exists, both of a primary and secondary nature. In respect of primary sources, the study was informed exclusively by publicly available documentation. While some use was made of official documentation of other countries, the abundant literature available and originating from the United States (US) proved particularly useful. Examples of such official publications by the US government are the following: *Report to Congress of the U.S.-China economic and security review commission* (US, 2009*e*), *Adjudicative desk reference - background for personnel security adjudicators, investigators and managers: counterintelligence module* (US, 2007*g*), and *Technology collection trends in the U.S. defense industry* (US, 2006*c*). Secondary sources included books, journals, conference papers, publications by research institutions and Internet sites.

Sources found as particularly instructive in respect of OSINT included Burke (2007), Steele (2007), a report on OSINT to the US Congress (US, 2007*e*), Mercado (2005), Jardines (2002) and NATO's (2001) O*pen source intelligence handbook*.

In addition to Bernhardt's research (2003, 2004), sources informative to risk identification and assessment in the statutory context were the Australian Security Intelligence Organisation's "structured approach to security risk management" as described by Wing (1999: 86-94) and Quiggin's (2007) book entitled *Seeing the invisible – national security in an uncertain age.*

6. THE STRUCTURE OF THE RESEARCH

The structure of the study is as follows:

CHAPTER ONE: INTRODUCTION
Articulation of the objectives, central research question, research problem and assumptions are presented. This is contextualised by a concise overview of existing literature on the theme. Subsequently, the theoretical approach, the methodology as well as the structure of the study are outlined.
CHAPTER TWO: A CONCEPTUAL AND THEORETICAL FRAMEWORK: NATIONAL SECURITY, INTELLIGENCE AND COUNTERINTELLIGENCE
Concepts central to the study theme are defined and demarcated. These include, but are not limited to national security, statutory intelligence, counterintelligence, espionage, risks and threats, environmental scanning, research and analysis. Concurrently contemporary views on the concepts and the relationship between these concepts are examined.
CHAPTER THREE: INTERNATIONAL SECURITY, INTELLIGENCE AND COUNTERINTELLIGENCE IN THE 21st CENTURY AS THE FOCUS OF OPEN-SOURCE COUNTERESPIONAGE ENVIRONMENTAL SCANNING
The manifestation of espionage as a national security threat to the nation state as well as the effective accomplishment of the statutory counterintelligence function is analysed in this chapter. The focus is not only on competing statutory intelligence structures but also on other espionage actors. For contextual purposes, reference is also made to the manifestation of espionage that, in a strict definition, falls outside the statutory realm (for instance industrial espionage between competing companies).

CHAPTER FOUR: REQUIREMENTS PERTAINING TO AN OPEN-SOURCE RISK IDENTIFICATION AND ASSESSMENT FRAMEWORK WITHIN THE STATUTORY COUNTERESPIONAGE MILIEU

Consequential to the current and expected counterespionage challenges, the requirements to which an effective environmental scanning and risk assessment framework should ideally comply are defined. Given the theme of the study, the chapter's emphasis is on describing the characteristics of such a framework as it pertains to the utilisation of overt information. In addition to *requirements to* the CE framework, the chapter sets out *requirements posed by* the CE framework's design. The latter comprise mainly of conceptual approaches that can serve as foundational 'building blocks' for the CE framework's construction.

CHAPTER FIVE: STATUTORY INTELLIGENCE PROCESSES AS THE FUNCTIONAL CONTEXT FOR OPEN-SOURCE, COUNTERESPIONAGE ENVIRONMENTAL SCANNING

This chapter examines existing conceptualisations of the intelligence process and cycle with a view on determining their flexibility in accommodating a counterespionage environmental scanning framework. Based on the assertion that existing conceptualisations are inadequate, proposals on the all-source counterintelligence and counterespionage processes are submitted. The chapter proceeds by positioning open-source, counterespionage environmental scanning and risk assessment within the context, and as part, of the proposed (all-source counterintelligence and counterespionage) processes.

CHAPTER SIX: AN INTEGRATED PROCESS FOR OPEN-SOURCE, COUNTERESPIONAGE ENVIRONMENTAL SCANNING AND RISK ASSESSMENT: THE METHODOLOGICAL LOGIC, DESIGN AND THE DEMARCATION OF THE REFERENT OBJECTS

Building on, and incorporating the different elements of the preceding chapters, this chapter introduces the integrated process for open-source, counterespionage environmental scanning and risk assessment. To this end, the methodological logic of the CE environmental scanning process in general is advanced. Subsequently, the process's initial phases are presented in more detail. These phases deal with the process's conceptualisation, design and planning as well as the first phase in the execution of CE environmental scanning *per se*, namely the delineation of the (environmental scanning's) referent objects.

CHAPTER SEVEN: AN INTEGRATED PROCESS FOR OPEN-SOURCE, COUNTERESPIONAGE ENVIRONMENTAL SCANNING AND RISK ASSESSMENT: ESPIONAGE ADVERSARIES, OWN STATE VULNERABILITIES AND COUNTERESPIONAGE ASSESSMENT
Chapter Seven addresses subsequent phases of the CE environmental scanning process. These phases are directed towards the identification of espionage adversaries and their activities, the ascertainment of own-state vulnerabilities to espionage and the compilation of an open-source counterespionage risk assessment.
CHAPTER EIGHT: EVALUATION
This chapter consists firstly of a cursory overview of the research conducted and key findings reached in preceding chapters. Secondly, the study’s main assumptions are evaluated. The chapter concludes with general observations and suggestions for further research.
SUMMARY
KEY TERMS
BIBLIOGRAPHY

CHAPTER TWO

A CONCEPTUAL AND THEORETICAL FRAMEWORK: NATIONAL SECURITY, INTELLIGENCE AND COUNTERINTELLIGENCE

1. INTRODUCTION

This chapter develops a conceptual framework on which the study is based. From a definitional perspective, concepts covered include national security, statutory intelligence, counterintelligence, counterespionage, environmental scanning as well as risks and threats. Conceptual discourses on national security and intelligence are also examined. In addition to addressing theoretical aspects central to the study, this chapter also provides a foundation for the following dimensions which are explored in subsequent chapters:

- A reflection on the limits and uses of intelligence and the implications thereof for the framework for counterespionage, environmental scanning and risk assessment;
- a theoretical postulation on the intelligence cycle and process; and
- the design, at a micro-theoretical level, of a framework for overt counterespionage, environmental scanning and assessment.

2. CONCEPTUALISING SECURITY, NATIONAL SECURITY AND NATIONAL SECURITY THREATS

The notion of ‘national security’ constitutes the overarching concept in the theoretical approach to this study. This section reflects views on what the term national security denotes as it varies from academic perspective to academic perspective and from state to state. Whatever view taken, a government demands from its statutory intelligence community to provide intelligence and services in support of optimally pursuing its national security strategy. From a counterespionage perspective, the conceptualising of national security is of even greater significance. Effective counterespionage, and therefore also overt environmental scanning and assessment, presuppose not only a profound understanding of the national security requirements of a state but also require knowledge and understanding of the intelligence priorities and needs of an opposing intelligence service, which in turn are derived from the national security perception of the government of which it is part.

2.1 SECURITY AND NATIONAL SECURITY AS AMBIGUOUS CONCEPTS

Semantically, 'national' in the concept 'national security' acts to qualify 'security'. For this reason, and as it will enrich the subsequent deliberation on the application of 'security' in the Security and Strategic Studies realm, it is prudent to commence with an examination of the concept 'security' in its more general sense.

2.1.1 Conceptualising security

The word 'security' has its roots in the Latin phrase *sine cura* which literally translates into *absence* (*sine*) from *care* or *worry* (*cura*). Its relatively clear lexicological relationship, however, belies the complexity in conceptually and more concretely demarcating 'security'. This leads Gallie to conclude that 'security' – similar to 'power', 'justice' and 'love' - is "essentiality contested" as a concept (Buzan, 1991: 7). These concepts, in the words of Little, "contain an ideological element which renders empirical evidence irrelevant as a means of resolving the dispute" (Buzan, 1991:7). Furthermore, Manunta & Manunta (2006: 629-631) found the differences in approaches, scopes and goals in the use of this term in various industries and disciplines so wide-ranging that the formulation of a generally accepted definition of 'security' would be "impractical".

As noted by De Vos (2006*a*: 32-33), a definition can also be enumerative. In contrast to a denotative definition, an enumerative definition describes the attributes of a concept and in this manner "conveys an 'idea' of the thing defined" (De Vos (2006*a*: 33). While not in any way universally accepted, there would appear to be at least some parallels in the views of certain authors on the essential nature and characteristics of security (Manunta & Manunta, 2006: 629-632; Quiggin, 2007: 7-11; Buzan 1991: 6-7, 18-21, 37-39; Hough, 2003: 1-12; Bernhardt, 2003: 29-33; European Commission, 2007: 15-17; Smith, 2002: 1). These include the following:

- Security signifies and includes the pursuit of a favourable condition associated with the absence of hazards, harm and threats. This favourable condition is an absolute ideal and therefore rarely, if ever, fully realisable.
- The referent object (whose security is referred to) varies from assets, individuals, societal collectives (such as business concerns and interest groups), nations, and states to regional and international collectives.
- Similarly, the security actor (the provider of security) can vary from individuals to international collectives.

- In respect of human collectives, security entails physical needs and philosophical ideas. Consequently, it is affected by subjective elements such as perception, beliefs, desires and fears. At its core security also subsumes more objective elements pertaining to physical wellbeing.
- Since measures to attain the said favourable condition are instituted by humans, these are influenced by emotional, cognitive and cultural factors. Such measures are instituted to decrease vulnerability to an endangering development, and will, in addition to the nature and extent of the vulnerability, be determined by the foreseen impact and probability of a detrimental development manifesting.
- The quest for security is not static, but a dynamic changing condition.
- Developments endangering or perceived to be endangering security as an ideal favourable condition, can emanate from various sectors such as the economic, environmental, societal, political and statutory security (inclusive of the military) spheres.

It is apparent from the preceding outline of security that the diversity of security actors and referent objects as well as possible sources of endangering occurrences present a multiplicity of variables.

2.1.2 National security as an ambiguous concept

Instead of clarifying the notion ‘security’, the addition of an equally ambiguous object, ‘national’, adds to an even further divergence in conceptualisations. Although Security and Strategic Studies was formed in the aftermath of World War II (WW II) around the concept ‘national security’, this nomenclature was essentially a misnomer (Buzan & Hansen, 2007: xvii). In the Western-orientated context of its use at inception, ‘national’ was intended to convey the idea of ‘nation state’. However, not all states include one culturally homogenous group predominantly within their geographical borders. Similarly, a collective with a shared cultural and ethnic identity can be located in more than one state. Retrospectively, ‘state security’ would have offered a more accurate phrasing of the concept that structured Security and Strategic Studies as an academic discipline.

The complex nature of this debate is further illustrated by the fact that even the ‘state’, as ostensibly a more concrete concept than ‘security’, lacks a precise, generally accepted definition (Buzan, 1991: 7, 27, 63-65; Smith, 2002: 1). Within the ambit of Security and Strategic Studies, a descriptive model forwarded by Buzan (1991: 63-65) to examine the nature of the state within the context of national security, nevertheless, serves as a useful premise. Buzan posits the notion of ‘state’ consisting of three interrelated dimensions. Firstly, he argues that the state’s population and geographical territory constitute its physical base. Secondly, the state also finds institutional expression in governmental organs such as its executive, legislative, administrative and judicial bodies. Thirdly, and on a more abstract level, the idea of the state refers to the attributes that validate its legitimacy in the collective psyche of its inhabitants and acts as the “binding ... holding the territorial-polity-society packages together” (Buzan, 1991: 64).

That states, however defined, seek to be secure and that this quest entails more than ensuring territorial sovereignty, is one of the axioms in international politics (Buzan & Hansen, 2007: xvii). Beyond this axiomatic consensus, there is sharp divergence on the nature, content and implications of this quest for international and national security (Buzan & Hansen, 2007: xvii). Despite various attempts to demarcate the concept ‘national security’, there is no definition that enjoys universal acceptance (Hough, 2003: 1). With reference to Schultze’s caution that “national security does not lend itself to neat and precise definition”, and with the qualification that he does not purport to offer a definition, Buzan (1991: 6, 16, 18) asserts that ‘security’ denotes a sense of “the freedom from threat” and, within the context of the international system, “the ability of states to maintain their independent identity and their functional integrity.”

The connotations a state affords to threats, freedom from threats and what variables will affect its identity and integrity are, however, not a constant as they vary from state to state (Hough, 2003: 1). Since states are dynamic and not fixed entities, this meaning will also differ depending on the specific time context. The internal and external environment within which states function will determine their views on national security and their interests in political, military, economic and environmental terms (Quiggin, 2007: 8-10; Buzan, 1991: 102-103). A useful distinction in this regard is the differentiation between ‘strong’ and ‘weak’ states which is further elaborated on in the next section.

In summary, arguably the only consensus within the theoretical discourse on national security is that there is no consensus on a generally accepted definition for it. Due to the divergent views, national security evades even the assigning of a consensus enumerative definition. Nevertheless, the reflection on national security does provide some contours for a broad conceptualisation of the concept. It is apparent that despite an attempt to broadly reflect on security, the connotations of the concept in relation to the state were emphasised. Within security thinking in general, the assumption of such a state-centred approach is far from uncontested.

2.2 VIEWS ON NATIONAL SECURITY

An examination of some of the main approaches to the notion of security not only serves to illustrate opposing views on a state-centred paradigm but, since it highlights various interpretations of, or relevant to national security, it further adds to conceptualise the notion.

2.2.1 Cold War views on national security

In contrast to the contemporary divergence in interpretations of national security the Cold War period was, from a Western-orientated perspective, characterised by a relatively broad-based consensus in the academic and governmental spheres on the understanding of this concept. Attesting to this, is the remark in the early 1950s by Wolfers (in Buzan & Hansen, 2007: xix): “The term national security, like national interest, is well enough established in the political discourse of international relations to designate an objective policy distinguishable from others.”

National security, articulated in politico-military terms, was seen as referring to the security of the nation state. The security of the state was further equated with the capacity to deter and effectively ward off external military threats. National security was inseparably linked to the international bipolar tension between the US and the Union of Soviet Socialist Republics (USSR). Through the lens of bipolarity aspects such as nuclear deterrence, the balance of power featured prominently in the discourse on national and international security (European Commission, 2007: 7-12). The Cold War concept of national security is illustrated by the following definitions articulated during this period. Luciani, (in Buzan, 1991: 17) succinctly declares: “[n]ational security may be defined as the ability to withstand aggression from abroad.” In a similar vein, Lippmann (in Oyebade,1998: 2) states that “[s]ecurity is about the possession by a state of a level of military capability sufficient enough to avert the danger of having to sacrifice core values, if it wishes to avoid war, and is able, if challenged, to maintain them by victory in such a war.”

The traditionalist notion of national security was overlaid on the realist approach to international relations. During the Cold War period, realism enjoyed hegemony in International and Security Studies. Realism is not a single theory and comprises theoretical strands such as classical realism, neo-realism, offensive realism and defensive realism (Lynn-Jones, 1999: 61-63). Certain foundational commonalities unify these diverse theories. As an approach, realism is in short, positivistic, state-centred and assumes the causal omnipotence of power (Sterling-Folker, 2006: 13; Lynn-Jones, 1999: 58-59). The nation state is posited as the primary referent object of security and state-level analysis is favoured (Buzan & Hansen, 2007: xvii). The nation state is viewed as pursuing the self-interested goal of its own survival and prosperity. The latter is inseparable from two concepts fundamental to the realist thought, namely power and sovereignty. Since realism accepts the notion that states are sovereign, anarchy is seen as the invariable foundation of the international system in which states are the primary security actors. The state's relative power will determine the outcome of interfacing with other actors in respect of cooperation, competition and conflict. Although 'cooperation under anarchy' occurs, such cooperation is not of an altruistic nature. It is motivated by the self-centred interests of the nation state (Lynn-Jones, 1999: 61-63). In this sense, cooperation is also overlaid upon conflict as it is temporary and only sustained for as long as it serves the state to maximise its power.

National security in the traditionalist view unambiguously referred, during the Cold War, to the "security of the state [as] defined in politico-military terms" (Buzan & Hansen, 2007: xx). The security of the state was equated with the capacity to deter and effectively ward off external military threats. Hence, military capability relative to that of other states was the ultimate measure of power (Snow, 2004: 161-165).

Although dominant, realism was not completely unchallenged during the Cold War period. In addition to Peace Researchers, the 1980s saw calls for the re-examination of the traditionalist state-centric conceptualisations of national security by scholars such as Buzan (1983) and Ullman (1983) (Buzan & Hansen, 2007: xxix-xxx).

2.2.2 Post-Cold War thinking on national security

It was, however, the demise of the Soviet threat that provided real impetus for the re-examination of the traditional state-centred notion of security (Hough, 2003: 2). Concurrently with the intensification of the discourse in the academic sphere the "disciplinary landscape" was characterised by the introduction of "more schools and labels" (Buzan & Hansen, 2007: xxxiv). In addition to realism which continued to exert a central influence, salient theoretical approaches participating in the debate included constructivism, critical theory, as well as the Copenhagen School of thought. The latter took form around the propositions of Buzan (1983, 1991) who, at least until the early 1990s, maintained a neo-realistic perspective (Smith, 2002: 2). He combined efforts with colleagues at the Copenhagen Peace Institute, notably de

Wilde ("liberal-pluralist") and Wæver, a "self-defined ... post-modern realist" (Smith, 2002:1-3; Buzan *et al*, 1998:2; Buzan & Hansen, 2007: xxv).

2.2.2.1 The 'widening' and 'deepening' of the security agenda

The post-Cold War discourse on security is essentially centred around the two dimensional expanding of the notion of security, phrased by Krause & Williams (1996) as the "widening" and "deepening" of the security agenda (Smith, 2002: 4). The widening of the agenda pertains to extending the focus of security to sectors other than the military. The widening dimension thus has a direct bearing on the sources of threats to security. A foundational proposition in this regard was forwarded by Buzan, who advocated the addition of the political, economic, societal and ecological sectors. Buzan (1991: 19-20) emphasises that these sectors do not function in isolation. Each sector defines a focal point within the security problem, which is interwoven in a web of linkages to other sectors. Subsequently, scholars from various theoretical perspectives argued for the security agenda to include a wide variety of non-traditional concerns as diverse as food and water security, unregulated mass population movement, the diffusion of contagious diseases, environmental degradation, drug-trafficking and other forms of organised crime.

As was noted, the debate on the extension of the concept of security also has as a dimension the 'deepening' of the agenda. This deepening dimension pertains to whether entities on levels other than the state should be considered as referent objects of security. These levels constitute a vertical spectrum that includes: global security, continental security, regional security, national security, regime security, communal security and human/individual security (Hough, 2003: 3). Increasing emphasis is placed on 'security independence' that entails the cooperation between states – on a global, continental and regional level – to address transnational security threats such as organised crime and environmental degradation. Some interpretations, notably those that pose individuals and not states as referent objects, extend security to "its widest possible sense" (Hough, 2003: 3). Such a broadening is vociferously advocated by critical theorists such as Booth and Jones. The former (in Buzan & Hansen, 2007: xxvi) proffers "individuals as the ultimate referent for security". For Booth (in Mutimer, 1999: 83), "true security" is produced by the "freeing of people" from physical constraints to their unrestricted independence. Such constraints include not only war and a threat of war, but also "poverty, poor education, political oppression and so on" (Mutimer, 1999: 83). In addition to its implication for the referent object of security, the 'deepening' of the security notion also impacts on the diversification of security actors. In contrast to Cold War views on the near monopoly of the state as the provider of security and of threats principally posed by other states, other multiple security actors (both as security providers and threats to security) are brought to the fore.

It must be emphasised that the widening and deepening of the agenda are symbiotically linked in the discourse on the expansion of the security agenda. Consequently, topical matters such as the impact of globalisation on national and international security, global warming and human security, have implications on a horizontal (widening) and vertical (deepening) level. Within the academic spheres, the necessity of an expanded security agenda enjoys relatively broad-based acceptance, also within the realist paradigm. Similarly there is relatively broad-based acknowledgment of the blurring distinction between the domestic (internal) and the external (foreign) dimensions of the security threat.

2.2.2.2 National security and national security threats

On the matrix resulting from the vertical (widening) and horizontal (deepening) of the security agenda, various theoretical approaches and scholars present an array of security concerns so wide that the state is put “at the hub of a whole universe of threats” (Buzan, 1991: 141). These threats range in spectrum from the “trivial and routine, through serious but routine, to drastic and unprecedented” Buzan (1991: 135). This prompted the emergence of an unavoidable question: which of these multiple security risks and threats can be considered as of the highest concern to the state and would require measures transcending routine governance? Phrased in realist terms: which issues can be deemed as posing significant threats to national security and what criteria can be used for categorising such threats as national security threats? The contributions of various approaches in this regard self-evidently correlate with the respective views on what the concept national security denotes.

Realists acknowledge the need for expanding the security agenda, the blurring between internal and external security threats as well as the need for global, continental and regional cooperation in addressing transnational security threats. Concern has been raised over an unbridled extension of the notion ‘national security’ as it would be impractical (Snow, 2004: 156-159). Non-traditional issues, realists maintain, can be added to the national security agenda but should not distract from the predominance of military threats.

The practicality of contributions by other approaches to prioritise the multiplicity of threats concretely to security varies considerably. Critical theorists, such as Booth, are vocal in their critique of the deficiencies of the state in enhancing human security, yet conspicuously silent in offering concrete solutions (Mutimer, 1999: 83). Similarly, the position held by constructivists is, in this respect, not particularly constructive. In the constructivist's view, concepts do not exist objectively to be academically 'revealed', but manifest as creations of human, intersubjective understanding. In general, constructivists have not addressed the notion of security to a similar degree as they have with other theoretical themes (Buzan & Hansen, 2007: xxxv). However, to extend on the widely quoted statement by Wendt: "Anarchy is what states make of it"; 'national security' would then also be "what states make of it" from a constructivist perspective (Smith, 2002: 3). It could be argued that constructivists implicitly view non-cooperation between security actors and "externalisation" as the principal threat to national security (European Commission, 2007: 32). For constructivists "externalisation" signifies, *inter alia,* security actors' lack of introspective examination and the consequent projection of a threat external to their own actions. Against this background, and since in the constructivist's view neither national security nor threat can be afforded at least some declarative content, this approach is deprived of criteria to distinguish national security threats from other security concerns concretely.

Although not endorsing the same theoretical connotations and qualifications, the Copenhagen School also views national security as "what states make of it." As was noted, and in contrast to constructivism, the Copenhagen School assigns a declarative value to security and national security. For reasons of argumentative coherence, Buzan's view is recapitulated and then elaborated upon. Security suggests a sense of "freedom from threat", while national security refers to "the ability of states to maintain their independent identity and their functional integrity" (Buzan, 1991: 6, 16, 18). National security is a subjective perception, ultimately a political choice and influenced by the nature of the state (Buzan, 1991: 132-138). The latter also determines its vulnerability to threat. In pronouncing on this and the vulnerabilities of the state, several variables need to be considered of which two are highlighted. Firstly, the degree of socio-political cohesion inherent to the state requires some scrutiny. States deemed as "strong" are seen as possessing a broad-based legitimacy among their citizenry and as having single sources of authority. Such states would tend to be more externally orientated in their pursuit of security. Conversely, domestic security issues will play a major role in states that are sociopolitically “weak”. Secondly, is the “power” of the state that entails its position relative to other states and as is determined, *inter alia*, by the extent of its physical base (population, territory, natural resources, infrastructure, economic wealth, etc.) (Buzan, 991: 102-103). Buzan (1991: 134) summarises the relationship between the power of states, the socio-political cohesion and vulnerability to threats in tabulated format as follows:

Figure 1: Vulnerabilities and types of states

		Socio-political cohesion	
		Weak	**Strong**
Power	**Weak**	**Highly vulnerable to most types of threats**	**Particularly vulnerable to military threats**
	Strong	**Particularly vulnerable to political threats**	**Relatively invulnerable to most types of threats**

Source: Buzan, 1991: 134.

In forwarding criteria to distinguish threats serious enough to constitute a threat to national security, the factors that need to be considered include specificity, proximity in time and location, probability of occurrence, consequences, and the historical context of threats (Buzan, 1991: 138-139). The Copenhagen School further proposes a hierarchical distinction between “non-politicised”, “politicised” and “securitised” issues (Buzan *et al*, 1998: 23-25). They hold that securitisation, similar to national security, is an inter-subjective, self-reflective phenomenon that could be used as justification for dealing with aspects normally resolved as part of the political procedure, and therefore propagate circumspection in assigning the label “security issue” (Buzan *et al*, 1998: 25-26, 29-31).

The contribution of the Copenhagen School has profoundly influenced the discourse on national security and has been espoused by various scholars within Security and Strategic Studies (Smith, 2002: 1-2). Of particular relevance to this study is Hough’s (2003) development of concrete criteria that could serve as yardsticks for pronouncing on whether a threat is of such a serious nature that it would warrant classification as a national security threat. Such criteria, Hough (2003: 18-19) argues, include the degree to which a threat actually or potentially:

- Impacts detrimentally on stability, sovereignty, territorial integrity and vital national values;

- manifests as widespread or localised, sporadic or continual;
- results in violence, serious conflict or the escalation of existing conflict;
- necessitates the institution of extraordinary measures;
- involves illegal or unconstitutional activities; and
- transcends borders and evokes a negative international response.

2.2.2.3 National security in the context of the Third World

Although criteria such as those outlined above have application to nation states in general, some scholars argued that the discourse on national security negated circumstances peculiar to the Third World. Even before the end of the Cold War, protagonists such as Bull (1976), Ayoob (1983), Azar & Moon (1988) and Thomas (1987) raised objections to what was viewed as the uncritical application of Western (First World) conceptualisations of national and international security to the Third World (Smith, 1999: 81; Buzan & Hansen, 2007: xxx, Bernhardt, 2003: 42-43). In this instance the debate also gained substantial momentum in the post-Cold War era (Hough, 2003, 4; Buzan & Hansen, 2007: xxx). A growing body of literature argued that the colonial legacy posed problems of security and insecurity peculiar to the Third World. The legacy of colonialism included the related aspects of arbitrary drawn state borders that divided ethno-cultural groups, weak domestic institutional capacities and poorly developed national communities (Buzan & Hansen, 2007: xxx). Extending on Buzan's notion of weak and strong states, it is contended that the Third World security dilemma is predominately centred on domestic rather than external threats (Hough, 2003: 4). The study of Third World security during the post- Cold War era also progressively extended its focus, with more attention afforded to the role played by substate state actors such as elites (Buzan & Hansen, 2007: xxx).

2.2.2.4 Official perceptions on national security

The end of the Cold War resulted in a perception, in general, by governments on the lessened probability of large-scale armed and nuclear conflict and optimistic assertions over a more secure world. In the wake of this optimism, the academic discourse centred on the 'deepening' and 'widening' of the security agenda to provide for concerns outside the traditional notion of national security and also reverberated in the governmental realm. Subsequent to, and in certain instances as a result of the dissipation of a bipolar world order, trends that were presented for inclusion as part of the expansion of the governmental security agenda gained momentum. These included, but were not limited to, the proliferation of weapons of mass destruction

(WMD), growth in organised crime, as well as an increase in the trafficking of conventional weapons. Furthermore, human security and environmental degradation have increasingly been regarded as relevant to national and international security. This is reflected in the US government's *National security for a new century* (2000*a*: 3-7), released in 2000, that views national security threats as including terrorism, drug trafficking, illicit arms trafficking and other international crimes, uncontrolled refugee migration, trafficking in human beings, as well as environmental and health threats. The so-called War of Terror (GWoT), following the attacks of 11 September 2001, has resulted in terrorism predominating the security agenda in countries such as the US and the United Kingdom (UK). Other non-military threats to national security also feature prominently on the agenda of especially First World governments. The *Annual Threat Assessment – 2008*, presented by the US Director of National Intelligence, for example, also deems food security, energy security and cyber threats as relevant to the US national security (US, 2008*a*).

The future discourse within governmental and academic spheres on international and national security will, as in the past, be fundamentally affected by the unfolding of events and trends in the international arena. At this stage it is unclear whether the GWoT will prove to be durable or whether the rise of China principally as well as the European Union (EU) could see a return of "great power politics" (Buzan & Hansen, 2007: xxxviii).

Within the academic realm, the literature since 2001, however, suggests that Security and Strategic Studies will maintain a multi-theoretical approach. Buzan & Hansen (2007: xxxviii) summarise this as follows:

> Traditionalists are still concerned about US Grand Strategy, nuclear proliferation, the RMA [revolution in military affairs], and BMD [ballistic missile defence]. The Copenhagen School continues to develop its ideas about security and regional security against the GWoT and the boundaries between domestic and international security. Poststructuralists pit their techniques against the GWoT and advocates of Human Security and CSS [Critical Security Studies] continue their criticism of state-centrism.

Regardless of the future direction of the academic discourse, national security is to remain a subjective concept varying from state to state and from time context to time context. The adage 'the only constant is change' is therefore particularly relevant to the notion of national security. The subjective values and content a state affords to national security as well as its perception of risks and threats to its security, are foundational to the direction of its security apparatus in which intelligence plays an increasingly important role. As was noted in the introduction to this section, effective counterespionage presupposes a profound understanding of both an own state's national security requirements and the intelligence priorities and requirements of an adversary. For purposes of the framework for overt environmental scanning and assessment, the variables that underlie the conceptualisation of national security as addressed in this section are of paramount importance and need to be considered in the design of the framework. Since counterespionage environmental scanning and assessment could potentially produce a near endless list of actual and potential espionage risks and threats to the state, the criteria for pronouncing a concern relevant to national security are of equal significance although part of the spectrum of risks and threats to national security, espionage risks and threats form a distinct category (of risks and threats). Asserting a concern to be an *espionage* risk or threat and assessing the counterespionage implications thereof necessitate a conceptualisation of further concepts central to the study, namely intelligence, counterintelligence and counterespionage.

3. CONCEPTUALISING INTELLIGENCE, STATUTORY INTELLIGENCE AND COUNTERINTELLIGENCE

The way in which intelligence is defined also delineates and "conditions" the approach to the subject and therefore this study (Scott & Jackson, 2006: 2; Goodman, 2006: 1). Moreover, conceptualising intelligence is both part of, and in certain respects a prerequisite for, theorisation on intelligence (Warner, 2002: 1). As a micro-theory, the study is thus positioned within the broader context of the definition and theorisation of intelligence.

This section firstly reviews contemporary conceptualisations of intelligence with reference to definitions of intelligence, its primary mission, essential facets or characteristics of intelligence, the various subdisciplines as well as the intelligence cycle. Secondly, and as foundational to a postulation towards a counterintelligence meso-theory, existing theories of intelligence are reviewed with specific emphasis on aspects of relevance to this study.

3.1 CONCEPTUALISING INTELLIGENCE

In the academic realm, definitions of intelligence vary considerably in both brevity and complexity. On the one hand, Troy (in Beer, 2006: 185) views intelligence as knowledge of actual and potential enemies. Der Derian (in Quiggin, 2007: 47) deems intelligence simply as "covert activity". Subsequent to a rather extensive examination of definitions of intelligence, Warner (2002: 9) concludes by submitting his own definition: "[i]ntelligence is secret, state activity to understand or influence foreign entities." On the other hand attempts are aimed at capturing the concept of intelligence in more extensive definitions. One of these, that incidentally exclude counterintelligence, is offered by Gill & Phythian (2006: 7):

> Intelligence is the umbrella term referring to the range of activities – from planning and information collection to analysis and dissemination – conducted in secret, and aimed at maintaining or enhancing relative security by providing forewarnings of threats and potential threats in a manner that allows for the timely implementation of preventative policies or strategies, including, where deemed desirable, covert activities.

Despite various attempts such as those provided above, doubts have been raised as to whether a precise and workable definition of intelligence exists (Quiggin 47, Warner, 2002: 1-9, Scott & Jackson, 2004: 2-4). Kahn (2001: 1), for example, states that "none of the definitions I have seen work." An examination of the debate on the definition of intelligence (Scott & Jackson, 2004: 2-7; Warner, 2002: 1-6; Beer, 2006: 185-187; Treverton *et al*, 2006: 1-3, 7-9) suggests contentious definitional criteria to pertain to the following:

- The inclusion or exclusion of covert action and other offensive and disruptive functions;
- the degree to which normative (what intelligence should be doing) and realist dimensions (what intelligence actually is doing) should be considered;
- whether intelligence is an instrument of power or only an informational guiding instrument of government;
- the emphasis that should be placed on the secrecy of intelligence in terms of both information and activities;
- whether intelligence should focus on adversaries other than only competing and hostile nation states, and
- the degree to which intelligence includes internal (domestic) security issues in addition to its external (foreign) dimension.

Given this divergence of opinion this study will not purport to offer a definition of intelligence that would enjoy unanimous acceptance. Nevertheless and although with different emphasis and qualifications, views expressed in the larger part of literature

(Beer, 2006: 197; Warner, 2002: 1-7; Quiggin, 2007: 47-49) are in the main congruent with Lowenthal's (2003: 8) "working concept" for a definition of intelligence, which reads as follows:

> Intelligence is the process by which specific types of information important to national security are requested, collected, analyzed, and provided to policymakers, the products of that process; the safeguarding of this information by counterintelligence activities; and the carrying out of operations as requested by lawful authorities.

As it will serve to further elucidate the concept of intelligence, three aspects foundational to Lowenthal's definition of intelligence warrant elaboration, namely, intelligence as a specialised statutory function; the essential facets of intelligence; and the distinct subdisciplines which constitute intelligence.

Intelligence is commonly accepted as existing because of, and for the state. Supporting the state constitutes statutory intelligence's reason for existence (Lowenthal, 2003: 2). Intelligence does so from a very pertinent perspective: a certain type of information ('intelligence') pertinent to national security. Intelligence has as its primary mission to provide information on risks and threats deemed by the nation state as relevant to national security (Bruneau & Dombroski, 2004: 8-9). In addition to its relevance to national security, intelligence is distinguishable from other categories of information in that it signifies a degree of secrecy.

This element of secrecy also extends to intelligence as organisation and process. In his pioneering work *Strategic intelligence for American foreign policy*, Kent (1949, 1966: 3, 69, 151-158) describes intelligence as "knowledge", "organization" and "activity". Contemporised by various authors (Lowenthal, 2003: 9; Johnson, 2004: 2, Shulsky & Schmitt, 2002: 159-168), the three facets identified by Kent essentially remain at the core of current descriptions. As suggested above, intelligence denotes a "specialized knowledge", indispensable to a nation state's "welfare and security" (Kent, 1966: 3). This specialised knowledge is pursued by an *organisation* of "living people" that is institutionally geared towards delivering such knowledge (Kent, 1966: 69). The organisation acquires and provides the specialised knowledge through the execution of certain *activities* such as collection and analysis (Kent, 1966: 151-158). In a more comprehensive sense, intelligence can lastly be seen as a combination of the three facets mentioned above.

In all three facets, intelligence is generally considered to be performed in four functional areas (subdisciplines), namely collection, analysis, covert action and counterintelligence (Codevilla, 1992: 4). Since all four subdisciplines have a direct bearing on the framework for overt counterespionage environmental scanning and are addressed in greater detail in subsequent parts of this study, this section will suffice with succinct conceptualisations that will be elaborated upon later.

Collection (more comprehensively addressed in Chapter Three) encompasses the procurement of information from three primary categories of sources, namely open, grey and clandestine sources. *Open-source intelligence* (OSINT) pertains to information publicly and freely available, such as newspapers, books, the internet, scientific academic journals and publications, open source high resolution imagery, radio and television broadcasts, certain governmental databases, business reports and the like (Quiggin, 2007: 161-162). Opinions on what *grey sources* comprise are divided, as indicated in Chapters Three and Four. Generally, the collection of information from grey sources is seen as pertaining to those not freely available, though not requiring the employment of clandestine methods and as a legal activity. The use of databases, privileged in the sense that payment for access is required, serves as an example (Steele, 2001: 118-119). Grey-source information, this study contends, also includes information generated by methods not necessarily illegal and clandestine but in some instances *male fide*. HUMINT pertains to procuring information directly or indirectly, resulting from interpersonal interaction, and forms by far the larger part of the third subdivision of collection, namely *clandestine collection*. The clandestine gathering of intelligence through HUMINT is commonly referred to as ‘espionage’. In addition to HUMINT, clandestine collection pertains to the use of various methods broadly clustered as TECHINT. The latter is divisible into three subcategories namely signal intelligence (SIGINT), imagery intelligence (IMINT) and measurement and signature intelligence (MASINT) (Lowenthal, 2003: 60; Bruneau & Dombroski, 2004: 9-10). The result of the whole of the collection effort is referred to as all-source information.

All-source information, however comprehensively and widely gathered, is just that - ‘information’ *and not* ‘intelligence’. Information in its raw form has limited utility value and is subjected to the second intelligence function, namely *analysis*. Analysis involves the conversion of collected information into descriptions, explanations, assessments, predictions and conclusions. The analysis product is delivered to clients in written format or verbally (Bruneau & Dombroski, 2004: 10). The clients are both external (primarily the decision-maker and government departments) and internal (for example intelligence managers and those providing direction to the collection function). The products emanating from analysis can be stratified as being either on a tactical or strategic level. Tactical intelligence is mostly descriptive, directed to the line-functional intelligence structures and focused on the immediate situation. Strategic intelligence is broader in scope, usually integrating several sources of information and has as aim to inform the external consumer (notably the policy maker) on threats and risks to national policy, objectives and strategy. As elaborated in Chapter Four, analysis products are wide-ranging in format and often contain both tactical and strategic dimensions.

Regardless of the format of the end product, the production of intelligence is generally accepted to be part of a sequentially phased intelligence cycle (Lowenthal, 2003: 41; Odom, 2003: 12-13, Quiggin, 2007: 52-53). Despite attempts to refine and elaborate on it, this cycle in current literature continues to have as its essential elements the following: direction (the client expresses a need); collection (of information using one or a combination of the methods described above); analysis; production and dissemination (distribution of the intelligence product to the client). These subsequently lead to further needs expressed by the client and the repetition of the cycle.

One of the inadequacies of the intelligence cycle is its failure to prominently accommodate the third subdiscipline of intelligence, namely counterintelligence. Counterintelligence comprises two interrelated dimensions: firstly, to defensively and offensively protect the integrity of statutory information deemed of national security interest and, secondly, to compromise the informational (intelligence) integrity of an adversary.

Counterintelligence activities, together with the fourth intelligence subdiscipline, *covert action*, are aptly described by Godson (2001) as the “trump cards” within the statutory intelligence realm. Covert action encompasses the targeting of an adversary through the influencing of events, conditions, individuals, groups or institutions to the benefit of a sponsor government in a manner not attributable to the sponsor or offering plausible deniability (Odom, 2003: 15). The influencing described can be of a wide-ranging nature and vary from paramilitary and political actions to propaganda and intelligence assistance (Godson, 2001: xxxi, 2-3). By definition, and with the *caveat* that the practice varies from state to state, only the informational aspects of covert actions are generally categorised as part of the statutory intelligence function.

3.2 THE DISCOURSE ON A THEORY OF INTELLIGENCE

A conceptual delineation of intelligence is an essential part, but not by any measure the sum of the broader theory of intelligence. In the words of Warwick (in Goodman, 2006: 2), the "definitional project" is only one of several "projects" (areas of academic enquiry) within Intelligence Studies. One of these which build on the "definitional project" is the "theory project" (Goodman, 2006: 2). What distinguishes this "project" from various others, is that it deals with a notional construct that cuts across and should ideally cohesively bind other fields of academic enquiry within Intelligence Studies, such as ethics and accountability, history, intelligence reform and organisational structuring, intelligence functions (analysis, collection, counterintelligence and covert action) as well as intelligence leadership and management (Goodman, 2006: 2; Johnson, 2007:2-9). It is required of a theory of intelligence to parsimoniously offer "explanatory power" of statutory intelligence as a social phenomenon by presenting over-arching similarities and differences in specific contexts of time and place (Treverton *et al*, 2006: 9, 10, 12). In addition to guiding academic research, a sound grand theory of intelligence is also foundational to the practice of intelligence. A good "theory of intelligence", in the view of Gill (2006: 4), is also a good "theory for intelligence [practice]". Further supporting the relationship between theory and practice is Betts' (2006: 27) assertion that "intelligence failures are a result of bad theory".

3.2.1 Relevance to the study of the discourse on a grand theory of intelligence

Despite the indicated importance of a grand theory of intelligence, the question can justly be posed: what is the relevance of examining the discourse on a grand theory of intelligence to this study? Such a reflection is both an academic imperative and a matter of utility. This thesis has at its core the design of a micro-level theory of counterespionage environmental scanning. The different levels of theories are symbiotically linked and stand in an "intimate, dynamic relationship with one another." (De Vos, 2006*a*: 38-39; De Vos, 2006*b*: 442-443).The postulation of a micro-theory, without considering the broader context of the theoretical discourse on the theory of intelligence, would therefore not only deprive the thesis of a theoretical context, but also infringe on its academic integrity. Although not used in the context of intelligence theorisation, a term used by Buzan (1991:16), namely "intellectual neatness", is nevertheless applicable. Academic "neatness" and methodological logic require thorough consideration of the discourse on the grand theory of intelligence as a prerequisite for the design of a micro-theory.

The aforementioned academic imperative is, of course, not an arbitrary inconsequentiality. It also serves a utility purpose. An examination of the discourse on the grand theory level could assist to enrich the design of the framework for counterespionage environmental scanning and assessment. Phrased differently, and by re-emphasising a previous assertion, the theory *of* intelligence (grand theory) is therefore highly relevant to the framework (for counterespionage environmental scanning) as a theory *for* intelligence.

Given the pivotal importance to both the academic and practical spheres, intelligence is, however, surprisingly deficient insofar as the development of a grand theory is concerned. In the words of Warner (2002: 1):

> In a business as old as recorded history, one would expect to find a sophisticated understanding of just what that business is, what it does, and how it works. If the business is “intelligence”, however, we search in vain. As historian Walter Laqueur warned, us, so far no one has succeeded in crafting a [generally accepted] theory of intelligence.

The absence of a universally accepted theory of intelligence does, however, not imply the absence of theorising on intelligence. A salient feature of this theorising is the pervasive influence still exerted on intelligence theorisation by the traditional (realist) view on national security shaped during the Cold War.

3.2.2 Discourse on a theory of intelligence during the Cold War

Reference to the realist approach to the theory of intelligence followed by the specific application thereof during the Cold War, is required. For reasons of brevity the realist view on statutory intelligence, that inevitably would require an encapsulation of previously stated views on national security, can be syllogistically summarised as follows (Snow, 2004: 58-59, Lynn-Jones, 1999: 49-60, Sterling-Folker, 2006: 13-17; Taylor, 2007: 3-5):

- Nation states are the dominant role players in an anarchic global environment. They are deemed as rational, sovereign and self-interested entities driven by the pursuit for survival and prosperity.
- This survival and prosperity require the protection and expansion of the vital interests of the nation state. National security constitutes a favourable condition of protection and expansion.
- In establishing and maintaining national security, as well as the pursuit of other interests, the state employs various categories of power.

- As the informational category of state power statutory intelligence has as *raison d'être* the provision of intelligence on risks and threats to national security.
- Simultaneously, statutory intelligence also involves the protection of state secrets from adversaries.

Similar to the security apparatus of the state in general, statutory intelligence defined threats to national security predominantly in military terms and as referring to opposing (foreign) nation states. From the Western perspective the threat was equated with the USSR and its allies. The most important factor shaping global affairs was deemed to be the USSR expansionism, and intelligence was geared towards the containment of this threat (Berkowitz & Goodman, 2000: 3). Although the focus of statutory intelligence during the Cold War also included political, economic, industrial and scientific dimensions, intelligence on such dimensions was ultimately translated into its implications for military power. By and large, counterintelligence and notably counterespionage were afforded a high priority on both sides of the 'iron curtain'. It was, for example, estimated that by the end of the Cold War the UK's Secret Service (better known as MI5) had allocated 50 percent of its total resources to the counterespionage function (Northcott, 2007: 458). At least insofar as the US and UK were concerned, the collection of information was progressively shaped by three factors. Firstly, the USSR and its allies were to a large extent "closed targets" and relatively difficult to penetrate through HUMINT operations (Lowenthal, 2003: 13). Secondly, technological advantages from the 1960s onwards diversified options offered by TECHINT collection (McNeil, 2004: 12). Lastly, the political and other risks associated with HUMINT collection resulted in the political leadership of, for example, the US to be antagonistic towards this collection method at times (Gilluffo *et al*, 2004: 33). Against the background of these three factors, the "remote" gathering of information, through a variety of TECHINT methods, was favoured (Lowenthal, 2003: 79). According to a 1970 estimate quoted by Gill & Phythian (2006: 63), Western statutory intelligence derived up to 80 percent of information from open sources in "peace time". This estimate is, however, questionable. As denoted by the term 'Cold War', this was in certain respects a period of 'war' and not "peace time." Hence, a more credible estimation suggests that at the height of Cold War only around 20 percent of US information on the USSR was derived from open sources (Lowenthal, 2003: 79).

Against the backdrop of the preoccupation of the 'practicalities' of the East-West conflict, theorisation on a grand theory of intelligence failed to gain substantial momentum for the duration of the Cold War. Despite obvious overtures of tacit realist theoretical assumptions, intelligence literature rarely articulated a grand theoretical position. The realist position was assumed but rarely explicitly linked in writing to the structure of the formal realist paradigm. The limited literature that indeed dealt with intelligence theory, set out to contribute on the micro- or meso-level and to specific areas of academic enquiry within Intelligence Studies, such as analysis and the organisational structuring/management of statutory intelligence. Attesting to this assertion are works singled out by Johnson (2007: 3-4) as noteworthy contributions to the theory of intelligence, namely, Betts (1983), Handel (1983), Hulnick (1986), Laqueur (1985) and Robertson (1987). What was lacking was an overarching grand theory cohesively integrating fragmented micro- or meso-level contributions.

The deficient development of an intelligence theory can largely be ascribed to the inherent nature of statutory intelligence as the referent object of Intelligence Studies. Since its inception as a theme within Strategic and Security Studies in the 1950s, Intelligence Studies was confronted with a dichotomy: the academic requirements of transparency were juxtaposed to a study subject that has secrecy as a salient feature. One of the consequences of the dichotomy was a narrow factual base for the academic enquiry into intelligence in general, and the development and testing of theories specifically (Johnson, 2007: 1, 3). Further impeding academic enquiry was the fact that statutory intelligence is, relative to other governmental functions, a ‘closed’ community and more reluctant to enter into public debate. Consequently, intelligence has, relative to other disciplines within Political Sciences, attracted limited academic interest (Scott & Jackson, 2004: 7-8). Works on intelligence were for the larger part authored by individuals with experience in statutory intelligence structures with limited contributions by other scholars. It is furthermore doubtful whether serving practitioners at any rate deemed the development of ‘academic theories’ at a high level of abstraction as a priority. The nature and content of declassified articles from the Central Intelligence Agency’s (CIA) internal journal for the period 1955 to 1992, suggest an emphasis on the theory of intelligence at micro- or meso-levels, rather than an interest in the development of a grand theory of intelligence (Westerfield,1995). The approach of practitioners appeared to have been, to loosely adapt a statement by the late US President, J.F. Kennedy: ‘’Ask not what you can do for theory, ask what theory can do for you?’’ Obviously contestable but at least warranting consideration as a related reason for the under-theorisation of intelligence at a grand theory level, might be the ‘transfer’ of the utility sentiment from the statutory practice of intelligence to the academic realm of Intelligence Studies.

During the Cold War period Intelligence Studies thus evolved as a discipline self-cocooned in secrecy, for the most part ex-practitioner driven, largely disregarded by scholars within Political Sciences, and with little self-awareness of its under-theorised status.

3.2.3 The post-Cold War discourse on the theory of intelligence

The first decade following the end of the Cold War highlighted the status of Intelligence Studies as a discipline on the fringe of mainstream academic discourse. The previously outlined post-Cold War debate in Security and Strategic Studies on the expansion of the security agenda and the re-examination of the notion of national security, reverberated within Intelligence Studies. In line with the thinking in Security and Strategic Studies, non-traditional threats such as human security, drug trafficking and other forms of organised crime arose and were mooted for inclusion in the statutory intelligence agenda (Watts, 2005: 2).

3.2.3.1 Intelligence Studies as an under-theorised discipline: from indifference to critical self-awareness

Relative to the discourse on Strategic and Security Studies, however, the enthusiasm in Intelligence Studies on a grand theory construction was markedly more limited. A more practical consideration dominated the debate, namely ‘proving’ the continued centrality of, and sizable budget allocations to governmental intelligence structures. This practical consideration had as context changing public opinion and government policies that manifested in the review and reform of statutory security structures. The perception that a more secure world implied less reliance on statutory intelligence services was illustrated by the budget allocation to the US statutory intelligence organs. In 1996, for example, it was foreseen that the US intelligence budget would be reduced by between ten and twenty percent (Goodman, 1996: 3). By the end of the 1990s support for spending on national security had reached its lowest level since the end of WW II (Berkowitz & Goodman, 2000: 24).

Notably in both the US and UK, the perceptions of a more secure world accompanied by declining budget allocations further accelerated the reliance of statutory intelligence services on TECHINT, which during the 1990s was increasingly seen as “representing the future” (Gill & Phythian, 2006: 77). Technological advances during the 1990s also fuelled the “information revolution” and presented OSINT, supplementary to TECHINT, as a low-cost and low-risk source of information (Berkowitz & Goodman, 2000: 2, 12-13, 24-25). In the US, the attractiveness of

TECHINT and OSINT was augmented by the Clinton administration's aversion towards the higher risk posed by HUMINT collection (Gilluffo *et al*, 2004: 33; Gill & Phythian, 2006: 77). Concurrently, the dissipation of a clear monolithic USSR threat and the subsequent diffusion of intelligence priorities resulted in reduced emphasis on statutory counterespionage. In the UK, for example, the allocation of total resources to counterespionage plummeted from an exclusively assigned 50 percent in 1991, to a 25 percent slice of resources shared with counter-proliferation in 1996 (Northcott, 2007: 458, 459, 470). Despite lip service being paid to all-source intelligence, it was the development and maintenance of a high quality HUMINT capacity that was increasingly decrepitating in the US and UK intelligence communities. The terrorist attacks on the US (2001), as well as the controversy over US and UK intelligence-based allegations on Iraq's possession of WMD, highlighted the penalty for the neglect of HUMINT. During 2004, governmental bodies of enquiry in the UK (the Butler Committee) and the US (the Senate Select Committee on Intelligence) concluded the neglect of HUMINT to have been one of the primary reasons for intelligence failure (UK, 2004: 107-111; US, 2004*a*: 24-27, 260-263).

The attacks of September 11, 2001, had as further consequence a profound sense of insecurity and vulnerability to asymmetric threats that stood in stark contrast to the view of a more secure world that prevailed during the first decade after the end of the Cold War. Statutory intelligence was raised in the public consciousness as well as in academic debate. On the one hand, the nature of this asymmetric threat emphasised the indispensable role of statutory intelligence. On the other hand, the unexpectedness of these attacks contributed to perceptions of intelligence inadequacies and failure. Such perceptions were further reinforced by the controversy over disproved allegations of Iraq's possession of WMD.

The aftermath of the September 11, 2001 attacks is proving to be a watershed for Intelligence Studies, notably in the UK and US, and in certain respects lifted the academic discipline from near anonymity. In the words of Goodman (2006: 1), and with reference to the UK:

> The key events of the early 21st century have already defined intelligence as a new cornerstone of government ... One consequence of this has been the larger scale growth of intelligence study and teaching academically, as reflected both in the number of courses being offered and in the jump in enrolment in such courses. As such, the public's desire to know more is reflected accurately in its academic existence.

Concurrently, an acute self-awareness has been the crystallising of Intelligence Studies as an academic discipline disconcertingly underdeveloped in its theoretical dimension. Observations in this regard, to name a few, include those by Johnson (2007: 6, 22-23), Gill & Phythian (2006: 6-7), Scott & Jackson (2004: 7) as well as Quiggin (2007: 87). The increased prominence of Intelligence Studies as an academic discipline resulted in the status of its theorising also being commented on from other academic fields. This is attested to by a comment from the field of History in *The Oxford Medievalist's* website (2007: 1-2): "There have been recent concerted efforts to develop a theory of intelligence ... After 50 years of energized scholarship a theory remains elusive."

A significant signpost in this self-critical awareness in US academic and statutory intelligence circles was the convening of a conference in June 2005 by the Office of the Director of National Intelligence and the RAND Corporation with the theme: *Toward a Theory of Intelligence* (Treverton *et al*, 2006: iii). In addition to contributing to the theorisation on intelligence, the convening and proceedings of the conference were of significance in three areas. Firstly, it signified recognition that improving the practice of statutory intelligence needed to be underpinned by a sound theory of intelligence (Treverton *et al*, 2006: iii, 2-3, 7-11). Secondly, that the then current theorisation on intelligence was deficient and needed to be prioritised in the academic and governmental spheres (Treverton *et al*, 2006: iii, 30-32). Lastly the list of participants in and proceedings at the workshop showed an acknowledgment of the need for cooperation between Intelligence Studies as an academic discipline and statutory intelligence practitioners in the development of a theory of intelligence (Treverton *et al*, 2006: iii, 7-9, 15-16, 25, 30-32, 35).

The realisation of the under-theorised status of intelligence is furthermore reflected in a surge in contributions to intelligence theory from 2001 onwards. Johnson (2007: 3-4) regards the following as noteworthy contributions to the theory of intelligence: Andrew (2005), Davies (2002), L. Johnson (2003), R. Johnson (2005), Kahn (2001), as well as Scott & Jackson (2005). Other more recent publications by Gill & Phythian (2006), Taylor (2007), Shulsky & Schmitt (2002), Quiggin (2007), Bruneau & Dombroski (2004) and Rathmell (2002) extend this list.

3.2.3.2 *Contemporary endeavours to construct a grand theory of intelligence*

A comprehensive review of the current discourse on a theory of intelligence presents an exhaustive task and is outlined in Chapter Eight as a fertile area for further research. This study presents but a succinct overview, supported by reference to only some endeavours. At the risk of oversimplification, a distinction is drawn between, on the one hand, ambitious attempts to present a grand theory proposition and, on the other hand, a more circumspect approach that considers the development of a grand theory as an incremental process.

In respect of ambitious attempts to propose a grand theory of intelligence those of Kahn (2001), Gill & Phythian (2006) and Taylor (2007) serve as examples. Although qualified as accounting for military intelligence, Kahn (2001) presents his *An historical theory of intelligence* as having an application for statutory intelligence in general. Within the parameters of the realist paradigm, this scholar's theory endeavours to explain the exponential increase in the importance of intelligence, "from its biological origins as a mere instrument of survival to its supreme capability: helping a nation win a war", Kahn (2001: 1, 3-4). The "biological roots" of intelligence are elucidated by way of an organismic analogy: "Every animal, even a protozoan, must have a mechanism to perceive stimuli, such as noxious chemicals, and to judge whether they are good or bad for it" (Kahn (2001: 1). The growing importance of statutory intelligence is ascribed to the predominance of "verbal intelligence" (obtained from written and oral sources) progressively gained over "physical intelligence" (the physical observation of "things"). Kahn poses the optimising of a nation's resources as the fundamental and ultimate purpose of intelligence. To optimally fulfil this role, Kahn (2001: 5-6) asserts that intelligence must fulfil its potential as predictive instrument.

A further endeavour employing a realist approach is that of Taylor (2007), which as premise for his postulation on a meso-theory of counterintelligence proposes cybernetics as the basis of a grand theory of intelligence. In line with his explicit subscription to the traditionalist (realist) approach to international security, the decision-maker is seen as the "helmsman" that requires a constant flow of information to steer the states to optimally pursue their interest in an anarchic global environment (Taylor, 2007: 4-5, 9). That, according to Taylor, is the purpose of intelligence.

Contrary to what is contended by Taylor (2007: 5), not "all theories of intelligence or counterintelligence are overlaid on the traditional realist approach to international affairs." In addition to contributions from a post-modernist premise, notably that of Rathmell (2002), Gill & Phythian's (2006) postulation on a grand theory of intelligence is rooted in the critical-realist paradigm. Gill & Phythian (2006: 20-36) posit the concept of "surveillance", with its connotations within sociology (and not its conventional meaning as an intelligence operational technique), as the premise for a grand theory of intelligence (Gill & Phythian, 2006: 27). Intelligence is seen as a subset of "surveillance" that has secrecy as an inherent characteristic (Gill & Phythian, 2006: 29-30).

A more circumspect approach towards the development of a grand theory of intelligence is epitomised in Johnson's (in Gill, 2006: 5; emphasis added) statement: "The *objective* is less to impart new knowledge than *to lay out what we know in such a manner as to suggest next steps in theory construction.*" This 'laying out' or 'mapping' needs to depart from a distinct premise. In this regard Johnson (2006: 12) asserts that:

> The starting place is with the basics of human nature. Humans are motivated by two dominant instincts. One is the fundamental desire to survive. Another is the hope for prosperity ... Survival is associated with the fear of danger, both at home and abroad, both real and perceived; prosperity, with a sense of ambition. In both cases, information is vital to success: Nations seek information about threats and opportunities.

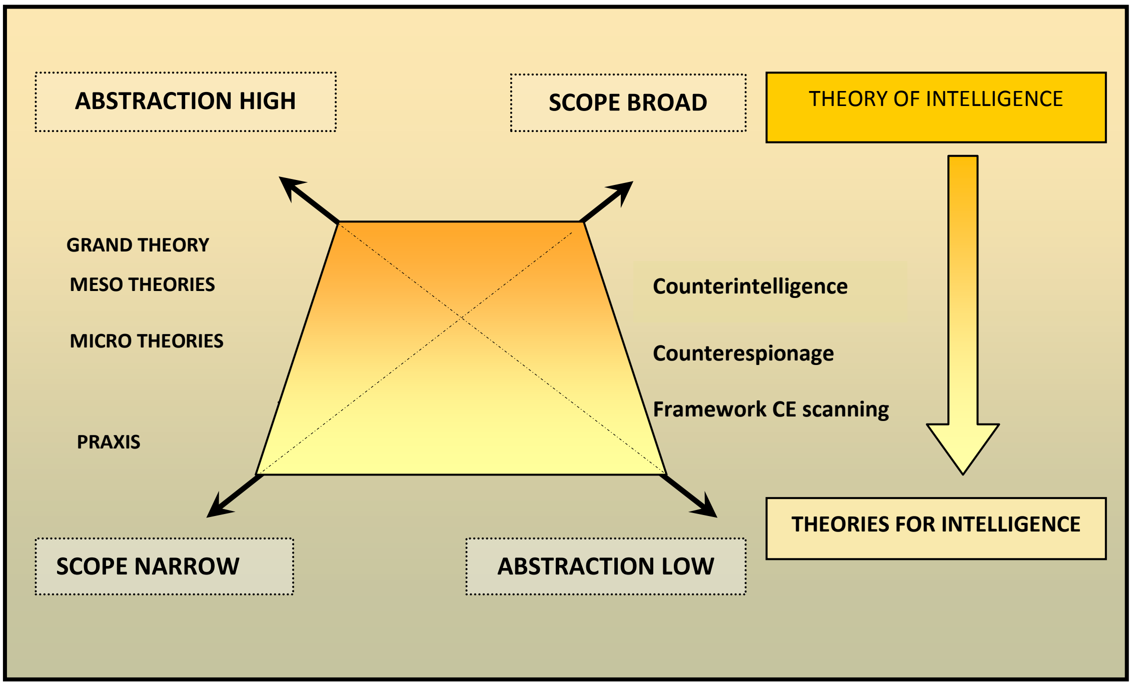
In his *Preface to a theory of strategic intelligence,* Johnson (2003: 638) more concretely sets out to answer what is simultaneously the most "theoretical and practical" question posed to statutory intelligence: "How much is enough?" More concretely phrased: what and how much intelligence does a nation state require and how many resources should be allocated to this function? Responding to this problem statement, Johnson (2003: 639-641) postulates certain variables that will determine the nature and extent of the intelligence endeavours of a state. These variables include a state's foreign policy goals; international presence and involvement; domestic homogeneity and stability; geographic location; perceived enemies, and alliances with other states. The parallels between the variables identified by Johnson and those posited by Buzan (in relation to national security) illustrate the interfacing of national security and statutory intelligence. Moreover, Johnson also extends the inherent subjectivity of national security to statutory intelligence. One of Johnson's (2003: 640) foremost conclusions is that the subjective *Weltanschauung* of a state's political leadership impacts fundamentally on the nature and extent of the intelligence activities of such a state.

Similar to Johnson (2003), Shulsky & Schmitt (2002) are circumspect in their postulation entitled *Toward a theory of intelligence*. Shulsky & Schmitt (2002: 159-168) primarily set out to delineate the concept 'intelligence' and offer positions on the aims of intelligence. They maintain a realist approach and contemporise Kent's previously discussed position on the essential facets of intelligence by pointing out that intelligence is not only externally directed but also has a domestic dimension; has secrecy as a defining characteristic, and should not depreciate the role and function of counterintelligence. This is exemplified by their statement: "Once we understand that intelligence is part of a struggle between countries, we see why counterintelligence is not an afterthought but is rather an integral part of it" (Shulsky & Schmitt, 2002: 172).

3.2.3.3 Prerequisites for advancing towards a grand theory of intelligence

The current status of the discourse on a grand theory of intelligence is aptly summarised by Johnson (2007: 4): "Overall, the studies on intelligence theory find that the discipline remains in its infancy, holding great promise for scholars interested in blazing new trails." This study asserts that optimal progression towards a theory of intelligence has three prerequisites. Firstly, and affirming Johnson's assertion (in Gill, 2006: 5), it is important that "we lay out what we know" in a manner facilitating the further development of a theory of intelligence. As was shown, literature is generally in agreement that the scope of a grand theory should in its vertical dimension encapsulate the various fields of academic enquiry such as ethics and accountability, history, intelligence reform and organisational structuring, intelligence functions (analysis, collection, counterintelligence and covert action) as well as intelligence leadership and management. Progress has thus been made on the vertical axis of mapping out of "what we know". 'Mapping' the current status of an intelligence theory and the deficiencies thereof are, however, impeded by the limited distinction in literature between the different levels of theory. As a grand theory needs to bind theories cohesively on lower levels of abstraction, the laying out of "what we know" could benefit by adding a horizontal axis, which accounts for the multilayered nature of theory. This study submits the following as a matrix enabling of the plotting of theoretical postulations on intelligence:

Figure 2: Matrix for the plotting of intelligence theories



A second, near axiomatic prerequisite for progression towards a grand theory is to emphasise *constructive* in 'constructive criticism' in relation to theoretical propositions. At these early stages of the discourse, postulations are understandably underdeveloped, deficient and unsubstantiated in certain areas. Gill & Phythian (2006), for example, fail to demonstrate the application of their critical-realist theory. Similarly, Taylor (2007: 4) mentions cybernetics as a "perfect paradigm or theory", yet his application of cybernetic-theoretical constructs is cryptic and more analogical than demonstrative. Kahn's theory is substantiated by references to incidents of war and conflict that span over millennia, are erratically anecdotal and not supported by consistent criteria for the selection of examples (*The Oxford Medievalist, 2007;* Quiggin, 2007: 84-85).

Despite these deficiencies, the postulations supplement and stimulate the discourse on a grand theory of intelligence. The discourse has already, this study suggests, provided grounds for considering the further development of a grand theory of intelligence within the ambit of systems theory. Bertalannfy (1967), as quoted by Ostroff (2000: 2-8), identifies the two main approaches within systems theory as cybernetics and the organismic approach. While differences and even contradictions exist between the cybernetics and the organismic constructs, there are overarching similarities and resonances (Ostroff, 2000: 8). As was previously indicated, cybernetics is foundational to Taylor's (2007) explication of a grand theory of intelligence. Without purporting to present an organismic theory, Kahn nevertheless employs the organismic notion at an analogical level. Such a theory would also be consistent with Johnson's (2006) premise for a theory of intelligence, namely the dominant human instincts of survival and prosperity. Indications are that an organismic theory would also accommodate other theoretical postulations rooted in the realist paradigm.

Whatever direction pursued in the development of a theory of intelligence, it would probably be an incremental process that would also benefit from theoretical postulations on the meso- and micro-levels. A third prerequisite for the development of a theory of intelligence therefore is for micro- and meso-level theoretical contributions to clearly state a paradigmatic position.

4. PRESENTATION OF A THEORETICAL POSITION: TOWARDS AN INTELLIGENCE, COUNTERINTELLIGENCE AND COUNTERESPIONAGE THEORY

In view of the above, this section explicates a theoretical position on the meta-paradigmatic, paradigmatic and grand theory levels. Within the context of a theoretical clarification on a high level of abstraction, this section proceeds to the formulation of a theoretical position on, and delineation of concepts central to counterintelligence and counterespionage.

This study does not in any way aspire to advance a grand theory that adheres to the characteristics of a construct at such a level. Hence, the theoretical postulation in this regard should be viewed merely as an endeavour to propose a further contour to the discourse on a grand theory of intelligence. As part of this theorisation, the organismic idea of the state is employed as an explanatory notion in respect of the statutory intelligence and counterintelligence functions. The concept of environmental scanning is introduced in expansion to the organismic idea. It must be emphasised that the organismic notion is employed merely as an analogy. Whether the organismic idea could indeed be expanded to qualify as a systems theory construct, would self-evidently require extensive research, and falls outside the parameters of this study.

4.1 META-PARADIGMATIC POSITION

Given the requirements posed to the statutory intelligence practitioner, a positivistic ontological and epistemological position is proposed as being the most apt. An objective world (reality) is deemed to exist separately from the researcher. The latter can maintain (a relatively high degree) of objectivity in discovering and describing reality. The framework for counterespionage environmental scanning aims to provide a description, explanation of, and in probabilistic terms, the projection of espionage risks to the state. This is expressed in terms of contextual constituents and variables such as the nature of the relationship that exists between a state and its adversaries. In line with the synthetic, positivistic approach the framework for environmental scanning is expressed in terms of contextual variables, such as the nature of the relationship between the state and its adversaries.

4.2 PARADIGMATIC POSITION

As it could digress into extensive deliberations on peripheral issues, an over-emphasis on typifying an approach as belonging to one or the other school of thought could, on the one hand, potentially constrain rather than aid a theoretical discourse. On the other hand, the specification of the roots of a theoretical postulation in a specific school of thought can be useful in providing an indication of the positioning of the theoretical construct within the theoretical landscape. This does not need to imply a dogmatic confirmation of all the core contentions of the applicable school of thought. With this qualification and with the *proviso* that it relies for substantiation on subsequent chapters, the broad theoretical configuration to follow can be seen as overlaid upon the realist paradigm.

Schools of thought outside the realist paradigm view the privatisation of statutory security functions as signalling the erosion of the sovereignty and power of the nation state. Similarly the role of international institutions (such as the United Nations) and regional formations (such as the European Union) are perceived to be diluting the sovereignty of individual nation states and limiting their execution of power. Critics of the realist paradigm view the hostility of the environment not as a constant but rather a self-fulfilling condition resulting from the realist view. As will transpire in subsequent chapters of this study, it is doubtful whether the outsourcing of certain security functions or the participation in regional and international formations, equates with an irrevocable cessation of the nation state’s sovereignty and its ultimate prerogative, the execution of power. It is also doubtful whether the post-Cold War era augured in a phase which provides grounds for optimism over the possibility of decline of large-scale conflict (including warfare). The recorded history of humankind supports an ontological view of self-interested preoccupation ultimately resulting in military conflict. More recently, and in a relatively short time span of a century, optimism over the end of large-scale international conflict has been disproved on two occasions.

Even though aspects of its *modus* might have been changing, warfare remains a further constant characteristic which accompanies hostility. As illustrated in Chapter Three, warfare in the contemporary era of information and globalisation presents the expansion of the battlefield to the cyber sphere. In short, trends and developments in the international arena confirm rather than cast doubt on the state as a self-centred entity in constant conflict with adversarial entities.

The self-centred nature of the state and the hostility of the environment within which it pursues survival and prosperity, are foundational to the employment of the organismic notion as an explanatory construct. In line with Kahn's (2001:1) contention, the state as "every animal, even a protozoan" is seen as functioning in a hostile environment. The hostility of the environment is a result of the covetous competition between adversaries seeking their own survival. Such competing and hostile adversaries are not only other nation states but any entity that could inhibit a state to optimally promote its vital interests within the context of limited resources. The state also strives to maintain its two foremost characteristics as organism, namely its sovereignty and, related to this, its prerogative in the execution of its power. These characteristics are posited as constants despite the continuous adaptation of the nation state to its environment.

4.3 A CONTOUR TOWARDS A GRAND THEORY OF INTELLIGENCE

As is the case with other organisms, the state depends for its survival on an ability to sufficiently 'sense' the environment. This 'sensing', Kahn (2001: 1) contends, is the primary function of statutory intelligence. The expansion of the notion of statutory intelligence as an environmental 'sensor' to that of environmental 'scanner' provides an ever more nuanced depiction of intelligence in its informational role. The *Encarta World English Dictionary* (1999: 1673) includes the following as part of its definition of the word "scan":

- "[E]xamine something in detail";
- "looking through something quickly";
- "examine something.... (in order to convert an image into digital or electronic form for further storage, retrieval and transmission)";
- "examine stored data";
- "to obtain an image of internal organs"; and
- "search area using radar".

As an outwardly directed scanner that collects information, intelligence serves as “radar” for identifying “objects” that could be detrimental to the state’s survival and prosperity. Subsequent to identification, intelligence also involves a detailed “examination” and “scrutiny” to confirm or refute the status of “objects” as risks or threats to national security. For both the “radar” sweep and the detailed “scrutiny” to be of use, the information gathered is “converted” into a legible “image” (an intelligence product). Information gathered and intelligence products compiled are continuously “stored”, “retrieved” and “transmitted” (to the client). Of particular relevance to counterintelligence, is the denotation of “scanning” as an introspective function “to obtain an internal ‘image’ of the state’s ‘organs’”. Thus, scanning also alludes to the identification and scrutiny of “internal” risks, of as well as to the integrity of the state and its apparatus. In addition, the introspective dimension of scanning can also be interpreted as signifying the focus of intelligence not only on the international but also the domestic spheres.

Contrary to Kahn’s contention, sensing is not only of primary importance in optimising defence. As will be illustrated in Chapter Three, the state’s (and its adversaries’) quest for intelligence that will increase its competitive edge manifests in increasing levels of espionage. Furthermore, as will still be elaborated upon, intelligence is more than an environmental sensor and processor; it also constitutes an instrument of power.

4.4 CONCEPTUALISING COUNTERINTELLIGENCE AND COUNTERESPIONAGE

The defensive and offensive function of intelligence as scanning is epitomised in the counterintelligence function. In organismic terms counterintelligence relates to integrity on two levels, namely offensively and defensively safeguarding the informational integrity of the state (organism). Various defensive counterintelligence measures, such as physical and information security, act as protective ‘membranes’ against adversarial actions that could compromise the informational integrity of the state. Counterintelligence is simultaneously part of the scanning (namely the ‘sensing of the environment for espionage and security risks’) and the protection of scanning conducted by positive intelligence. Counterintelligence is furthermore an offensive ‘arm’ that serves to disrupt the informational integrity of other organisms (adversaries).

4.4.1 Counterintelligence definitions and assumptions

Notwithstanding variances in definitions afforded to counterintelligence, the application of the organismic and scanning constructs is in the main congruent with the core meaning of such definitions. The following serve as examples:

> Counterintelligence refers to efforts taken to protect own intelligence operations from penetration and disruption by hostile nations or their intelligence services. It is both analytical and operational (Lowenthal, 2003: 113).
>
> Counterintelligence refers to information collected and analysed, as well as activities undertaken to protect a nation (including its own intelligence-related activities) against the actions of hostile intelligence services (Shulsky & Schmitt, 2002: 99).

Taylor (2007: 89) describes four assumptions that underlie the existence of statutory counterintelligence. These four assumptions are that:

- A state possesses information that if compromised to an adversary would negatively impact on national security;
- a state has an intelligence structure(s) that collects information and will endeavour to protect it from “falling into enemy hands” ;
- foreign intelligence services [and other adversaries] will attempt to obtain such information, and
- a low level of trustworthiness must be assumed in respect of most people.

Taylor (2007: 9-10) rightly emphasises the importance of the fourth assumption by means of a more elaborate explanation indicating this to be a human level manifestation of realism.

4.4.2 A conceptual structuring of counterintelligence and counterespionage

Counterintelligence functions and measures are expounded on in Chapters Three, Five, Six and Seven with different aims and from distinctive perspectives. Since it is necessary as context, brief observations are nonetheless required here. To limit repetition, assertions made in this section rely for substantiation on further chapters.

Existing attempts to conceptually structure counterintelligence are clouded by an inadequate distinction between counterintelligence missions, functions and measures. This, Chapter Five argues, partially explains the absence in literature of an intelligence process and cycle congruent with the requirements of counterintelligence.

Current conceptualisations are, in short, both oversimplified and confounding. It is an oversimplification in the sense that certain counterintelligence measures and/or functions are rigidly categorised as exclusively relating to a specific mission. It is confounding in that this rigid categorisation, coupled with deficiencies in the clear distinction between functions, missions and measures, create multiple categorisations varying from author to author and from study to study.

In espousing the meso-theoretical postulation, counterintelligence has only two *missions*:

Firstly, to defensively and offensively protect the integrity of statutory information deemed of national security interest. To this end, all four counterintelligence elements (functional areas) are involved. It entails the employment of measures usually categorised as part of protective security such as information security and personal security. It also entails utilising measures in current conceptualisations assigned to offensive counterintelligence. In this instance the measures serve as the defensive mission.

Secondly, counterintelligence has an offensive mission. The offensive mission comprises measures instituted to compromise the informational (intelligence) integrity of an adversary. This includes measures, traditionally categorised as offensive, and also such measures typified by existing conceptualisations as defensive measures.

The said missions are executed in a synergetic fashion involving all four *functional areas (elements) of counterintelligence*. In this respect counterintelligence mirrors the statutory intelligence service it is part of. Counterintelligence is thus a service within a service. Codevilla (1992: 26) remarks that in this regard:

> It is easy to confuse CI with a host of other intelligence activities – collection, analysis, covert action – because good CI does everything that the full-fledged intelligence service does, and takes a hand in everything the rest of the service does. Adequate attention to hostile intelligence services is a prerequisite for making one's own collection, analysis, and covert-influence activities succeed.

While counterintelligence mirrors the functional areas of an intelligence service in general, these functions (within counterintelligence) have distinct offensive-defensive qualities that place a high premium on the practitioner's specialised knowledge. The distinct character of the analysis function within counterintelligence, for example, is described by Godson (2001: 187) as follows: "Perhaps the queen of the counterintelligence chess board is counterintelligence analysis, both offensive and defensive." A certain dimension of covert action also forms part of counterintelligence. This is aptly captured by Codevilla (1992: 349) in that he states that: "[a]ction against the enemy through the enemy's own intelligence is the very consummation of CI." In its function of collection, CI uses an array of measures. In addition to OSINT, HUMINT and TECHINT, counterintelligence also has as a source information generated by its security function. Therefore, counterintelligence has, in addition to the other points mentioned, a unique fourth functional area, namely security.

From the above it is clear that the assigning of certain *measures* to one or the other mission is more confusing than clarifying them. Chapters Three and Five will introduce measures as representing a spectrum from, on the one hand, being non-aggressive and passive to, on the other hand, aggressive and offensive measures. It is only at the very end of this spectrum that certain measures do not have an application to more than one function and mission. The following serves as some indication of the array of measures at the disposal of counterintelligence: pre-employment personnel security; in service personnel security; technical surveillance countermeasures (TSCM); encryption; surveillance (physical, static, mobile and electronic); double agents; agents; continued monitoring, and even assassination.

It is only within the above context that counterespionage can be succinctly delineated. The conceptual structuring of counterintelligence as outlined above renders redundant the need for long-winded and complex definitions. Counterespionage is, in short, a category of counterintelligence measures, directed against the collection efforts of adversarial intelligence structures. It has a bearing on both missions of counterintelligence and is executed in all four functional areas.

4.4.3 Distinction between an espionage risk and threat

Although more comprehensively addressed and substantiated in Chapter Four, a tentative delineation of the concepts espionage risk and espionage threat is necessary to serve as context for Chapter Three. As was noted, espionage is often deemed as referring to only the clandestine HUMINT collection by an adversary of the state. Chapter Three shows the restriction of the term espionage to clandestine HUMINT collection to be problematic. The reality of espionage and counterespionage rather suggests a conceptualisation of espionage to also include categories of adversarial collection to be more apt.

The criteria for categorising a security concern as a risk or threat to national security are self-evidently also applicable to the counterespionage field. Counterespionage does, however, require a differentiation between a risk and threat that is distinct from positive intelligence. In his hierarchical distinction between risk and threat, Bernhardt (2003: 142-144) points to general acceptance within the academic discourse of a threat denoting “a sense - or perceived sense - of imminence, certainty and urgency, as well as definite connotations in terms of expected or real security implications.” In citing Cohen (1989) mention is made that a threat has also been defined “as the presence – or perceived presence – of a menacing intention and capacity on the part of one entity to cause harm, injury or damage to another entity. This ‘menacing intention and capacity manifests in the form of an adversarial relationship of a unilateral or mutually aggressive nature between two entities.” (Bernhardt, 2004: 64-65). The two key elements in this relationship thus are a menacing intention and the capacity to give effect to such intention. A security issue which is not necessarily an immediate danger, clearly imminent, certain or urgent or where the capacity and/or the intention is not clear, is – subject to variables and preconditions - defined as a risk. Two key variables postulated are “probable occurrence” and “probable adverse impact”. Bernhardt (2003: 144) concludes a risk as being “a conditional event: it has not yet occurred and certain preconditions must first be realised before it comes to pass” (Bernhardt, 2003: 144).

Neither the aptness of these definitions in a framework for a risk and threat assessment in a domestic intelligence environment informed by all-source intelligence, nor the conceptualisation of a threat, is in dispute. What is, however, clear is that a framework focused on counterespionage, as informed by the scanning and assessment of overt sources, requires a distinct definition of a ‘risk’. As reflected in the definition provided for purposes of the counterespionage environmental scanning framework in Chapter One, the term risk embodies as central concepts: plausibility, origin/nature and (possible) impact. Since the counterespionage environmental scanning framework is focused on espionage and relies on overt information, ‘plausibility’ rather than ‘probability’ serves as a definitional criterion for an espionage risk. In its core, espionage is clandestine, deceptive and tailored to avoid detection. An analyst within this field is to a larger degree confronted not only with an unknown future, but relative to positive intelligence, also with a more uncertain present. In the words of Codevilla (1992: 326): “by far the hardest part of a

CI case is to realize that it exists." Therefore, the concept 'risk' is more encompassing than a "conditional event in the future" – it also pertains to (the more uncertain) present. As suggested, this is compounded by the counterespionage environmental scanning framework's reliance on overt information in projecting on security issues of statutory concern. Within the counterespionage milieu, judgment on certainty/probability without considering operationally procured information is rare. The outcome of the counterespionage environmental scanning framework will inevitably carry a quality of uncertainty. Hence, and as was noted, the term 'plausibility' rather than 'probability' offers a more apt criterion for categorising a security concern as an espionage risk.

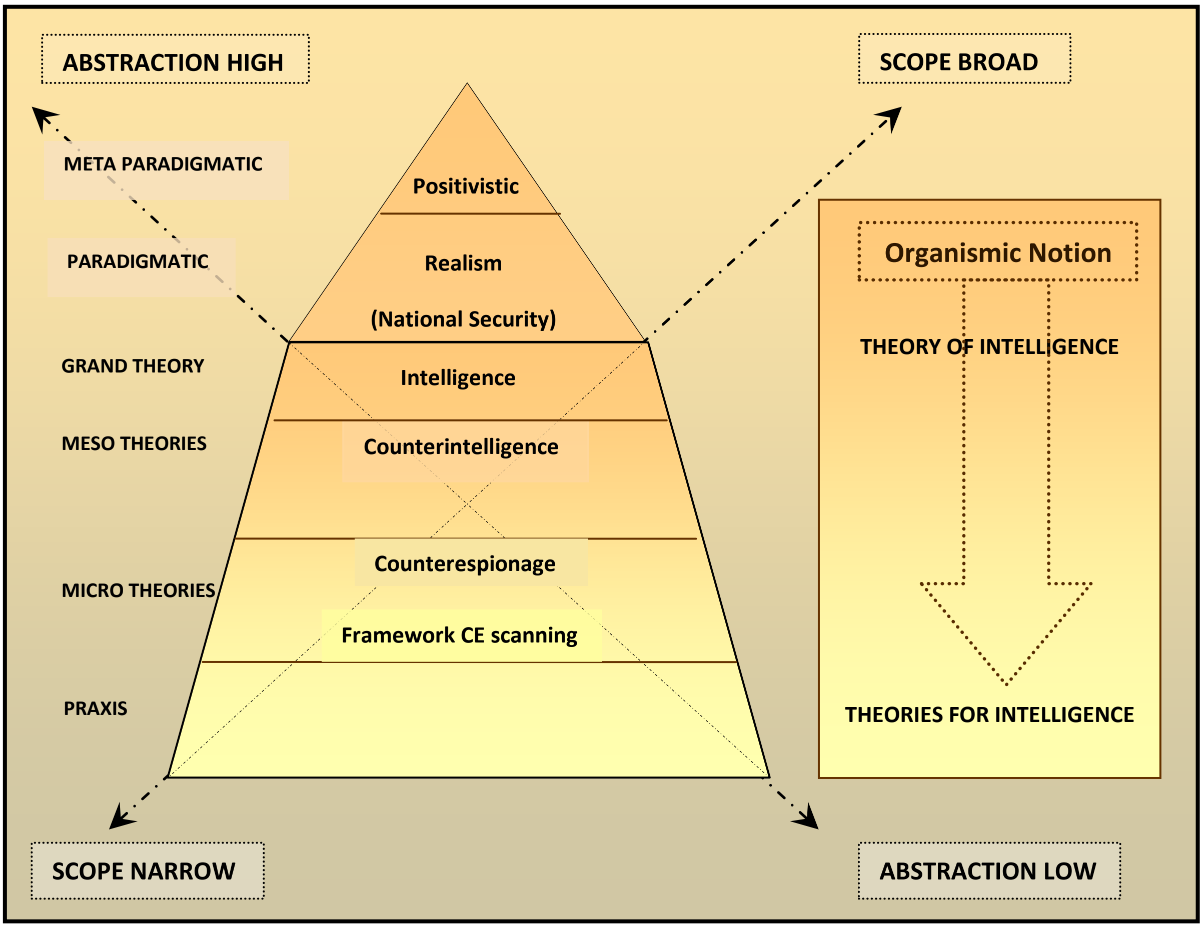
The theoretical outline provided in this section enables the typological positioning of the framework for overt counterespionage environmental scanning. In its micro-level dimension the framework is a constituent part of counterespionage. The framework also has meso-level denotations in that it spans all four the counterintelligence functional areas. Firstly, the framework involves counterintelligence *analysis* as a specialised function that, as identified by Godson (2001: 187-200), includes counter-deception analysis as well as the assessing of the own and adversarial vulnerabilities. Secondly, to inform this analysis the framework is geared towards the overt *collection* of information. Thirdly, it has as aim to detect espionage risks that are intertwined with adversarial (informational) *covert action*. Lastly, within the *security* functional area, the framework needs to consider in its design the computation of 'own' state and service vulnerabilities.

4.5 INTEGRATED THEORETICAL POSTULATION

The typological positioning and the primary aim of the framework for counterespionage environmental scanning, namely the identification and assessment of 'real' espionage risks to the nation state, reflect the meta-paradigmatic positivistic premise of the study. On a paradigmatic level this positivistic premise underpins the realist position assumed on national security. In line with the realist view, the state is seen as covetously pursuing its survival and prosperity in conflict with other role players. The self-interested nature of the state and the hostility of the environment within which it functions, are foundational to the employment of the organismic notion as an explanatory construct. Applied on the level of a grand theory of intelligence, the organismic analogy serves as a parsimonious, explanatory construct. Similar to other organisms, the state depends on the ability to sufficiently 'sense' the environment for its survival. This environmental 'sensing' constitutes one of the two primary missions of intelligence. The broadening of the notion of statutory intelligence as an environmental 'sensor' to that of an environmental 'scanner' provides an even more nuanced depiction of intelligence in its informational role. Intelligence is, however, more than an environmental sensor and processor. In its counterintelligence subdiscipline, intelligence also fulfils a protective and offensive function. It is this protective and offensive role that constitutes the second primary mission of intelligence. Employed at the meso-level of a counterintelligence theory, the organismic construct is also in this instance congruent with the requirements posed to theories in general in that it is parsimoniously explanatory. In organismic terms, counterintelligence acts as both a protective membrane and an offensive mechanism. As a subfunction of counterintelligence, counterespionage fulfils both an offensive and defensive role. Within this context, the counterespionage environmental scanning framework is geared towards optimising the offensive and defensive capacity of the organism (state).

Against the background of the above, the integrated theoretical postulation of the study can graphically be depicted as follows:

Figure 3: Integrated theoretical postulation



5. CONCLUSION

This chapter provided a theoretical and conceptual framework foundational to the rest of the study. It commenced with a conceptualisation of the term ‘national security’ as the overarching concept in the theoretical approach to the study. It emerged that national security evades the assigning of even an enumerative, universally accepted definition. As national security was ascertained to be largely subjective and the outcome of a political choice, the connotations afforded to it vary from state to state. Of pivotal importance to this study is the finding on the variables decisive to a nation state’s view of national security as well as its perception of threats and risks (to national security). Since the perception of national security of a nation state determines its espionage endeavours, these variables will be considered in projecting espionage risks as part of the design of a counterespionage environmental scanning framework. Following an overview of the discourse on the expansion of the security agenda, it was concluded that not all issues of security concern constitute a threat or risk to national security. Therefore, criteria for categorising a security concern as a threat/risk to national security were examined. Also these criteria are informative to the design of a counterespionage environmental scanning framework.

Within the broader context of national security, the chapter proceeded to conceptualise the notions of statutory intelligence, counterintelligence and counterespionage. The conceptual structuring of counterintelligence and counterespionage in current literature was found to be inadequate and an alternative was proposed. Interlocked with the conceptualisation of intelligence, an overview was provided of the discourse on a theory of intelligence. On the grand theory level, intelligence was determined to be critically under-theorised with the discourse only having gained significant momentum since 2001. Nevertheless, two aspects of central importance to the study emerged. Firstly, variables were identified that shape the nature and extent of the intelligence endeavours of a state. These variables are congruent with the factors identified as foundational to the perception of the national security of a nation state and will likewise be incorporated in the design of a framework for counterespionage environmental scanning and assessment. Secondly, the overview of the discourse on intelligence not only provided an essential context for, but also proffered the organismic notion as an analogical construct for a broad theoretical configuration on the grand and meso-levels. The organismic notion was extended to include that of (environmental) scanning as an analogical explanatory concept. In the main, the said theoretical configuration is accommodative of realist conceptualisations of intelligence and counterintelligence. Therefore, it can be deemed as presenting a workable theoretical context for the design of a framework for counterespionage environmental scanning and risk assessment in the statutory milieu.

In addition to theoretical and conceptual imperatives, the design of the framework for counterespionage environmental scanning and assessment also needs to consider more concretely, as the primary focus of Chapter Three, the manifestation of espionage directed against the nation state and the counterespionage challenges it poses.

CHAPTER THREE

INTERNATIONAL SECURITY, INTELLIGENCE AND COUNTERINTELLIGENCE IN THE 21ST CENTURY AS THE FOCUS OF OPEN-SOURCE COUNTERESPIONAGE ENVIRONMENTAL SCANNING

1. INTRODUCTION

Building on the theoretical and conceptual basis provided in the preceding chapter, Chapter Three examines the imperatives placed on the framework for counterespionage environmental scanning by the rapidly evolving international security milieu. More specifically, the implications of the changing environment for national security, statutory intelligence and counterintelligence are addressed. The concrete manifestation of espionage against the nation state as well as the counterintelligence measures the state employs are highlighted. In essence, this chapter thus provides the basis for configuring the framework for counterespionage environmental scanning and risk assessment in accordance with 'reality'.

In its *scanning dimension*, the framework for counterespionage environmental scanning and risk assessment (hereafter referred to as the CE framework) includes two complementary levels of collection. On the one hand, there is the broad scouting of the macro-environment for aspects of possible counterespionage concern to the nation state. On the other hand, there is the closer scrutiny of these concerns to confirm or refute their status as espionage risks or threats. In its design the framework for counterespionage environmental scanning therefore needs to be calibrated in accordance with the reality of the generality of the macro-environment as well as the specificity of espionage (against the nation state).

At least insofar as the CE framework is concerned, unanalysed information obtained through collection would rarely render apparent espionage risks and threats. Phrased differently, the counterintelligence 'picture' of such risks and threats emerging from collected information would in most instances be fragmented, opaque and indistinct. Interlocked and in continual interaction with the collection process, the CE framework therefore also has an *analysis (assessment)* component as constituent. Similar to collection, the analysis constituent needs to be designed in a manner that meets the distinct challenges posed by open-source counterespionage analysis.

As will be espoused on in Chapter Four, open-source counterespionage analysis demands a systemised process that combines estimative approaches (such as variable-depended matrixes and models) and indicator-based methods. The identification of useful variables does of course require a factual basis. Seeing that this chapter is directed toward 'practically' outlining the 21st security 'reality', it does not venture into the theoretical realm of variables, indicators, models, matrixes and the like. It, rather, aims to provide a factual basis that informs the postulation of notional constructs in subsequent chapters.

The chapter's advancement of the said 'reality' is, however, unpinned by a stratified theoretical distinction. In order of ascending specificity, a differentiation is made between the 'contextual focus', 'focus areas' and 'focal points' of the CE framework. These thee-layered focuses are a loose adaptation of the varying levels of environmental scanning intensity widely ascribed to in Business Management (Choo, 1998, 2001; Daft & Weick, 1984). Also in this case, subsequent chapters will bear out the relevance of this distinction to the design and application of the CE framework.

2. THE MACRO-ENVIRONMENT AS CONTEXTUAL FOCUS OF COUNTERESPIONAGE ENVIRONMENTAL SCANNING

Contemporary changes in the international security arena are more fundamental than a mere reactive response to the end of the Cold War and 9/11. Although events such as the end of the Cold War and 9/11 are of undisputed significance to international security, they are in certain respects only symptomatic manifestations of a rapidly evolving global environment. It is the whole of this global environment that is foundational to the state's subjective conceptualisation of national security and the concurrent counterintelligence strategies it employs in safeguarding national security and pursuing its national interest. The trends characterising and factors underlying this global security order and disorder underlie not only the manifestation of espionage risk and threats to the nation state, but also the counterintelligence measures instituted by the state (US, 2005*a*: 1-2, 16-17). Consequently, these factors and trends constitute the area of *contextual focus* of the CE framework and are examined in this section.

2.1 DRIVERS OF CHANGE

In recent years comprehensive and ongoing initiatives have been launched within the UK and US statutory security establishments to describe and project the transformation of the global environment and the implications thereof for international and national security (UK, 2007; US, 2005*a*; US, 2004*b*; US, 2004*c*; UK, 2003; US, 2003; US, 2000*b*). Similar efforts are also part of research projects conducted by institutions such as the UK-based Institute for Public Policy research and the RAND Cooperation in the US (Kearns & Gude, 2008; Treverton, 2005; Karoly & Panis, 2004). A common methodological and conceptual complexity transpiring from the projects is to distinguish clearly among related constructs such as 'drivers', 'impact', 'characteristics,' and 'manifestation' by definition. For reasons of simplicity and brevity, this study views a "driver" as "a factor that directly and profoundly influences or causes change" (UK, 2003: 6).

The said projects and endeavours concur in their identification of globalisation as one of the overarching mega-drivers of the global security environment (Kearns & Gude, 2008: 5 -11; UK, 2007: xiii; 3-4; Treverton, 2005: 2, 8; US, 2004*b*: 10, 13 - 15; Karoly & Panis, 2004: 2; US, 2003: 12). While there is agreement on the primacy thereof as a driver, 'globalisation' evades a generally accepted definition. In the words of Dunne (1999: 20): "Like most concepts in politics and international relations, the meaning of globalization is contested." A definition that nevertheless conveys the essence of the notion 'globalisation' is provided by the Geneva Centre for Security Policy Study (Al-Rodhan & Stoudman, 2006: 2). Following a comprehensive review of attempts at defining the concept, the centre concludes 'globalisation' to be "the process ... that encompasses the causes, course, and consequences of transnational and transcultural integration of human and non-human activities" (Al-Rodhan & Stoudman, 2006: 2). As implied by this definition, globalisation is an accelerating force rather than a realised condition. Abstractly, globalisation denotes the homogenisation of values and beliefs that favours cosmopolitanism over heterogeneous ethno-cultural and religious divides (UK, 2007: 11-13; US, 2000*b*: 25; Godson, 2001: xviii-xx). More concretely, globalisation in the socio-civilian sphere is associated with the transnational mobilisation around humanitarian, environmental and other causes of such a nature (UK, 2007: 11-13). In the economic domain, globalisation is linked to the ideal of the unconstraint movement of goods, capital and humans, that would enable the full integration of financial, consumer, labour and production markets (Karoly & Panis, 2004: 2; Treverton, 2005: 2; US, 2000*b*: 22). Globalisation in its political dimension is associated with the move towards global governance in regulating the relationships among states for purposes of collective prosperity and security (Kearns & Gude, 2008: 5; *Farlex Dictionary*, 2008: 1, 5, 6).

Globalisation is fuelled by a further salient driver in the changing global environment, namely technological advances. Technological advances in, for example, communication and transport, increase the level of interconnectivity between markets, people, and infrastructure (US, 2000*b*: 18). Interwoven with technological advances is the "information revolution" as a further driver of change (Berkowitz & Goodman, 2000: 12-13). The informational revolution is, however, more encompassing than only information technology. It also pertains to the way in which information is utilised and the crystallisation of an information-driven global community (Berkowitz & Goodman, 2000: 12-13).

In contrast to the trends towards homogenisation outlined above, "fissiparous trends" are concurrently gaining momentum (Godson, 2001: xix). Such forces of fragmentation and identification are, in part, a counter-reaction to globalisation and a rejection of heterogeneous assimilation. Instead, emphasis is placed on a narrower identification that is rooted in one or more of the following: race, ethnicity, religion, tribal roots, as well as a common history and destiny (UK, 2007: 3; US, 2004*c*: 78; Godson, 2001: xix; Treverton, 2005: 4). This sentiment appears to be especially prevalent in developing non-Western regions that perceive globalisation as, in the words of Neeraj (in Rodhan & Stoudman, 2006: 15), "nothing but 'recolonisation' in new garb." Anti-globalisation is fuelled by material factors such as the inequality in material prosperity exacerbated by globalisation (UK, 2003: 10).

Prosperity, be it global or limited to certain regions, is increasingly affected by natural and environmental drivers (UK, 2007: 2; Kearns & Gude, 2008: 6). Arguably the most important of these "ecospheric" and "antropospheric" environmental forces, are demographic factors (such as population growth and migration), climate change and the scarcity of vital natural resources (Brauch, 2005: 19).

2.2 A CONCEPTUAL STRUCTURING OF THE MACRO-ENVIRONMENT

The indicated drivers of change impact on certain 'domains' or 'sectors' of society. It must be emphasised that the categorisation of the macro-environment in such domains is a conceptual, schematic tool and, measured against the synergetic reality, 'artificial'. With this *caveat*, such a categorisation, however, serves to systematise a complex and extensive terrain for purposes of environmental scanning conceptually. Moreover, as elucidated in Chapter Six, a sectorial structuring of this nature is pivotal to an analysis of the relationship between role players within a specific environment. Since categorisation is a schematic tool and not a rigid compartmentalisation, it can be customised according to the purpose and the requirements of the environmental scanning envisaged. Despite differences in premise and purpose there are, nevertheless, some discernible commonalities in approaches to environmental scanning that span across different fields of academic enquiry. A comparison between approaches in the conceptual structuring of the environment respectively in the business sphere and the academic disciplines of Security and Strategic Studies, serves as an example. In the field of Competitive Business Intelligence the environment is commonly structured according to the "STEEP" guideline (Fleisher & Bensoussan, 2003: 271-273; Pollard, 1999: 4, 12). "STEEP" is employed as an acronym for segmenting the environment into the following sectors: societal/sociological, technological, economic, ecological and political. As was indicated in Chapter Two, the segmentation of the environment as a conceptual instrument of analysis is also employed within Security and Strategic Studies. Reference was additionally made to an authoritative notion forwarded by the Copenhagen School of thought. The latter, to re-encapsulate, propagates as part of a framework for analysing the international security environment, a demarcation that provides for the political, economic, societal, economic and military sectors (Buzan *et al*, 1998: 7-8). The Copenhagen School and Competitive Business Intelligence are thus in agreement in conceptually segmenting the environment into political, societal, economic, and ecological/environmental sectors. A key difference between these approaches relates to the 'military' and 'technological' sectors. Whereas the Copenhagen School provides for a military sector (to the exclusion of a technological segment), Competitive Business Intelligence favours the inclusion of a technological sector (to the exclusion of the military sector).

A combination of the above-mentioned approaches provides a premise for postulating a conceptual structuring of the environment for the purpose of this study. Concurring with the commonalties between the two approaches, the political, societal, economic and ecological sectors are included as part of the conceptual structuring of the environment. As this study essentially centres on the conflict between the state and its adversaries, some of which have armed capacities, the military sector self-evidently warrants inclusion. From the perspective of this study, the inclusion of the military sector does not necessarily preclude the addition of a 'technological' segment. Trends in the technological sector profoundly shape the international security environment and statutory counterintelligence practice. This chapter furthermore presents the informational sector as an arena for conflict between the state and its espionage adversaries, and its theme further reinforces the requirement to provide for the inclusion of a distinct informational sector. As was noted, the study is centred on the collection and assessment of a specific category of information, namely counterintelligence.

In summary, to structure the macro-environment for scanning and assessment conceptually, this study segments the environment into the following sectors: political, military, social, technological, economic, ecological (environmental) and informational. The macro-environment thus segmented, and the drivers of change in particular, constitute the contextual focus of the CE framework. International security and national security are dimensions of, but not separable from the macro-environment. It is from this holistic perspective that the subsequent examination of international and national security in the 21st century should be viewed.

3. INTERNATIONAL AND NATIONAL SECURITY IN THE 21st CENTURY

Traversing the indicated environmental sectors, the drivers of change generate strategic trends which acutely affect the role of, and challenges to the nation state. The design of a framework that aims to contribute to meeting the counterespionage challenges posed by the 21st century should have, as a nearly self-evident premise, a delineation of the strategic changes that mould the international security environment. It is after all this environment that is the object of the scanning process.

3.1 STRATEGIC TRENDS AFFECTING INTERNATIONAL SECURITY AND INSECURITY

While there is consensus that the international security milieu is changing profoundly, few scholars will contest Godson’s (2001: xvii) assertion that the contours of this ‘new era’ are, for a substantial part, only dimly understood. The trends shaping and characterising the international security order of the 21st century are a combination of the ‘old’, the ‘new’ and the-still-unfolding. Counterespionage environmental scanning has as aim not only to identify manifesting risks and threats, but also to provide early warning on unfolding espionage-related developments. Consequently, counterespionage environmental scanning needs to consider, as *focus areas,* current trends shaping the international security order in a manner that explicates on the likely future development thereof. The previously mentioned projects of the US and UK governments to assess, in collaboration with academics and other nongovernmental experts, international security from a pro-active perspective are therefore of particular value. Emerging from these and other studies are a multiplicity of strategic trends, of which only the most salient will be concisely highlighted.

A primary strategic trend commonly identified is the reconfiguration of the geopolitical order, which is accompanied by shifts in political, military and economic power. The geopolitical remoulding is essentially of a six-dimensional nature. Firstly, a sharp increase in the number of nation states that results, in certain respects, in a diffusion of power. Nation states recognised by the United Nations (UN) increased from 51 in 1945 to 192 in 2006 (Quiggin, 2007: 14). Measured over a shorter time span, and linked to the end of the Cold War, the number of recognised states increased by 25 percent in the decade 1990 to 2000 (US, 2000*b*: 25). Secondly, a gradual shift in the balance of power, from US dominance to a "global more heteropolar matrix" (Der Derain, 2005: 1). States that are gaining in strength as *arriviste* powers include the PRC, India, Indonesia and Brazil (UK, 2007: 30, 44; US, 2004*b*: 9-10; US, 2000*b*: 8). *Arriviste* nation states are not the only actors relevant to the power shift in the international arena. Despite domestic constraints and internal conflict, Russia is projected to advance its status as "an important, if troubled, partner for both the established powers such as the United States and Europe, and the rising powers of China and India" (US2004*c*: 54). As was the case during the Cold War, some states are deemed as increasing their leverage in the international arena by virtue of establishing, developing, or aspiring to establish chemical, biological, radiological and nuclear (CBRN) capabilities (UK, 2007: 17). Serving as examples are: North Korea, Pakistan and Iran (US, 2006*a*: 32; UK, 2007: 17, 54; US, 2004*b*: 10). Advantaged by extensive oil resources, other states (such as Qatar, Algeria and Venezuela) and certain regions (Central Asia and the Caspian Sea area) are expected to gain more significance as international role players (Kearns & Gude, 2008: 6). The third characterising feature of the emerging global order is the escalating impact of failed and failing states on regional and international security. In this regard Der Derian (2005: 6) states:

> Failed and failing states provide a potential refuge for transnational terrorists, transnational criminal organizations, pirates as well as drug and human smugglers. They are breeding grounds for refugee

crises, political and religious extremism, environmental degradation and organized criminal activity.

There are growing indications that international security is, fourthly, likely to be subjected to realignments in transnational political, economic and military alliances. Strategic projections, for example, foresee the interests of the US and the EU diverging to such an extent that the forging of new alliances is not improbable (UK, 2007: 44; US, 2004*c:* 57; US, 2000*b*: 8). The fifth cluster of trends associated with the emerging international security order is the pervasive influence and power being exerted by nonstate actors. The nature of such nonstate actors is wide ranging and include transnational business corporations, nongovernmental organisations, organised crime syndicates and terrorist groups (Treverton, 2005: 5; US, 2000*b*: 7, 47). The accessibility and the proliferation of substances with destructive capacity (such as nuclear and biological materials) heighten the asymmetric threat posed by nonstate actors such as terrorist and criminal groupings. Lastly, a growing body of literature in geopolitical theory and Strategic Studies poses the “digital infosphere” (digital information sphere) as the sixth dimension of strategic power analysis, alongside sea power, land power, air power and space (Rennstich, 2003: 1-2). The cyber sphere, commonly used interchangeably with the term digital information sphere, is also recognised in statutory security assessments as reinforcing its centrality as an arena of conflict in respect of both state and nonstate actors (US, 2004*c*: 16; US, 2000*b*: 6, 9).

In whatever arena, the conflict between states and nonstate actors alike over vital natural resources is intensifying (Der Derian, 2005: 5-6). The burgeoning world population, changing consumer patterns as well as the modernisation and industrialisation of countries such as the PRC and India, fuel the competition for energy, mineral and other resources (UK, 2007: 6, 32-33; US, 2000*b*: 6). In addition, climatic change is progressively expected to have a more profound impact on international security (UK, 2007: 7). While the world population is expected to increase from 6,1 billion in 2000 to 7, 2 billion in 2015, climatic change is pressurising fresh water resources and arable land (UK, 2007: 7-8; US, 2000*b*: 5). Food and water security have consequently joined energy security as permanent features on the security agendas of even prosperous nation states.

The intensification of competition and conflict over scarce resources is contributing to the widening of global inequality. On its part, the disparity in the concentration of wealth among states is accelerating mass migrations to more prosperous regions such as Western Europe and North America (Treverton, 2005: 10; US, 2004*c*: 73). One of the outcomes of mass migrations is minority ethnification which denotes the increase in diasporas of segregated ethno-communities not assimilated in host countries (UK, 2007: 10; Godson, 2001: xix). Mass migration, coupled with greater mobility and technological advances, renders nation states more vulnerable to a range of threats, varying from organised crime and terrorism to the spread of bio-pandemics (Der Derian, 2005: 7-11). Technological advances also underpin global interconnectivity and ultimately the vulnerability of nation states to the ramifications of developments in other states, regions and subregions (UK, 2007: 57-60).

The impact of the drivers of change on the nation state is of a dichotomous nature. On the one hand, dimensions of change have in certain respects infringed on the dominance of the nation state. On the other hand, forces of change are strengthening the nation state (Kearns & Gude, 2008: 6; US, 2004*c*: 30). One factor strengthening the nation state is the increasing demands on the state as 'provider' (of prosperity and welfare) and 'protector' (Quiggin, 2007: 8-10; US, 2004*c*: 61). It is doubtful whether the core functions of the state as provider and protector have changed. What is changing is the increasing complexity of the environment and the *modus operandi* of the state in executing these core functions. The role of the state and that of the provider is interwoven. These roles are distinguishable but not separable. Nevertheless, the focus of this study emphasises the role of the state as protector and therefore the guardian of national security.

3.2 SOME IMPLICATIONS OF THE STRATEGIC TRENDS FOR NATIONAL SECURITY

Risks and threats to national security, as is clear from the preceding subsection, are increasingly more diverse and diffuse. This diversification and diffusion pertain to the multiplicity of security actors and adversaries; sectors from which risks and threats emanate as well as the more unexpected and asymmetric nature of risks and threats. Moreover, risks and threats of a military, semi-military and non-military nature are merging. In varying degrees and in different permutations, the outlined strategic trends have ramifications for the national security of most, if not all states. In keeping with the focus of the study, observations are made on only some aspects considered as having high relevance.

In response to the fusion of the different categories of risks and threats, the employment by the state of its instruments of power in the protection and advancement of its vital interests is more varied and nuanced. In this regard, the related notions of ‘informational power’, ‘informational warfare’ and ‘cyber warfare’ are central to this study. Since the said concepts have only crystallised relatively recently in Security and Strategic Studies, conceptualisations and definitions are often vague, frequently divergent and sometimes even contradictory (Der Derian, 2005: 11; Parks & Duggan, 2001: 122-125; Snow, 2004: 59; Mena, 2003: 42; Rennstich, 2003: 1-5; Borden, 1999: 1; Lewis, 1998: 1; Molander *et al*, 1996: xi, 1-2, 11-12). Consequently, this study refrains from delineating these concepts on a definitional level. In an endeavour to offer some clarity, enumerative descriptions that selectively draw on elements of existing definitions are nonetheless provided.

Similar to other categories of power (political/diplomatic, economic and military), informational power is employed by a state in safeguarding national security and optimising its vital interests. In its broadest sense the informational capacity of the state encompasses, firstly, the whole body of the information at its disposal. Secondly, it denotes the systems, institutions and people that gather, store, process, communicate and otherwise utilise information. The degree to which informational capacity translates into informational power depends on the effectiveness with which the state employs the informational capacity in the defence and advancement of national security. Defensively and offensively, informational power includes the ability of the state to disrupt, manipulate and debilitate the informational capacity of an adversary. Informational warfare, simply put, refers to the state’s use of informational power to gain or maintain supremacy over an adversary (Mena, 2003: 423). Therefore, informational warfare adopts various forms like, for example, infowar. In its “most immaterial form, infowar is warring without war, an epistemic battle for reality in which opinions, beliefs, and decisions are created and destroyed by a contest of networked information and communication systems” (Der Derian, 2005: 11). In respect of the “battle” for “opinions, beliefs, and decisions”, informational warfare also includes the use of other mediums such as the print and electronic media. Cyber warfare (of which cyber espionage forms part) is, however, restricted to the digital realm of information and communication systems. In its most material dimension, informational warfare is an extension of armed conflict and includes the aim to destroy or disrupt an enemy’s informational systems.

As is clear from the above, the strategic trends shaping the international order present increasingly diverse risks and threats to national security. Simultaneously, these trends also present to the state a widening 'arsenal' for defending and advancing national security. A further consequence of the strategic trends, however, is a predicament growing in complexity, namely, which are the relevant national security interests and values the state must guard and promote? Examples of factors confounding the concrete demarcating of vital national interests, values and national security are the state's political and economic interdependence *vis-à-vis* other role players, the nature of corporate conglomerates as well as an expanding predilection among the socio-economic elités of nation states that place 'cosmopolitism' above patriotism. These factors also complicate the hierarchical order in which states - formally or informally - rank interests, namely as: indispensible to survival, vital, major or peripheral (Snow, 2004: 52). National security has, as was indicated, at its core the protection and advancement of values and interests. Therefore, alterations in delineating national values and interests hold direct implications for the 'substance' of national security and thus the direction of the statutory security apparatus. More practically, statutory security structures are consequently often faced with the practical predicament to maintain and promote national security without sufficiently clear political guidance on prioritised values, interests and thus national security (Godson, 1989: 19). Counterintelligence, in particular, has as a prerequisite a clear understanding of what information needs to be protected (Godson, 1989: 20).

Self-evidently this, or any other study, is unlikely to present a universally acceptable solution. Nevertheless, the CE framework needs to incorporate a generic postulation on the types of information that are of national security relevance and require offensive and defensive counterintelligence safeguarding. These are among the reasons for the CE framework to be not only externally but also internally (own state) directed. The 'introspective' scanning and assessment provide a basis for demarcating the information that is critical to the national security interest and thus warrant counterintelligence protection.

The utility of internal scanning extends beyond the mere demarcation of information relevant to national security. More generally, 'introspective' scanning provides direction and parameters for the optimal execution of the statutory counterintelligence missions, and ultimately counterespionage. Of equal importance in determining this direction and these parameters are challenges arising from the international security order to the statutory intelligence service of which counterintelligence is part. Therefore, the demands that the 21st century security environment pose on statutory intelligence structures will subsequently be examined.

4. THE ROLE OF, AND CHALLENGES TO, STATUTORY INTELLIGENCE IN THE 21st CENTURY

As part of the statutory security apparatus, the effectiveness of a statutory intelligence service depends on its proactive alignment to meet the challenges posed by the international and national security environment. Relative to the other security organs of states, and given the indicated changes in the macro-environment, the centrality of statutory intelligence in meeting the challenges of the 21st century can hardly be overstated. The greater dependence of nation states on their statutory intelligence services has a bearing on: (a) intelligence as a guiding instrument; (b) intelligence as an offensive and defensive instrument of power; and (c) intelligence as a 'maximiser' of other instruments of power. Resulting from the described strategic trends, factors augmenting the dependence on statutory intelligence are a combination of the following:

- The information 'explosion' which increases rather than diminishes governments' need for intelligence. The accessibility of vast volumes of information, coupled with 'real time' reporting by international and national mass media networks, results in governments being entrapped in an "information glut" (Meyer, 1987: 28). The decision maker's quandary, as described by Meyer (1987: 29-30) more than two decades ago, has subsequently deepened even further:

  > Today's senior government and business executives are choking on raw information. To their astonishment and growing distress, they are discovering that the only thing as difficult and dangerous as managing a larger enterprise with too little information is managing one with too much information ... they need it [information] in a form that they can readily absorb. That is what an intelligence outfit is designed to do.

- The exponential ascendance in importance of informational power and the cyber sphere as a 'battle ground' for competition and conflict between the nation state and its adversaries. More so than other organs of state, the core

> functions, missions, and *raison d'être* of statutory intelligence services are centred on information. The information age and the concurrent increase in the importance of informational power therefore raise the centrality of statutory intelligence as not only an "outfit" providing readily absorbable information, but also as an offensive and defensive instrument of power. Equally important, is the imperative resting on statutory intelligence to serve as 'a maximiser' of other instruments of power. The extent and nature of risks and threats combined with the escalating demands on the nation state as 'provider' necessitate sharply focused prioritisation in the allocation of limited state resources to those areas of the highest national security concern. Sharply focused prioritisation is dependent on intelligence.

The impact of the changing environment extends further than national security and the role of statutory intelligence services. It also affects the *modus operandi* of the intelligence service in the execution of its core functions. Despite their indispensability, and as an ostensible contradiction, statutory intelligence structures in certain respects compete with information and news networks that provide easy accessible, near instantaneous coverage on wide-ranging issues (US, 2007*f*: 14; Berkowitz & Goodman, 2000: 93-94). To maintain optimal relevance, statutory intelligence is required to collect, assess, and disseminate a unique product and service with a flexibility that equals, and ideally surpasses, that of its 'competitors'. Statutory intelligence has to do so considering not only the near overbearing number of open sources, but also information from clandestine sources. The sheer volume of clandestine information collected, notably SIGINT, is in itself often overwhelming and contributes to the information glut (Gill & Phythian, 2006: 70, 72). One consequence of the information overflow is the pivotal role assigned to the analysis function as arguably the most critical component of a contemporary intelligence service. The analyst serves as open-source collector, all-source information 'assessor' and the "voice" of the intelligence community (US, 2005*b*: 388, 389, 391-398). This role is fulfilled in the face of logistic-administrative constraints and without all the analysis tools available to "counterparts in the private sector" (US, 2005*b*: 388, 389, 424).

The emphasis on the centrality of analysis is relatively new, but not uniquely limited to the 21st century. On the situation before the end of the Cold War, Meyer (1987: 8-9) remarked that in "virtually all of the world's best intelligence services, the action has shifted from the operational to the analytical side." What is distinctive of the 21st century is the acceleration of this trend that outpaces the earlier expectations of authoritative authors such as Meyer.

Contrary to the fictional representation in popular culture of espionage and counterintelligence as a 'cloak-and-dagger', operationally driven domain, analysis is also at the core of the intelligence subdiscipline of counterintelligence (Scott & Jackson, 2004: 17; Godson, 1989: 160). Within the counterintelligence realm, the proliferation and diffusion of espionage risks and threats to the nation state are augmenting the pivotal role fulfilled by especially counterespionage analysis. These espionage risks, threats and challenges are addressed in the following section.

5. 21st CENTURY ESPIONAGE THREATS, RISKS AND CHALLENGES TO THE NATION STATE

Since "good CI does everything that a fully-fledged intelligence service does, and takes a hand in everything the rest of the service does", the 21st century challenges to statutory intelligence, in general, acutely affect all dimensions of counterintelligence (Codevilla, 1992: 26). Although an integral part of an intelligence service, counterintelligence has a focus distinct from the other intelligence subdisciplines. Therefore, an examination of the manifestation of espionage threats and risks facing the nation state is required. The latter is fundamental to the design of the CE framework in both its 'collection' and 'assessment' dimensions. In respect of the CE framework's dimension of information collection, the current manifestation of espionage risks and threats presents the parameters for defining the *focal points* of scanning. It is these risks and threats that the CE framework needs to identify and describe. Phrased differently, the contemporary manifestation of espionage risks and threats presents a factual basis for a 'high resolution' configuration of the CE framework towards specific issues for comprehensive, yet focused, collection. These focal points, simply put, entail providing answers to the following interrelated questions: 'Who spies?', and, 'How is being spied?' Answering these questions requires more than the mere collection of information. 'Pictures' emerging from collected information are fragmented and unfocused. Such 'pictures' lack what valuable intelligence demands, namely sharp resolution. It is especially in the counterespionage domain that risks and threats are seldom apparent or obvious. Consequently, dovetailed and in continual interaction with information collection is, as was elucidated in more detail in a preceding section of this chapter, the assessment or analysis constituent of the counterespionage framework. This section, together with Section Six, provides the factual basis for the postulation, in subsequent chapters, of variables that can guide this analysis.

Although Chapter Four outlines the challenges that the nature of espionage, counterespionage and counterintelligence pose to the CE framework, a few brief remarks in this regard are required as context for this section. Seeing that public assertions on an entity's involvement in espionage could prompt it to institute litigation, overt material often refers to espionage by certain types of nonstate actors generically and without explicitly naming such groupings. The fact that counterespionage operations and information are characteristically protected by a high degree of secrecy, thus further adds to the paucity and opaqueness of source material. Similar to the act of espionage, the countering thereof is, for a substantial part, of a clandestine nature. Therefore, documentation made publicly available by governments mostly refers to general espionage trends, while refraining from identifying and describing in detail the activities of espionage adversaries. Through inferences, however, the limitations of source material can at least partially be compensated for. Espionage is a means to an end and frequently precedes a more visible action. An act of terror could, for instance, have been preceded by espionage on targets. The act of terror is visible, although the preceding espionage might have gone undetected. Consequently, the act (preceded by espionage) and/or the existence of an adversarial relationship between the state and other actors, occasionally serve/serves as the only 'concrete' indicator(s) of espionage acts (against the nation state). It is within this context, that examples provided by this study in substantiation of arguments, should be viewed.

5.1 ADVERSARIAL ESPIONAGE ACTORS AS FOCAL POINTS OF COUNTER-ESPIONAGE ENVIRONMENTAL SCANNING

An overview and assessment of espionage conducted between the intelligence apparatuses of respective nation states serve as the premise for expanding the overview to adversarial espionage activities by nonstate actors. The reason for this approach is threefold. Firstly, nation states remain the most dominant espionage role players in the international arena. Secondly, espionage activities by nonstate actors have in certain respects been 'modelled' on statutory intelligence practice. Thirdly, and as outlined later on, espionage by nonstate actors is in some instances sponsored or supported by nation states.

5.1.1 Nation states as adversarial espionage actors

Although the resources, and probably the intelligence capacities too of some nonstate actors exceed the capabilities of some weaker nation states, statutory intelligence services by and large remain the dominant role players in the international espionage arena. Attesting to this, are recent publicly disclosed official assessments of some Western intelligence services, as well as certain secondary works (Germany, 2005: 264-281; US, 2007*b*; 1; US, 2005*b*: 486; Canada, 2003: 7-8; Northcott, 2007: 466, 468, 469; Wettering, 2000: 269-294). Neither the end of the Cold War nor the multiplication of nonstate espionage adversaries to the state has thus lessened the threat posed to the nation state by foreign intelligence services. On the contrary, indications are that state-sponsored espionage has increased. According to official estimates, for example, the number of Russian intelligence officers currently operating in the UK, is no fewer than that which represented the entire USSR complement during the Cold War (Edwards, 2006: 8). It is furthermore estimated that the intelligence services of at least 20 countries are targeting the UK (Northcott, 2007: 468), while the intelligence services of more than 50 nation states are actively conducting espionage on US soil (Wettering, 2000: 275). The total number of nation states that targeted US interests through espionage internationally, reportedly numbered 108 in 2005 (Kitfield, 2007: 2; Edwards, 2006: 8).

A hierarchical assertion, on which intelligence services are globally the most aggressive and extensively involved in espionage against other nation states, would inevitably be contestable. Furthermore, the degree to which the foreign intelligence service of one state poses a threat to another state is, as elaborated upon in Chapter Six, determined by certain variables underpinning the relationship between such states. Nevertheless, there are sufficient grounds to suggest that the intelligence services of major espionage role players globally include the intelligence services of the US, the PRC, Japan, Russia and other countries that form part of the Commonwealth of Independent States (such as Belarus, Armenia, Georgia, Kazakhstan, Ukraine and Uzbekistan), India, France, the UK, Pakistan, Germany, Israel, Italy, North Korea, South Korea, Taiwan, Egypt, Iran and Libya (US, 2007*b*: 1; US, 2005*b*: 486: Canada, 2003: 7; Burgess, 2008: 1-16; Kitfield, 2007: 1-7; Wettering, 2000: 269-294; Germany, 2005: 264-281).

As was the case during the Cold War, shared security concerns provide the basis for cooperation between intelligence services of different states. Such cooperation can be institutionalised with structures such as the North Atlantic Treaty Organisation (NATO), the Commonwealth of Independent States (CIS), or on an *ad hoc* basis (Germany, 2005: 264-281). Whether on an *ad hoc* basis or institutionalised, cooperation between states on common security concerns is self-centred and does not preclude espionage between allies. That adversarial espionage continues to traverse the 'boundaries' of alliances is one of the axioms of the international espionage terrain (Lowenthal, 2003: 114; Kalaris & McCoy, 1989: 130; US 2005*b*: 488). In this regard, Lowenthal (2003: 114) quotes a remark attributed to former US Foreign Secretary, Henry Kissinger: "There is no such thing as 'friendly' intelligence agencies. There are only the intelligence agencies of friendly powers." It is highly doubtful whether there is even "such a thing" as "friendly powers." A claim closer to reality would be that relationships of convenience exist within specific time contexts. Due to, *inter alia*, political sensitivity and the interest in broader cooperation, instances of espionage between 'allies' are infrequently exposed. This infrequency in reporting does, however, not equate with the absence of spying between 'friends'. Lowenthal's (2003: 114) remark that the US, UK, Australia and Canada do not spy on one another is therefore rather perplexing and perhaps alludes to formal intelligence cooperation agreements. With this *caveat*, a privileged relationship indeed exists between the US, UK, Australia and Canada. These countries, for example, share a signal interception and deciphering system called Echelon.

Illustrating the self-centred nature of alliances between the intelligence services of different nation states, are wide-spread allegations by Western European countries that the US supplied the country's companies with Echelon-generated intelligence (to the detriment of Western European economic interests). Reflecting this growing mistrust is the European Parliament's appointment in 2000 of a commission to investigate whether "the United States is spying on European business" and, as part of the inquiry, to "scrutinize the Echelon spy system" (Nasheri, 2005: 23, 24). On its part the US, counter accuses particularly France of aggressively targeting the US for espionage and infiltrating companies such as IBM, Texas Instruments and Corning (*Industrial Espionage News,* 2008: 7-10).

The aforementioned allegations and counterallegations are underpinned by a primary battle line international espionage arena in the 21st century, namely economic espionage. While alliances during the Cold War were mainly formed around military cooperation, the economic advantage of respective nation states features as a powerful cohesive force in contemporary positioning. In the post-Cold War era, nation states prioritised their support of 'national' private enterprise in respect of both intelligence and counterintelligence support. Economic espionage, defined as espionage between nation states in the economic and technological sphere, has consequently crystallised as the international battle cry of the 21st century's statutory intelligence services. Information sought by means of economic espionage pertains to aspects such as aerospace, biotechnology, chemicals, communications, information technology, mining and metallurgy, nuclear energy and 'know how', oil and gas, as well as environmental technologies (Canada, 2003: 8).

Given the reality of the 21st century, it is hardly conceivable that the intelligence services of a nation state would not have economic espionage as a primary collection priority. Countries known to have prioritised foreign economic intelligence gathering, to list but a few, include: Russia, the PRC, Cuba, Japan, the US, France, Algeria, Italy, Azerbaijan, Belarus, Moldavia, Israel, India, Turkmenistan, Ukraine, Georgia, Iran, Iraq, Libya, Syria, Taiwan, Pakistan and Uzbekistan.

5.1.2 Private enterprise

Private enterprise, as mostly embodied in companies, is not only a passive recipient of intelligence gathered by nation states. Companies are frequently used by statutory intelligence services in the gathering of economic, technological and other categories of intelligence. The FBI, for example, estimates that the PRC utilises more than 3000 businesses in the US as "front companies" for espionage (Kitfield, 2007: 2). In more authoritarian regimes, such as the PRC, the demarcation of the cooperation between statutory intelligence and 'national' companies in espionage and counterintelligence endeavours is, relative to liberal democracies, less complex. One factor compounding such a demarcation in liberal democracies is transnational ownership and joint ventures as chartering features of global enterprise. Even the arms industry that is of high national security importance is, in this sense, often multinational rather than a strictly 'national' enterprise. Further complicating the relationship between state and enterprise, insofar as espionage and counterintelligence are concerned, is that intense competition for government contracts could result in a government being targeted by the country's 'own' business enterprises. An example would be a company's illegal or irregular procurement of information on tenders submitted by other companies competing for government contracts.

Congruent with this reality, the CE framework considers corporations as distinctive espionage role players and thus focal points of scanning. Such a supposition is supported by the power some multinational companies and super-empowered individuals yield. In a relatively recent survey of the 150 largest economic entities in the world, 97 were found not to be nation states but companies and transnational conglomerates (Berkowitz & Goodman, 2000: 7).

The persuasive power and influence corporate conglomerates yield in the international arena is, in itself, not sufficient justification for the inclusions of such entities as focal points of the CE framework. Similarly, the fact that such entities are in competition or conflict with a government is supportive, but not adequate, validation. The decisive factor to be considered is the degree to which such conglomerates' power translates into espionage capacities that can be employed against the nation state and its interests.

During the past two decades, it has generally been accepted that business, in the 'age of intelligence', depends on effective environmental scanning and intelligence for its survival and success. In this regard Meyer (1987: 8) states: "Throughout the world of commerce and industry, 'intelligence' is on its way to becoming a key management tool for corporate chief executives and their policy making lieutenants." Assertions such as those by Meyer are used with reference to the practice of Competitive Business Intelligence, of which 'competitor intelligence' forms part. By definition competitor business intelligence entails the use of legitimate methods and open sources. Various, if not the majority of large international enterprises, possess such business intelligence capacities. These include: Motorola, Sony, Shell and most other international oil companies, as well as mining enterprises with international interests (Hall, 2005: 4; Eells & Nehemkis, 1984: x). Commenting on this trend, Brenner (National Counterintelligence Executive of the US) recently stated at least on two occasions that: "The world is also moving toward *private* intelligence. The corporate world creates, commissions, and buys intelligence analysis to a degree that would surprise many of our colleagues" (US, 2007*e*: 15; US, 2007*f*: 14; emphasis in originals).

Within the legislative dispensation of liberal democracies, Business Intelligence is a legal practice. Legal also is the vast range of services rendered to private enterprise (and governments) by companies specialising in Business Intelligence and other security services. These services vary from the more mundane (alarm installation and response functions, private and forensic investigations, close personal protection) to the more controversial (military services). Better known companies rendering one or more of these services include: Group4Securicor, ADT, DynCorp, Kroll Associates, Control Risks Group, Haliburton Corp, CACI, and Titan (Schlesinger, 2004: 1-3; Miller, 2003: 1; Holmqvist, 2005: 57; *Industrial Espionage News*, 2008: 3).

Undoubtedly, a substantial part of private enterprise engages in legal Business Intelligence and the larger part of security services rendered is *bona fide*. However, the tacit impression, projected in some secondary sources dealing with statutory intelligence (Burgess, 2008: 1-11; Wettering, 2000: 265-300) of foreign intelligence services as the overpowering actors at the centre stage of economic/industrial espionage is incongruent with reality. Industrial espionage is still more prevalent than economic espionage. In other words, the extent to which business entities engage in illegal clandestine collection (espionage) in the economic and technological fields exceeds that of cases sponsored or conducted by foreign intelligence services. In its 2004 report the US Office of the National Intelligence Executive (as quoted by Kabay, 2008: 7-8) provided the following statics in relation to attempts to illegally acquire sensitive technology from the US:

> [F]oreign state actors accounted for about one-fifth of suspicious incidents and government-related organizations accounted for another 15 percent ... Commercial organizations and private individuals with no known affiliation to foreign governments together account for nearly half – 36 percent and 12 percent respectively – of all suspicious incidents. In another 16 percent, the contractors were unable to determine the affiliation of the foreign parties involved in the elicitation.

Evidently, such espionage is to the disadvantage of competing businesses and in some instances it is in contravention of legislation and/or to the direct detriment of the nation state. The widely reported case of Boeing's illegal procurement of proprietorial information from Lockheed in a bid to secure a US Air Force rocket contract, serves as an example. In 2003, the US government suspended Boeing's rocket division from further contracts after an investigation found Boeing to have obtained, through industrial espionage, more than 66 000 pages of proprietorial information from Lockheed (Bowermaster, 2005: 1-7). Two more recent incidents pertain to Russia and South Korea respectively. In 2007, South Korean authorities indicted employees of Korean auto-manufacturers and steel producers for illegally procuring, through industrial espionage, key technologies from other Korean firms and sharing that information with Chinese firms (Burgess, 2008: 11). The Russian Federal Secret Service (*Federal'naya sluzhba bezopasnosti Rossiyskoy Federatsii* - FSB) detained two employees of the oil firm TNK-BP on allegations of industrial espionage in March 2008 (*The Earth Times,* 2008/02/20). According to Russian authorities the industrial espionage was conducted to the direct detriment of that country's (national) economic interest (*The Earth Times,* 2008/02/20).

Even if a case of reported industrial espionage was not directed at the state, as such it obviously demonstrates a company's *ethos* and capacity to engage in espionage. This capability could have been directed against a nation state(s). German authorities, for example, are currently investigating allegations that the telecommunications giant Deutsche Telekom, which competes extensively on the (German) local and international market, employed illegal, clandestine methods in the gathering of intelligence (*Spiegelonline*, 2008/05/26). It must be indicated that the actual acts of espionage are not necessarily executed by corporate entities themselves. The espionage can be wholly or partially outsourced to other parties, notably individuals or companies within the private security sphere. The outsourcing of the physical perpetration of industrial espionage, particularly to individuals or companies within the private security sphere, offers a lower risk and presumably a more cost-effective avenue (Crane, 2003: 1- 5). It therefore also offers an attractive proposition for other adversaries hostile to a nation state – including other nation states.

5.1.3 Organised crime groups as a civilian counterintelligence concern

In general, however, the private security industry, other fields of private enterprise and governments are united in combating a common adversary, namely organised crime. This study views organised crime syndicates as espionage adversaries of such increasing influence that they warrant inclusion as a focal point of the CE framework. Relevant in this regard is the following remark by Steele (2001: 94; emphasis added): "Today we are in a world in which transnational criminal gangs have more money, better computers, *better information* and [are] vastly more motivated to act and act ruthless than most states." While the combating of crime falls within the mandate of statutory police forces, crime is also of (civilian) statutory counterintelligence concern due to two inter-related factors. Firstly, some organised crime syndicates possess intelligence gathering capacities targeting the interest of the state. Secondly, the endeavours and intelligence capacities of certain crime syndicates are interfaced with the activities and intelligence capacities of other espionage adversaries such as terrorist groups and even some nation states (Godson, 2001: xxiii). Crime syndicates form alliances with and take control of regions within failing and failed states (US, 2004*c*: 96). Crime syndicates known to possess intelligence capacities include the Chinese triads, the Russian and Italians mafias, the Japanese yakuza, Columbian cartels, and Nigerian criminal organisations (Williams, 1997: 321, 327; 333). The intelligence capacities of organised groupings are augmented by the cooperation that exists between such networks (Williams, 997: 328). The US Federal Bureau of Investigation (FBI) projects that "criminal groups will expand their intelligence capacities to thwart law enforcement investigations" (2004*c*: 17).

5.1.4 Nongovernmental organisations as espionage actors

While ostensibly the normative anti-pole of organised criminal syndicates, this study contends that nongovernmental organisations (NGOs) also present espionage actors of relevance to state security. NGOs are deemed as mostly non-profit groupings mobilising around issues varying from ethical and humanitarian causes to environmental concerns (US, 2007*d*: 2). Examples of prominent NGOs include Greenpeace and Amnesty International (Berkowitz & Goodman, 2000: 7). It is estimated that international nongovernmental organisations (INGOs) alone have grown from 4 518 in 1988, to in excess of 25 000 in 2001 (Godson, 2001: xxxi). The sheer number of NGOs raises the question as to which of these are of statutory intelligence concern. In the words of Berkowitz & Goodman (2000: 8): "So, whom should the intelligence community be watching; and what threats should it be worried about? The answer is *all of them, potentially*." Given the limited source material in the public domain of NGOs engaging in espionage against the state, a question could justly be raised on the inclusion of this sector as a focal point of the CE framework. In response, it must be emphasised that the CE framework is proactive in its design. Therefore, categories of role players, which are likely to be increasingly of high counterintelligence relevance in the near future, should be included as focal points for environmental scanning. NGOs, it is argued below, constitute such a category.

NGOs are recognised as forces within the societal sector with increasing relevance to, and in some instances in competition with the nation state (Treverton, 2005: 5). Mounting mobilisation around issues such as the environment and (anti-) globalisation increasingly put the agendas of NGOs in conflict with the policies and practices of governments. From a counterintelligence perspective, this intensifying conflict serves as a motive for NGOs, and individuals that form part of such movements, to procure sensitive and classified governmental information. This information typically forms part of exposés of governmental practices perceived to be contradictory to 'good governance' and the cause of an NGO. In 1999, for example, the Russian government charged an environmental activist with treason and espionage for exposing the Russian Navy's practice of dumping nuclear material (*EUR News Service*, 2000/11/20). As this study is not intended as a normative guide to ethical governance, the Russian government's action is immaterial (to the focus of this study). The CE framework is designed around the premise that the state could perceive such incidents as espionage and as compromising sensitive or classified information. It can reasonably be accepted that, albeit with different permutations, incidents such as the example quoted will increase in frequency and occurrence in other nation states.

The counterintelligence relevance of NGOs extends beyond the concerns nation states could have over the compromising of sensitive information. NGOs are also attractive targets for exploitation by foreign intelligence services, both as cover for espionage and as instruments of influence. The counterintelligence relevance of NGOs is reflected in a recent discussion document of the US National Intelligence Council (2007*d*) entitled *Nonstate actors: impact on international relations and the implications for the United States.* The document firstly signifies a concern that "nongovernmental organisations" – in which foundations of "philanthropist capitalists" such as Gates, Soros and Branson are included – exert power and influence that could be detrimental to US interests. It is further noted that NGOs such as "the Gates Foundation have greatly expanded notions of what a charitable NGO *should look like*" (US, 2007*d*: 1; emphasis added). Secondly, concern is expressed that countries such as the PRC and Russia, have been "highly effective" in not only suppressing "benign nonstate actors", but also:

> In creating their own substitutes, some of which have demonstrated their power to counter US objectives and even to challenge global rules of engagement ... From that standpoint, a key concern for the

> United States may not be that these actors have become too powerful, but that in many parts of the world their influence is limited – a factor that is contributing to the tilting of the global playing field away from the United States and its developed-world allies.

A further conclusion reached in the US (2007*d*: 5) National Intelligence Council's document reads as follows:

> Although their [nongovernmental organisations'] relationship with national governments may be somewhat adversarial, they have significant influence on policy formation and may even be employed by states as a means of outsourcing foreign policy.

As is clear from the above, NGOs are regarded as entities that exert influence both advantageous and disadvantageous on the nation state – in this case the US. In the context of the US document and even more so in the lexicon of statutory intelligence practice, notions such as 'foreign policy', 'influence', 'adversarial', and 'may be employed as a means', are seldom far removed from 'intelligence targets', 'potential to exploit for informational covert action', and 'potentially useful for intelligence gathering'. In the view of at least the Russian government, NGOs are indeed exploited for espionage purposes. In 2006, Russia placed a moratorium on the activities of several NGOs (such as Human Rights Watch, Amnesty International, the National Democratic Institute, and the International Republican Institute) on the grounds that they were "harbouring" spies (Chivers, 2006: 1).

5.1.5 The mass media as focal point of counterespionage environmental scanning

Similar to nongovernmental organisations, the interface between the nation state and the journalistic sector invokes controversy on a normative level. The issue of the relationship between journalism and statutory intelligence, for example, was especially prominently debated in the US in the mid-1990s. This discourse was fuelled, in 1996, by the release of the report on US intelligence-gathering policies and practices by the US Council on Foreign Relations (Houghton, 1998: 1). The report concluded that the CIA extensively used journalists for the gathering of intelligence. Inadvertently, and contrary to the intention, the report prompted the passage of the first US law that sanctioned the utilisation of journalists for statutory intelligence practices (Upano, 2003: 2-3; Houghton, 1997: 1-2). A comment in the same year by Maj. Gen. Kobaldze of the Russian Foreign Intelligence Service (*Sluzhba Vneshney Razvedki* - SVR), in partial response to the furore in the US, aptly summarises the reality of the interface between journalism and intelligence (Upano, 2003: 3; Houghton, 1997: 2):

> There is no essential difference between the work of a spy and a journalist; both collect information in the same way - just the end consumers are different. Journalists make the best spies; they have more freedom of access than diplomats. The Americans' moral stand on not using journalists is artificial, and not a little duplicitous.

There are no signs that the practice of utilising journalists, and journalistic cover, for espionage purposes has receded in the decade subsequent to Kobaldze’s statement. Indications are that the use of journalists and the employment of diplomatic cover by the CIA, FBI and even the US Internal Revenue Service, are continuing (Upano, 2003: 1-4). This is also the case in respect of the other intelligence services. In 2007, the Swedish Security Service reported that (unnamed) foreign intelligence services persisted in using journalistic cover in their espionage endeavours (Burgess, 2008: 6). That trend was confirmed by the Czech Republic’s counterintelligence service, which specifically mentioned that “Russian intelligence officers are operating as journalists” within that country (Burgess, 2008: 6).

As is the case with NGOs, the media’s counterintelligence relevance extends beyond its exploitation as a cover and instrument of espionage. The mass media has a pervasive influence on domestic and international perceptions. The latter, in turn, are central to a nation state’s corporate image and have direct implications for vital national interests. The nation state’s corporate image affects its diplomatic and economic relationships with other states and nonstate actors. The importance of the mass media to the corporate image of nation states was clearly illustrated in the aftermath of the US-led invasion of Iraq. Negative international perceptions of this invasion underscored the significant role of the media in respect of informational power. Albeit for a large part euphemistically phrased, assessments by the UK and US statutory intelligence communities have as a central theme the ‘managing’ of international perceptions (UK, 2007: 40 - 42; US, 2005*c*: 1). Put more bluntly, the mass media is pivotal to effective informational warfare. In an article commended with a US Army award, Ecklund (2005: 1) asserts that:

> Few Americans would argue that the US is not currently experiencing the result of a gradual decline in its global image ... This essay will

> prescribe a new paradigm for managing strategic communications within the framework of information as an instrument of state power. Informational power refers to a country's ability to control and influence world opinion through informational channels.

Statutory security structures will obviously refrain from publicly declaring their intention to use the media as an instrument of informational covert action. At best, a permeable line divides, on the one hand, the "control and influence of world opinion" from, on the other hand, informational covert action. Similar to the thwarting of clandestine collection, the countering of informational covert action is (as was indicated) a counterintelligence function. The countering of informational covert action is thus dovetailed with the counterespionage responsibility of detecting and neutralising the exploitation of the media for espionage purposes.

The inclusion of the mass media as a focal point of the CE framework is further validated by the counterespionage relevance of the media 'in its own right' (in other word 'divorced from its exploitation by adversarial intelligence services'). Journalism in general including investigative journalism in particular, has at its core the reporting of the publicly unknown. Consequently information deemed by the state as of national security relevance is procured, as implied by Kobaldze's statement, through methods which practically equate with espionage. Such practices are prohibited even in Western democracies. Northcott (2007: 476), for example, observes that changes to the UK's *Official Secrets Act* removed the "public interest defensive clause" previously resorted to by investigative journalists (Northcott, 2007: 476). The question of classified information contained in media reporting is equally topical in Germany. During 2007 it emerged that 17 journalists from leading publications such as *Der Spiegel*, the *Süddeutsche Zeitung*, *Die Zelt,* and *Die Welt*, were investigated by German authorities for having quoted from classified documents (Penketh: 2007, 1; *Spiegelonline*, 2008/04/25; Jackson, 2008: 1-4). The US government has also, as part of a commission report (2005*b*: 381) voiced concern over the "problem of media leaks." The report (US, 2005*b*: 381) states that "hundreds of serious press leaks have significantly impaired U.S. capabilities against our hardest targets ... we detail several leaks that have collectively cost the American people hundreds of millions of dollars, and have done grave harm to national security."

5.1.6 Terrorist and other extremist groupings

While a news item in some instances acts as a concrete manifestation of journalistic espionage, acts of terror often serve as more chilling signposts of extremist groupings having procured (through espionage) information of national security relevance. Arguably the most graphic example in this regard is the terrorist attack of 9/11. In a US Commission *Report to the President of the United States on the intelligence capabilities of the United States regarding weapons of mass destruction*, terrorist groups such as Hizbollah and al-Qaeda are described as conducting "classical intelligence activities" against the US (2005*b*, 488). The report continues by referring to a senior CIA counterintelligence officer's assessment that "the [Central Intelligence] Agency is only just beginning to understand the intelligence capabilities of terrorist organizations"(US, 2005*b*: 488). It is estimated that in total "some 35 suspect terrorist organizations target the United States or its interests for intelligence collection principally through human espionage." (Van Cleave, 2007: 4). The FBI expects the targeting of US law enforcement agencies by not only foreign, but also domestic extremist groups, to significantly increase in the near future (US, 2004*c*: 26-27). Such 'targeting' of course also includes espionage directed against these law enforcement agencies. Although the references made in respect of the espionage risks and threats posed by extremist and terrorist groupings pertain to the US, there would be little disagreement that such groupings are of counterintelligence concern to nation states in general.

5.1.7 Unaffiliated espionage actors

Whereas the rationales of extremist and terrorist groups are frequently of a political/ ethno-religious nature, the motives of another category of espionage actors are more difficult to define. This category consists of individuals and groups driven by varying motives, acting on their own accord and not 'affiliated' to other espionage actors already discussed. Financial gain may play a role, but it is not the sole motivational factor. The gratification ('thrill' or 'revenge') of succeeding in obtaining government secrets appears to supersede material considerations frequently (Nasheri, 2005: 114). Whatever the precise motivation, the cyber sphere serves as an easy and accessible low-cost conduit for espionage by unaffiliated groups and individuals (Nasheri, 2005: 114). Such individuals and groups pose espionage risks and threats of such significance that they warrant inclusion as focal points of the CE framework. Since the relationship between ‘hacking’, ‘espionage’ and ‘counterintelligence’ is discussed later in this chapter, only two examples are concisely mentioned here:

- McKinnon, a British citizen, faced extradition to the US in 2008 on charges of repeatedly hacking into dozens of computers used by the Pentagon, the National Aeronautics and Space Administration (NASA), the US Army, the US Navy, and the US Air Force (Grant, 2008: 2-3; *Global Security System*, 2006: 1). Damage caused by McKinnon to US information systems and data files, during the period February 2001 to March 2002 is estimated to have been in the region of £350,000 (Grant, 2008: 2-3). McKinnon‘s actions appear to have been motivated by his “curiosity” and conviction that the US government has undisclosed evidence of extra-terrestrial life and energy forms (Grant, 2008: 2-3; *Global Security System*, 2006: 1).

- In 1999, unidentified hackers reportedly seized digital command of a UK military satellite and demanded money in exchange for the ‘return’ of its control (Christensen, 1999: 2).

5.1.8 “A wilderness of mirrors” – alliances between espionage adversaries

While the preceding paragraphs followed a particularised approach in advancing espionage adversaries as focal points, it must be noted that the nation state faces a reality in which the various espionage adversaries are interlinked. Such links exist between and among nation state and nation state(s), nation state(s) and nonstate actors, and nonstate actors of various categories. Insofar as adversarial espionage alliances are concerned, the nation state is thus, to borrow a phrase from Angleton (a former head of CIA counterintelligence), confronted with a “wilderness of mirrors” (Henwood, 1988:1). Due to limitations in source material it is not possible, and it would indeed serve little purpose, to explore the diversity of such alliances in full. Some examples, even if based on inferences, are nevertheless required to elucidate the diversity of alliances between the espionage adversaries of the state. Terrorist groups such as Hizbollah, for example, are sponsored by the state actors Iran and Syria (US, 2007*b*: 2; Canada, 2003: 5). It can reasonably be accepted that the cooperation between these state and terrorist groupings extends to assistance and mutual collaboration in espionage. In a similar vein, partnerships between terrorists groups and crime syndicates are increasing (US, 2004*c*: 17). Enabled by the extent and nature of their networks, some criminal syndicates have the capacity to provide components of WMDs to "pariah states" and terrorists (Williams, 1997: 330, 331, 333). Since secret government information is also a prized commodity, a logical inference would be that cooperation between terrorist groups, crime syndicates, and "pariah states" also extends to espionage against (other) nation states.

In summary, the nation state faces espionage adversaries that vary from individuals and small groupings to intelligence services which command vast resources. Around common interests these adversaries form alliances in permutations that pose espionage risks and threats that are multi-faceted and frequently interwoven. These espionage adversaries, individually and in combination, serve as focal points of the CE framework. Undoubtedly pivotal to the CE framework, the mere identification of adversarial espionage role players is insufficient; for it is the acts of espionage that constitute the substance of the risks and threats to the nation state. The reality of espionage sources and methods in the 21st century are therefore part of the focal points of the CE framework and require examination.

5.2 ADVERSARIAL ESPIONAGE COLLECTION – SOURCES AND METHODS

Against the background of the above, this subsection attempts to answer the problem statement: ''How do adversaries 'spy' on the nation state?'' To this end, contemporary sources and methods employed by espionage actors are examined. As OSINT is discussed in more detail in Chapter Four, only brief remarks will be made here. This subsection distinguishes between the categories of information espionage adversaries collect and the methods (tools) employed in the collection of such information. Expanding on the premise set out in Chapter Two, it is argued that the collection methods transverse the categories of information gathered. The same collection 'tool' can, in other words, be employed for the gathering of more than one 'type' of information. Given the interwoven nature of methods and categories of information, a certain degree of overlapping is inevitable in the discussion that follows.

5.2.1 Categories of information collected by espionage adversaries

Like the intelligence service(s) of the nation state itself, espionage adversaries would for the most part endeavour to collect a combination of principal categories of information, namely open-source information, grey-source information, and information generated through clandestine sources. Since the notions of 'espionage' and 'counterespionage' in conventional conceptualisations centre on clandestine information, a question could arise as to the relevance of addressing the other categories of information sought by an espionage adversary in this study. Reality, of course, is not conventional, it is increasingly unconventional. The distinction between grey-source information and clandestinely procured information is, as the term suggests, 'grey'. Moreover, an adversary's collection of open and grey-source information serves as a vital indicator of its undetected clandestine collection efforts. By definition, open-source and grey-source intelligence collection is not clandestine and, from a counterespionage perspective, such endeavours could be more readily identifiable. Therefore, as pointed out later in this chapter, the adversarial collection of all three information categories has implications for counterintelligence countermeasures. A further compelling reason for distinguishing between the different categories of information relates to the study's primary research theme: the use of open sources. By implication, open-source information is that category of information that excludes information originating from grey and clandestine sources. Since open and clandestine sources are opposites on a notional level, differentiating between these two categories is fairly unambiguous. More complex, yet critical to the focus of this study, is differentiating between open-source and grey-source information. This section demarcates 'grey sources' mainly from the perspective of a category of information collected by espionage adversaries. By delineating the boundary between grey and open sources, a basis is thus provided for a more detailed examination of OSINT in relation to counterespionage, later on in the study.

5.2.1.1 Open-source information

Open-source information is publicly available and obtainable at a relatively low cost. Examples include newspapers, books, the Internet, academic journals and publications, open-source imagery, radio and television broadcasts, certain governmental databases, business reports and the like (Quiggin, 2007: 161-162; Gill & Phythian, 2006: 63-64). With some exceptions, literature reviewed tends to equate 'open sources' with 'open-source intelligence' and uses these terms interchangeable. However, as will be elaborated upon in Chapter Four, the concept OSINT is more encompassing and denotes much more than the mere use of open sources. It would have been noticed that the examples of open sources listed above include 'open-source imagery'. Imagery Intelligence (IMINT) as described in more detail below, forms part of TECHINT. Companies such as

Google present Internet imagery of up to one metre resolution (Quiggin, 2007: 174). Open-source imagery thus serves as one example of open sources, which includes TECHINT.

5.2.1.2 Grey-source information

Steele (2001: 118-119), one of the foremost proponents of OSINT, defines “grey literature” as “information that is both legally and ethically, available, but only from specialized channels or through direct ... access” and often at substantial cost. The following more useful and detailed description is forwarded by NATO in its *Open source intelligence handbook* (2001: 8-9):

> Grey literature includes working papers, pre-prints, technical reports and technical standards documents, dissertations, data sets, and commercial imagery. Producers of grey literature include: non-profit and educational organizations; commercial enterprises creating documents for internal use as well as clients and suppliers; local, state, and national government agencies producing materials for internal use as well as for citizens and vendors, and, a wide variety of informal formal associations, societies, and clubs. Examples include university yearbooks, yacht club registers, corporate trips reports, and personal notes from public events that are posted to a public bulletin board, [as well as] overt human experts and observers.

Four aspects emanating from NATO’s description of grey sources are particularly relevant to this study. Firstly that grey sources include dimensions of HUMINT (‘overt experts and observers’) and variations of TECHINT (‘commercial imagery’). As opposed to freely available ‘open-source imagery’ with a resolution of up to one metre, ‘commercial imagery’ with a finer resolution (of up to 20 cm) is obtainable at a substantially higher cost (NATO, 2001: 9-11). Commercial imagery is thus considered as part of grey sources, while open-source imagery forms part of open sources.

A second aspect emanating from NATO’s definition that warrants inclusion is grey-source ‘materials’ produced by “local, state, and national government agencies ... for internal use as well as for citizens and vendors.” An imperative rests on a government, specifically as part of counterintelligence, to ensure the accurate classification of information. Deficiencies in the classification of information effectively put information relevant to national security in the open source and grey source domains. Deficient classification will therefore aid adversarial collection. Thirdly, and of equal counterintelligence relevance, is the role that visits by 'outsiders', to *inter alia* government institutions, play in the collection of grey-source information. The information garnered during such visits is not necessarily the result of illegal actions (such as the theft of documents). Grey-source information can be procured merely through expert observation. Illustrative in this regard is a finding in 1999 by the Cox Committee which investigated the PRC's espionage against the US. The committee concluded that the PRC "relies heavily on the use of professional scientific visits, delegations, and exchanges to gather sensitive technology" (Wettering, 2000: 269). The Cox Committee appealed for circumspection in the hosting of visits to sensitive facilities (Wettering, 2000: 269). Concerns over the use of such visits to procure information to the detriment of national security are not limited to the US. Such concerns have also been raised by, *inter alia*, the governments of the UK and Canada (Canada, 2003: 8; Kabay, 2008: 3).

A fourth aspect resulting from NATO's description pertains to the omission of legal considerations as part of the defining of grey sources. 'Grey', this study posits, also has a bearing on the area of uncertainty between legal and illegal (mostly clandestine) collection of information. What constitutes 'legal collection' or 'illegal collection' of information would evidently be determined by the legislation of a specific country. That a 'grey area' exists between illegal and legal collection is indisputable. The definition of the concept 'grey sources' should consequently also include information generated by methods of uncertain legality as well as through questionable methods. An example from the Competitive Business Intelligence field serves as elucidation. Self-regulatory bodies such as the International Society of Competitive Intelligence Professionals adhere to codes that prescribe information to be used by its members and affiliates as limited to open sources and *bona fide* sources available at a cost (Nasheri, 2005: 76-78). The utilising of information procured through methods such as reverse engineering and 'dumpster diving' falls outside these parameters. In private security industry lingo, 'dumpster diving' denotes the searching through of refuse and discarded materials (Kabay, 2008: 4). The said methods are also prohibited in the policies and procedures of reputable companies that either possess their own Business Intelligence structure or outsource this function to specialised companies. Policies and reality are often widely divergent and the methods described are not uncommon. One widely reported incident of industrial espionage in the US, involving the US "archival branded-goods companies" Unilever and Proctor & Gamble, serves as illustration (Crane, 2003: 4). In 2001, it emerged that private investigators hired by Proctor & Gamble gathered unshredded documentation relating to Unilever's marketing plan for a new product. Although not illegal, this 'dumpster diving' transgressed Proctor & Gamble's "internal guidelines on intelligence gathering" (Crane, 2003: 4). Since Proctor & Gamble possessed a Business Intelligence capacity, the company's pretext of "supposedly 'rogue operators' who had apparently overstepped the mark in their eagerness to provide high level intelligence", was transparently questionable (Crane, 2003: 4-5). Questionable methods, and the outsourcing of higher risk, grey-source gathering, are of course not limited to nonstate actors. They also form part of, and are in certain respects modelled on, the *modus operandi* of statutory intelligence services.

5.2.1.3 Information from clandestine sources

Describing the notion 'collection of clandestine information', this study argues, can essentially be reduced to two interrelated aspects. Firstly, it has a bearing on the nature of the information. 'Clandestine' in this context suggests information that the custodian ('owner') regards to be of such a sensitive nature that the unsanctioned disclosure thereof would be detrimental to the custodian's interest. In the statutory milieu, such information would mostly be protected through classification and other security measures. In the private sector, such information is deemed as 'proprietary sensitive' and is often also subject to protective measures. Secondly, 'clandestine' refers to the *modus operandi* employed in procuring information. Since an espionage adversary seeks information to which open access is denied, the procurement thereof requires clandestine activities. Clandestine collection activities are characterised by an endeavour on the part of the adversary to achieve one or more of the following, namely to: (a) conceal the activity of collection; (b) circumvent protective measures; and (c) conceal the identity of the sponsor (namely the adversary itself) and/or the collector.

5.2.2 Collection disciplines – the tools of collection

From whatever source, espionage entails the utilisation as 'tools' of collection a combination of humans (HUMINT) and 'machines' (TECHINT). A central theme in the review of these methods is the following problem statement: which, and to what degree do certain methods remain within the prerogative of the nation state? This statement has a direct bearing on the counterintelligence and notably counterespionage measures employed by the state. The same methods employed by espionage adversaries against the state are utilised by the state as part of counterintelligence in general and counterespionage specifically. A central contention is that clandestine collection methods, once the prerogative of nation states, are increasingly at the disposal of nonstate espionage adversaries. The proliferation of clandestine collection methods therefore needs to be considered in the design of the nation state's counterintelligence efforts (of which the CE framework forms part).

5.2.2.1 HUMINT collection

HUMINT pertains to the procuring of information through interpersonal interaction with and by humans. Serving as examples of open-source HUMINT collection are interaction with readily accessible experts (at little cost) and the attendance of seminars (also at little cost). In its dimensions as grey-source collection, HUMINT includes the interaction with experts that charge consulting fees and/or the participating in seminars on invitation and at cost.

The clandestine gathering of intelligence through HUMINT is commonly referred to as 'espionage'. As was noted in Chapter Two, the period between the end of the Cold War and 9/11 was characterised by an increasing reliance on SIGINT and a concurrent decrepitude of especially Western intelligence services' HUMINT capacities. It was also noted that the Islamic extremist terror attacks against notably the US and UK, as well as the controversy over US and UK intelligence-based allegations on Iraq's possession of WMD, highlighted the penalty for such neglect of HUMINT. Subsequent governmental bodies of inquiry in the UK (2004: 107-111) and the US (2004*a*: 24-27, 260-263) concluded the neglect of HUMINT to have been among the primary reasons for these intelligence failures. While neglected in several Western intelligence services, HUMINT continued to be afforded a high priority by intelligence services in general. Wettering (2000: 331), for example, states: "Most of the more than 50 foreign intelligence services which operate in the United States (and numerous which operate against Americans when they are abroad), practice ethic recruiting." Since ethnic recruitment is a *modus operandi* within the HUMINT realm, Wettering's observation serves to illustrate the continued importance intelligence services generally attach to HUMINT. During the past three years relatively broad agreement emerged in literature that the current use of HUMINT is at least equal to, but more likely exceeds the Cold War levels.

As was illustrated in the preceding sections, the espionage activities of state and nonstate actors are intertwined. On the one hand, the state employs nonstate actors as part of its HUMINT collection efforts. On the other hand, nonstate actors target the state by means of HUMINT collection. To limit repetition, only one example illustrating a nonstate actor's targeting of the governments of several Western European nation states, through collection methods that included HUMINT, is provided. In 2006, Italian authorities arrested and charged 21 individuals for illegally collecting and storing personal information on politicians, chief executive officers of companies, bankers, soccer players and 'common citizens' (*European Tribune,* 2006/10/03). Evidence seized by the Italian police included documents originating "from police and intelligence services of other European nations" (*European Tribune,* 2006/10/03). The arrest warrants listed allegations that included, amongst others, the illegal possession of government documents, violation of state archives and police records, corruption, blackmail, intimidation and the impersonation of public officials. The leading figures in this criminal spy ring were a former high-ranking member of the Italian security forces (at the time of his arrest the head of security at the company Telekom) and the owner of a private security company (*European Tribune,* 2006/10/03). The financial power yielded by this criminal 'spy ring' is reflected in the fact that the seized assets of just one of the suspects amounted to € 210 million (*European Tribune*, 2006/10/03).

The example above further validates a previous assertion that, within the reality of 21st century international espionage, the intelligence capabilities of nonstate actors in all likelihood exceed that of some states. Even within this reality, some clandestine HUMINT collection methods remain within the prerogative of the nation state. These exceptions are related to the recognition of the nation state as a sovereign geopolitical authority. This recognition translates practically into diplomatic status and protection that the nation state's representatives enjoy in other countries. In one form or the other, nation states' missions in foreign countries have, over centuries, provided platforms for clandestine HUMINT collection. In the contemporary era such missions typically take the form of High Commissions, embassies, consulates and diplomatic offices. They serve as a basis for HUMINT espionage mainly in three ways. Firstly, as part of its diplomatic corps, and depending on the relationship with the host country, a nation state includes members of its statutory security apparatus. Declared to the host country, the function of such intelligence officers is to liaise with the security structures of the said country on matters of mutual intelligence concern. In practice, and additional to official liaison, declared intelligence officers are frequently also involved in clandestine HUMINT collection through the 'handling' of source networks. These handlers enjoy diplomatic immunity that their sources ('agents') mostly do not. Adding to the nuanced nature of clandestine HUMINT is the variety in categories of agents 'serviced' by handlers. Since these categories of HUMINT sources also form part of the countermeasures and to limit repetition, the different types of agents will be addressed at a later stage.

The second manner in which a nation state's mission serves as a platform for HUMINT collection relates to the inclusion, as part of the diplomatic corps, of 'undeclared' intelligence officers. As denoted by the term, the status of such officers as members of an intelligence service is not declared to the host country. In addition to some authentic diplomatic functions, undeclared members are involved in clandestine HUMINT collection while also enjoying diplomatic immunity. The diplomatic mission can, thirdly, serve to augment the credibility of the cover of clandestine HUMINT collection by 'illegals'. 'Illegals' are individuals not attached to the diplomatic corps and who employ non-official cover (Godson, 2001: 221-224). Trends in statutory espionage and counterespionage generally defy methodically defendable quantification. Published accusations of diplomatic missions exploited for (especially HUMINT) intelligence gathering and the expulsions of foreign diplomats from host countries, nevertheless serve as useful barometers for the vibrancy of HUMINT collection by nation states. The post-Cold War era is replete with such episodes. Considering the diplomatic sensitivity surrounding such incidents and the inherent secretive nature of espionage and counterespionage, publicly available information on the expulsion of diplomats is, however, for the most part of a cursory nature. With this qualification, incidents of espionage and counterespionage relevance during the period 2006 to 2008 include the following (*BBC News*, 2007/03/15; *Deutsche Welle*, 2007/12/15; Burgess, 2008: 2-8; *Eurasian Secret Services Daily Review*, 2007/11/12; Richter, 2007: 1):

- The Czech counterintelligence service reported that half of the 60 Russian diplomats based in the Czech Republic were in fact (Russian) intelligence officers collecting sensitive information on their host country.
- Similarly, the UK asserted that 30 Russian intelligence officers were operating in London under the cover of the Russian embassy, consulate, and trade delegation. Four Russian diplomats were expelled from the UK.

- Russia expelled diplomatic representatives of the UK and Lithuania.
- An Indian diplomat was expelled from Pakistan. In a reciprocal action, India expelled a Pakistani diplomatic representative.
- US diplomats were expelled from Kyrgyzstan and Belarus.
- Germany expelled an Iranian diplomat.
- The US expelled diplomats from Venezuela and Kyrgyzstan.

5.2.2.2 TECHINT collection

The indicated importance that HUMINT enjoys within the 21st century espionage arena does not translate into a diminished priority attached to TECHINT. On the contrary, all indications are that TECHINT capabilities are expanding in respect of both state and nonstate actors (US, 2005*a*: 16-17). TECHINT and HUMINT are not part of a zero sum equation. Internationally espionage is on the increase, and so is the concurrent importance afforded to both the principal categories of collection methods.

TECHINT is employed as a collective term for wide-ranging, subdisciplines of collection. These subdisciplines are broadly clustered as Signal Intelligence (SIGINT), Imagery Intelligence (IMINT), and Measurement and Signature Intelligence (MASINT). Without claiming a fully inclusive listing, and drawing on various literature sources, TECHINT collection methods can be summarised in tabulated format as follows (Johnson & Wirtz, 2004: 44, 45; Bruneau & Dombroski, 2004: 9,10; Lowenthal, 2003: 60, 63-74; Gill & Phythian, 2006: 70-81):

Figure 4: Tabulated summary of TECHINT subdisciplines

SIGNAL INTELLIGENCE (SIGINT)		
SIGINT essentially refers to the interception of various types of electronic signals. Some forms of SIGINT, explained below, are COMINT, ELINT, FISINT, and TELINT.		
Communication intelligence	COMINT	Interception of communications between two or more parties. Encryption and decryption are deemed as part of COMINT.
Electronic intelligence	ELINT	Interception of (non-communication) electronic signals, such as radar and navigation systems.
Foreign instrumentation signals intelligence	FISINT	The monitoring of electronic magnetic emissions, notably pertaining to aerospace, surface and subsurface systems.
Telemetry intelligence	TELINT	The collection of data relayed by weapons during, for example, tests. TELINT therefore constitutes a subcategory of FISINT.
IMAGERY INTELLIGENCE (IMINT)		
In its most basic form IMINT can be seen as information gleaned from 'pictures'. Such pictures can be conventional photographs (PHOTINT) or imagines based on spectrum radiation (for instance infrared). IMINT can be collected by, amongst others, satellites (SATINT), conventional aero-platforms (such as aeroplanes) and unmanned areal vehicles (UAVs).		
MEASUREMENT AND SIGNATURE INTELLIGENCE (MASINT)		
Lowenthal (2003: 73) aptly remarks on the "arcane debate that rages" between those who see MASINT as a distinctive technical collection subdiscipline, and others who consider it "simply as a product, or even by-product, of SIGINT and other collection disciplines." Basically MASINT refers to information gathered and analysed as it pertains to a 'signature' (such as emissions, sounds, radiation and movement). Indicated below are only some of the vast array of 'MASINTs'		
LASINT	Laser intelligence.	
DMPINT	Dynamic measurement photography.	
IRINT	Infrared intelligence.	
ELECTRO-OPINT	Electronic, optical intelligence.	
CYBER INTELLIGENCE (CYBINT)		
Discussed and motivated as an additional subcategory in the subsequent paragraphs.		

As would have been surmised from the above, the description of a TECHINT subdiscipline refers to the origin or source of the information generated. A seemingly straightforward example would be that of SATINT, referring to images obtained by means of satellites. Satellites can, however, presumably also be used for the interception of communications. Therefore, the tabulated representation should be viewed as a conceptual demarcation and not a rigid compartmentalising. The indicated subdisciplines are related and cut across conceptual distinctions.

Given the proliferation of 'INTS' which shows no sign of abating, intelligence practitioners may view, with understandable despondency (if not cynicism), a suggestion for the addition of yet another 'INT'. Nevertheless, this study argues for the addition of Cyber Intelligence (CYBINT) as a fourth main category of TECHINT. The realities of 21st century international espionage compel such an addition. It is an addition that might also contribute to simplifying a dimension of statutory intelligence (and as part thereof counterintelligence) proliferated with a magnitude of technological terminology and concepts. Surprisingly, very limited reference was found in the literature consulted on the concept of 'cyber intelligence/cyberintelligence'.[1] As far as could reasonably be ascertained no substantiated postulation exists for the addition of CYBINT as a fourth primary TECHINT subdiscipline. Although numerous elaborated and technical definitions can be forwarded, 'cyber' essentially pertains to the "world of connected computers" (Mena, 2003: 421). CYBINT, this study contends, is more encompassing than just that which is accessible on the Internet. It also includes clusters of digital 'instruments' and 'methods.' Although not used with reference to the concept of CYBINT and espionage, the following, as described by Mena (2003: xv), serve to elucidate some such 'instruments' and 'methods':

[1] No reference to CYBINT was found in consulted secondary and primary sources available in hard copy. Even very recent publications such as Quiggin (2007) and Gill & Phythian (2006) do not refer to CYBINT. The result of searches with Yahoo and Google mostly had a bearing on private enterprise. The term CYBINT appears to have entered into use, to a very limited degree, in documentation of the US Air Force during 2008. In the context used in the US Air Force, CYBINT seemingly is employed within the context of electronic warfare. As far as could be determined, CYBINT is thus not postulated as part of a substantiated proposal for inclusion as the fourth main sub-discipline of TECHINT. Hard copies were made of the Yahoo and Google search results, should they be required for verification purposes.

- Software agents for the monitoring, retrieval, analysis of, and the “acting on” information;
- text mining for the scrutinising of “terabytes of documents, Web pages, and e-mails”;
- neural networks that aid in projecting the “probability of crimes” and “new terrorist attacks”; and
- machine-learning algorithms for “extracting profiles of perpetrators and graphical maps of crimes.”

Not mentioned by Mena (2003: xv-xvi) is that the above-mentioned ‘instruments’ and ‘methods’ are equally useful in the processing of the vast volume of information in the counterintelligence, and especially, the counterespionage spheres. The conceptualisation of CYBINT as extending beyond merely the ‘raw’ information and/or its source is congruent with the practice regarding the other three TECHINT clusters. SIGINT, IMINT, and MASINT not only denote the ‘raw’ signal or image, but also systems and processes that deliver an output refined to a degree that renders it useful for analysis. Similar to SIGINT, IMINT, and MASINT, CYBINT has a bearing on intelligence collection by the state and its adversaries in respect of all three information categories. Open-source CYBINT collection would, for example, include the use of (low-cost, freely accessible) Internet searches. In the realm of grey sources, ‘instruments’ and methods (discussed above) are available at a substantially higher cost.

It is perhaps the clandestine dimension of CYBINT that provides the most compelling grounds for its addition as another ‘INT’. The exponential ascendance during the past decade of the cyber sphere as an arena for adversarial espionage against the nation state can hardly be overstated. With reference to the introductory paragraph to this section, it is re-emphasised that cyber warfare and cyber espionage are intricately linked. A cyber attack serves as a signpost of preceding cyber espionage. With this *caveat*, the following illustrate the prominence that cyber warfare and cyber espionage have assumed in the 21st century:

- According to a 2007 report by the authoritative computer security company McAfee, approximately 120 nation states are using the Internet for cyber espionage and attacks (Hoffman, 2007: 1).
- It is projected that Taiwan will spend 12 percent of its military budget over the next five years on “Internet warfare” (Burgess, 2008: 3).

- In August 2007, on the eve of a meeting between the German Chancellor and the Chinese Premier, an extensive volume of information was siphoned off the computers of the German Chancellery, as well as the foreign, economic and research ministries. The cyber attack was detected and reportedly traced back to the Chinese security forces (Burgess, 2008: 4).
- In what is believed to be a Russian state-sponsored cyber attack, Estonia's information and communications network was crippled for a two-week period in 2007 (Warren, 2005: 1).
- In 2004, South Korea claimed that North Korea recruited a team of 500 computer hackers to "wage war on the US and other countries" (Warren, 2005:1).
- Subsequent to the US's seemingly inadvertent bombing in 1999 of the Chinese embassy in Belgrade, the PRC allegedly launched a cyber attack that exposed "an astonishing 3,000 - 4,000 'backdoors' into US computer systems that had apparently been created by Chinese agents" (Wettering, 2000: 276).

Other TECHINT measures, as suggested earlier, are no longer exclusively available to the nation state. In this regard, Brenner (US National Counterintelligence Executive) remarks: "Governments no longer have a monopoly over world-class collection vehicles, like satellites, and word-class communications equipment" (US, 2007*f*:14). The "once top-secret world of overhead reconnaissance using satellites", Hulnick (2002: 4) observes, is now in the commercial domain and "can be purchased on the Internet by anyone with a credit card." According to one estimate at least eleven private companies would have had "high-resolution commercial remote sensing satellites in orbit" by 2003 (NATO, 2001: 10). The quality of satellite images generated by commercial satellites is of such a nature that these products are used by NATO countries (NATO, 2001: 10). As with CYBINT, nation states in some instances draw on the expertise of nonstate actors also in respect of other TECHINT fields. Since advances in TECHINT, be they as products or systems, are on the 'open market' they also, to varying degrees, augment the espionage capacities of nonstate adversaries of the state such as criminals and terrorist groups (Treverton, 2005: 3, 4).

From the preceding discussion the question arises: 'Which TECHINT methods remain within the prerogative of the state?' The concise response is: 'Conceivably none'. It is the magnitude, rather than the nature, of TECHINT capacities that differentiates between more powerful nation states and nonstate actors. Some SIGINT operations, for example, require resources of such a magnitude that they are, at least for the present, within the preserve of some of the more powerful nation states. In addition to collective capacities (such as the Echelon system previously discussed), nation states singled out by Gill & Phythian (2006: 70) as individually possessing significant SIGINT capacities are: the US, Russia, France, the PRC, the UK, Germany, India, Canada, Israel, Pakistan and "a number of other Asian and Middle Eastern states" (Gill & Phythian, 2006 : 70). One further advantage that nation states enjoy over nonstate actors relates to the utilisation of their foreign (diplomatic) missions' premises as platforms, notably for the employment of SIGINT equipment (Gill & Phythian, 2006: 70).

As is clear from the above, the equalising effect of technological advances and globalisation is nowhere more apparent than in the field of TECHINT collection. Whereas intelligence is the 'maximiser' of other instruments of power, the accessibility of TECHINT collection methods is the 'equaliser'. Globalisation, coupled with the other driving forces previously discussed, puts these collection methods at the disposal of a widening array of espionage actors adversarial to the nation state. The diversification of TECHINT collection methods does not entail a lesser importance being attached to HUMINT collection. The information-driven nature of society increases the premium placed on secret, statutory information procured through a combination of TECHINT as well as HUMINT collection methods. Furthermore, espionage adversaries combine their espionage endeavours in varying degrees.

From a counterintelligence perspective, the nation state is thus confronted with a multifarious matrix of espionage threats and risks posed by many adversaries with access to a proliferating array of collection methods. Corresponding with the diversity of the collection methods employed by its espionage adversaries, the nation state utilises a combination of HUMINT, TECHINT and other measures in the countering of espionage risks and threats.

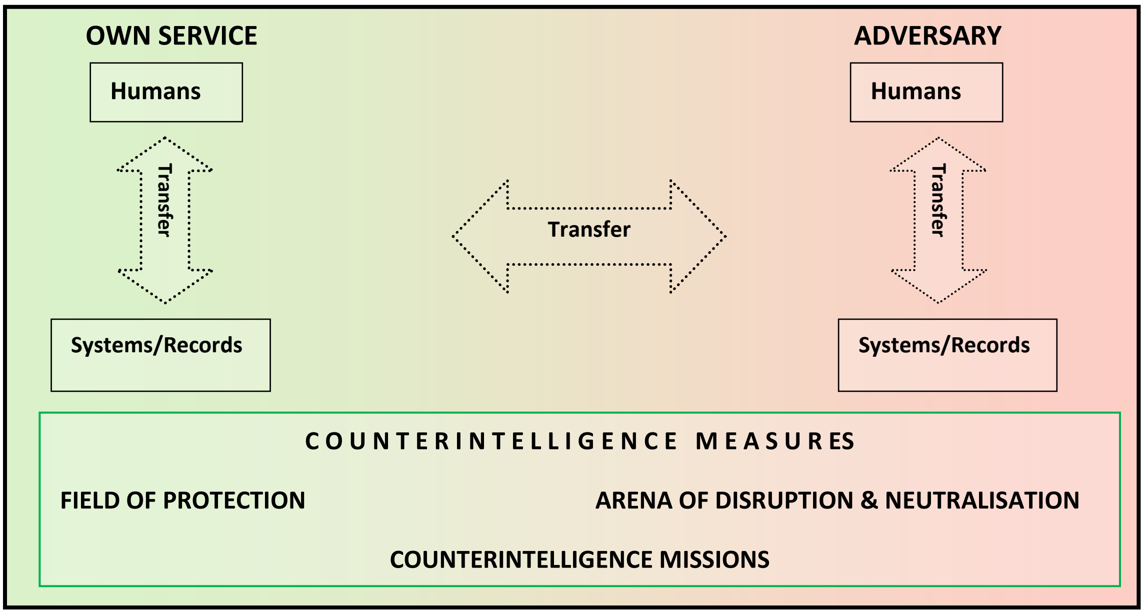
6. STATUTORY COUNTERINTELLIGENCE METHODS AND MEASURES

Against the background outlined above, this section discusses the range of 21st century counterintelligence methods and measures the nation state employs in confronting espionage risks and threats. A theme running through the entire section is the substantiation of the unfeasibility of rigidly assigning specific counterintelligence methods and measures to only certain counterintelligence functions and missions. In line with this postulation, counterespionage is not synthetically addressed as a self-sufficient cluster of activities, but as interwoven with other dimensions of counterintelligence. In a similar vein, and despite its distinctive character, counterintelligence functions are in synergy with other intelligence subdisciplines. While this symbiotic relationship has served as tacit assumption and context throughout this section, it is explicitly addressed as part of Chapter Five.

6.1 LINKING COUNTERINTELLIGENCE THEORY AND PRACTICE

The two primary counterintelligence missions previously remarked on from a theoretical perspective also underpin this section. It was asserted that counterintelligence has as its first function to protect, defensively and offensively, the integrity of statutory information deemed to be of national security interest. As its second priority, counterintelligence aims to compromise the informational (intelligence) integrity of an adversary. Counterintelligence is, to re-emphasise, part of informational power and warfare. However, the emphasis of this section is not on the theory of counterintelligence. The main objective here is to explore the practice of counterintelligence in the 21st century as it finds concrete manifestation in specific measures taken by the nation state. Since theory and practice do not stand in isolation of each other a conceptual link that connects their notional and practical dimensions is nevertheless required. To this end the following graphical representation is provided and then explicated:

Figure 5: Counterintelligence missions and measures – linking theory and practice



Crucial to counterintelligence in its offensive and defensive role, is the notion that information resides in systems (including physical records) and humans. This information is transferred between humans and systems. In its defensive function counterintelligence thus protects these records and transfers. Should an unauthorised transfer be detected it could indicate adversarial espionage activities. In its offensive dimension, counterintelligence seeks to exploit this transfer, (through for example disinformation) and thus compromise an adversary's informational integrity.

In the execution of the graphically outlined offensive and defensive counterintelligence dimensions, a spectrum of measures is employed. These measures and methods range from, on the one hand, non-aggressive passive measures to, on the other hand, aggressive offensive measures.

6.2 PHYSICAL SECURITY

Arguably the most passive and defensive cluster of counterintelligence measures is directed towards the physical security of facilities "where secrets are produced and stored" (Taylor, 2007: 6). These include access and movement control, perimeter security, alarm systems, safes and vaults, fire prevention measures, key control and the control of the removal and transfer of information from facilities where classified, statutory information is located (Taylor, 2007: 6). A civilian intelligence service could be required to ensure the maintenance of such measures at other organs of state. The potentially severe consequences of non-adherence to physical security measures were recently illustrated in the UK. During June 2008 an unnamed "senior civil servant working in the Cabinet Office's intelligence and security unit", transported and 'left' the documents on a train, in breach of regulations. This documentation, contained intelligence on an "Islamic terror network" and was classified "Top secret - for UK, US, Canadian and Australian eyes only" (*Mailonline*, 2008/06/13).

Being integral to counterintelligence in general, the application of effective physical security measures is growing in complexity. The 21st century challenge to physical security is aptly encapsulated in a recent US (2005*b*: 545) official report:

> [Physical] security, as a discipline, has historically been dominated by "police" type management, processes, and enforcement approaches. Although the police function is still required, today's security

vulnerabilities are increasingly technical in nature and related to information technology systems, software, and hardware.

6.3 INFORMATION AND TECHNOLOGICAL SYSTEMS SECURITY

The previous quotation as well as the example provided, reflects the overlap and the inseparability of physical security from, what is termed from this study's perspective*, information and technological systems security*. 'Systems' as used in this context is deemed as referring to a variety of information and communication systems. For easier reference the acronym INSYSEC is subsequently employed.

Relatively contemporary theoretical publications tend to cluster counterintelligence measures into categories or subfunctions, and use terminologies that predate technological advances. Such conceptualisations are not congruent with the converged reality presented by contemporary practice. Illustrative in this regard is the separation into distinctive counterintelligence subfunctions of 'Information Security' (INFOSEC - sometimes erroneously deemed as synonymous with 'computer security'); 'Technical Security Countermeasures' (TSCMs); and Communication Security (COMSEC). Technological advances have blurred the distinction between the security of information (in whatever format) and the security of systems as communication and information systems are, by and large, an aggregate. Against this background, this study therefore posits INFOSEC TSCMs and COMSEC all as dimensions of INSYSEC.

As part of INSYSEC, 'information security' pertains, *inter alia*, to the classification, distribution and control of access to information. Depending on its sensitivity, information is usually classified in order of declining frequency as 'confidential', 'secret', or 'top secret' (Taylor, 2007: 6). Access to such information will be determined by the level of security clearance an individual has, as well as the relevance of the information to his/her line-function. The latter is usually defined as the need-to-know or compartmentalisation principle (Wettering, 2000: 274-275; Taylor, 2007: 6). Information classification and the need-to-know principle provide parameters according to which personnel are afforded access to information, communications- and other systems. System security is, however, far more encompassing than mere internal access to systems. In addition to limiting access to authorised users ('confidentiality'), its other two primary goals are the 'integrity' and 'availability' of information/communication systems (Crampton *et al*, 2006: 358). Phrased differently, system security has a threefold aim, namely to protect against: (a) 'compromising information' (unauthorised access to information); (b) ‘integrity violation’ (altering of information through replacement and manipulation) and, (c) ‘denial of service’ attacks (which result in systems being wholly or partially incapacitated for the intended users) (Crampton *et al*, 2006: 358-359). System security therefore serves as a shield against cyber warfare. From this line of reasoning, it is clear that COMSEC forms an integral part of INSYSEC. In addition to securing digital interaction, COMSEC also safeguards other communication instruments such as conventional telephones, cellular phones and faxes. To this end encryption and decryption are used. COMSEC thus overlaps with ‘Cyber Security’ (CYBSEC). TSCM is not, as projected by authors such as Wettering (2000; 277-288), a distinct and separate “collection of technical efforts to detect the technical penetrations of facilities by foreign intelligence services to collect intelligence”. Resulting from the integration of systems outlined, TSCMs are interwoven with several dimensions of INSYSEC.

6.4 PERSONNEL SECURITY

However protected by internal and external measures, the fidelity of personnel with access to information of relevance to national security remains arguably the most critical factor in counterintelligence. As will be discussed at a later stage, several of the most damaging espionage breeches followed ‘insiders’ volunteering their services to foreign intelligence services, while multiple others involved foreign intelligence services’ recruitment of ‘insiders’. Pre-employment and in-service personnel security are consequently of self-evident significance. Methods utilised as part of determining the security competence and suitability of personnel include: biographical verification, criminal record checks, lifestyle and financial analysis, interviews, and polygraph tests (Taylor, 2007: 5-6; Wettering, 2000: 270-274). Furthermore, personnel security upholds ‘background investigations’ as a specialised function (Wettering, 2000: 271).

The price paid in human lives for deficient in-service personnel security was poignantly exemplified by the case of Ames, a convicted former CIA official. Ames operated as a double agent for the Soviet Union, and later, Russia between 1985 and 1994. As a direct result of information Ames provided to the Soviet Union, at least ten CIA agents were executed by the KGB, while numerous others were compromised (Taylor, 2007: 285). Various danger signs relating to Ames either went undetected or simply disregarded during the CIA’s in-service personnel re-vetting. Professionally Ames was a poor performer. He failed to submit reports, showed signs of alcoholism, and on several occasions breeched CIA security regulations. Ames' exorbitant lifestyle, funded by the Soviet Union and then Russia, stood in sharp contrast to his CIA salary (Godson, 2001: 197).

6.5 COUNTERINTELLIGENCE COLLECTION METHODS – FROM SHIELD TO SWORD

Investigation has its pillars in both methods; on the one hand, relatively non-aggressive measures (the 'shield') and, on the other hand, aggressive counterintelligence measures (the 'sword'). In combat, to expand on this analogy, the 'sword' and the 'shield' function in synergy. The shield can be used defensively and offensively. Similarly, the sword defends ('blocks') and attacks. It is against the background of this analogy that the typifying of defensive and offensive counterintelligence collection methods should be seen. 'Aggressive' in this context denotes actions of actively pursuing an espionage adversary. As implied, investigation illustrates the inseparability and blurred distinction between relatively non-aggressive and more aggressive counterintelligence collection methods. Through investigation as part of personnel screening, and probes into the breeches of security regulations, indications of possible adversarial espionage activities could emerge. Such indicators provide grounds for more aggressive investigations. The latter could take as premise the analysis of existing information as generated by, *inter alia*, INSYSEC and personnel security. Movement and key control registers, closed circuit television (CCTV) footage, and records of access to digital databases, serve as examples of information generated by the security function. As a basis for more aggressive investigation, counterintelligence draws on all the collection instruments used within the positive intelligence realm. The role of analysis is, as too is the case in counterintelligence generally, pivotal. Based on the information requirements emanating from analysis, decisions are taken on the specific combination of further investigative actions. Depending on the specific case, a combination of HUMINT and TECHINT collection methods and sources is usually employed.

Surveillance as a collection method demonstrates the interaction between technical and HUMINT dimensions. Marx (2004: 78-98) as well as Gill & Phythian (2006: 29-30, 95-101) rightly points out 'surveillance' as a value-laden concept with diverse denotations. In the concrete sense of observing the activities of an espionage adversary, surveillance is one of the most common counterintelligence collection methods (Wettering, 2000: 281). Although reality is also in this case more complex, three subcategories of surveillance can be distinguished conceptually. These are: (a) static surveillance; (b) mobile surveillance; and (c) electronic surveillance (Wettering, 2000: 281-284).

More varied than surveillance, is the range of HUMINT sources that could be employed as part of the statutory counterintelligence collection effort. HUMINT sources include, but are not limited to: peripheral agents, agents-in-place, access agents, 'moles', defectors, double agents, multi-turned agents (for instance triple agents), agent *provocateurs*, 'walk ins', agents of influence, unwitting agents, penetration agents, infiltration agents, false flag agents, witting agents and 'sleepers'. These different descriptors of HUMINT sources are not mutually exclusive. Under certain conditions a HUMINT source can, for example, be typified simultaneously as a 'mole', a defector and a double agent. In more detail, and with the understanding that it does not present a rigid compartmentalisation, some of the more common categories of HUMINT sources are discussed below.

The term 'walk in' refers to a person that has volunteered information to an opposing intelligence service or other espionage adversary. This volunteering of information can assume various forms. Ames offered his service to the USSR by literally walking into the Soviet Embassy. A 'walk in' can, however, present his services without physical contact and the exposure of his identity. A case in point is that of a former FBI member (Hanssen) convicted in 2001 of spying for the USSR and Russia for 22 years. Hanssen initiated contact with the KGB by means of an anonymous letter. Since both Ames and Hanssen were members of statutory intelligence structures on the pay roll of an adversarial intelligence service, they can also be described as 'moles'. Although some conceptualisations would deem Hanssen and Ames as double agents, this term more accurately refers to persons that are not members of an intelligence service. A criterion employed for the classification of a source as a double agent is that he/she serves as a source for two opposing intelligence services to the ultimate benefit of only one (of these services). Individuals, whether they are members of an intelligence service or not, and who offer their services to a foreign intelligence structure are under certain conditions known as defectors. A defector is distinguishable from a 'walk in' in that a defector would generally expect some degree of diplomatic protection (normally) should his contact with the opposing government be exposed. An example to this effect recently occurred in Belgium. In 2002 a senior Chinese intelligence officer, then stationed in Belgium, defected (to Belgium) and applied for political asylum. The individual is said to have been in charge of a Chinese economic, espionage network in Western Europe and to have provided

Belgium authorities with the names of “several hundred other spies” (*Industrial Espionage News*, 2008: 6).

6.6 NEUTRALISATION, DECEPTION AND EXPLOITATION

The collection of information, as outlined above, has as one of its aims to detect and determine hostile intelligence activity. Frequently, this detection’s means and its ends are simultaneously defensive and offensive. On a more passive level, the information could prompt the enhancement of physical security measures, INSYSEC, and personnel security measures. Offensively, the information is at the core of assailing the informational integrity of an adversary through manipulation, disruption, deception and neutralisation (Zuehlke, 1980: 16-19, 28). As with most other counterintelligence dimensions, measures on the offensive and defensive levels are a converged reality that defies strict compartmentalisation. Measures commonly deemed as offensive and aggressive can have a defensive purpose. This is attested to by an observation made by Webster, who served as director of the CIA and FBI respectively, to a US Senate hearing in 2002: “Almost every spy we have found both in the CIA and FBI, has been found with the aid of recruited sources of our own in other hostile intelligence agencies” (as quoted by Taylor, 2007: 8). Further augmenting the convergence in counterintelligence practice is the fact that collection methods are also exploited for neutralisation and deception.

The effective exploitation and neutralisation of adversarial espionage activities, as will still be discussed, are dependent on an assortment of factors and variables. One of these factors is the timing of more visible counteraction. Even were adversarial espionage activities to have been determined beyond reasonable doubt and incontrovertible evidence procured, it could be in the broader- and longer-term counterintelligence interest to adopt a stance of continued monitoring. The latter presents the opportunity to expose undiscovered adversarial espionage agents and networks. It does not apply only to HUMINT operations, but also holds sway in the TECHINT field. Should cyber espionage be detected, immediate termination is also not advisable in all instances. The ‘fish bowling’ of cyber espionage could render invaluable information. A “fish bowl” is described by Mena (2003: 423) as the action to “contain, isolate, and monitor an unauthorized user within a system in order to gain information about the user.”

The continued monitoring of HUMINT and TECHINT espionage can be accompanied by the deception of and ‘feeding’ of disinformation to an espionage adversary. In the case of HUMINT this deception is achieved by the ‘feeding’ of information to known access areas of an adversarial espionage network. In a similar manner, misleading information can be relayed through electronic communication channels known to be monitored by an adversary. Disinformation and deception can also be pursued by means of, for example, double agents or/and agents of influence. Other counter-measures at the avail of the nation state include the following:

- Preventing the entering of known and suspected foreign spies through the refusal of a visa application; the refusal to accept a diplomatic letter of introduction; and/or the declaration of an individual as a *persona non grata*.
- The lodging of various levels of diplomatic protest over the involvement of a foreign state’s diplomats or other citizens’ engagement in espionage. Such protest ranges from the verbal confrontation of declared intelligence members or the head of the diplomatic mission, to the expulsion of diplomats. Official protest from one state to another may be followed by the public exposure of alleged espionage activities. A recent incident involving the UK and Russia serves as an example. During 2005 the Russian FSB confronted a senior declared MI6 member (placed in Russia) over the alleged espionage activities of four British diplomats. In January 2006, the Russian television station *Rossiya* broadcasted a report containing footage of the espionage perpetrated by the four British diplomats. The following year (2007) four British diplomats (presumed to be the same four individuals) were declared *persona non grata* and expelled from Russia (Kramer, 2007: 1-2).
- Should sufficient evidence exist of espionage in contravention of legislation, a nation state has as further countermeasure the option of criminal prosecution. The previously mentioned cases of Hanssen and Ames serve as examples. In cases where foreign citizens do not enjoy diplomatic immunity, such individuals can also be arrested and prosecuted.
- Whereas prosecution is a counterintelligence measure within the legal framework, other more extreme countermeasures are mostly deemed to be illegal. Extraordinary rendition is one such countermeasure. In 2007, the EU Parliament adopted a report that condemns the CIA and the US for actions of extraordinary rendition in EU member states (*BBC News*, 2007/02/14). The report (as quoted by *BBC News*, 2007/02/14) describes extraordinary rendition as instances where "an individual suspected of involvement in terrorism is illegally abducted, arrested and/or transferred into the custody of US officials and/or transported to another country for interrogation which, in

the majority of cases involves incommunicado, detention and torture" (*BBC News*, 2007/02/14). Although not specifically mentioned in the report, and given the previously discussed relevance of terrorist groups as espionage actors, it can reasonably be assumed that terrorist suspects abducted by the US included individuals suspected of espionage.

- Similar to extraordinary rendition, assassination would generally be deemed as an illegal counterintelligence countermeasure. A much published incident centred on the death in 2006 of Litvinenko, a former member of the Russian FSB, serves as illustration. The British security services accused Russian intelligence services of involvement in the lethal, radiation poisoning of Litvinenko. Litvinenko defected to the UK in 2000 and was granted political asylum (*CI Centre*, 2008: 1-4, 9-23). Subsequent to his defection Litvinenko published several exposés implicating the Russian government and intelligence services. It is widely speculated that Litvinenko was a paid agent of MI6 (Wright & Williams, 2007: 1-2).

This section outlined the counterintelligence measures and methods at the avail of the nation state. These measures and methods are as diverse as the espionage risks and threats confronting the nation state (De Graffenreid, 1989: 148). Effective counterintelligence is a multi-disciplinary endeavour that requires the synergetic employment of measures. On a notional level these measures can indeed be ‘conceptually bee-hived’. In their practical execution, however, the respective measures are dimensions of a multi-facetted entirety.

7. CONCLUSION

This chapter examined the 21st century’s international security environment with emphasis on the phenomena of espionage and statutory counterintelligence. The specific aim was to present the ‘reality’ according to which the CE framework’s focus can be configured. To this end a distinction was made between the ‘contextual focus’, ‘focus areas’ and ‘focal points’ of the CE framework.

As *contextual focus* of the CE framework, the drivers affecting, and the strategic trends characterising the international security order, were indicated. The primary drivers of the international security environment were found to be globalisation, technological advances, the information revolution, fissiparous forces and ecological changes. The indicated drivers of change impact on certain ‘domains’ or ‘sectors’ of society. Since the CE framework could benefit from a conceptual structuring of the macro-environment, a segmentation providing for the following sectors was forwarded, namely: political, military, social, technological, economic, ecological (environmental), and informational sectors. Traversing these, the indicated drivers were shown to generate strategic trends which profoundly affect the role of, and challenges to the nation state and national security.

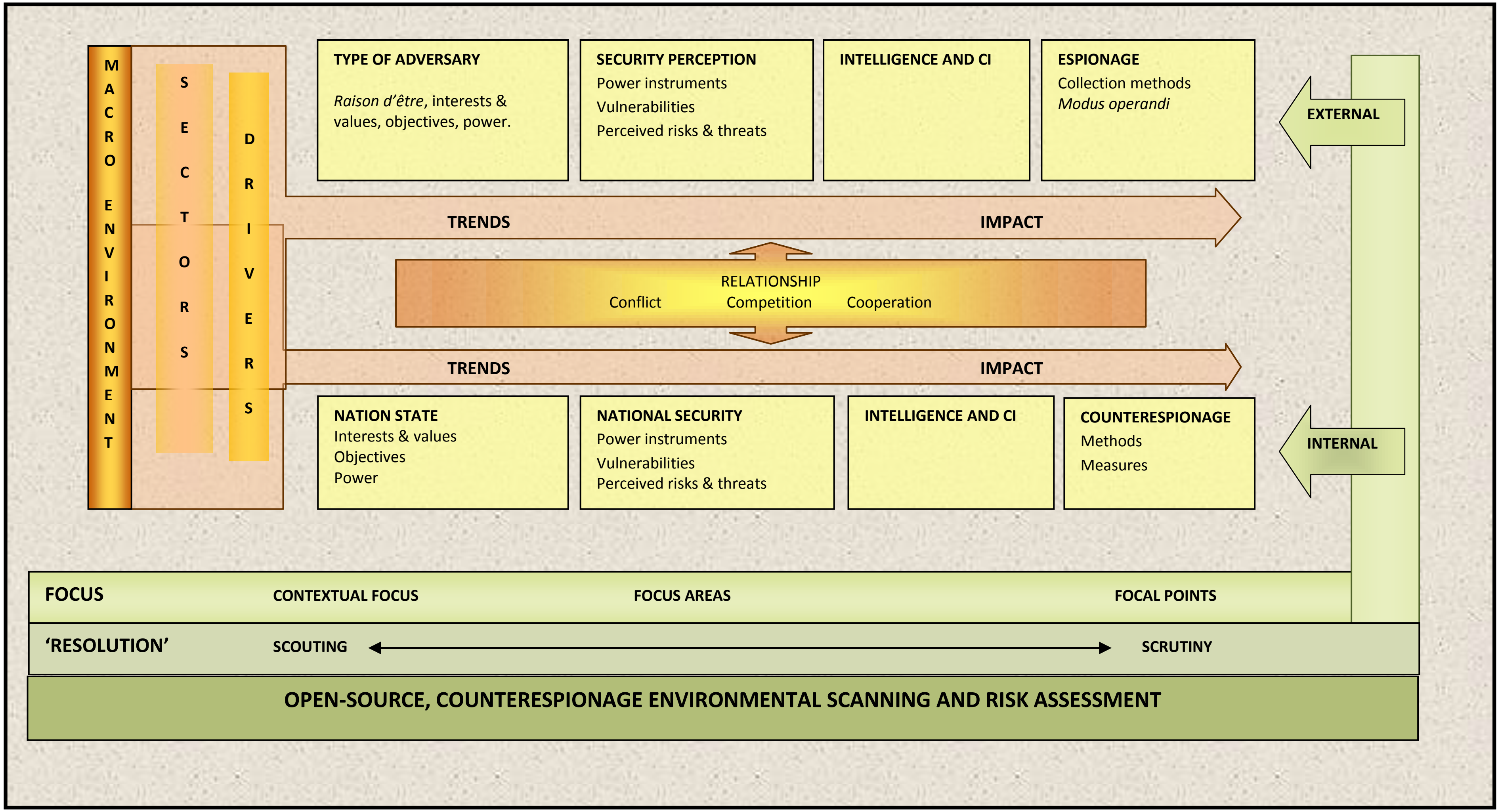
The impact of the strategic trends on national security and statutory intelligence services crystallised as the *focus areas* for the CE framework. Of particular importance to this study is the emergence of the 'digital information sphere' as the fifth dimension of strategic power analysis, alongside sea power, land power, air power and space. The ascendance of informational power increases the dependence of the nation state on its intelligence service(s). This dependence was found to have a bearing on intelligence as a guiding instrument, intelligence as an offensive and defensive instrument of power in its own right, and intelligence as a 'maximiser' of other instruments of power.

The 21st century manifestation of espionage risks and threats against the nation state were presented as the parameters for 'calibrating' the CE framework's *focal points*. The delineation of the focal points essentially consisted of a response to a twofold problem statement. The first dimension of the problem statement entailed answering the question: 'Which are the nation state's most salient espionage adversaries?' Adversarial espionage actors concluded to be of particular relevance are other nation states, entities within private enterprise, NGOs, entities within the mass media, terrorist and extremist groupings, as well as unaffiliated individuals and groups. While a particularised approach was followed in advancing espionage adversaries as focal points, it was emphasised that the nation state faces a reality in which the various espionage adversaries are interlinked. These espionage adversaries, individually and in combination, serve as focal points of the CE framework. The second dimension of the problem statement had a bearing on the question: 'How do these espionage adversaries spy against the nation state?' To this end, contemporary sources and methods employed by espionage actors were outlined. As a key finding it was pointed out that clandestine collection methods, once the prerogative of the nation state, are increasingly at the disposal of other espionage adversaries. Whereas intelligence is the 'maximiser' of other instruments of power, the accessibility of TECHINT collection methods is the 'equaliser'. Globalisation, coupled with the other driving forces discussed, avail these collection methods to a widening array of espionage actors adversarial to the nation state. In respect of TECHINT, a proposal was forwarded for the inclusion of CYBINT as a fourth main subdiscipline (alongside SIGINT, IMINT and MASINT).

Subsequently, the range of 21st century counterintelligence methods and measures the nation state employs in confronting these espionage risks and threats in counterespionage were outlined. Existing categorisations of these countermeasures were found to be inadequate to provide for the 21st century's 'converged technological reality'. Therefore, INSYSEC was submitted as a subcategory of countermeasures. Effective counterintelligence, it was emphasised, is a multi-disciplinary endeavour that requires the synergetic employment of countermeasures.

With a view to the CE framework's design, and as was explained above, the chapter notionally structured the contemporary manifestation of adversarial espionage risks and threats confronting the nation state in accordance with three intensity ('resolution') levels of environmental scanning, namely 'contextual focus', 'focus areas' and 'focal points'. As a prefigurement of subsequent chapters, a diagram integrating this differentiation with some other aspects addressed in the chapter is provided *per* Figure Six. The diagram also serves as a conceptual background for assessing the role of open-source information in statutory counterintelligence in general, and counterespionage specifically. This role of open- source information as part of counterintelligence, with emphasis on the uses and limits of OSINT in relation to counterespionage, is among the aspects addressed in the next chapter.

Figure 6: An outline of open-source, counterespionage environmental scanning and risk assessment - contextual focus, focus areas and focal points



CHAPTER FOUR

REQUIREMENTS PERTAINING TO AN OPEN-SOURCE RISK IDENTIFICATION AND ASSESSMENT FRAMEWORK WITHIN THE STATUTORY COUNTERESPIONAGE MILIEU

1. INTRODUCTION

The preceding chapters examined the imperatives posed to the CE framework by an intelligence theory and by the contemporary manifestation of espionage against the nation state. This chapter derives concrete requirements for the CE framework from within the context of these imperatives. It therefore, as a central focus, addresses the following research question: Given the contemporary views, as well as the current manifestation and expected developments regarding national security in general – and counterespionage in particular – with which requirements should the CE framework comply? A primary requirement forwarded in this chapter is that the CE framework should be able to identify and describe, from open-source information, diverse espionage risks posed by role players adversarial to the nation state. This requirement applies to both dimensions of CE environmental scanning, namely the 'looking for' (collection) and the 'looking at' (assessment) of open-source information.

Since the research questions are interrelated, the specification of requirements for the CE framework brings to the fore other facets of the study's research problem. In this regard, four further research questions are central to this chapter, namely:

- What definition can be assigned to an espionage risk, and in which respect is a risk distinguishable from an espionage threat?
- Do current notions of 'threat' and 'risk' provide a definition that could be feasibly employed within the CE framework or are specifically tailored conceptualisations required?
- What criteria can be used to categorise and prioritise espionage risks?
- Given the near overwhelming extent of overt information, how can CE environmental scanning be systemically structured?

The response of this chapter to the above-mentioned questions should, of course, be viewed in the light of the study's problem statement. The latter, to re-encapsulate, centres around the challenge of using open-source information to bridge the degenerative, self-feeding counterespionage cycle caused by an over-reliance on classified information. The CE framework does not purport to offer a panacea for this or other challenges. A recurring theme in this chapter is therefore the delineation of the uses and limitations of the CE framework.

In addition to the requirements *posed to* the CE framework, requirements *posed by* the design of this framework are explored. The latter pertains to contextual constituents for its construction. More simply phrased: What foundational ‘building blocks’ need to be in place to allow for the CE framework to be designed? Since consulted literature is largely silent on such conceptual approaches, propositions in this regard are forwarded.

The structural approach to the chapter is in part guided by the different facets of the research theme. These form subthemes around which respective sections have been built. This approach entails examining the requirements and some constituents emanating from the CE framework as an instrument that:

- Has as its aim the identification and assessment of ‘espionage risks’ ;
- is located within the statutory intelligence milieu, and
- has the utilisation of open sources as an essential feature.

A stated aim of this study is to contribute toward the development of a specialised (micro-) counterespionage theory. In the formulation of requirements and constituents in respect of the CE framework, both dimensions of intelligence theory construction are employed. Firstly, constituents and requirements are partially the laying out of ‘what we know’ in a manner aiding micro-theoretical theory construction. In the latter sense, constituents and requirements are based on the structuring of existing knowledge according to the needs of the CE framework. Secondly, an attempt is made to ‘impart new knowledge’ through enriching requirements and constituents with fresh perspectives.

2. REQUIREMENTS RELATING TO THE COUNTERESPIONAGE FRAMEWORK AS A STATUTORY ESPIONAGE RISK ASSESSMENT INSTRUMENT

The CE framework has as its foremost requirement, the identification and assessment of espionage risks from a statutory intelligence perspective. The attainment of this requirement depends on the meeting of two subrequirements. Firstly, a clear demarcation of the concept ‘espionage risk’ and, secondly, a structured approach to the assessment of espionage risks. Risk assessment is a multifaceted process and various aspects thereof are addressed further on in the study. This chapter examines risk assessment with specific reference to its dimensions of ‘categorisation’ and ‘prioritisation’. These not only exemplify the qualities of risk assessment in general, but are also intrinsically linked to the definition of espionage risks and threats.

2.1 A SELECTIVE OVERVIEW OF CONTEMPORARY CONCEPTUALISATION OF RISK, THREAT AND RISK ASSESSMENT

Whereas the notion ‘espionage’ has so far been extensively explored from a theoretical and practical perspective, only brief reference has been made to the concept ‘risk’. In a broad sense, statutory espionage risks can be described as the distinctive cluster of national security concerns relating to adversarial espionage actions directed against a nation state. In order to arrive at a more specific description of an espionage risk, a selective overview of contemporary conceptualisations of the notions ‘risk’, ‘threat’ and ‘risk assessment’ is subsequently provided.

The purpose of this overview is to determine whether existing conceptualisation can feasibly be employed in relation to the CE framework or whether alternative propositions (as befitting the needs of the CE framework) are required. Since this is an exploratory study, such an overview also serves the purpose of acknowledging and clearly stating the present body of knowledge on which the CE framework as a risk identification and assessment instrument is built.

Chapter Two reflected on the concept ‘national security threat’ from a theoretical perspective. While some recapitulating thereof is required, the concept of a ‘national security threat’ is examined in this chapter with a view on demarcating the notions of ‘espionage risks’ and ‘risk assessment’.

2.1.1 Recapitulating Security and Strategic Studies’ views on the concept national security threat

It was previously mentioned that to assign an issue the status of being of national security relevance implies the elevation thereof above “trivial and routine” governance (Buzan, 1991: 8). The ‘widening’ and ‘deepening’ of the security agenda were shown to have resulted in a near indiscriminate assigning of the label ‘national security threat’ to a multiplicity of security concerns. This trend prompted scholars such as Buzan (1991: 8, 134, 138-139) and Hough (2003: 18-19) to forward criteria for assessing whether an issue is a matter of routine governance or whether it warrants categorisation as a national security threat. Criteria forwarded include the degree to which such an issue (actually or potentially) detrimentally impacts on a nation state’s stability, sovereignty, territorial integrity, vital interests and values. A further criterion posited was whether a situation could obligate the state to institute extraordinary measures.

2.1.2 Business Risk Management as a focus of Intelligence Studies propositions on risk, threat and risk assessment

Due to reasons discussed afore, scholars of Intelligence Studies as well as statutory practitioners were late in joining the academic debate around the concepts national security and national security threat. During the first decade of the post-Cold War era, deliberations within Intelligence Studies were dominated by justifying the continued centrality of statutory intelligence structures in government apparatuses. Consequently, theoretical and academic aspects received scant attention within this discipline. The concepts national security threat and national security risk were, and to a large degree still are, used interchangeably within Intelligence Studies (Quiggin, 2007: 24). From the late 1990s onwards, endeavours not only to distinguish theoretically between national security risks and national security threats, but also to systemise the assessment of such risks and/or threats began emerging. In pursuit of credible and justifiable propositions scholars of Intelligence Studies turned to the theory and practice in the corporate world in general, and Business Risk Management in particular (Gill & Phythian, 2006: 85; Bernhardt, 2003: 143). As the latter discipline strongly influences Intelligence Studies' postulations on risk, threat and risk assessment, a concise outline of prevailing thinking is provided within Business Risk Management regarding these concepts.

Within the private sector formalised academic interest in the concept 'risk' which gave rise to the establishment of Business Risk Management as a study field dates back to the 1960s (Bernhardt, 2003: 143; Garcia, 2006: 510-513). Notwithstanding the relative maturity of Business Risk Management Studies as a discipline, a uniform definition of risk, however, still eludes. Four authoritative textbooks within this field (Burstein, 1994; Fisher & Green, 1998; Hess & Wrobelski, 1996 and Timm & Christian, 1991), for example, each offer a different definition of a 'business risk' (Garcia, 2006: 510). However, Garcia (2006: 510) views a definition forwarded by Merkhofer (1987) as encapsulating the core meaning afforded to a risk within the field of Business Risk Management. Merkhofer (1987) posits a risk as "an uncertain situation in which a number of possible outcomes might occur, one or more of which is undesirable" (Garcia 2006: 510). Extending on Merkhofer's (1987) proposition, the qualification and quantification of a risk as the "measure of probability and severity of adverse effects", also gained wide acceptance within Business Risk Management (Garcia, 2006: 510). The "measure of probability and severity of adverse effects" is thus central to the assessment and prioritisation of risks (Garcia, 2006: 510). Within this discipline, a risk is commonly seen as the more encompassing concept having a threat as a subset. According to this view, a threat is an "entity" capable of causing "an undesired event or events" (Rogers, 2006: 79-80; Manunta & Manunta, 2006: 634).

2.1.3 Views on risks, threats and risk assessment within Intelligence Studies

Relative to Business Risk Management, the discourse in Intelligence Studies on the relationship between the concepts of risk and threat, and even more so systematic assessment is still in its infancy. It can be safely assumed that such formalised systems are common practice in various statutory intelligence services. Systemised propositions within the academic realm of Intelligence Studies are, however, markedly limited. In the reviewed literature, only three relatively comprehensive propositions in this regard were identified, namely those provided by the Australian Security Intelligence Organisation (as described by Wing, 1999: 86-94), Bernhardt (2003, 2004) and Quiggin (2007: 24-30) respectively.

Because this study needs to take cognisance of and build on existing knowledge within Intelligence Studies, the propositions by the Australian Security Intelligence Organisation (ASIO) and Quiggin (2007) are concisely reviewed. For reasons to be provided later in this chapter, Bernhardt's (2003, 2004) research is discussed more comprehensively.

The ASIO's proposal clearly reflects the influence of Business Risk Management thinking. The ASIO "applies a structured approach to security risk management" and, to this end, employs a "Security Risk Matrix" (Wing, 1999: 86-87). Wing (1999: 87) summarises the "Security Risk Matrix (SRM)" by way of the following illustration:

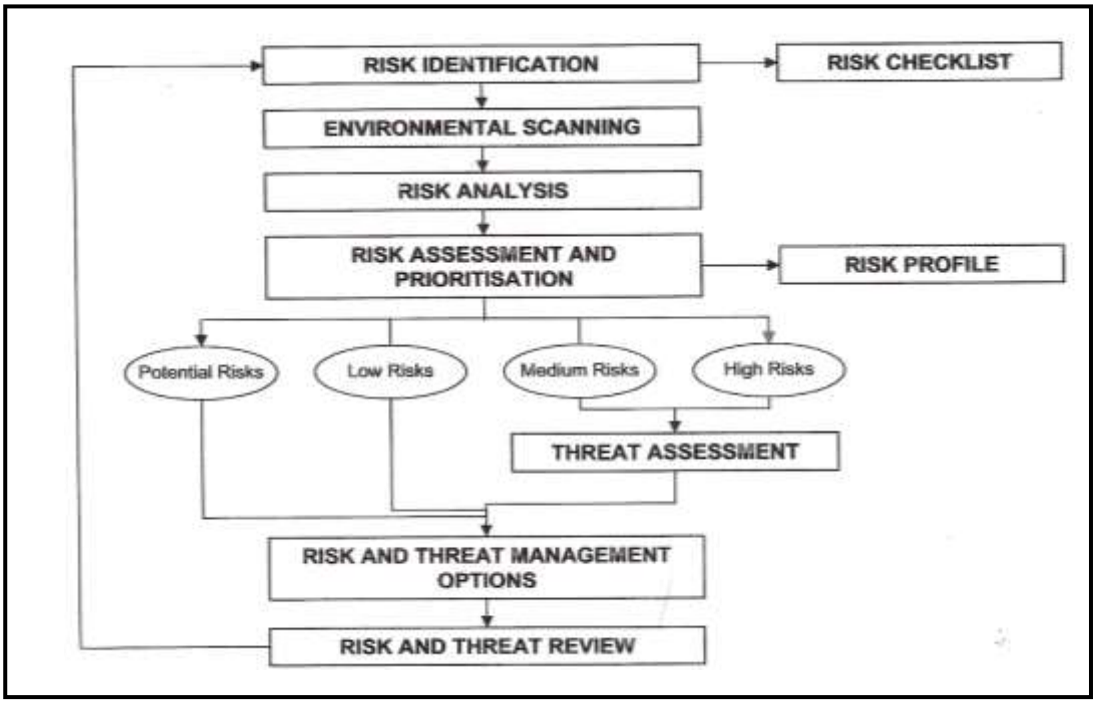
Figure 7: Security risk matrix

- **Likelihood of Threat x Nature of Consequence = Risk**
    - **Intent x Capability = Likelihood of Threat**
        - **Desire x Confidence = Intent**
        - **Resources x Knowledge = Capability**

Source: Wing, 1999: 87.

Similarly to the ASIO, Bernhardt (2004: 63) locates a threat within the broader notion of a risk. For Bernhardt (2003: 142-144), however, a threat is not distinguishable merely as a subset in the computation of a risk. A threat, Bernhardt (2003: 142-144; 2004: 63-64) argues, is “relatively easily definable” and there is general acceptance of the concept (‘threat’) denoting aspects such as a unilateral or mutually aggressive relationship between entities, menacing intent, the capacity to execute menacing intent, and the imminence of such adversarial action. Whereas a “threat” thus is of “an imminent and serious nature, and ... require[s] immediate priority action from government”, a ”risk” could “possibly [be] serious in nature” but is “not necessarily about immediate danger”. Bernhardt (2003: 144) contends a risk to be “a conditional event: it has not yet occurred and certain preconditions must first be realised before it comes to pass”. On the basis of this distinction between a risk and a threat, Bernhardt (2004: 67) posits “Intelligence Risk Management” as the “dominant discipline with a macro-analytical approach” within which “Intelligence Threat Assessment” operates. An “Intelligence Threat Assessment” is therefore “a specialised subdiscipline within the broader confines of Intelligence Risk Assessment; and ... has a distinct micro-analytical approach” (Bernhardt, 2004: 65). Bernhardt (2004: 67) elucidates this postulation on the relationship between intelligence risk and threat assessment by means of the following graphic depiction:

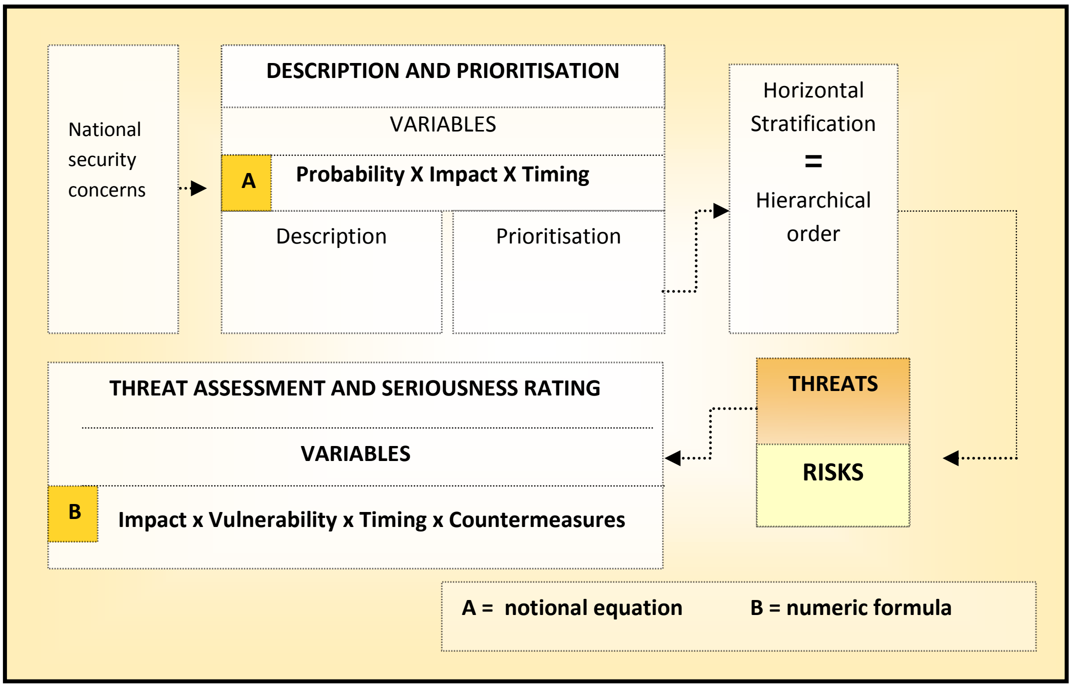
Figure 8: The relationship between intelligence risk and threat assessment



Source: Bernhardt, 2004: 67.

The figure above illustrates Bernhardt's (2003, 2004) key contention that places 'threats' essentially as 'risks' on a higher hierarchical order. Threats are, essentially, high and medium risks. This hierarchical order is arrived at by employing three variables, namely probability of manifestation, actual or potential impact on national security, and the timing or imminence of an undesired situation. Following the hierarchical stratification indicated, threats are subject to a "seriousness rating", which utilises the criteria of impact, vulnerability, timing and countermeasures. Although not graphically depicted as such in his research, the following figure summarises Bernhardt's (2003, 2004) variable-based postulation on risk and threat prioritisation:

Figure 9: Variable-based risk and threat assessment


National security concerns
DESCRIPTION AND PRIORITISATION
VARIABLES
A
Probability X Impact X Timing
Description
Prioritisation
Horizontal Stratification = Hierarchical order
THREAT ASSESSMENT AND SERIOUSNESS RATING
VARIABLES
B
Impact x Vulnerability x Timing x Countermeasures
THREATS
RISKS
A = notional equation
B = numeric formula

Source: Bernhardt, 2004: 63-88.

While Bernhardt's hierarchal order of risks and threats is determined by means of a notional equation (indicated as "A" in Figure 9), a numeric element is added to the "seriousness rating" of threats (indicated as "B" in Figure 9). Bernhardt (2003: 187) provides the following as an example of a rating system in which weight is assigned to threat-related variables:

Figure 10: Intelligence threat assessment – assigning relative weights to threat variables

	Threat 1	Threat 2	Threat 3	Threat 4	Threat 5
Impact	2	2	5	1	4
Vulnerability	2	3	2	4	3
Timing	5	4	2	3	5
Countermeasures	1	4	5	4	4
Seriousness rating	10	13	14	12	16

Key: Least = 1, most = 5.

Source: Bernhardt, 2003: 187.

In what is seemingly a position directly contrary to that of Bernhardt (2003; 2004), Quiggin (2007: 24-25) describes the use of the term ‘threat’ in relation to statutory intelligence as “vague”, “meaningless” and “useless” to the policymaker. For Quiggin (2007: 25) a threat is a “potential for an individual or group to exercise an action which exploits vulnerability. It does not automatically imply the level of danger that exists”. As an alternative, Quiggin (2007: 26) favours the use of the term ”risk”, which is defined as “the probability of harmful consequences which arise[s] from an action taken by a source to exploit a known vulnerability”. In addition to ‘probability’ and the potential extent of ‘harm’, the vulnerabilities of a state and the ‘time horizon’ in relation to an undesired event are posed as key criteria in risk assessment and prioritisation (Quiggin, 2007: 23-43, 199-202, 227-238). Excluding a terminological difference regarding a threat, Quiggin’s view essentially corresponds with that of Bernhardt (2003, 2004). Both Bernhardt (2003, 2004) and Quiggin (2007) present probability, impact/harm and time horizon as central to the assessment and hierarchical prioritisation of national security concerns.

The preceding overview of contemporary views on the concepts ‘risk’, ‘threat’ as well as ‘risk prioritisation’ within Business Risk Management and Intelligence Studies, has highlighted differences in approach and emphasis. Despite these differences, contemporary views within Intelligence Studies share two fundamental suppositions. Firstly, the likelihood of a harmful occurrence and the impact (degree of harmful consequence) of such an occurrence are forwarded as key definitional criteria. Secondly, these definitional criteria are employed as factors in the assessment and prioritisation of risks. Varying from one proposition to the other, additional criteria are added in respect of both the definition and prioritisation of risks. Most of the criteria employed within Intelligence Studies are linked to the factors forwarded within Security and Strategic Studies by Buzan (1991: 8, 134, 138-139) and Hough (2003: 18-19) for differentiating between issues of routine governance and those of relevance to national security. With a view to their utilisation further on in the study, salient risk and threat-related criteria that transpired thus far can be listed as follows:

- The degree to which an occurrence detrimentally impacts or could impact on a nation state’s stability, sovereignty, territorial integrity, fundamental national values and vital national interests.

- The time horizon associated with an undesired situation that entails assessing whether the occurrence is already manifesting, imminent, latent or only foreseen as developing further in the future.
- The adversarial intent, desire and motive to engage in actions that would significantly and determinately impact on national security.
- The capability of an adversary to execute the intended action.
- The vulnerabilities of a state to such adversarial action.
- The effectiveness of existing countermeasures in safeguarding the state against adversarial action and whether extraordinary measures are necessary.

2. 2 THE REQUIREMENT FOR A DISTINCTIVE COUNTERESPIONAGE POSTULATION ON RISK DEFINITION AND ASSESSMENT - AN APPRAISAL OF EXISTING CONCEPTUALISATIONS

The location of the CE framework within the statutory intelligence milieu presents the factors listed above as of obvious relevance to both defining and assessing espionage risks. Less obvious is the manner in which these factors should be aligned and structured to the optimal benefit of the CE framework. If the discourse within Intelligence Studies on risk, threat and risk assessment is in its infancy, such a debate in relation to counterespionage has yet to crystallise. Consulted literature remains silent on a systemised approach to be followed in this regard.

The question thus arises as to whether existing propositions within Intelligence Studies can be applied to the counterespionage sphere. Such a feasibility appraisal should first and foremost consider contextual variances between existing propositions and the CE framework. The indicated proposals within Intelligence Studies assume the utilisation of all-source information and are focused on the analysis functional area (of statutory intelligence). The CE framework, conversely, is restricted to the utilisation of open-source information and has collection as an added dimension. These contextual differences do not necessarily discount the feasibility of adapting existing propositions to the needs of the CE framework. It is the counterespionage focus of the CE framework that constitutes a fundamental difference from current Intelligence Studies propositions. The latter are, without exception, directed at the positive intelligence domain.

The location of the CE framework within counterespionage, this study contends, renders positive intelligence propositions inadequate for viable employment as part of a counterespionage environmental scanning framework. The CE framework requires a conceptualisation of 'risk', 'threat' and 'risk assessment' capable of meeting the distinctive demands posed by the counterespionage milieu. Such a conceptualisation cannot be constructed in isolation from all-source statutory counterespionage. To be of optimal use, the CE framework (as an open-source based espionage risk identification and assessment instrument) needs to be in synergy with, and conceptualised as part of, all-source counterintelligence and counterespionage processes. The CE framework thus requires what does not exist in consulted literature, namely a distinctive counterespionage (conceptual) approach to the notions of risks, threat and risk assessment.

In substantiation of the need for a conceptual approach germane to counterespionage, reference will mostly be made to Bernhardt's research (2003, 2004). As far as could be established, Bernhardt (2003, 2004) currently provides the most comprehensive academic study on statutory intelligence risk assessment and, additionally, his research contains elements highly useful to this study. The use of his work (2003, 2004) as point of reference is reinforced by the previously noted contentions which they share with the proposals forwarded by Quiggin (2007) and the ASIO (1999).

Despite similarities, there are also fundamental differences in the nature, focus and *modus operandi* of counterespionage and positive intelligence. These differences were rather extensively examined in Chapter Two, and only some are referred to in the subsequent validation of the need for a counterespionage approach to the notions of risks, threat and risk assessment.

Relative to positive intelligence, counterespionage is decisively more offensive in its orientation. Consequently, the factors Bernhardt forwards in describing and prioritising risks would rarely carry 'equal weight' or have exactly the same connotations. As shown in Figure 9, factors forwarded by Bernhardt are: 'probability', 'impact', 'timing', 'vulnerability' and 'countermeasures'. By virtue of its offensive function, countermeasures often take centre stage in the counterespionage process. In assessing espionage risks and threats, counterespionage moreover needs to consider opportunities that could be derived from the execution of countermeasures. Such opportunities pertain, *inter alia*, to the disruption of an adversary's informational integrity by means of deception and exploitation. 'Opportunity' thus needs to be added as a factor in assessing espionage risks and threats.

Viewed from a counterespionage perspective, an appraisal of Bernhardt's use of probability in further defining and prioritisation risks and threats illustrates the requirement of a postulation apposite to counterespionage. Probability as used by Bernhardt conveys the degree of certainty over a situation detrimental to national security. As will shortly be demonstrated, 'probability' is appropriate in the demarcation of one but not all categories of counterespionage concerns. Similar to positive intelligence, 'certainty' indeed is central to the description and prioritisation of other counterespionage concerns. However, as a criterion, counterespionage requires a specific form of certainty applicable to all categories of counterespionage concerns. In postulating such a criterion cognisance needs to taken of the distinctive connotations that certainty has in relation to counterespionage.

Certainty, already in short supply within statutory intelligence in general, is an even scarcer commodity in the counterespionage sphere. Thus far, this study has shown espionage to be clandestine, designed to avoid detection and therefore more difficult to detect. On the one hand, and relative to positive intelligence, counterespionage is consequently confronted with a higher degree of uncertainty. On the other hand, and again relative to (civilian) positive intelligence, civilian statutory counterespionage arguably more often requires a higher measure of certainty. Some widely used counterespionage measures, such as criminal prosecution, depend on information that has been verified beyond reasonable doubt. Espionage cases are also notoriously difficult to prosecute successfully. Successful prosecution hinges on the submission of information (in the form of evidence) to which end civilian intelligence services closely cooperate with prosecuting authorities. Other countermeasures requiring information bearing a high level of verification include diplomatic protest, public exposure and *persona non grata* expulsions. Against this background, 'verification' rather than 'probability' emerges as a criterion more apposite to the categorisation of counterespionage concerns.

Similar to other factors discussed, the nature of espionage and counterespionage warrants a different angle in approach to 'time horizon' as criterion for differentiating between categories of counterespionage concerns. It was indicated that Bernhardt holds the "imminence" of an event as a pivotal factor in differentiating between high-order security concerns (threats) and those of a lower order (risks). To briefly recapitulate, Bernhardt (2003: 142-144; 2004: 63-64) deems a "threat" as an "immediate priority", while a "risk" is described as "a conditional event: it has not yet occurred and certain preconditions must first be realised before it comes to pass." In the counterespionage sphere the actual or foreseen impact of an event, rather than the time horizon of the event's actual occurrence, is the decisive consideration in prioritising national security concerns. Arguably more so than in the case of positive intelligence, the time horizon of counterespionage, in respect of the actual occurrence of an event, can also be of a retrospective nature. Classified information procured by adversarial action could, for example, hold present and future ramifications for national security relatively long after the actual perpetration of espionage. In summary, time horizon is as central a factor in counterespionage assessment as it is in positive intelligence, but needs to be clearly qualified in respect of the impact of an occurrence or situation.

A further point to consider against the application of formulae and equations containing equally weighted factors is the predominance that 'impact' more often than not takes over 'certainty' in appraising the seriousness of counterespionage concerns. A suspected act of adversarial espionage, however unverified, with a potentially serious impact on national security will frequently, in priority, exceed another adversarial act of espionage that has been verified beyond reasonable doubt but that has significant, yet less serious ramifications. The weighing of, on the one hand 'impact' and, on the other hand 'certainty', (whether expressed as 'probability' or 'verification') defies quantification by means of notional equations and numeric formulae. Pertaining especially to counterespionage, the following cautionary remark by Lowenthal (2003: 101) is relevant: "Such numerical formulas may be more satisfying than words, but they run the risk of conveying to the policy client a degree of precision that does not exist."

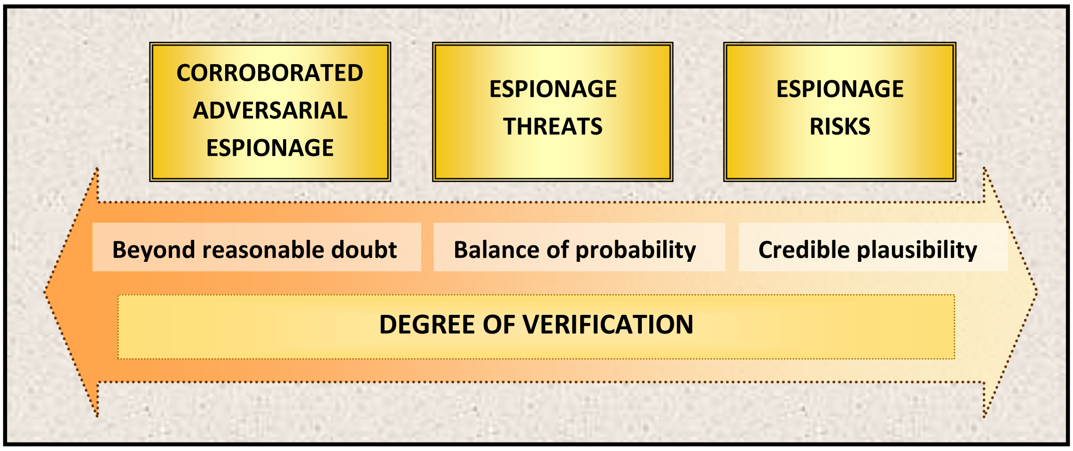
2.3 PROPOSITION ON THE DEFINITION AND ASSESSMENT OF COUNTERESPIONAGE CONCERNS

The foregoing appraisal of Bernhardt's postulation clearly demonstrates the requirement of the CE framework for a conceptual counterespionage approach to the notions risk, threat and risk assessment. The need for a postulation germane to counterespionage does not preclude the employment of factors used in positive intelligence to define and assess risks or threats. On the contrary, reconceptualised in line with the counterespionage reality, and differently aligned, most of these factors are indispensable to the conceptualisation of risk, threat and risk prioritisation that could feasibly be employed in the counterespionage realm.

2.3.1 Defining the concepts corroborated adversarial espionage, espionage threat and espionage risk

A conceptual approach for the defining of counterespionage concerns can, for purposes of subsequent explication, be graphically depicted as follows:

Figure 11: Conceptual approach for the definition and assessment of counterespionage (national) security concerns



The term ‘verification’, previously argued as a form of certainty apt to the counterespionage field, presents an appropriate criterion for the definition and categorisation of counterespionage concerns. At the one end of the spectrum, ‘corroborated adversarial espionage’ pertains to espionage cases verified beyond reasonable doubt. At the other end of the spectrum, an ‘espionage risk’ denotes the possible existence, or future development of a situation that could detrimentally impact on national security. Assertions on the presence of espionage risk are typically based on information that is mostly unverified and often of a circumstantial nature. Nonetheless, tenuous claims on the existence of espionage risks serve little purpose in facilitating effective counterespionage processes. Hence, affirmations on espionage risks have credible plausibility as requisites. As a midpoint, ‘espionage threats’ pertain to verification at a level that justifies assertions on a balance of probability.

Contrary to Bernhardt’s definitional distinction between hierarchically based risks and threats, Figure 11 depicts a horizontal approach to the categorisation of espionage-related security concerns. The labelling of an issue as an ‘espionage threat’ would thus not necessarily imply that it enjoys a ‘higher order of priority’ than an ‘espionage risk’. The horizontal categorisation of counterespionage concerns obviates the reservation earlier expressed that an unverified situation of adversarial espionage with far-reaching impact on national security, would in priority exceed another adversarial act of espionage that has been verified beyond reasonable doubt, but with less far-reaching, yet significant, ramifications for national security.

The use of the term ‘threat’ to denote a higher measure of verification than a ‘risk’ is informed by the semantic and lexicological meaning of these terms. The *Collins Essential English Dictionary* (2006 - online: 2008/08/14; emphasis added) defines a “threat” as “a *strong possibility* of something dangerous or unpleasant happening”, while a “risk” is seen as “the *possibility* of bringing about misfortune or loss.” While this semantic comparison is helpful, more precise definitions pertinently linked to the concept ‘espionage’ are necessary. Within the context of the preceding examination of the concepts risk and threat, and based on the requisites of statutory counterespionage and the CE framework, the following definitions are proposed:

- An espionage risk is a credible plausible situation, resulting from the activities of an opposing intelligence entity, which exists or may develop in a manner which significantly impedes a government’s optimal pursuit of its national security strategy and the realisation of its objectives.
- An espionage threat is a situation, resulting from the activities of an opposing intelligence entity which, on a balance of probability, is deemed to exist or is foreseen to develop in a manner which significantly impedes a government from optimally pursuing its national security strategy and realising its objectives.
- Corroborated adversarial espionage pertains to a situation, verified beyond reasonable doubt, that existed, exists or is developing in a manner which significantly impedes a government from optimally pursuing its national security strategy and realising its objectives.

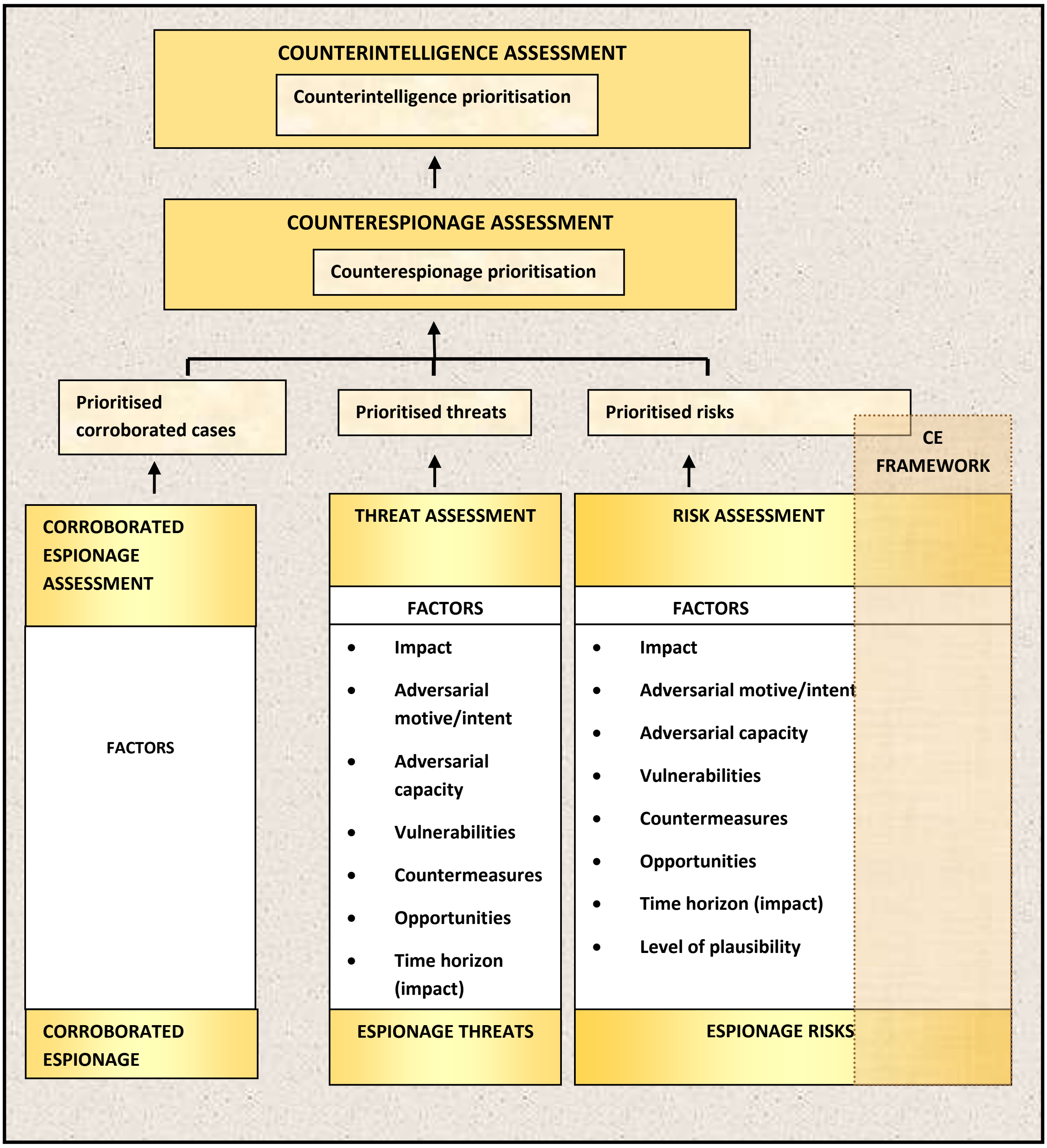
The study frequently refers to espionage risks and espionage threats, while corroborated adversarial espionage is alluded to far less often. This is ascribable to the theme of the study. As substantiated further on in this chapter, the CE framework is an OSINT instrument and does not purport to have an outcome verified beyond reasonable doubt. Figure 11 depicts espionage risks and corroborated adversarial espionage as the two outmost poles on the verification continuum. Both in theory and in practice the distinction between these categories of espionage-related concerns is comparatively unambiguous.

Conversely, and while theoretically differential, the line between espionage risks and espionage threats is in some instances opaque. Moreover, approaches to the collection and assessment of information in relation to espionage risks and espionage threats correspond in various respects. Since corroborated adversarial espionage has been verified beyond reasonable doubt, counterespionage activities in such cases often accentuate the advanced phases of aggressive countermeasures, neutralisation and in some instances the procurement of supporting evidence. Consequently, the *modus operandi* in counterespionage practice of corroborated adversarial espionage in certain respects differs from that followed with regard to espionage risks and threats. Nevertheless, all categories of espionage-related concerns form an integral part of an overarching conceptual (counterespionage) construct. This overarching construct (Figure 11), of which further aspects are examined below, provides the foundation for the configuration of risk assessment within the CE framework.

2.3.2 The assessment of counterespionage concerns with specific reference to prioritisation

In presenting the said overarching conceptual approach, ‘prioritisation’, as one of the facets of the assessment of counterespionage concerns, is used for further elucidation. Later in the chapter, the CE framework is described as a ‘parallel’ counterespionage tool. Within the confines of the CE framework as a parallel instrument, prioritisation in certain respects represents the culmination of the assessment process. It is for this reason that the study’s problem statement specifically included the research question: ‘What criteria can be used to categorise and prioritise espionage risks?’ ‘Prioritisation’ epitomises ‘risk assessment’ in general, and aspects thereof are pivotal to the rest of the chapter. The following conceptual approach, which highlights prioritisation as a facet of assessment, is proposed in this regard:

Figure 12: A conceptual approach to the assessment of counterespionage (national) security concerns with specific reference to prioritisation



Similar to statutory intelligence in general, counterespionage prioritisation involves the ranking of issues in order of importance. It must be emphasised that the 'ranking' should not be equated with 'rating'. Rating involves the assigning of numeric values, whereas ranking as used in this context has a purely qualitative premise. The counterespionage prioritisation process is guided by a qualitative consideration of predetermined factors.[2] As reflected in Figure 12, risk assessment as part of the CE framework, is not the whole of risk assessment within all-source counterespionage. The CE framework's outcome is, in other words, incorporated with espionage risks determined through the all-source counterespionage effort.

Although the factors pertaining to the assessment and prioritisation of corroborated adversarial espionage are not unrelated to those employed in relation to espionage risks and espionage threats, there are variances. However, since this study has open-source based *risk* assessment as theme, these variances are not examined. Of greater relevance is the outline of factors pertaining to the prioritisation (as part of the assessment) of espionage risks, namely:

- The degree to which a credible plausible instance(s) of adversarial espionage could detrimentally impact on a nation state's stability, sovereignty, territorial integrity, fundamental national values and vital national interests.
- Whether an adversary or adversaries have a motive for engaging in espionage (against the own state). Should motive have been established, and whether there are indications of adversarial intent?
- The capacity of an adversary to execute espionage in accordance with the motive and intent.
- The vulnerabilities of the own state to such adversarial action.
- The effectiveness of existing countermeasures in safeguarding the state against the adversarial espionage endeavour, and whether further extraordinary measures are necessary.
- The opportunities that could be obtained by the exploitation of adversarial espionage.
- The time horizon associated with the impact of an undesired situation, which entails assessing whether the impact is already manifesting, imminent, latent or only foreseen as developing further on in the future.

[2] Note that researchers, such as Bernhardt (2003, 2004), rightly refer to such 'factors' as 'variables'. Within the context of this study, the term 'variable' has specific connotations which are elaborated later in this chapter. For purposes pertaining to this section, the term 'factor' is thus used.

- The level of credible plausibility (grounds) on which affirmations of the existence or development of an instance of adversarial espionage and its impact are based.

The first phase of counterespionage prioritisation involves the ranking of concerns within the respective categories. An espionage risk is, for example, appraised against other espionage risks in order to determine its relative importance (priority). Within counterespionage, these factors are not 'checklists' or 'join-the-dots analysis' blueprints. These factors are interrelated, overlap and intended as beacons for directing qualitative analysis. As depicted in Figure 12, the outcome of the first phase is an inventory for each of the respective categories of espionage-related concerns.

As the second phase, a counterespionage assessment holistically prioritises corroborated (adversarial) espionage, espionage threats and espionage risks; arriving at an inventory of statutory counterespionage concerns. The said inventory comprises the listing, description and ranking of espionage concerns in order of priority. In so doing some espionage risks may take precedence over espionage threats and corroborated espionage.

A final prioritisation is done within the broader construct of a counterintelligence assessment. The latter also appraises priorities and challenges in respect of other counterintelligence facets such as personnel security, INSYSEC and physical security. In so doing, the prioritisation of espionage-related concerns is integrated with 'counterintelligence prioritisation' as a whole.

This section examined the assessment of espionage risks from a statutory intelligence perspective as a primary requirement posed to the CE framework. Meeting this challenge requires two preconditions as was indicated. Firstly, a clear definition of espionage risk, and secondly, a structured approach toward the assessment of such risks. It was emphasised that the CE framework (as an open-source based espionage risk identification and assessment instrument) needs to be in synergy with and form part of all-source counterintelligence and counterespionage. Achieving such synergy hinges on a coherent conceptual construct of the notions risk, threat and risk assessment. Existing conceptualisations within Intelligence Studies regarding risk, threat and risk assessment were appraised for feasibility in application to the counterespionage sphere and thus the CE framework. The said conceptualisations were found to be directed towards positive intelligence and not unconditionally apposite to the demands of counterespionage theory and practice. Nevertheless, propositions within Security and Strategic Studies on the concept of a national security threat, as well as postulations within Intelligence Studies, offer useful elements in the construction of a distinctive counterespionage approach to the notions of risk, threat and risk assessment (including risk prioritisation). The proposed overarching counterespionage conceptual approach provides the foundation, and sets the parameters, for the design of a practice-directed 'risk assessment and prioritisation' in Chapters Six and Seven as a constituent of the CE framework.

The parameters for the design of the CE framework are not only rooted in its counterespionage focus but, as the subsequent section argues, the uses and limits of the CE framework are conjointly determined by the nature of statutory intelligence in general.

3. REQUIREMENTS AND CHALLENGES ARISING FROM THE COUNTER-ESPIONAGE FRAMEWORK AS AN AGGREGATE OF INTELLIGENCE TYPES

The preceding section examined some of the requirements that the distinctive nature of statutory counterespionage poses for the design of the CE framework. Although specialised in its counterespionage orientation and its use of open-source information, the CE framework shares an axiomatic, yet central, requirement with other intelligence subdisciplines, namely the generation of a useful intelligence product. Inferring from this seemingly clear-cut requirement, more specific requisites for the CE framework are more complex.

The outcome of the intelligence process is not a homogeneous product. Chapter Two alluded to the fact that 'intelligence as product' in reality consists of various types of intelligence. The product is also not provided to a single consumer. Certain types of intelligence are directed toward the policymaker, while others aim to inform the activities of the state security apparatus in the execution of its core functions. Therefore, the outcome of the intelligence process is accustomed to the needs of the client and in practice varies considerably in terms of the type(s) of intelligence emphasised, included or excluded. More often than not, the product provided to a client is an aggregate of more than one intelligence type.

Which type(s) of intelligence is the CE framework then required to have as outcome? Clarity on the composition of the outcome of the CE framework (in relation to the types of intelligence) is of twofold importance. Firstly, each intelligence type has its distinct uses and limitations. Describing the composition of the outcome of the CE framework, therefore partially defines the uses and limits of this OSINT instrument. Secondly, specific intelligence types are associated with corresponding analytical approaches and nuances in collection. Consequently, the types of intelligence the outcome of the CE framework should consist of profoundly influence its design in both its assessment and collection dimensions.

An academically justifiable description of the outcome of the CE framework needs to be informed by an appropriate typological schema. While the consulted literature makes limited reference to concepts such as strategic and tactical counterintelligence, such descriptions are not in any measure presented as part of a coherent schema (Van Cleave, 2007: 1-3; Zuehlke, 1980: 33-35; Godson, 2001: 187-200). By contrast, literature is replete with descriptions and typologies of intelligence in general (Codevilla, 1992: 204-216; Gill & Phythian, 2006: 85. 88-89; Hulnick, 2007: 5-9; Shulsky & Schmitt, 2002: 41-64; Hough, 2004: 24-30; US, 2006*b*: 36-37; Fleischer & Bensoussan, 2003: 13; Lowenthal, 2003: 2-4; 88-89, 101-103; Kent, 1966: 11-68, 209-220; Steele, 2002*a*: 14, 22-23; Dilworth, 2003: 256-262; Bar-Joseph & Scheaffer, 1998: 332-335, 342-344; Goodman, 1996: 38; Odom,1992: xxiii-xxiv). The variation in typologies and descriptions within Intelligence Studies can mainly be ascribed to differences in emphasis. Typologies and descriptions for the most part are not discrepant, but rather highlight different facets of intelligence. By inferring from these typologies and descriptions, and utilising the limited postulations in literature on counterintelligence and counterespionage, the following is proposed as a typological schema for purposes of this study:

Figure 13: A typological schema for the categorisation of the counter-espionage framework as an aggregate of intelligence types

SCOPE AND LEVEL OF APPLICATION	
This intelligence facet pertains to two dovetailed aspects. Firstly, ‘scope’ as referring to the spectrum and array of national security issues focused on and, secondly, the level of decision-making at which the intelligence is directed. The subtypes of intelligence (strategic, tactical and operational) are conventionally deemed to correspond with consumers’ hierarchical position in the governmental apparatus. A further criterion, tied to the level of decision-making, is the magnitude of the implications such intelligence has for the (own) state’s interests and resources.	
Strategic intelligence	Strategic intelligence is mostly directed toward the policymaker and the top executive level of the state apparatus. It deals with matters that significantly affect vital national interest. Strategic intelligence commonly has a broad scope and provides a ‘distilled’ assessment of multiple longer-term issues relevant to a nation state’s national security objectives and policy. On a strategic level, counterespionage deals with adversarial intent and countermeasures requiring sizable (own) state resources. Strategic counterintelligence and counterespionage, as described by Van Cleave (2007: 2) are about “engaging CI collection and operations as tools to advance national security policy objectives, and, at the strategic level, to go on the offensive to degrade hostile external foreign intelligence services and their ability to work against us.”
Tactical intelligence	Similar to strategic intelligence, tactical intelligence could inform policy and strategy, but is primarily associated with the day-to-day national security decisions. Typically, tactical intelligence is shorter-term orientated and has a more limited scope in that certain issues, rather than multiple trends, are addressed. Relative to strategic intelligence, tactical intelligence has lesser implications regarding the usage of national resources as countermeasures. The larger part of tactical intelligence has as its consumer line-functionaries within a government and notably the security apparatus. The level of application of tactical intelligence is therefore interdepartmental (government departments) and intradepartmental (within the intelligence service itself). As with strategic intelligence, aspects such as adversarial intent are important. The emphasis within tactical intelligence, however, is the practical manifestation of intent in adversarial activities. Tactical counterespionage focuses on the respective adversarial espionage actors’ capabilities, their *modus operandi* and their targets, as well as the effectiveness of own state countermeasures.

<table>
<tr><td>Operational intelligence</td><td>In some states, especially within the military context, ’operational intelligence’ is posited as the intermediary between strategic and tactical intelligence. Within the civilian counterespionage domain, however, operational intelligence can possibly best be described as concerning “the activity of CI itself” (Zuehlke, 1980: 34). It aims to inform the day-to-day activities of a statutory intelligence service and mostly has intelligence practitioners as the consumers.

Hence, operational (counterespionage) intelligence informs pertinent line-functional activities against specific adversarial espionage actions. It involves highly detailed information on adversarial espionage operations, individual clandestine (adversarial) operatives, their psychological profiles and their activities, as well as the operational status of adversarial TECHINT actions. Operational counterespionage also continuously assesses the effectiveness of the day-to-day running of an own service’s neutralisation and collection operations (including the reliability of HUMINT sources).</td></tr>
<tr><td><b>Application to the CE framework</b></td><td>On a strategic level the CE framework aims at determining adversarial motive and intent to engage in espionage against the nation state. The assessment of the relationship between the own state and actual or potential adversaries is, as indicated in Figure Six (Chapter Three), pivotal to such an assessment and is, by its very nature, of a strategic nature. In pronouncing on the capabilities of an adversary to execute such intent, the CE framework incorporates aspects of strategic as well as tactical intelligence. Although adversarial espionage targets and <i>modus operandi</i> have obvious strategic implications, estimations on aspects such as targets and <i>modus operandi</i> constitute the tactical dimension of the CE framework.

The CE scanning process’s outcome has as one of its primary objectives to deliver a product that can be converted to all-source operational activity (Section Eight, Chapter Seven). Since the CE framework is solely reliant on open-source information it would not in all instances provide information of the nature and detail conventionally associated with operational intelligence. Operational intelligence, in its narrower definitional sense, would within the context of CE scanning be generated through the application of espionage indicators.</td></tr>
<tr><td colspan="2"><b>TIME ORIENTATION</b></td></tr>
<tr><td colspan="2">Long-term (mostly strategic) intelligence, at the one end of the spectrum, addresses far-reaching national security implications, and serves to inform policy over a period stretching over months and years. At the other end of the spectrum, operational intelligence is concerned with the immediate situation. In relation to counterespionage, it was previously argued,</td></tr>
</table>

<table>
<tr><td colspan="2">intelligence also has a ‘retrospective time-orientation’. Although with a firm view on current and future implications, transpired acts of adversarial espionage are also the subject of assessment and collection (investigation). Follow-up actions subsequent to the identification of moles (e.g. Ames and Hansen as was discussed in Chapter Three) serve as examples. At an operational level, retrospective analysis evaluates concluded counterespionage operations or incidences with a view to inform own service tradecraft in collection, countermeasures, as well as counterespionage analysis practice (Zuehlke, 1980: 34).</td></tr>
<tr><td colspan="2"><b>Application to the CE framework</b></td></tr>
<tr><td colspan="2">The CE framework retrospectively assesses transpired incidences of espionage not primarily to inform own service tradecraft, but with a view on identifying current and future (counterespionage) ramifications for national security. The CE framework’s focus also extends relatively far into the future. Identifying unfolding trends in the macro-environment expected to affect international security in the next decade (or even further) is part of the aim of the CE framework. While taking into account the past, the outcome of the CE framework should firmly reflect on the present and the future.</td></tr>
<tr><td colspan="2"><b>TYPES OF ANALYSIS AND PRODUCTS</b></td></tr>
<tr><td colspan="2">Arguably the most complex to conceptually structure, this facet of intelligence refers to one or (in most instances) more of the following aspects: the nature of the analysis activity and methodology used; the subject matter of analysis and collection; and the kind of product provided to the client. In the consulted literature, reference is often made to Kent’s (1966: 1-68, 209-220) seminal assertion on the three main forms of intelligence, namely “basic-descriptive”, “current-reportorial” and “speculative-evaluative” intelligence.</td></tr>
<tr><td>Estimative intelligence</td><td>Estimative intelligence can be seen as a contemporised labelling of Kent’s (1966: 39-40) notion of “speculative-evaluative” intelligence. Estimative intelligence is of a strategic nature and provides judgment on possible future developments of national security relevance. Estimative intelligence should not pretend to offer an exact vision of the future. In the words of Lowenthal (2003: 102): “‘Prediction’ foretells the future – or attempts to do so. Estimates are more vague, assessing the relative likelihood of one or more outcomes.” No compelling reason could be found for not broadening, in relation to counterespionage, ‘estimative intelligence’ to include ‘speculative-evaluative’ propositions on current developments and past events (with present and/or future) implications for national security.</td></tr>
<tr><td>Current intelligence</td><td>As suggested by the term, ‘current’ intelligence denotes reportorial reporting with the aim of providing the consumer with the latest information available on current events. Products of this nature often constitute the bulk of intelligence</td></tr>
</table>

	production. Current intelligence shares characteristics with journalism and its time orientation is usually not beyond "a week or two in future" (Lowenthal, 2003: 88).
Warning intelligence	Warning intelligence, also described as 'indications and warning intelligence', incorporates elements of current, estimative and other types of intelligence (Hough, 2004: 24). Warning intelligence can be of a tactical and a strategic nature. It is of pivotal importance to this study and is examined in more detail later on.
Basic intelligence	This type of intelligence entails what has been described by Kent as "basic descriptive intelligence". Quantitatively, basic intelligence is by far the most comprehensive and can be of an encyclopaedic proportion. Within counterespionage, basic intelligence would include, for example, comprehensive profiles on countries sponsoring adversarial espionage as well as background memoranda on actual and potential adversarial espionage actors.
Target intelligence	Adopted from military intelligence, target intelligence within the counterespionage context refers to products compiled on adversarial entities targeted for offensive measures. In its broadest sense target intelligence is informational warfare's 'order of battle'. In a narrower connotation, target intelligence identifies and nominates specific adversarial assets as well as vulnerabilities for offensive counterespionage action and serves as a status report on the progress of such offensive action. Target intelligence is therefore a specialised category of intelligence on an operational level.
Specialised intelligence	Various criteria can be used for delineating 'specialised intelligence'. At the strategic and tactical levels, specialised intelligence can be used in reference to the subject matter, such as political intelligence, economic intelligence, environmental intelligence and technological intelligence. Specialised intelligence can also refer to the various intelligence fields that require specialised knowledge and distinctive methodologies, like counterterrorism, counterproliferation (of WMD) and counterintelligence. On its own, counterintelligence consists of interrelated subfields of specialisation such as counterespionage and intelligence psychology (which is used defensively as part of personnel vetting and offensively in the profiling of HUMINT targets).
Application	The open-source identification and description of espionage risks necessitate the collection and assessment of a substantive amount of basic intelligence in relation to both the 'own state' (Section 6.1, Chapter Six) and potential

to the CE framework	espionage adversaries (Section 3.3, Chapter Seven). While indispensible to the environmental scanning *process*, the CE framework's *outcome* however precludes basic intelligence of such an encyclopaedic nature. The CE framework is a form of specialised intelligence in two respects. Firstly, the CE framework serves counterintelligence, which in itself is a specialised form of intelligence. Secondly, the CE framework is required to identify and assess espionage risks emanating from specialised intelligence fields such as political, economic and technological intelligence. This should be reflected in the CE framework's design and its outcome. The CE framework's final product should furthermore be balanced in its inclusion of estimative, warning, current and target intelligence (Figure 64, Chapter Seven). In addition, the CE scanning process should be designed to allow for the issuing of interim, warning products during the scanning process (Section 3.3, Chapter Six).

In line with an earlier contention, the foregoing categorisation shows that the CE framework is envisaged to be an aggregate of various intelligence types, with the *caveat* that it is interwoven with other intelligence types, such as 'indications and warning intelligence' (hereafter referred to as 'warning intelligence') which can be seen to be the predominating core of the CE framework. Warning intelligence aims to limit "surprises" that could have detrimental implications for national security (Gill & Phythian, 2006; 81; Hulnick, 2007: 6-7; Quiggin, 2007: 45-46, 117-118, 131-145; Hough, 2004: 24-25; Lowenthal, 2003: 2-4 88-89, 101-103; Shulsky & Schmitt, 2002: 62-64). The CE framework is essentially about warnings on a specific category (counterespionage) of "surprises", namely adversarial espionage activities not detected through the all-source endeavour.

Such surprises can be of a tactical or strategic nature. According to Lowenthal (2003: 2), a "strategic surprise" pertains to "threats, forces, events, and developments that are capable of threatening the nation's existence". Conversely, a tactical surprise "when it happens, is not of sufficient magnitude and importance to threaten national existence" (Lowenthal 2003: 2). Differentiating between tactical and strategic surprises, however, is more encompassing than considering only the "magnitude and importance" in endangering national security.

Whether it is at a strategic or tactical level, the signature role of warning intelligence – and thus the CE framework – is to discern the intentions of adversaries of a nation state. In this respect, the tactical and strategic warning dimensions of the CE framework are inseparable and of equal importance. At a strategic level, the macro-environmental and adversarial security perceptions are assessed in order to project adversarial strategic (espionage) motives and intent estimatively. At the tactical and operational levels, information is gathered and assessed to infer an adversary's *modus operandi,* targets and activities.

As implied above, the dualistic strategic-tactical focus of the CE framework has methodological implications. The CE framework is a warning intelligence instrument, required to consider in its design approaches and methodologies befitting this intelligence type. Approaches and methodologies in relation to warning intelligence vary from formalised systems that rely on predetermined indicators, to estimative practices such as trend exploitation (Hough, 2004: 24). By virtue of providing 'tangible' pointers, indicator-based methods are useful in guiding collection and assessment. Indicator-based methods, however, also have an inherent weakness: Setting the warning threshold too low, results in the "crying wolf" syndrome (Lowenthal, 2003: 102). Setting the warning threshold too high, has as likely consequence the failure to warn on developments of national security concern. Estimative approaches allow more flexibility in both qualitative anticipation and the issue of warnings, but lack the specificity of indicator-based methods. Best suited for the CE framework is a systemised process that combines estimative approaches and indicator-based methods.

This section, in summary, forwarded a typological schema according to which the desired outcome of the CE framework was assessed. While most intelligence types were found to be relevant to its focus, the CE framework is primarily required to serve as a warning instrument. Meeting this challenge poses certain requisites for the CE framework, of which the postulation of indicators and variables is arguably the most central. The measure of the effectiveness of the CE framework was indicated to be its contribution in limiting national security surprises. Yet, the next section contends, within the statutory intelligence realm surprises and failure can be limited, but are to a certain degree inevitable.

4. THE MODERATION OF INTELLIGENCE FAILURES AS REQUIREMENT FOR THE COUNTERESPIONAGE FRAMEWORK

Requirements posed to the CE framework, such as those emanating from the CE framework as a warning intelligence instrument; serve as benchmarks for the successful utilisation of this instrument in the counterespionage milieu. Absolute success within statutory intelligence is, however, an unachievable ideal. The CE framework does not escape the predicament of statutory intelligence in general, namely the inevitability of failure. While statutory intelligence is fallible, sound intelligence practice can reduce the propensity for failure. Successful statutory intelligence services therefore recognise and manage factors in intelligence practice that contribute to failure. The CE framework has to accommodate factors underlying intelligence failures and contain propositions for the moderation of failure. Pronouncing on failure and factors contributing thereto, have as a precondition a delineation of the concept 'intelligence failure' in general, and as it pertains to the CE framework in particular.

4.1 A DELINEATION OF THE NOTION OF STATUTORY INTELLIGENCE FAILURE WITH SPECIFIC REFERENCE TO THE COUNTERESPIONAGE FRAMEWORK

Unsurprisingly, recent bodies of inquiry in the US (2004*a*; 2005*b*) and UK (2004) are vocal in their criticism of the 'failure' of these countries' intelligence communities in respect of incidents such as 9/11, 7/7 and the WMD allegations levelled against Iraq. Bodies of inquiry are appointed by decision-makers *de facto*. Equally unsurprising therefore, is the scant attention afforded in the inquiry reports on the role that decision-makers' flawed comprehension and inept utilisation of intelligence played in manifested intelligence failure. Still valid after more than two decades since it was first made, is the following assertion by Betts (2004: 97):

> In the best-known cases of intelligence failure, the most crucial mistakes have seldom been made by collectors of raw information, occasionally by professionals who produce finished analyses, but most often by the decision makers who consume the products of intelligence services.

The decision-maker *per se* is not infrequently the source of actual and perceived intelligence failure. More recently, and with reference to Betts's assertion, Hulnick (2007: 6) remarked that: "[P]olicy officials expect the intelligence system to be all-knowing, all-seeing, and always correct." Perceived intelligence failure thus comprises unrealistic expectations that disregard the limitations of intelligence. Such perceptions are, in other words, 'false' in the sense that intelligence is demanded to deliver what it cannot. The predicament concerning counterespionage is even more complex. Attesting to this is the following assertion by a former Director of the CIA, William Webster (in Wettering, 2000: 294): "When you're catching spies, you have a bad counterintelligence service.

When you're not catching spies you have a bad counterintelligence service. You can't have both ways!"

Applied to the context of this study, the outcome of the CE framework should be gauged against the limits of statutory intelligence which are the limits of the framework. In addition to the limits inherent to statutory intelligence, the sole reliance of the CE framework on open sources restricts the 'certainty threshold' of its outcome, as was previously noted, to assertions at the level of plausibility. Moreover, the CE framework is not a crystal ball or a definitive spy-catching horoscope through which espionage risks can clairvoyantly be determined. Information gathered and assessed will be "circumstantial not conclusive" (Gilluffo, Marks & Salmoiraghi, 2002: 72). The motives of adversarial espionage actors can be understood; an espionage adversary's 'mind' can, however, not be 'read' (Gilluffo, Marks & Salmoiraghi, 2002: 72). Within the context of these qualifications arises the question: "What then would constitute an 'actual' failure in respect of the CE framework?" The CE framework would be deficient if it does not allow for, with reasonable consistency and accuracy, collecting and assessing open-source information in a manner that:

- Identifies and anticipates trends in the macro-environment that impact or could potentially impact on adversarial espionage and the practice of own state statutory counterespionage;
- provides warning on espionage risks that could plausibly be deemed as detrimental to the advancement and protection of the own state's vital national interests; and
- infers from open-source information plausible adversarial espionage priorities and *modus operandi*.

To this end, and with reference to Betts's (2004: 97) quoted assertion, it is required of the CE framework to take cognisance of, and moderate through its design, factors generally deemed as causal to deficient analysis and collection. These factors, as reflected in consulted literature, can concisely be listed and described as follows (Gill & Phythian, 2006: 104-124; Lowenthal, 2003: 6-8; Shulsky & Schmitt, 2002: 64-69; Godson, 2001: 187; Lapstra & Knip, 2005: 174; Quiggin, 2007: 56-58; Gilluffo *et al*, 2002: 61-62, 67, 70, 72-73):

- An own-state centric view, which refers to the assumption that adversarial entities 'think and act' in the same manner as the own state. In the case of counterespionage, this mindset presupposes that adversarial intelligence actors 'reason' and operate in the same fashion as the own state's intelligence service(s). An implication of this mindset is that the intentions and capabilities of espionage adversaries could be misread, underestimated, overestimated or otherwise wrongly assessed. Depending on the definitional preference of Intelligence Studies scholars, 'own state centrism' is alternatively labelled as 'ethnocentrism' or 'mirror imaging'.

- Mirror imaging, in the view of this study, refers to the projection of the intentions and especially the *modus operandi* of one espionage adversary onto another. A hypothetical example would be the assumption that the intentions and *modus operandi* of the intelligence services of EU member states mirror one another.
- Over-reliance on 'trusted' sources and certain categories of information. In counterespionage especially, and at the expense of balanced all-source fusion, the importance of classified information is not infrequently overstated. In so doing, receptiveness to information that does not concur with the prevailing 'intelligence picture' is also impeded.
- Stagnation, which suggests a conceptual inflexibility to accommodate rapid changes in the espionage and statutory counterespionage milieu. Chapters Two and Three, for instance, showed certain contemporary views on counterintelligence as still retaining the Cold War paradigm that holds foreign intelligence services to be virtually the whole of the espionage threat confronting the nation state.
- Received opinion, as referring to the uncritical application of 'conventional wisdoms' (assumptions widely accepted to be valid).
- Groupthink that denotes an ethos in which conformity takes precedence over critical judgments and whereby the dominant opinion prevails in the interest of consensus.

4.2 THE COUNTERESPIONAGE FRAMEWORK AS AN INSTITUTIONAL SOLUTION TO AN INSTITUTIONAL PREDICAMENT OF FAILURE

The aforementioned factors causal to deficient counterespionage analysis and collection are simultaneously at the root of, and symptomatic of, an institutionally atrophic counterespionage structure. The problem statement of the study highlighted counterespionage atrophy as a consequence of an over-reliance on classified information, which leads to a self-feeding cycle of prioritisation, collection and analysis. Over-reliance on classified information on its part is interlinked with other factors, mutually reinforcing, yet causal to counterespionage failure. Received opinion, for example, reinforces the self-feeding cycle of prioritisation, collection and analysis. On its part the self-feeding cycle 'validates' received opinion. Experience has revealed an over-reliance on classified information also to be accompanied by an institutional ethos which is inflexible to information and notions not congruent with the prevailing counterespionage intelligence picture. Typical manifestations of an over-reliance and a rigid ethos include mindsets such as own-state centric views, mirror imaging and stagnation.

Since causes of intelligence failure are interrelated, the aim of the CE framework to address an over-reliance on classified information by delivering a high quality OSINT product, would also moderate other factors causal to failure. Depending on the manner in which it is institutionally implemented within an intelligence service, the CE framework could hold more benefits than the mere delivery of a supplementary OSINT product. It can be part of an institutional solution to the institutional predicament of espionage failure. As such, it is an expansion of the existing notion, within the statutory intelligence milieu, of "competitive analysis". Although Betts (2004: 103-105) takes a rather sceptical view, several other authoritative authors (such as Shulsky & Schmitt: 2002: 70-73; Lowenthal, 2003: 13-14, 99-100, 103-105; Gill & Phythian, 2006: 106-107) as well as official documentation (US, 2005*b*: 404-407), posit "competitive analysis" and the establishment of a "devil's advocate" as having merit as institutional measures in addressing intelligence failures. Although related, the concepts of a 'devil's advocate' and 'competitive analysis' are differentiable. A 'devil's advocate' approach comprises a formalised measure that has as explicit aim holding views that directly oppose prevailing assessments (Gill & Phythian, 2006: 106-107). 'Competitive analysis', conversely, is not necessarily implemented with the principal aim of advancing directly opposing views. As suggested by the term itself, competitive analysis has as purpose to foster the parallel production of competing assessments which are compiled by project teams located in "analytical centres within a government, each of which has the right to formulate and distribute its own assessments" (Shulsky & Schmitt: 2002: 70). Competitive analysis can entail 'contests' between the analysis centres of the respective intelligence services within an intelligence community and/or be of an intradepartmental nature (i.e. competing teams within a single statutory intelligence service).

In its aim to create an objective distance from which to arrive at an 'independent' intelligence assessment, the CE framework is, at a notional level, comparable to competitive analysis. Similar to the latter, the application of the CE framework would in most instances not be a task performed by an individual, but requires a dedicated working group that is described in US statutory intelligence lexicon as a “red team” (US, 2005*b*: 409). Despite notional and methodological similarities, the CE framework diverges from competitive analysis in four respects.

Firstly, the CE framework is directed toward an outcome that is parallel and supplementary to, but not in competition with, the broader counterespionage function. Secondly, the CE framework is not only about analysis, it also has a collection constituent. It is this process of parallel collection that is central to limiting the self-feeding cycle of prioritisation within counterespionage. The fact that the information collected for assessment is exclusively open-source based gives rise to a third difference with competitive analysis, which typically involves the assessment of not only open sources, but also grey and classified information. Despite their aim to arrive at independent and contesting products, the different competitive analysis teams more often than not use the same informational database. Self-evidently, access to the same information is not most conducive to the generation of innovative insights and analyses. The fact that the CE framework also bases its assessments on information independently collected, enhances its (the CE framework’s) capacity to provide fresh perspectives. Lastly, competitive analysis and the CE framework differ in client market and dissemination process. Whereas competitive analysis typically results in products being distributed to the top leadership of a statutory intelligence structure and/or the policymaker, the CE framework has as its consumer the counterespionage structure.

While similarities thus exist with competitive analysis, the CE framework cannot be categorised as a ‘competitive’ analysis instrument. In addition, the use of the qualifier ‘competitive’ (in relation to competitive analysis) would be confusing within the context of this study. Chapter Six, for example, refers to easily confusable concepts employed within Business Intelligence Studies, such as ‘competitive intelligence’, ‘competitor intelligence’ and ‘competitor analysis’. For the indicated reasons, the CE framework can more aptly be described as a ‘parallel statutory intelligence instrument’.

This section examined the phenomenon of statutory intelligence failure with specific reference to the CE framework. Although intelligence failure is in certain respects inevitable, factors causal to failure can be moderated through intelligence practice. As a parallel instrument of collection and assessment, the CE framework can contribute toward limiting the propensity of failure within the statutory counterespionage sphere. The usefulness of the CE framework as a 'parallel counterespionage instrument' stands in direct correlation with the effective utilisation of open-source information and is explored in the next section.

5. REQUIREMENTS AND CHALLENGES EMANATING FROM THE COUNTERESPIONAGE FRAMEWORK AS AN OPEN-SOURCE INTELLIGENCE INSTRUMENT

In highlighting the differences between a parallel intelligence instrument and competitive analysis, the preceding section emphasised that the CE framework has both analysis and collection as composites. In a similar vein, but from a theoretical perspective, Chapter Two also posited environmental scanning as consisting of collection and analysis. It was indicated that scanning extends beyond the gathering of bits of data, to the processing of information and the rendering of 'legible images'.

This section concretises the theoretical supposition in Chapter Two by explicating the CE framework as the 'sensing' of the environment through the gathering of *open-source information* and the rendering of 'eligible images' by means of *open-source intelligence*. Two interrelated requirements for the CE framework flow from this assertion.

Firstly, the CE framework should be congruent with 'what OSINT is'. A clear demarcation of the concept 'OSINT' is thus essential. This would include answering the questions: "What is OSINT and what is it not?" and, "What can OSINT do and what can it not do within the statutory intelligence context?" In responding to these questions, further essential features and elements of the CE framework are demarcated. It must be emphasised that this demarcation is done as part of an overview of OSINT within the statutory intelligence milieu in general. Since the CE framework function is envisaged to be performed as part of the broader statutory OSINT function, an examination of OSINT, in broader terms than only in its application to the counterespionage sphere, provides a vital context. In addition, an overview of this nature conceptually integrates the CE framework as part of statutory OSINT. Secondly, it is required of the CE framework to draw optimally on the advantages OSINT offers, while simultaneously limiting the pitfalls associated with OSINT.

5.1 DISTINGUISHING BETWEEN OPEN-SOURCE INTELLIGENCE, OPEN SOURCES AND RELATED CONCEPTS

As suggested above, open-source information is used in, but is distinguishable from open-source intelligence. Similarly open-source data is distinctive from open-source information and open-source intelligence.

5.1.1 Defining open-source data, open-source information and open-source intelligence

Burke (2007: 10) defines and explains the relationship between these concepts as follows:

> The [OSINT] process begins with open source data (OSD), the raw information from the primary source, and must then be assembled through an editing process to filter and validate. This then results in open source information (OSIF) that can be disseminated as newspaper articles, books, TV and radio broadcasts, and on the internet. Only after OSIF has been deliberately discovered, analyzed, and disseminated to a select audience in reference to a specific question [in this case counterespionage] is true OSINT created.

The *NATO open source intelligence handbook* (NATO, 2001: 2-3; emphasis in the original), from which Burke's description is partially drawn, defines OSINT more comprehensively as follows:

> OSINT is information that has been deliberately discovered, discriminated, distilled, and disseminated to a *select audience* ... in order to address a *specific* question. OSINT in other words, applies the proven process of intelligence to the broad diversity of open sources of information, and *creates intelligence*.

The filtering, validation and formatting of OSD is an elementary process and frequently involves the use of software agents, which are increasingly expanding into the realm of artificial intelligence. The generation of OSIF from OSD is, for the larger part, at the praxis level. This study is primarily a micro-theory and consequently excludes the derivation of OSIF from OSD. What is at the centre of the study's focus is the generation of OSINT from OSIF.

5.1.2 Distinguishing between open sources and open-source information

OSIF, to state the obvious, yet important, is captured in open sources. Although brief reference has previously been made to the notions of 'open sources' and 'open-source information', these concepts are of such centrality to OSINT that a more in-depth examination is required. After all, the stance taken on the nature of open sources profoundly influences the way in which OSINT is produced. Dimensions warranting further elaboration are the delineation of open sources *vis-à-vis* grey sources and clandestine sources; the recorded format of open-source information; and the different types of open sources.

By implication, open-source information is that category of information that excludes information originating from grey and clandestine sources. Chapter Three remarked on the fact that open and clandestine sources are definitional opposites and the distinction between these two informational categories is thus fairly unambiguous. In the more complex differentiation between open and grey sources, criteria employed were indicated to be, *inter alia*, the cost of acquiring information ('financial cost') and the acquisition risk ('operational risk'). Acquisition risk includes, but is not limited to, the degree to which the procuring of information could compromise the own state's intelligence priorities, as well as the level to which a statutory intelligence service desires to conceal the activity and content of information procurement. In comparison to grey sources, open-source information acquisition is commonly accepted to carry a substantially lower financial cost and acquisition risk. It must be emphasised that the procurement of open-source information is, contrary to a popular misconception, neither completely free nor deprived of all acquisition risk (US, 2007*c*: 7; NATO, 2001: 28; US, 2006*b*: 18-19). The procurement of even basic open-source information, such as newspaper articles, items and Internet searches, involves some cost. Similarly, widely used open-source retrieval methods can compromise an intelligence service's activities, interests and *modus operandi*. Examples of such potentially compromising methods include the retrieval from a public source (for example a library), articles on a specific topic (which reveal an intelligence service's 'profile of interest'), and Internet searches (which leave an electronic 'footprint').

While useful, the criteria used in distinguishing between open sources and grey sources are relative and determined by an acquirer's perception. For a private individual the cost of ascribing to premium information databases and information services may seem astronomical. Measured against the total financial resources of many statutory intelligence services though, the cost of utilising such commercial databases and services is minuscule. Not more than one percent of the US statutory intelligence budget is, for example, allocated to OSINT (Mercado, 2005: 2). For statutory intelligence services, acquisition risk is thus frequently the predominating criterion in differentiating between open and grey sources. As a result, open sources within the statutory intelligence milieu could include - what in other contexts would be regarded as - grey sources. Appropriating its location in the statutory intelligence sphere, the CE framework likewise considers open sources to include those available at some financial cost but at a low acquisition risk. Drawing on the views of NATO (2001, 5-11) and the US (2007*c*: 6-7), and without claiming a fully inclusive listing, open sources in respect of the CE framework are deemed as pertaining to the following:

- Traditional media sources such as newspapers, television, radio and magazines.
- Commercial information databases and information services, which are increasingly of an on-line nature. Premium databases provide editorially selected, authenticated and user-friendly information (NATO, 2001: 7). *Factiva*, *Lexis-Nexis* and *Dialogue* are examples of market leaders in the provision of such premium services (NATO, 2001: 7).
- Information derived from commercial imagery.
- Information overtly obtained from "professional and academic sources such as conferences, symposia, professional associations, academic papers, dissertations and theses, and experts" (US, 2007*c*: 6).
- Information procured at a low acquisition risk from a diverse range of entities within the private sector such as NGOs, commercial enterprises, associations, societies, and clubs.
- Unclassified governmental information which includes certain government reports, legislation and legislative debates, public speeches, press conferences and the like.
- Information obtainable through the Internet, which will be discussed in greater detail below.

As a premise for further observations on the Internet, and as a background for comments on the format of open-source information, it is necessary to briefly recapitulate and expand on an aspect raised in Chapter Three. Information of all categories resides in a combination of humans and systems. If not recorded, information residing in humans (be it as the source, collector or assessor) or generated by systems (e.g. communication signals) remains intangible. Information of whatever category is usually recorded in electronic (including digital) and/or 'hard copy' format. Depending on the nature thereof, a system performs one or more of the following functions: generating information, recording/capturing of information, serving as a repository of information, and as a mechanism for the retrieval of information. The Internet is highly flexible in fulfilling all these functions and has evolved into an indispensable OSINT tool. In this regard the NATO's (2001: v) *Open source intelligence handbook* states that: "The Internet is now the default C4I [Command, Control, Communications, Computers and Intelligence] architecture for virtually the entire world. The principal exceptions are most militaries and intelligence organizations ... To exclude the information flow carried by the Internet is to exclude the greatest emerging data source available." The Internet has indeed opened "remarkable doors" and the "onward march of discovery and technology" in the coming decades is certainly difficult to "imagine or comprehend" (Clift, 2003: 6). Just as certain are the "formidable new challenges that the Internet era poses for the work of intelligence" (Clift, 2003: 6). Meeting these challenges requires that due cognisance be taken of the nature and limitations of the Internet.

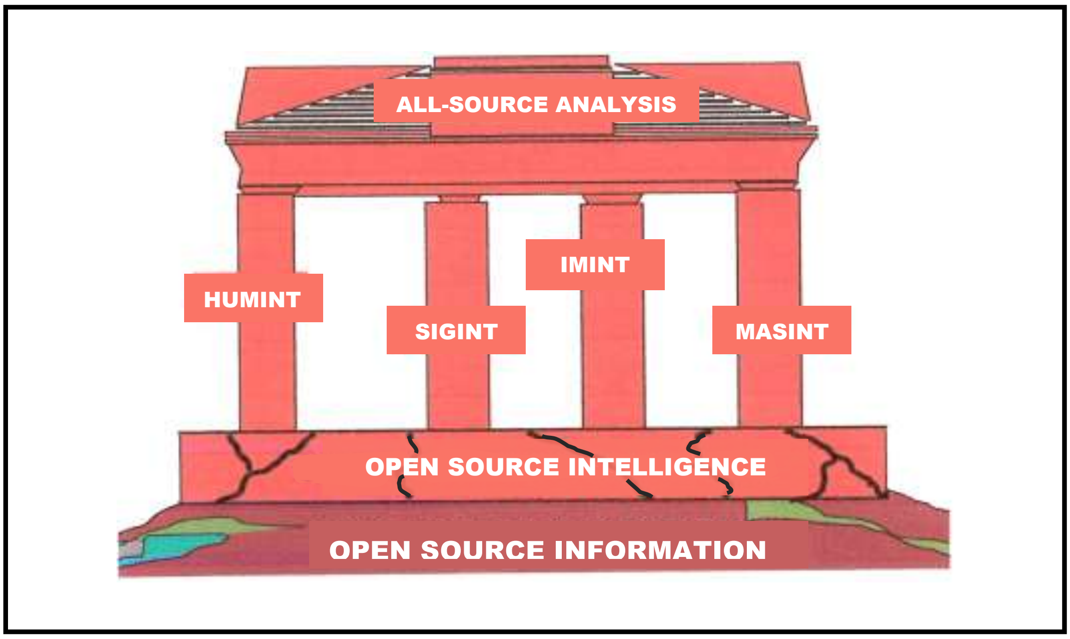
It is precisely the Internet's positive attributes that can, and probably have fuelled an over-reliance on, and unbalanced utilisation of, this open source within various civilian intelligence communities. Over-reliance on an information source, as was earlier noted, invites intelligence failure. Experience increasingly demonstrates the Internet to be neither the alpha and omega of open sources, nor the wonder solution of the need for timely, relevant information (Bjore, 2002: 81). According to some estimates up to 80 percent of information remains in printed form in libraries and similar repositories (Jardines, 2002: 10). This figure corresponds with findings of studies conducted by the US intelligence community which established that "some 80% of what a commander requires, is neither digital in format, in English or, often, unpublished" (NATO, 2002: 5). While the 'information age' is characterised by a rapid expansion in digital information, this growth is matched by a collateral rise in the volume of printed material. The 80:20 ratio is thus unlikely to change significantly in the foreseeable future (Jardines, 2002: 10). With the average lifespan of Internet sites at less than two months, note should also be taken of the volatility of the Web (Jardines, 2002: 10). Moreover, the manner in which the Web operates allows for practically unrestricted additions (‘posting’) of unaccredited and unverified information. Maximising the benefits that the Internet has to offer clearly places a high demand on skilful analysis (Bjore, 2002: 82). In as far as the CE framework is concerned, effective utilisation of the Internet as open source also requires proficient collection.

The Internet, central as it is to OSINT, is just one of a number of open sources. Similarly, CYBINT of which the Internet forms part, is one of several collection subdisciplines. Effective OSINT presupposes a balanced and integrated approach that incorporates the diversity of open sources and the various collection subdisciplines. The *modus operandi* by which such integration is achieved is determined by the conceptual position taken on the relationship between, on the one hand OSINT, and on the other hand, collection subdisciplines and other information categories (grey and secret information). Phrased more practically and applied to this study, the view on the relationship between OSINT, other information categories and the collection subdisciplines will impact decisively on the design of the CE framework. The CE framework therefore has a requirement to forward a conceptual proposition on this relationship best suited for overt counterespionage environmental scanning.

5.1.3 Open-source intelligence within the context of collection subdisciplines and other informational categories

NATO (2001: 36) which is seen as the leading authority on OSINT in the statutory arena (Burke, 2007: 10), provides the following graphical representation of the relationship between OSINT, the “traditional collection disciplines” and other informational categories:

Figure 14: Open Source – all-source relationship

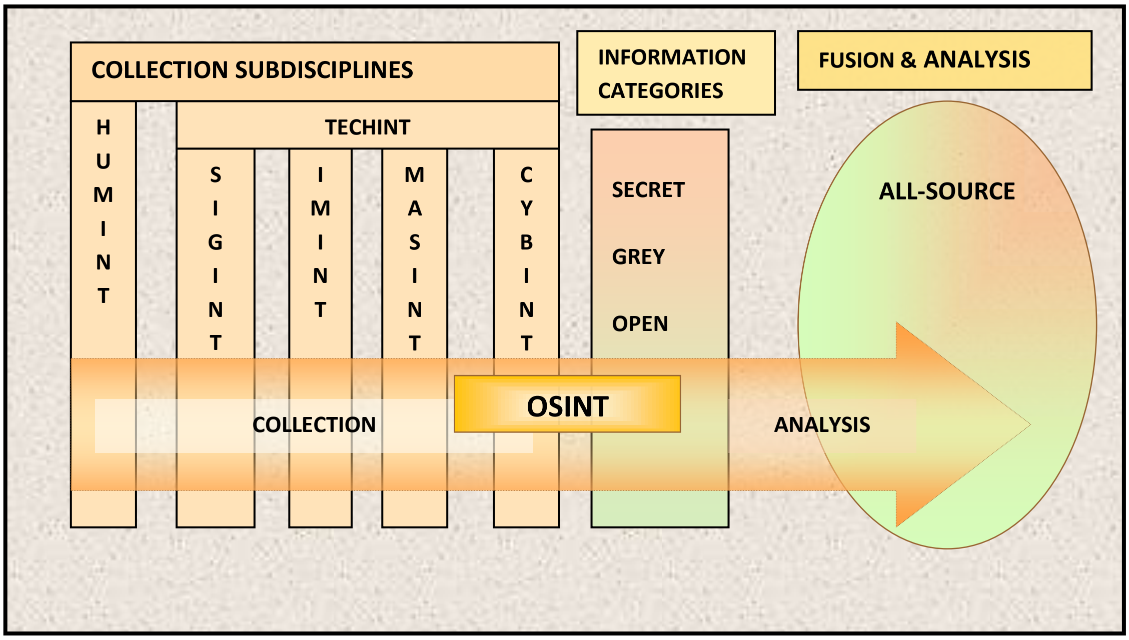


Source: NATO, 2001: 36.

NATO's proposition on the relationship between OSINT, the traditional collection subdisciplines and other informational categories as contained in the preceding figures is not apposite to the needs of the CE framework for several reasons. OSINT and OSIF are posited by NATO (2001: 36-37) as related to, but distinct from, the traditional collection subdisciplines. Traditional collection subdisciplines are thus implicitly assumed to gather secret but not open-source information. NATO thus posits OSINT as an additional collection discipline. Furthermore, NATO's conceptual approach as *per* figure 14 depicts 'analysis' as informed by, but not conceptually integrated with, OSINT. Lastly, provision is not made for a grey-source informational category.

A high quality product, this study asserts, depends on the employment of all the collection subdisciplines as part of OSINT. A key contention, in other words, is that the gathering of all information categories (i.e. open, grey and secret) should ideally involve using the full range of collection subdisciplines. OSINT is not a separate collection subdiscipline; it is rather a process according to which open-source information is gathered by means of collection subdisciplines. An alternative to NATO's proposition can graphically be depicted as follows:

Figure 15: An integrated conceptual approach to open-source intelligence



Seeing that Chapter Three argued for the addition of CYBINT as a collection subdiscipline, an example within this field is used in elucidation of the preceding figure. At a clandestine level, the interception of an espionage adversary's digital communication and/or the 'fish bowling' of such an adversary could generate secret information. In CYBINT's open-source dimension Internet searches and the monitoring of 'blogs' render information of significant importance. Under certain conditions, the soliciting of information by means of online 'chat rooms' would typically be categorised as having been derived from a grey source.

Is the foregoing proposition on an alternative approach to OSINT apposite to the CE framework, mere theoretical faultfinding? On the contrary, conceptual approaches condition the practice of intelligence, and OSINT is no exception. OSINT's value is attained to its full potential if amalgamated with an all-source effort that incorporates grey and secret information. Through the alternative approach, OSINT is synchronically integrated with other intelligence processes and informational categories. Contrary to existing conceptualisations (by for example NATO, 2001), the alternative approach aligns OSINT not as a separate 'pillar' or 'foundation', but as a dimension of the statutory intelligence entirety. The alternative conceptual approach furthermore facilitates a balanced approach to OSINT in that the various collection subdisciplines are purposefully employed in this (the OSINT) process. Balanced OSINT precludes the over-reliance on one collection discipline at the expense of others. Since the CE framework is an

OSINT instrument, the postulation as *per* Figure 15 also positions the CE framework as an integral part of a multidisciplinary, all-source effort. In addition, OSINT (like the CE framework) is presented in a manner incorporating both ‘analysis’ and ‘collection’.

Thus far, the section delineated notions pivotal to OSINT. It was emphasised that the focus of the study is on the derivation of OSINT from OSIF. In demarcating ‘open sources’, specific reference was made to the need for circumspection in the utilisation of the Internet. An alternative conceptual premise was further provided in the facilitation of a well-balanced approach to OSINT, which is in synergy with other statutory intelligence processes. It was argued that OSINT’s full value is realised only if amalgamated with the all-source effort. Opinions on the value of OSINT, relative to this all-source endeavour, are divided and are subsequently reviewed.

5.2 VIEWS ON THE ROLE AND THE VALUE OF STATUTORY OPEN-SOURCE INTELLIGENCE

Although not in the sense of a formalised field of interest named ‘OSINT’, the use of open-source information is not a recent phenomenon. In this regard Burke (2007: 11) is of the opinion that: “the value of OSINT is not new, if anything it is the oldest intelligence discipline”. Statutory intelligence services have traditionally concentrated their analysis on classified sources, while simultaneously relying upon the utilisation of unclassified sources “to provide verisimilitude to the classified product” (NATO, 2002: 4-5). There would be little opposition to the assertion that the importance intelligence services attach to open sources has increased significantly during the past two decades, and that this trend is reflected in the composition of the intelligence product. Estimates on what portion of the intelligence product is derived from open sources vary considerably. In the US, some put this figure at 35 percent, whereas others deem 95 percent as closer to reality (Friedman, 2002: 17; Burke, 2007: 11; Mercado, 2005: 2). Whatever the exact figure, there is agreement that a considerable part of the finished intelligence product is derived from open sources (Friedman, 2002: 17).

While there is agreement on the usefulness of open sources for statutory intelligence, opinions are divided on the relative value of open-source information *vis-à-vis* clandestine collected information (US, 2007*c*: 2-3). This divergence of opinion is overlaid upon differences in positions on the limits of open sources in the ‘secrecy-enshrouded’ statutory intelligence practice. Three views identified in a report to the US Congress (US, 2007*c*: 2-3), are prevalent also within Intelligence Studies and are probably not uncommon to the statutory intelligence communities of other nation states.

The first view maintains the predominance of secret, clandestine-collected information. Proponents of this position relegate the role of open-source information to that of supplementing and contextualising secret information. Open sources are rarely seen as providing “insight into an adversary’s plans and intentions” (US, 2007*c*: 2). The assumption therefore is that “information becomes more valuable as its classification rises” (Burke, 2007: 2). From this perspective open sources are useful, though unable to deliver the metaphoric ‘gold nuggets’. In essence, this view negates OSINT as an intelligence field in and of its own right.

From the second perspective, open-source information “should be viewed not only as an important supplement to classified data, but also as a potential source of valuable intelligence, in and of itself” (US, 2007*c*: 2). OSINT is projected as being able to create most of the ‘gold nuggets’ in statutory intelligence. This view is epitomised in the following assertion by Lieutenant General Sam Wilson (retired), a former Director of the US Defence Intelligence Agency (as quoted by Friedman, 2002: 17): “Ninety percent of intelligence comes from open sources. The other ten percent, the clandestine work, is just the more dramatic. The real intelligence hero is Sherlock Holmes, not James Bond.” This position can be described as zealous enthusiasm over, and confidence in, OSINT.

Occupying the middle ground between the two positions outlined above, a third view acknowledges the valuable role of open-source information and gives qualified support to the concept of OSINT (US, 2007*c*: 2). Proponents of this position concede that OSINT can produce ‘gold nuggets’. The ‘purity’ and value of OSINT nuggets are, however, seen as inferior to those produced by secret information. The following remark by Dr Joseph Nye (in Jardines, 2002: 10; emphasis added), a former chairman of the US National Intelligence Council, illustrates this view.

> Open source intelligence provides the outer pieces of the jigsaw puzzle, without which one can neither begin nor complete the puzzle. But they are not sufficient of themselves. The *precious inner pieces of*

> *the puzzle*, often the most difficult and most expensive to obtain, *come from the traditional intelligence disciplines*. Open source intelligence is the critical foundation for the all-source intelligence product, but it cannot ever replace the totality of the all-source effort.

In contrast to the extensive discourse on OSINT in general, literature is markedly more limited on the role of open sources in counterespionage. Within US statutory counterintelligence "[m]any if not most, operators prefer to rely on clandestine sources" (Godson, 2001: 203). In accordance with the first position outlined above, this perspective relegates open sources to a subservient, supplementary role within counterintelligence. Open sources are generally not considered valuable and are "rarely mined to the fullest" (Godson, 2001: 225). Conversely, an authoritative counterintelligence scholar such as Godson (2001: 202-26) views open sources, and by implication OSINT, as central to successful counterintelligence and counterespionage. Open sources, Godson (2001:203) maintains, offer a "significant opportunity to reconstruct the priorities and thinking and to understand the techniques of foreign intelligence operatives." Excellence within counterintelligence and counterespionage is increasingly dependent on optimally "blending open and secret sources" (Godson, 2001: 203).

Godson's stance on the value and role of open sources defies any compartmentalisation into one of the three primary positions, and is indicative of the nuanced nature the debate on OSINT is assuming within Intelligence Studies. Advantages in information technology and availability are sure to be accompanied by a further diversification in points of view.

5.3 OPEN-SOURCE INTELLIGENCE LIMITS, ADVANTAGES AND PITFALLS IN RELATION TO THE COUNTERESPIONAGE FRAMEWORK

This study forms part of the diversification in the discourse within Intelligence Studies on OSINT's value in relation to statutory intelligence. The research was prompted by a presupposition about the indispensable value of OSINT in relation to the all-source counterespionage endeavour. Zealous enthusiasm and over-confidence though, are as hazardous as the relegation of OSINT to an auxiliary intelligence function. Similar to an over-reliance on a single source of information, an overestimation of the value of any informational category invites counterespionage failure. In statutory counterespionage, and in response to Wilson's (2002: 17) metaphor, both Sherlock Holmes and James Bond share the winner's podium. Some 'gold nuggets' are uncovered by Holmes and others by

Bond. For the larger part 'gold nuggets' are collected in tandem in a all-source and multidisciplinary effort. In the words of Studeman (2002: 57): "The highest form of intelligence enlightenment is the dynamic and continuous fusion of data from all available sources".

The CE framework needs to be seen and designed within the boundaries of all-source primacy in the counterespionage arena. The uses and limits of OSINT, to reiterate a point previously made, practically translate into the parameters for posing realistic requirements for the CE framework. The advantages of OSINT equate with the benefits to be derived from the CE framework, while the limits of OSINT are also the limitations of the CE framework. It is required of the CE framework to draw optimally on the advantages OSINT offers, while simultaneously limiting the pitfalls associated with OSINT. Against this background, OSINT's limitations, advantages and potential pitfalls are subsequently explored with specific reference to the CE framework.

5.3.1 The limitations of open-source intelligence as pertaining to the counterespionage framework

Contrary to zealous protagonists' averments, OSINT has definite limits within the statutory intelligence context. Disregarding these limits in an unreserved, overestimation of what OSINT can realistically achieve is potentially the most perilous pitfall of this intelligence field. The following assertion by Friedman (2002:22) regarding OSINT in general, is equally relevant to counterespionage and the CE framework:

> Claims of open source enthusiasts need to be examined in context. Those making extravagant claims sometimes have little vested interest in the role and value of open source materials, or even the knowledge or experience to make reliable judgements about the broader issue of multidisciplined all-source analysis by skilled intelligence analysts.

OSINT zealots quote instances of open sources as often surpassing classified information and/or the 'conventional' all-source product (Mercado, 2005: 1-4; Steele, 2004: 115-116; Vlahos, 2005: 1-3; Barlow, 2002: 1-5). These examples pertain to the positive intelligence field and assessing the merits thereof would distract from the counterespionage focus of the study. Suffice to state here that differences in the nature of secret, grey and open information should not be confused with the superiority of one informational category over the other.

Absent in the consulted literature is the provision of comparable instances by OSINT zealots in ‘substantiation’ of open-source superiority in statutory counterespionage. Even should such examples exist, they are highly likely to be isolated, probably anecdotal and would not validate an assertion on OSINT’s capability to consistently ‘outperform’ the ‘conventional’ counterespionage effort. Within counterespionage, OSINT can serve to verify information obtained from other informational categories and *vice versa*. While there could be some rare exceptions, OSINT in itself and by itself, is unlikely to credibly assert on counterespionage concerns beyond the level of plausibility. It is for this reason that the CE framework is intended as a ‘parallel intelligence tool’ that has the statutory counterespionage structure (and not the policymaker) as consumer. Within the counterespionage structure, to re-emphasise, the outcome of the CE framework is amalgamated as part of an all-source endeavour.

5.3.2 Further advantages to be derived from the counterespionage framework as an open-source intelligence instrument

The primary aim of the CE framework, namely the identification and assessment of espionage risks, is self-evidently its principal benefit. The latter was already discussed extensively and further elaboration would be superfluous. Likewise, the advantages of the CE framework as a ‘parallel instrument’ were previously indicated. With the *caveat* that they are in some respects an elaboration of the benefits and advantages discussed so far, the CE framework in its capacity as an OSINT instrument offers additional advantages. Inferring from the advantages of OSINT in general, and drawing on the findings of the study thus far, the following are additional advantages that the CE framework is required to attain:

- Relative to a process solely reliant on clandestine assets, the CE framework can cover, for purposes of collecting and assessing counterespionage-related information, an environment that is significantly broader in spectrum and more diverse. OSINT’s still broadening range is attributable not only to technological advances but also to political and societal changes. During the past decade especially, “denied areas” (such as nation states that exerted strict control on open media and information flow) have been rapidly shrinking (US, 2002: 5).

- Since OSINT is more flexible in shifting its focus than, for example, clandestine HUMINT collection (Steele, 2002*b*: 65-66), the CE framework can provide a rapid response to unexpected or new developments of counterespionage relevance. In such cases the CE framework would establish the 'first line' platform for a subsequent initiation of an all-source effort.
- In some instances the CE framework could provide at least some insight into adversarial espionage activities not yet covered by (own service) clandestine counterespionage collection. Burke (2007: 10), for example, remarks that OSINT "can be extremely useful and is often the only way of penetrating dark and covert networks". Since 'penetration' in the statutory counterespionage lexicon carries the connotation of establishing direct clandestine access, Burke's (2007:2) statement should preferably be paraphrased to the effect that 'OSINT can be extremely useful and is often the only way to gain insight into the intent and the dynamics of adversarial networks'. Nevertheless, Burke's assertion does underline the paradox of OSINT as an open-source instrument, in some instances being the only available means to procure at least some information on clandestinely operating adversaries.
- Because the outcome of the CE framework is based on information overtly available, it enables the focusing of the clandestine counterespionage collection effort on areas that actually warrant higher risk and cost methods. The critical role of systemised OSINT, in directing the clandestine effort, is illustrated in a finding of the US Aspin-Browne Commission, which in 1995 estimated that between 80 and 90 percent of information gathered by clandestine collectors was publically available (Goodman, *et al* 1996: 21). A related advantage of the CE framework's solely open-source based outcome is that it serves not only as context for and supplement to secret information, but also acts as a benchmark for the reliability and value of information generated by clandestine sources. In relation to clandestine HUMINT sources, by way of illustration, the outcome of the CE framework can be used to determine whether information provided by human agents is indeed of a clandestine nature or whether it is merely masqueraded as such.
- Mass media, as was shown in Chapters Two and Three, is central to informational warfare. It provides a conduit for adversarial informational warfare action such as propaganda and deception. Seeing that mass media also forms a major part of open sources, the CE framework is positioned to identify incidents and trends plausibly linked to adversarial informational

warfare activities. Likewise, opportunities can be identified and support rendered to own service informational warfare. Such support includes, but is not in any measure restricted to, utilising the outcome of the CE framework as a basis for providing an espionage adversary with deceptive information through own-service double agents as well as developing credible cover for own-service clandestine counterespionage actions.

- Without distracting from its primary aim to identify and assess espionage risks, the CE framework can also be expected to deliver by-products to other intelligence fields. Despite having been made nearly six decades ago, the following remark by Kent (1949,1966: 216) is still valid and applicable, also to the CE framework:

> Pursuit ... of spies is the job of the counterespionage branch of security intelligence and theoretically of no formal concern to positive intelligence. To a certain degree this is the case. But there are by-products from the counterespionage activity that are of the highest concern to positive intelligence.

Attaining the indicated benefits requires the CE framework to take note of, and to minimise pitfalls related to open sources and OSINT in the statutory intelligence environment.

5.3.3 The moderation of pitfalls associated with open-source intelligence as a requirement of the counterespionage framework

Pitfalls and drawbacks cited in literature as associated with open sources and OSINT can broadly be clustered as pertaining to, firstly, the voluminous extent of open sources and, secondly, assertions on the unreliability of open sources.

5.3.3.1 The information explosion as a challenge to the counterespionage framework

The exponential increase in open sources as well as the projection that this ‘information explosion’ is likely to accelerate at an even steeper incline was noted in Chapter Two. It is this sheer volume of open-source information that is cited as *the* “main disadvantage of OSINT” (Lowenthal, 2003: 80). The primary challenge associated with the proliferation of open-source information is often described as the “wheat from the chaff” or alternatively as the “noise versus signal problem” (Gilluffo *et al* , 2002 : 67 ; Lowenthal, 2003 : 80). Should OSINT be deemed as just a collection subdiscipline, open sources be seen as a nebulous body of data, and OSINT be conducted in a conceptually and methodologically unstructured manner; these pitfalls would indeed appear to be insurmountable.

It is precisely the challenge posed to statutory intelligence services by the exponential growth in publicly available information that prompted this study. The latter forms part of the quest for theoretical and conceptual frameworks that do not only delineate the analysis process, but also enable the focused collection of overt information relevant to national security. The importance of a systemised and symbiotic relationship between analysis and collection in enabling picking up the ‘signals’ from ‘noise’ can hardly be overstated. While the ‘signal to noise’ problem in relation to OSINT is often accentuated, surprisingly less emphasis is placed on clearly demarcating the ‘signals’ that are being looked for. Also by way of analogy, it is nearly impossible to find a needle in a haystack without a definite visualisation of what a needle looks like. In the absence of such a visualisation of ‘needles’, it would understandably be, to paraphrase Winston Churchill (in Barlow, 2002: 2), a riddle wrapped in a mystery inside an enigma. Applied to this study, the CE framework therefore has to be clear on what constitutes an ‘espionage risk’. Moreover, and to guide the ‘picking up’ of espionage risks, the CE framework has as a requirement translating focus areas and focal points into variables and indicators.

5.3.3.2 The purported ‘unreliability’ of open-source information as a challenge to the counterespionage framework

Whereas views on the challenge posed by the voluminous extent of open sources have merit, the notion of indiscriminately perceiving open sources as being, *de facto*, more unreliable than other categories of information rests on less solid ground. Open-source information (on, for instance, the Internet), can indeed be “intentionally or unintentionally” added to, deleted, modified or otherwise altered (US, 2006*b*: 19; Studeman, 2002: 57). Much of the information on the Internet is undoubtedly inaccurate, irrelevant or simply out-of-date (NATO, 2002: 4; Bjore, 2002: 80). Since open sources include mass media and mass communication, the “echo” effect surely needs to be considered (US, 2007*c*: 8-9; Lowenthal, 2003: 80). One example of the ‘echo effect’ occurring is when more than one “media outlet” carries the same news item and the resulting repetition “imbue[s] a particular news item with more credibility and importance than is warranted” (US, 2007*c*: 8-9). However, these pitfalls are not in any measure limited to open sources, they also are endemic to secret and grey sources.

Quiggin (2007: 161) rightly points out that there is no actual body of evidence to support the “widely held assumption that classified intelligence is more reliable than OSINT.” This misconception is predicated on a further erroneous assumption, namely that secret sources are as a rule more reliable than open sources. The said assumption appears to equate ‘what is available on the internet and the mass media’ to open sources, and ‘data’ to ‘information’. Not only were open sources shown to be more encompassing, but the principles applying to determine the reliability of open sources are also applicable to OSINT. A reputable academic publication is typically subject to critical peer review and would, for instance, not infrequently be more reliable than a report compiled from the debriefing of a dubious, secret HUMINT agent. To gauge the reliability of open sources against the reliability of ‘what is available out there on the Internet and in the newspapers’, is therefore questionable. The employment of this doubtful yardstick would be comparable to using information obtained through the debriefing of a number of randomly selected individuals at a jamboree as indicative of the reliability of secret HUMINT.

Similar to secret sources and classified information, determining the credibility and reliability of open sources and information is critical. The CE framework therefore has as a requirement, and as part of Chapter Seven proposes, an evaluation matrix for open sources and open-source information. Furthermore, approximating ‘conventional’ all-source intelligence, and equally imperative, is the requirement for the CE framework to be diverse and balanced in its utilisation of the respective collection subdisciplines. It may be recalled that a conceptual approach in this regard was previously discussed and illustrated (Figure 15). This conceptual approach is key to the CE framework achieving its primary challenge, namely determining espionage risk through open-source information. A further imperative, as outlined in the next section, is for the execution of this conceptual approach to be guided by sets of variables and indicators.

6. THE UTILISATION OF VARIABLES AND INDICATORS AS A REQUIREMENT FOR THE COUNTERESPIONAGE FRAMEWORK

The requirements posed for the CE framework as an OSINT instrument, as discussed above, are interlinked with other requisites addressed in this chapter.

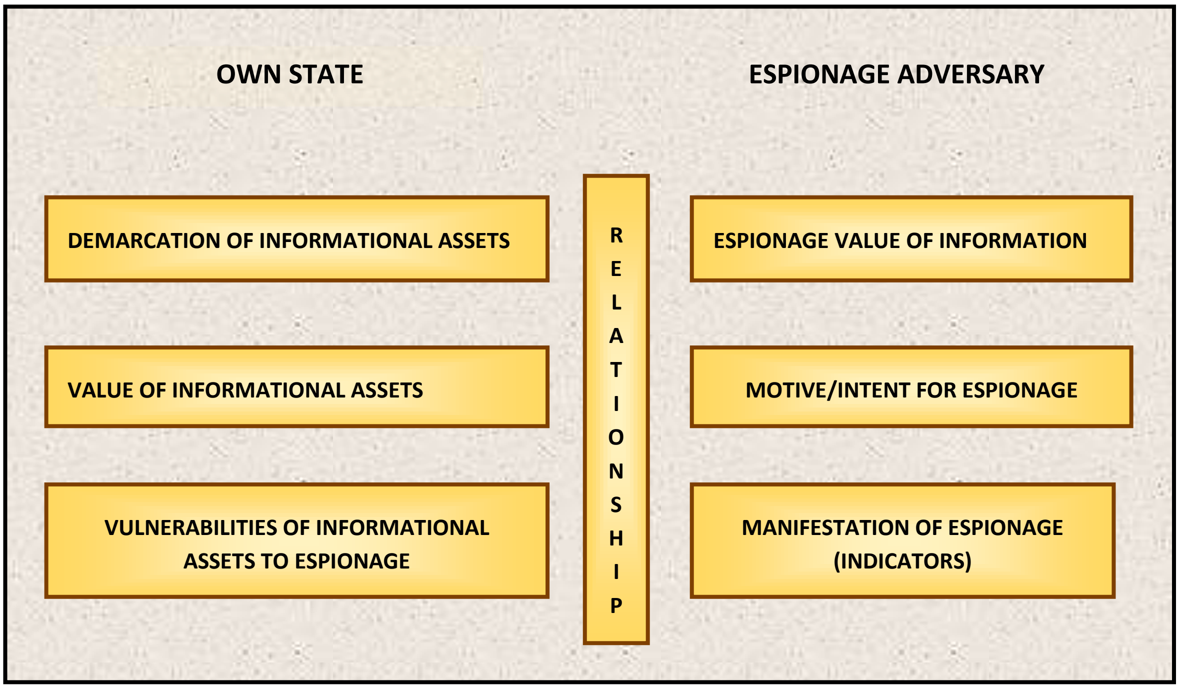
These requisites, to recapitulate, pertain to the CE framework as being respectively a statutory espionage risk assessment instrument, an aggregate of intelligence types, and a parallel counterespionage process. The outcome of the CE framework as an aggregate of intelligence types (with 'warning intelligence' predominating), is achieved *through* OSINT and *from* the CE framework's location as a parallel counterespionage process. In addressing these requirements, some reference was made to the ostensible contradiction that stems from the CE framework, which is, on the one hand, an open-source based intelligence tool and, one the other, intended to function in the secrecy-enshrouded espionage and counterespionage milieu. This apparent anomaly, which underlines the need for a systemised process that combines estimative approaches (such as variable-depended matrixes and models) and indicator-based methods, was alluded to, but not previously coherently examined.

By virtue of its status as a parallel OSINT instrument, the CE framework excludes classified and privileged information in two respects. Firstly the CE framework precludes the use of clandestinely collected information regarding the intentions and activities of espionage adversaries. Secondly, the CE framework excludes the use of classified and privileged information concerning the own state and the own intelligence services, which are conventionally deemed as indispensable to counterespionage. Statutory counterespionage obligates as a premise a profound knowledge and understanding of the policymaker's strategic objectives and strategy. In the counterespionage realm, as discussed in Chapters Two and Three, information is both a vital national interest and a category of state power. Effective counterespionage consequently presupposes a clear demarcation of what information is of such national security interest that it warrants protection from adversarial espionage, and which areas of an espionage adversary's informational integrity would be to the benefit of the own state to disrupt, deceive and exploit. Such demarcation is conventionally presumed to depend on a sound relationship between intelligence practitioners and the consumer/policymaker and would typically be guided by intelligence practitioners' assessment of classified information. Classified information is also typically deemed as being critical to two additional aspects central to effective counterespionage, namely, determining the own state's informational vulnerabilities and directing own state (counterespionage) countermeasures.

In view of the above, a primary requirement posed to the CE framework is to use open-source information in determining not only 'external' espionage risks but also 'internal' vulnerabilities and strengths (including countermeasures). Since Chapter Two forwarded a proposition on the CE framework as a dualistic environmental scanning process that is simultaneously introspectively and outwardly directed, no further theoretical elaboration is necessary. Of relevance here is the more practical consideration of forwarding structural constituents ('core areas') that can guide the dualistic environmental scanning in respect of both the 'looking for' (collection) and 'looking at' (assessment) of information. It is in relation to these core areas, this study contends, that estimative approaches (such as variable-depended matrixes and models) and indicator-based methods should be designed. Bar-Joseph & Scheaffer (1998: 332-333) define an indicator as a "piece of information" that serves as a "clue" of an enemy's "move or intention". For purposes of this study an indicator is seen as a specific incident or occurrence ('smoking gun') that plausibly points towards the manifestation of adversarial espionage. A variable is deemed as a circumstantial condition or factor that subtracts from, or reinforces the plausibility of, adversarial espionage against the own state. Variables, in conjunction with indicators, guide the collection and assessment of open-source information in a manner conducive to the identification and description of espionage risks. In the case of the CE framework, indicators and variables should naturally be open-source detectable.

The formulation of these variables and indicators, as well as a proposal on a systemised process (for employing variables and indicators), are addressed in the chapters to follow. Since this chapter focuses on requirements for the CE framework, it is, however, necessary to the core areas in respect of which variables and indicators are required. Drawing on, and expanding on, Figure Six (presented in Chapter Three under the heading: *Framework for counterespionage environmental scanning: contextual focus, focus areas and focal points*), the seven areas for which sets of variables and indicators are required, can be graphically depicted as follows:

Figure 16: Areas for the design of variables and indicators for the counterespionage framework


OWN STATE
ESPIONAGE ADVERSARY
DEMARCATION OF INFORMATIONAL ASSETS
VALUE OF INFORMATIONAL ASSETS
VULNERABILITIES OF INFORMATIONAL ASSETS TO ESPIONAGE
RELATIONSHIP
ESPIONAGE VALUE OF INFORMATION
MOTIVE/INTENT FOR ESPIONAGE
MANIFESTATION OF ESPIONAGE (INDICATORS)

It must be emphasised that Figure 16 does not purport either to provide a fully inclusive representation of, or indicate the relationship and interaction between, variables and indicators. Figure 16 illustrates an earlier contention, on the centrality to the design of the CE framework, of factors previously identified in this chapter as pivotal to the assessment of espionage risks (Figure 12, Section 2.1.3.2). Subsequent chapters will reveal these factors as also being central to other dimensions of CE environmental scanning.

7. CONCLUSION

Building on the theoretical basis and context of the contemporary manifestation of espionage against the nation state, as put forth in the preceding chapters, Chapter Four set out to determine concrete requirements relating to the CE framework. Requirements posed to the CE framework as well as requirements posed by the design of this framework were explored.

The primary, and self-evident, requirement posed to the CE framework was found to be the open-source-based identification and assessment of statutory espionage risks. In order to attain this primary requirement, the CE framework must clearly define an espionage risk as its principal focus. Existing postulations within Intelligence Studies were found to be directed toward positive intelligence and as being apposite neither to counterespionage nor the CE framework. Verification emerged as the most apt criterion for the categorisation of counterespionage concerns. An espionage risk was defined as a 'credible plausible situation, resulting from the activities of an opposing intelligence structure, which exists or may develop in a manner significantly impeding a government's optimal pursuit of its strategy and realisation of its objectives.'

Although distinctly counterespionage focused, the CE framework is required, in its design and outcome, also to be congruent with statutory intelligence in general. While its outcome is an aggregate of intelligence types, the CE framework is required to serve foremost as a warning intelligence instrument. The measure of the effectiveness of the CE framework was indicated as its ability to contribute to limiting national security surprises within the counterespionage sphere.

As part of statutory intelligence, however, the CE framework shares the propensity toward failure. Its framework, therefore, has as a requirement taking cognisance of factors underlying intelligence failure, and putting forward propositions for the moderation thereof. With reference to the study's problem statement, it was emphasised that the CE framework is intended as a parallel counterespionage instrument with the concurrent requirement of serving as a (partial) institutional solution in remedy of an institutional propensity toward failure.

The CE framework is to meet the aforementioned requirements through optimising the benefits and limiting the pitfalls inherent to OSINT. It was emphasised that, as an OSINT tool, the CE framework, in itself and by itself, is unlikely to assert on counterespionage concerns beyond the level of plausibility. It is within the parameters of the CE framework as an open-source *risk* identification and assessment tool that other requirements should be considered.

A recurring theme throughout this chapter was the requirement for the CE framework to be in synergy with, and part of, all-source counterespionage and the practice of OSINT (within statutory intelligence). The manner in which 'parallel' or 'competitive' instruments are employed in practice would naturally vary from the intelligence community of one state to another. This being an academic study, it is nevertheless imperative – at a conceptual level – to integrate the CE framework with all-source counterespionage and the practice of statutory OSINT. Conceptual approaches after all condition practice. The design of the CE framework, it was emphasised, thus requires appropriate conceptual approaches that can serve as foundational building blocks (for the CE framework's construction). At least insofar as consulted literature is concerned, such conceptual approaches appropriate to statutory counterespionage do not exist. Consequently, the following contextual constituents for the design of the CE framework were forwarded:

- A definitional categorisation providing for 'espionage risks', 'espionage threats' and 'corroborated adversarial espionage'.
- An overarching conceptual construct for the assessment and prioritisation of counterespionage concerns.
- An alternative approach by means of which OSINT is synchronically integrated with all-source intelligence. Contrary to existing conceptualisations, the alternative approach aligns OSINT not as a separate 'pillar' or 'foundation', but as a dimension of statutory intelligence as a whole. OSINT was depicted as being amalgamated with the all-source effort, and as involving all collection subdisciplines.
- A typological schema of intelligence types with specific reference to counterespionage. This schema provides the basis for aligning the outcome of the CE framework with that of all-source counterespionage.

In addition to the requirements addressed in this chapter, the CE framework needs to consider in its design the statutory intelligence cycle and process. The next chapter examines the intelligence cycle and process with a view to establishing their flexibility in accommodating the CE framework.

CHAPTER FIVE

STATUTORY INTELLIGENCE PROCESSES AS THE FUNCTIONAL CONTEXT FOR OPEN-SOURCE, COUNTERESPIONAGE ENVIRONMENTAL SCANNING

1. INTRODUCTION

Optimising the benefits that the CE framework offers, the previous chapter contended, presupposes synergy between the CE framework and the all-source intelligence endeavour. The all-source intelligence endeavour is conducted by means of a methodologically structured approach that is commonly referred to as the 'intelligence process' or 'intelligence cycle'.

In practical terms, the CE framework cannot be effectively designed without clarity about the intelligence, counterintelligence and counterespionage processes. Argued from the theoretical perspective provided in Chapter Two, the CE framework is a micro-process that needs to be superimposed on the 'templates' of the 'higher order' intelligence, counterintelligence and counterespionage processes.

This chapter contextualises the CE framework as a process located within higher order processes. Furthermore, a broad structural outline of the process of open-source, counterespionage environmental scanning is provided. Two inter-related research questions posed in the introductory chapter are thus addressed. Firstly, and considering the voluminous extent of overt information, how can the CE framework be methodically structured? Secondly, is the CE framework in synergy with existing conceptualisations of the intelligence process and, if not, what modification(s) or alternative(s) can be postulated in respect of the latter?

Should propositions have existed on the intelligence and counterintelligence processes that were apposite to the CE framework, this would have been a concise and undemanding chapter. Regrettably, this study contends, the discourse within Intelligence Studies on such processes that are indeed congruent with statutory intelligence practice and reality, is still incipient. Prior to the design of the CE framework as a process, a cogent response to the said research questions therefore needs to consider the following inter-related aspects in syllogistical sequence:

- Are existing propositions of the all-disciplinary intelligence process an accurate reflection of, and are they feasibly employable as part of, contemporary statutory intelligence practice?
- Do current postulations on the all-disciplinary intelligence process adequately accommodate the counterintelligence process?
- Is the counterespionage process sufficiently provided for in existing proposals on the counterintelligence process?
- Are the propositions of processes of higher abstraction germane to the requirements of the CE framework as a parallel, OSINT instrument?
- Since the CE framework is a parallel instrument and in certain respects mirrors processes of higher abstraction, what elements do these processes of higher abstraction offer that are useful in the design of the open-source CE scanning process?

The aptness of the indicated approach, as well as the concomitant relatively extensive appraisal of views on the higher order intelligence process, will transpire as the chapter progresses. Hence, the introduction suffices with two observations that warrant the prominence the chapter affords to the evaluation of several existing views on the 'higher order' intelligence process. Firstly, and given the centrality of intelligence process's functioning in Intelligence Studies' thought, this appraisal is pivotal to the mapping out of 'what we know' theoretically. Secondly, the chapter will show the prevalence within Intelligence Studies thinking of either positing the counterintelligence process as replicating the conventional intelligence cycle (and variations thereof) or tenuously referring to counterintelligence as being performed throughout the said cycle. Since counterespionage is part of counterintelligence, a review of existing postulations on the intelligence process is simultaneously an appraisal of views on how counterespionage (within which the CE framework is located) 'works'.

2. AN OVERVIEW AND APPRAISAL OF EXISTING CONCEPTUALISATIONS OF THE STATUTORY INTELLIGENCE PROCESS

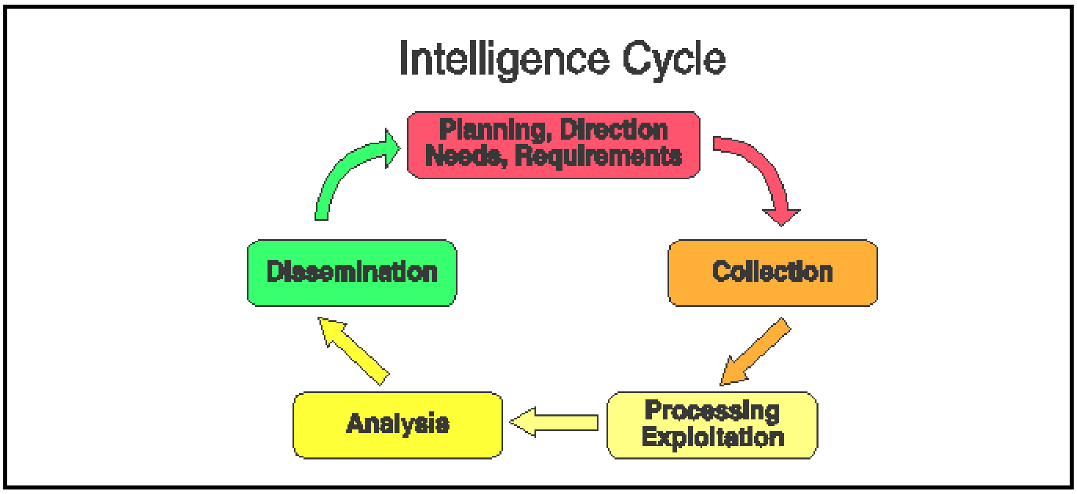
The concept 'intelligence process', in the words of Lowenthal (2003: 41), "refers to the various steps or stages in intelligence, from policymakers perceiving a need for information to the [intelligence] community's delivery of an analytical product to them." Propositions on the intelligence process are presented as models that act as "idealizations of processes that are more subtle and more complex in practice." (Berkowitz & Goodman, 2000: 72). As an idealisation, a model is "an aimpoint, of what the process should look like if everything goes as planned." (Berkowitz & Goodman, 2000: 72). A model of the intelligence process thus serves as an "organization principle" for both the work of intelligence (intelligence practice) and as a notional concept for theorising on intelligence (Lowenthal, 2003: 51; Berkowitz & Goodman, 2000: 72). As suggested earlier, the use of the term 'intelligence process', explicitly or (as often in consulted Intelligence Studies) implicitly denotes the overarching process that binds and accommodates processes within the various intelligence subdisciplines and fields.

2.1 THE TRADITIONAL VIEW OF THE INTELLIGENCE PROCESS

The theoretical reflection on statutory intelligence, as *per* Chapter Two, mentioned a widely held acceptance of intelligence being generated through a circular, sequentially phased process. Given its circular and repetitive nature, this model is generally referred to as the 'intelligence cycle'.

Since its conceptual crystallisation in the late 1940s, the intelligence cycle has continued to have as its essential elements: direction (the client expresses a need and intelligence requirements are formulated); collection (of information using one or a combination of methods); the processing and analysis of information; and dissemination (distribution of the intelligence product to the client), which then leads to further needs expressed by the client and the repetition of the cycle (Berkowitz & Goodman, 2000: 68-69). The degree to which the traditional view of the intelligence cycle has retained its core features over a period stretching more than six decades, is reflected in the following graphical depiction contained in a recent US government commission report (US, 2005*b*: 584):

Figure 17: The intelligence cycle



<u>Source</u>: US, 2005*b*: 584.

Commenting on the enduring subscription to the traditional intelligence cycle, Hulnick (2007: 1) asserts that “[n]o concept is more deeply enshrined in the literature than that of the ‘intelligence cycle’”. In a similar vein, Berkowitz & Goodman (2000: 69) view the concept of the intelligence cycle as continuing to pervade “thinking” about intelligence.

2.2 DEFICIENCIES OF THE TRADITIONAL INTELLIGENCE CYCLE

The traditional intelligence cycle maintains its dominance, despite mounting recognition of deficiencies at theoretical and practical levels. These deficiencies are not only multiplying in number, but what originally might have been fissures between the reality of statutory intelligence practice and the process as depicted by the intelligence cycle, are widening into irreconcilable discrepancies. Since these deficiencies need to be considered later on in the design of counterintelligence and counterespionage processes in general, and the construction of the CE process specifically, some elaboration is required.

For purposes of this study, only some of the most prominent deficiencies are concisely highlighted and clustered into three areas for reasons of brevity. Firstly, the activities conventionally assigned to the intelligence circle’s respective phases (needs/requirements, collection, processing/exploitation, analysis and dissemination) oversimplify and distort the reality of the statutory practice. The notion that the intelligence process is initiated by the policymaker expressing needs and requirements serves as example. More often than not, such clear guidance is not forthcoming (Quiggin, 2007: 52-53). The statutory intelligence services themselves, and in particular the executive leadership (of such services), are compelled to decide on priorities and requirements (Hulnick, 2007: 2). “Intelligence managers”, Hulnick (2007: 3) contends, are the “real drivers” of the intelligence collection process. To this end, the executive leadership of an intelligence service strongly relies on the analysis function. The symbiotic relationship of analysis and management therefore stands central to, and in reality often is the real driver, of the intelligence process.

Secondly, the traditional intelligence cycle is incongruent with statutory intelligence practice in that it presents the intelligence process as the neat finalisation of one stage of the intelligence process before sequentially proceeding to a subsequent phase (Bernhardt, 2003: 22-23). The intelligence cycle, explains Lowenthal (2003: 51), is “overly simple” in the sense that it has an “end-to-end-completeness that misses the vagaries in the process ... It is also oddly one-dimensional. A policymaker asks questions and, after a few steps, gets an answer. There is no feedback, nor does the diagram convey that the process might not be completed in one cycle." (Lowenthal, 2003: 51). In fact the different stages overlap, and rarely operate as part of a "single neat circle" (Lowenthal, 2003: 52). The formulation of intelligence requirements, for example, is not a one-off action, but generated and refined during various stages of the intelligence process. This refinement involves analysis and management - which in turn continuously guide collection. Analysis and collection thus operate in a parallel and not a sequential manner (Hulnick, 2007: 3). The intelligence management function synchronises, and adds to, the parallel interaction between analysis and collection.

The third cluster of deficiencies in relation to the intelligence cycle entails the omission of pivotal activities and functions demanded by contemporary intelligence practice. Lowenthal (2003: 41, 51-52) views the "feedback" and "consumption" stages as such omissions. Of obvious importance to this study is the intelligence cycle's failure to capture the "dynamic nature" of the interaction between the intelligence process and the "external environment" (Gill & Phythian, 2006: 3). The reciprocal impact of the external environment and the intelligence process is thus negated. This exclusion manifests itself in the absence of the "scanning or scouting" phase, which hampers a primary intelligence mission of issuing strategic warning to the client (Bernhardt, 2003: 27). What is thus missing is what Pollard (1999: 13, 65) terms "radar/awareness intelligence".

Infrequently mentioned in consulted literature, yet fundamental to this study, is the intelligence cycle's neglect of the counterintelligence subdiscipline. Since this indifference to the subdiscipline is discussed in Section Three, one example would suffice here. A US (2005*b*: 579-589) official commission report includes as an appendix a "primer" on the functioning of statutory intelligence. The appendix, entitled *An intelligence community primer*, devotes a subsection to a discussion of the intelligence process by means of a schematic depiction (Figure 17). Neither counterintelligence nor covert action is mentioned as part of the discussion of the intelligence cycle. Instead the directly following subsection, with the heading *Other intelligence activities: counterintelligence and covert action*, explains these two intelligence subdisciplines without making reference to the intelligence cycle at all (US, 2005*b*: 584-585).

If the intelligence cycle does not accommodate counterintelligence, counterespionage is inevitably also excluded. Since the CE framework itself is part of all-source counterespionage, the traditional intelligence cycle can clearly not serve as a 'template' upon which the micro-theoretical CE scanning process can be superimposed. Moreover, the deficiencies of the intelligence cycle limit the degree to which aspects thereof can be utilised in the design of the CE scanning process. The next subsection examines some alternative postulations on the intelligence process in order to establish their suitability for accommodating the CE scanning process. Examples of alternative propositions are limited to those that offer elements useful in the design of the CE process.

2.3 THE QUEST WITHIN INTELLIGENCE STUDIES FOR ALTERNATIVES TO THE TRADITIONAL VIEW ON THE INTELLIGENCE PROCESS

While the intelligence cycle still dominates views held within Intelligence Studies and statutory intelligence practice, contesting ones are emerging. Positions crystallising in this regard range from orthodox defence to the categorical rejection of the traditional intelligence cycle.

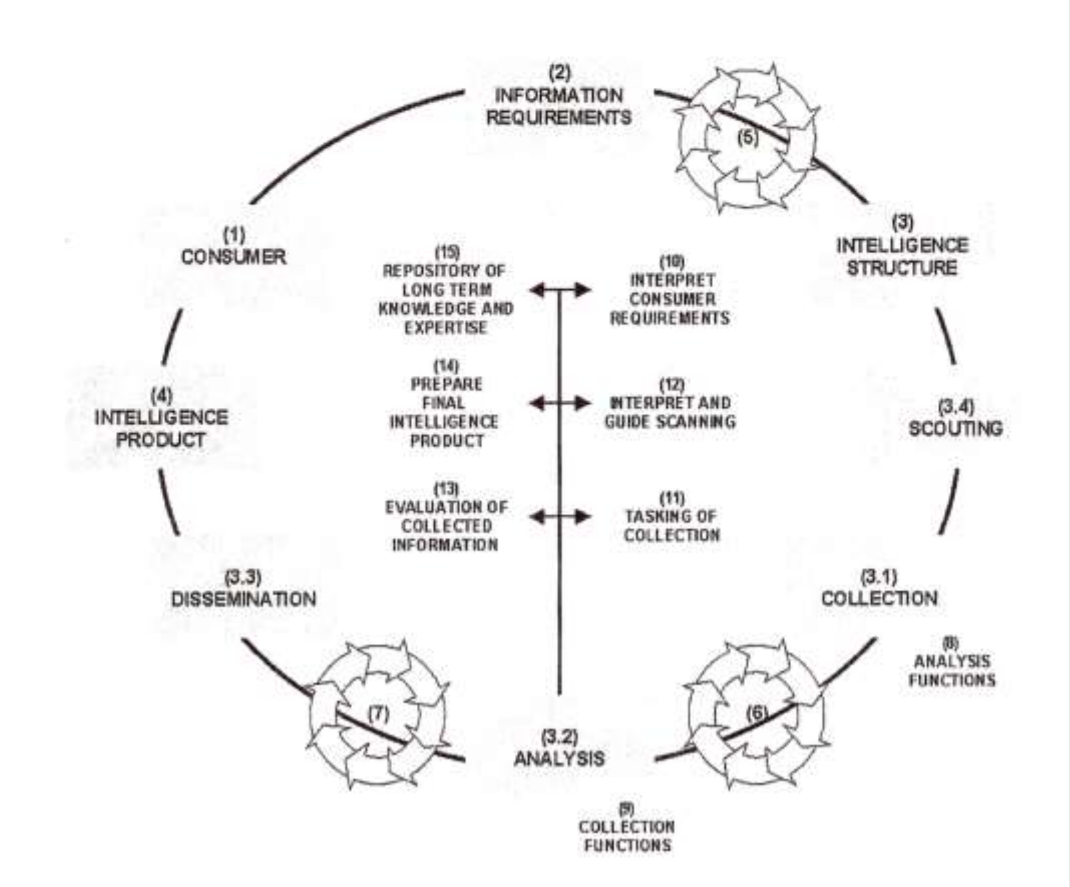
2.3.1 In defence of the intelligence cycle – the orthodox (traditionalists) and the reformists

The traditional view on the intelligence cycle, this study argues, has almost acquired the elevated status of a 'Holy Grail' within statutory intelligence practice and Intelligence Studies. Unfortunately, this status is intrepidly defended by what would appear to be most 'knights of the intelligence order'. The nature of this defence, however, varies.

With the 'armour' of conceptual inflexibility, some works omit even mentioning weaknesses in the intelligence cycle (US, 2005*b*: 583-585), while others maintain that – despite its deficiencies – the intelligence cycle "remains a useful way of understanding" how intelligence (Quiggin, 2007: 52-53) works. Both these viewpoints are orthodox in that the traditional view of the intelligence cycle remains 'untouched'.

Conversely, reformist 'knights of the intelligence order' are constructive in their defence. Employed in this regard are the 'shield' of expanding qualifications (added to the description of the cycle) and/or the 'sword' of ever-growing contemporisations. 'Sword-yielding' reformists are more offensive in their defence, and not only recognise the deficiencies of the intelligence cycle, but also forward propositions in moderation. These moderations, it must be emphasised, are done within the parameters of both the circular nature and the essential features of the traditional view of the intelligence process. Serving as an example is the following proposition by Bernhardt (2003: 27) which includes an (environmental) scouting phase and is consequently pertinent to the CE scanning process:

Figure 18: The intelligence cycle (contemporary view)

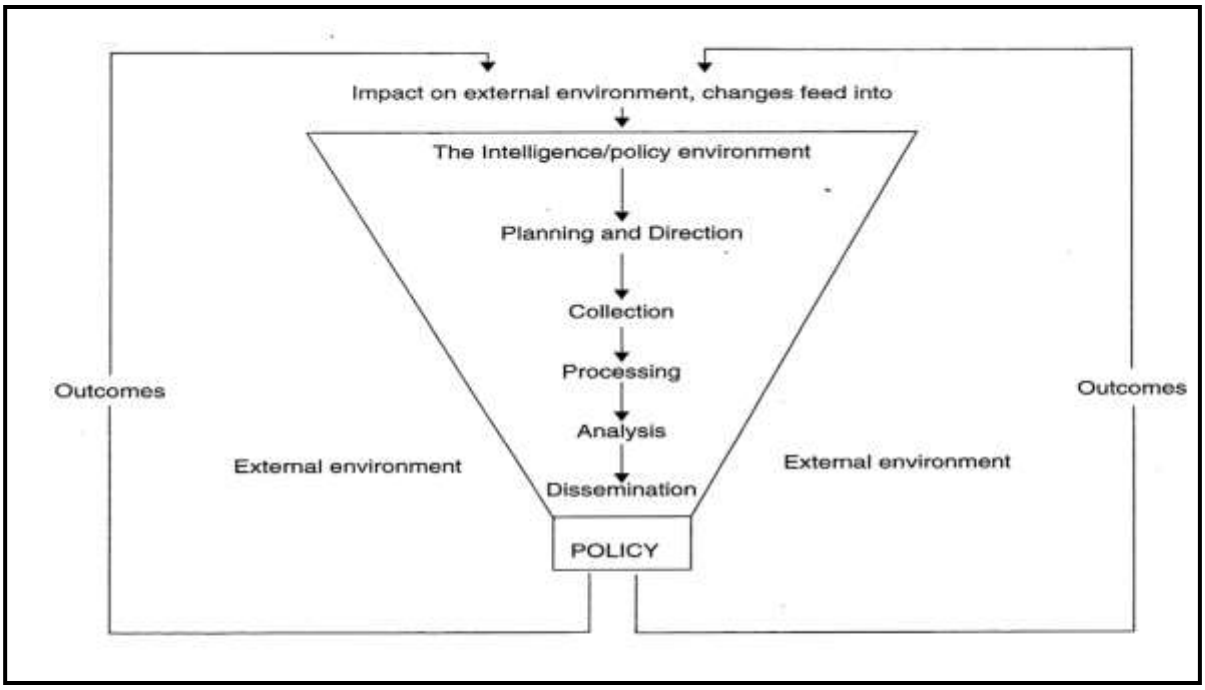

(2) INFORMATION REQUIREMENTS
(5)
(1) CONSUMER
(3) INTELLIGENCE STRUCTURE
(15) REPOSITORY OF LONG TERM KNOWLEDGE AND EXPERTISE
(10) INTERPRET CONSUMER REQUIREMENTS
(4) INTELLIGENCE PRODUCT
(14) PREPARE FINAL INTELLIGENCE PRODUCT
(12) INTERPRET AND GUIDE SCANNING
(3.4) SCOUTING
(13) EVALUATION OF COLLECTED INFORMATION
(11) TASKING OF COLLECTION
(3.3) DISSEMINATION
(3.1) COLLECTION
(8) ANALYSIS FUNCTIONS
(7)
(6)
(3.2) ANALYSIS
(9) COLLECTION FUNCTIONS

Source: Bernhardt, 2003: 27.

Markedly absent from Bernhardt’s (2003) proposal is the incorporation of, or even reference to, the counterintelligence and counterespionage functions as part of the intelligence cycle.

In a similar vein, the following proposition on the intelligence process, by Gill & Phythian (2006: 3-6) provides for interaction with the external environment, but neither escapes the circular view on the intelligence process nor refers graphically or narratively to counterintelligence:

Figure 19: The intelligence process



Source: Gill & Phythian, 2006: 4.

2.3.2 The revisionists of the intelligence process

However constructive, expanding moderations of, and the adding of qualifications to the intelligence cycle are signals of its anachronistic nature. In this regard, Berkowitz & Goodman (2000: 72-73) argue that:

> We should have known that something was wrong with the traditional model. One sign was that, if you read between the lines, even intelligence experts knew the model was a simplification that often – perhaps usually – did not hold practice. Writers who described the intelligence cycle in recent years almost always added qualifications.

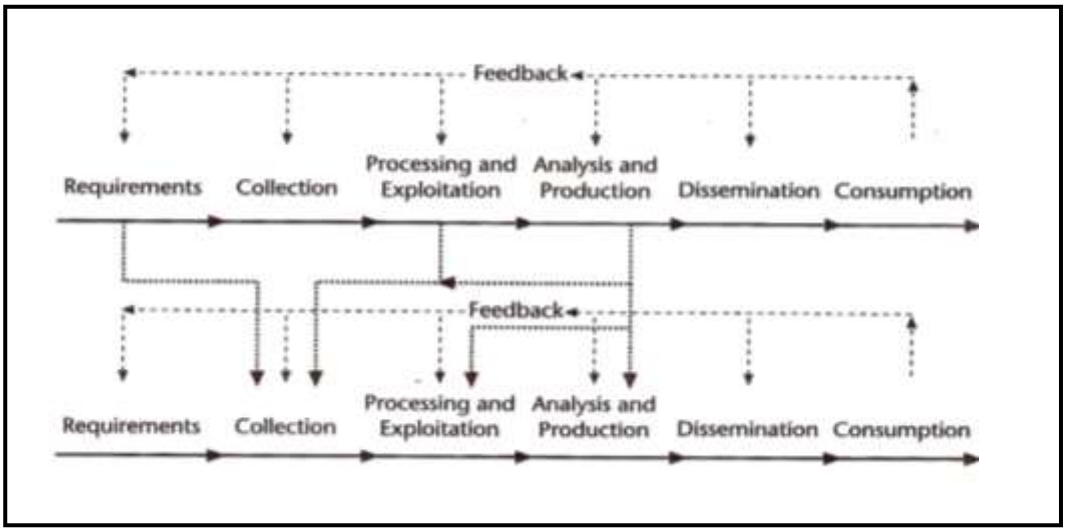
Albeit currently limited, a growing number of authoritative scholars are appealing for a fundamental review and redesign of the intelligence process as both a “concept and organising principle” (Lowenthal, 2003: 51). Additional to Lowenthal (2003: 51-52) and Berkowitz & Goodman (2000: 72-73), O’Connel (2005: 190) views the “traditional approaches to intelligence and intelligence-policy boundaries” as progressively more “challenged or broken down entirely”. O’Connel (2005: 190) continues by categorising the intelligence cycle as an “increasingly old-fashioned way of how intelligence is conducted.” In starker terms, Hulnick (2007: 19-20) concludes his appraisal of the intelligence cycle with the following assertion:

> I suspect that, despite my preaching about alternatives to the traditional intelligence cycle, it will continue to be taught both inside government and elsewhere ... [W]e know that people tend to look for confirming rather than disconfirming data. They will seek to defend the intelligence cycle, rather than consider alternatives. Nonetheless, the intelligence cycle is a flawed vision, and thus poor theory. One need only ask those who have toiled in the fields of intelligence.

While positions within the debate are still crystallising, revisionists seemingly do not reject all the elements of the traditional intelligence cycle, but in the main question the oversimplified, unidirectional and circular flow of intelligence activities. Consequently, the use of the term ‘intelligence process’, in these circles, appears to be gaining ground over the use of ‘intelligence cycle’ (O’Connel, 2005: 190; Lowenthal, 2003: 51-52; Gill & Phythian, 2006: 3-6; Berkowitz & Goodman, 2000: 72-73).

As an alternative, Lowenthal (2003: 52) proposes a model according to which the activities of the intelligence process are aligned with reality and are “linear, circular, and open-ended all at the same time.” The notion of a multidirectional activity flow, which is useful to the design of the CE framework, is graphically depicted by Lowenthal (2003: 52) as follows:

Figure 20: The multilayered intelligence process



Source: Lowenthal, 2003: 52.

At least in the literature reviewed, the different schools of thought (traditionalists, reformists and revisionists) share a common feature, namely scant or no attention to – and the failure to conceptually integrate – counterintelligence as part of the intelligence process. The insufficient conceptual integration of counterintelligence as part of the intelligence process by traditionalists, reformists and revisionists alike is subsequently examined. Included in this examination is an alternative viewpoint which, prompted *inter alia* by the negation of counterintelligence, doubts the existence of a viable, all-discipline intelligence model (Hulnick, 2007: 1-21).

3. VIEWS ON THE STATUTORY COUNTERINTELLIGENCE PROCESS

The propositions discussed thus far, either categorically or implicitly (i.e. in the absence of a qualification to the contrary) purport to provide a model for the all-disciplinary, all-source intelligence process. Yet, even a cursory view of the graphic depictions (Figures 17 to 20) suggests the contrary.

3.1 THE COMPLEXITY OF COUNTERINTELLIGENCE AS AN INTELLIGENCE SUBDISCIPLINE

This neglect is perhaps in part ascribable to the complexity of counterintelligence in general, and counterespionage in particular. Given its location within the counterintelligence subdiscipline, this complexity is relevant to the design of the CE framework. The relevance of the intricacy of counterintelligence to this study goes beyond the design of the counterintelligence, counterespionage and open-source CE scanning processes as such. Because of the complexity of this intelligence sub-discipline, the foundational constituents for the design of the CE framework and scanning process are lacking. Since an academically accountable design of the CE framework and scanning process needs to be overlaid upon such foundational constituents, considerable parts of this and other chapters are devoted to addressing this theoretical paucity. Therefore, the following observations, spanning across decades, are pertinent not only to this chapter but the study in general:

- “CI is one of the most difficult intelligence topics to discuss.” (Lowenthal, 2003: 113).
- “Counterintelligence is perhaps the most demanding intellectually of any of the intelligence functions.” (Smith, 1980: 216).
- Counterintelligence, Taylor (2007: 12) contends, “is the most difficult of all intelligence work.”
- “Of all the elements of intelligence, counterintelligence is probably the hardest to define.” (Shulsky & Schmitt, 2003: 99).

- "We need an entirely new theory and practice of counterintelligence (CI) capable of dealing with both the expanded access of representations of foreign governments, and the more pervasive and subtle threat from a virtually unlimited '5th column' of criminals, narco-terrorists, and cult zealots." (Steele, 2001:141).
- "It is easy", to requote Codevilla (1992: 26), "to confuse CI with a host of other intelligence activities – collection, analysis, covert action – because good CI does everything that the full-fledged intelligence service does, and takes a hand in everything the rest of the service does."

3.2 VIEWS ON THE LOCATION OF COUNTERINTELLIGENCE WITHIN THE ALL-DISCIPLINARY INTELLIGENCE PROCESS

The deficient incorporation of the 'thorny' subdiscipline 'counterintelligence' as part of the all-disciplinary intelligence process not only traverses the respective positions of thought (i.e. orthodox, reformist and revisionist) but varies in form from scholar to scholar.

For the greater part, the intelligence process is presented by the outright omission of mentioning the location and role of counterintelligence as part of the intelligence process. Counterintelligence is, as is justly asserted by Hulnick (2007: 1), simply "ignored". It could be counterargued that these omissions are rooted in the tacit axiomatic assumption that counterintelligence (nebulously) 'fits in somewhere' with the 'processing and exploitation' phase or that counterintelligence is (somehow) performed throughout the intelligence process. This study contends that such tacit assumptions are not the fruits of axiomatic roots, but rather symptomatic of the fact that 'actually we do not know how to conceptually integrate the fiddly counterintelligence subdiscipline as part of the intelligence process'.

Even though similar to tacit assumptions in argumentative logic, and in some respects still vague, explicit contentions of counterintelligence as interwoven with, and performed throughout the (all-discipline) intelligence process, are naturally more helpful to the academic discourse. Arguing from an orthodox premise, Codevilla (1992: 4, 26, 325-326) views counterintelligence as being an integral part of all the sequential phases of the traditional intelligence cycle and as linked throughout this process with the other intelligence functional areas of 'analysis', 'collection' and 'covert action'. Codevilla (1992: 325) summarises his contention in this regard as follows: "CI concerns all aspects of intelligence ... It must use all of the elements of intelligence as part of itself, while at the same time CI as a whole must be part of the analysis, collection, and covert action practiced by intelligence services." (Codevilla, 1992: 4, 26, 325-326). While accentuating the distinctive demands that counterintelligence poses on the statutory context, Godson (2001: 3-6, 184-187) in essence shares Codevilla's (1992) stance. Albeit from a revisionist perspective, Lowenthal (2003: 113) too is in agreement with Codevilla's (1992: 35) approach by asserting that counterintelligence is "not a separate step in the intelligence process but ... an important function performed throughout the process."

The foregoing assertions on counterintelligence being inseparable from the all-disciplinary intelligence processes are, of course, not in dispute. Unfortunately these postulations are patently vague. The way in which counterintelligence is performed throughout the process or where it exactly slots in, is virtually left unexplained.

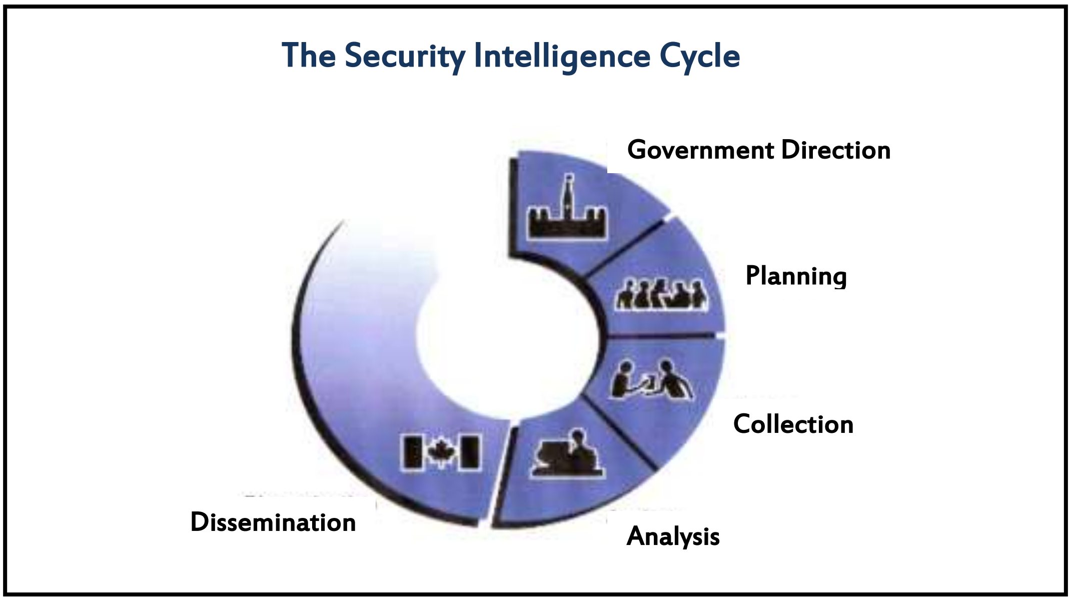
3.3 VIEWS WITHIN INTELLIGENCE STUDIES ON THE COUNTERINTELLIGENCE PROCESS *PER SE*

Equally amorphous, and in this instance highly disputable, is the tacit or explicit contention of the counterintelligence process itself mirroring the all-disciplinary intelligence process. The counterintelligence process, in other words, looks like and is a 'midi-version' of the intelligence process. The format of the counterintelligence process *per se* would thus be determined by the view taken on the broader all-disciplinary intelligence process.

3.3.1 Counterintelligence as a 'replica' of the all-disciplinary intelligence process

From an orthodox premise, the counterintelligence process would consequently be both a 'replica' and an integral part of the intelligence cycle. In this regard Hulnick (2007: 10) refers to the following depiction of the "security intelligence cycle" which constitutes an attempt by the Canadian Security Intelligence Service to adapt the intelligence cycle into a counterintelligence model:

Figure 21: The security intelligence cycle



Source: Canada, 2004:1.

Chapter Three indicated that counterintelligence consists of a range of defensive and offensive activities and measures. Although not presented as a model, the execution of counterintelligence functions is also well-described by, *inter alia*, Taylor (2007), Wettering (2000) and Godson (2001). No example could be found within the consulted Intelligence Studies' literature of an endeavour that demonstrates the conceptual moulding of the diverse counterintelligence functions and measures to fit the traditional intelligence cycle or any alternative model. Own efforts in this regard have strayed into a conceptual quagmire. Reassuring then was to note seemingly similar experiences by authoritative and seasoned scholars. Hulnick (2007: 10) asserts that counterintelligence "is not part of the traditional intelligence cycle – although some writers have tried to adapt the cycle into a counterintelligence model". Commenting on counterintelligence both as a process in itself and as part of the all-disciplinary intelligence process, Lowenthal (2003: 113) simply remarks that "CI does not fit neatly".

3.3.2 An alternative proposition on the counterintelligence process

Pointing out the distinctive nature of counterintelligence and the implications thereof for this intelligence subdiscipline's accommodation as part of the intelligence cycle, Hulnick (2007: 10, 14) states the following:

> In my view, counterintelligence follows an entire different and unique path of its own ... It has nothing to do with the intelligence cycle. Instead there is counterintelligence methodology that is unique ... So when one looks at the pattern of counterintelligence functions, it does not look at all like the intelligence cycle.

As an alternative, Hulnick (2007: 14-17) proposes the following “counterintelligence model” that resembles the “pattern of counterintelligence”:

Figure 22: The counterintelligence model

IDENTIFICATION

PENETRATION

EXPLOITATION

INTERDICTION

CLAIM SUCCESS

Source: Hulnick, 2007:14.

Summarised, Hulnick’s (2007: 14-17) description of the phases of the counterintelligence model are as follows:

- The identification of espionage adversaries;
- the penetration of espionage adversarial intelligence structures;
- exploitation – seen as including the collection of information (on adversaries) and the institution of measures such as deception;
- interdiction, which ensues when the “the case is turned over to law enforcement”; and
- public declarations by authorities of successful counterintelligence actions.

Hulnick (2007:10) explicitly limits the counterintelligence model above to what he terms “active counterintelligence”. The latter includes but is more encompassing than just counterespionage. Hulnick (2007: 10) explains this view as follows: “Today, counterintelligence has become much more diverse than just stopping spies. It now means countering terrorism, narcotics flows, global organized crime, and subversion.” In adding a qualification, “defensive measures in counterintelligence”, are described as not fitting into “either the traditional intelligence cycle or the model just described.” (Hulnick, 2007: 16).

3.4 SUMMARY AND IMPLICATIONS FOR THE OPEN-SOURCE COUNTERESPIONAGE ENVIRONMENTAL SCANNING PROCESS

The two preceding sections (Two and Three) appraised some propositions within Intelligence Studies on statutory intelligence processes. This appraisal was done from the premise that the CE framework would ideally need to be presented as part of a multilayered unison of intelligence, counterintelligence and counterespionage processes.

The traditional intelligence cycle, contemporised versions thereof as well as other intelligence process propositions reviewed, are deficient in accommodating counterintelligence. Vaguely alluding to counterintelligence as interwoven with the intelligence processes or conjuring counterintelligence into, for example, the 'exploitation phase', is highly questionable on both theoretical and practical grounds. Propositions in the consulted literature that either implicitly or explicitly purport to represent the all-discipline intelligence process, should perhaps be seen for what they apparently are, namely endeavours to explain the positive intelligence process.

With the exception of Hulnick's (2007) model, views on the counterintelligence process *per se* are confounding to the extent of becoming conceptual quagmires. The nature and range of counterintelligence activities simply do no fit contentions of the counterintelligence process as being a meso-level 'replica' of the all-discipline process.

A proposition by Hulnick (2007) regarding the counterintelligence process is limited to "active" counterintelligence. Offensive and defensive measures, however, are closely interlocked and in some instances hardly distinguishable from one another. Hulnick's (2007) model, moreover, provides for only a few of the wide range of "active" measures addressed in Chapter Three. Should Hulnick's (2007: 10) assertion that counterintelligence has "nothing to do with the intelligence cycle" be interpreted as strictly referring to the traditional notion, it would be in line with the study's contention. Counterintelligence has, of course, everything to do with a viable and still elusive all-discipline intelligence process.

Conceptualisations of the intelligence and counterintelligence processes in consulted literature are clearly insufficient in serving as foundational constituents for the design of open-source CE scanning. Also apparent is the predicament this poses to the study – the CE framework needs to be integrated with, and draw in its design on, a higher-order process of which viable models (as far as could be reasonably ascertained) do not exist.

Nevertheless, the overview does provide elements useful to the construction of the CE scanning process. These include: the multidirectional functioning of the intelligence process (Lowenthal, 2003), Hulnick's (2007) counterintelligence model as well as the importance to the intelligence process of both the external environment (Gill & Phythian, 2006) and environmental "scouting" (Bernhardt, 2003).

Given the theoretical poverty within Intelligence Studies in respect of viable models on intelligence processes, an examination of these concepts within Business Intelligence warrants an examination with a view of ascertaining aspects of possible relevance to the construction of the CE scanning process.

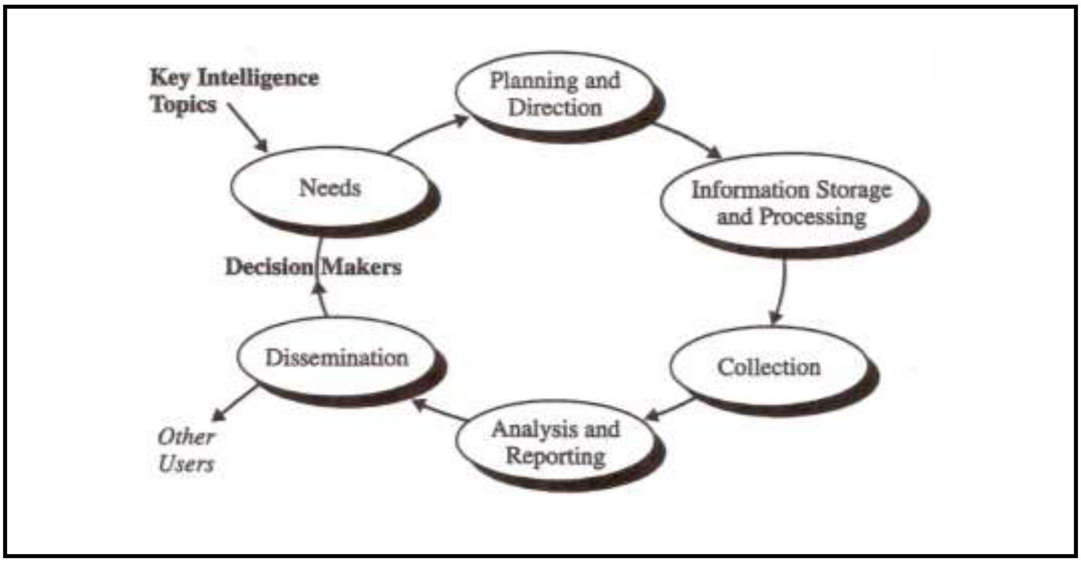
4. VIEWS WITHIN BUSINESS INTELLIGENCE ON THE INTELLIGENCE AND COUNTERINTELLIGENCE PROCESSES

The desirability of an exploration of the intelligence and counterintelligence processes as perceived in the corporate milieu, is reinforced by the fact that 'ethical' Business Intelligence – like the CE framework – is reliant on open/grey-source information (on competitors), and accentuates the 'environmental scanning' concept to a larger degree than is the case within Intelligence Studies.

4.1 THE APPLICATION OF THE INTELLIGENCE CYCLE IN BUSINESS INTELLIGENCE

The pervasive influence of the intelligence cycle concept is not limited to Intelligence Studies and is also apparent within Business Intelligence. Similar to Intelligence Studies, nuanced variants of the intelligence cycle are not in short supply in the Business Intelligence discipline. If scrutinised, these variants can likewise be reduced to four main sequential elements namely: planning and determining "key intelligence needs", collection, analysis, and dissemination (Nolan, 1997: 56, 59: Muller & Whitehead, 2002: 4, Brouard, 2004: 4). This commonly held view of the business intelligence process is graphically depicted by Fleisher & Bensoussan (2003:6) as follows:

Figure 23: The business intelligence cycle



Source: Fleisher & Bensoussan, 2003: 6.

As was mentioned, the notion of 'environmental scanning' features more prominently in explanatory descriptions of the business intelligence cycle. Illustrative in this regard is the following synoptic overview offered by Brouard (2004: 4; emphasis added):

> Environmental scanning could be defined as an informational process by which an organization stays attuned to its environment in order to make decisions and then acts in pursuit of its objectives. Business intelligence is the result of that process ... As the terminology is still in flux ... environmental scanning and business intelligence [are used] interchangeably as comprehensive terms that include both process and results ... The *process of scanning itself is termed the intelligence cycle*.

Within the broader Business Intelligence discipline, the concept 'intelligence process' is widely used as denoting only – what in statutory terminology would be deemed as – the generation of 'positive intelligence'.

4.2 THE DEFENSIVE CORPORATE INTELLIGENCE PROCESS

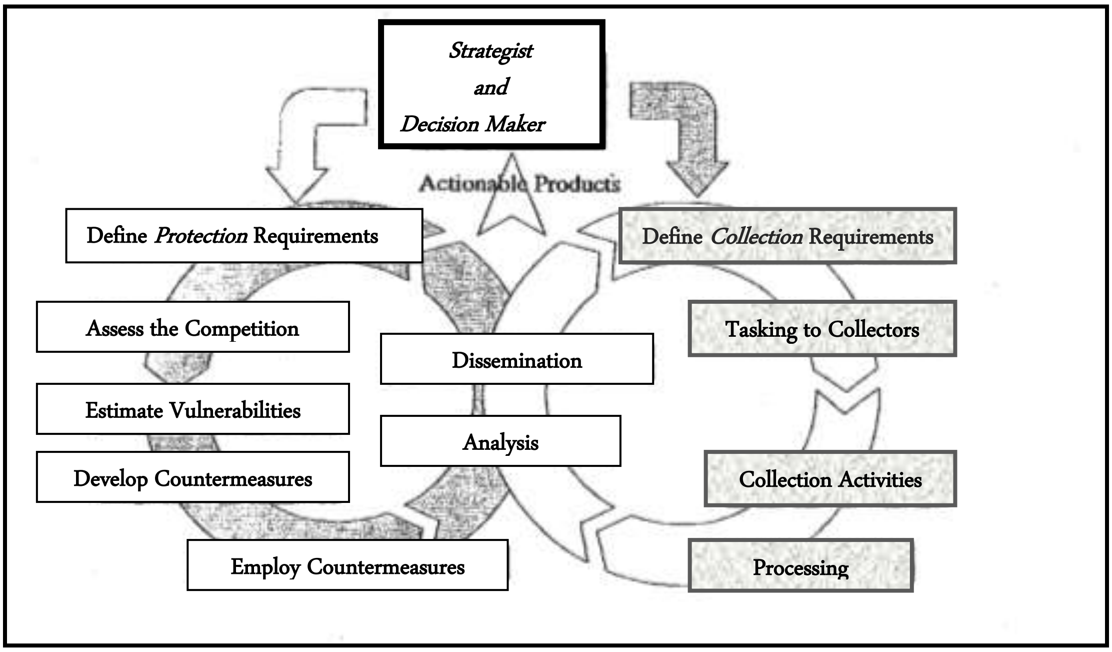
Within the Competitive Intelligence subdiscipline and the specialisation field (within Competitive Intelligence) of Competitor Intelligence, however, the delivery of 'intelligence' has additional 'defensive' and 'offensive' connotations. Since the terminologies are still in flux in this respect, the terms "protective competitive intelligence”, “defensive competitive intelligence” or “defensive intelligence” are used interchangeably as referring to the corporate equivalent of statutory counterintelligence (DeGenaro, 2005: 12-14, Brouard, 2004: 1, 5; Nolan, 1997: 57; Muller, 2002: 4). With the *caveat* that some variations do exist, ‘protective competitive intelligence’ is widely accepted to consist of the following steps (DeGenaro, 2005: 14-15; Muller, 2002: 4-5, 8; Francq, 2000: 85):

- The identification of critical information warranting protection in order to arrive at protection requirements;
- an appraisal of the threat (‘external danger’) posed by competitors;
- an assessment of those corporate vulnerabilities that increase the risk of information being compromised;
- the development and implementation of countermeasures; and
- the continual assessment and adaptation of the effectiveness of countermeasures in accordance with the changing environment.

In the main, ‘protective competitive intelligence’ is deemed to include two principal components, namely ‘security measures’ and ‘counterintelligence’. Nolan (1997: 55; emphasis in the original) draws the following concise distinction between these components: “[S]ecurity seeks to protect a firm’s assets, counterintelligence seeks to actively engage and *neutralize* a competitor’s collection effort.” Security is deemed as being of a passive nature and seeks to reduce corporate vulnerabilities as well as protect a firm’s tangible and intangible assets (such as sensitive information) through a combination of policies, procedures and practices – on a lighter note referred to as “gates, guards, guns and dogs” (Francq, 2000: 85, 71). ‘Corporate counterintelligence’ on the other hand is considered to be of an offensive nature and aims to neutralise a competitor’s collection efforts through “a variety of imaginative, flexible, and active measures” (Francq, 2000: 71; Brouard, 2004: 5, Nolan, 1997: 53). Descriptions of what these “imaginative, flexible, and active measures” (Nolan, 1997: 53) entail, testify to the similarities between contemporary competitive business intelligence and statutory intelligence. In what in practical application, and under certain circumstances may resemble statutory informational covert action, “deception” (used interchangeably with “perception management”) is classified by scholars such as Francq (2000: 75) as “[p]erhaps the most proactive, aggressive, and effective” of competitive counterintelligence measures.

Statutory intelligence provided the theoretical and practice-directed cornerstones for the establishment of Competitive Intelligence. Paradoxically then, is Competitive Intelligence's overtaking of Intelligence Studies in endeavouring to structure the counterintelligence and counterespionage processes notionally. Over a decade ago, Nolan (1997: 53-61) forwarded a seminal model that not only conceptually structures corporate counterintelligence, but also aims at integrating the latter with positive business intelligence. Nolan (1997: 59) graphically depicts the synergy between positive business intelligence (process on the right represented as a white circle) and corporate counterintelligence (process on the left represented as a grey circle), as follows:

Figure 24: Integrated business intelligence model

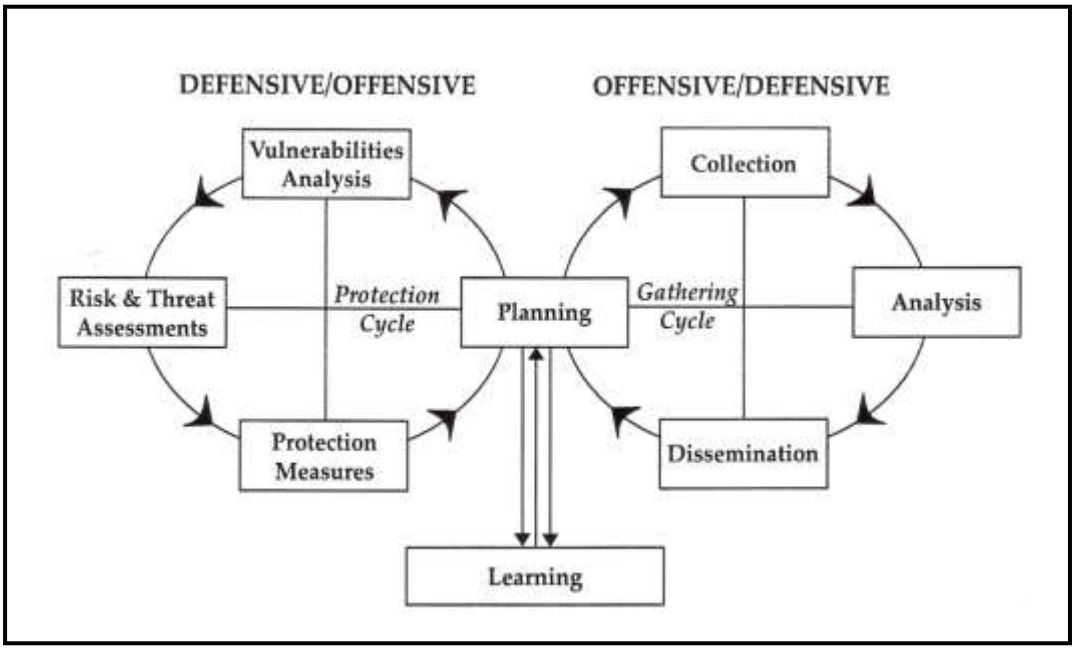


Source: Nolan, 1997: 59.

In line with general Competitive Business Intelligence lexicon, 'corporate counterintelligence' as used by Nolan (1997) refers to the 'active' countermeasures. Nolan (1997: 53-61) categorically precludes 'corporate security measures' from counterintelligence. The interaction between corporate counterintelligence and corporate security measures is, however, not negated – especially in as far as the estimation of organisational vulnerabilities is concerned (Nolan, 1997: 55-58). The distinction between corporate counterintelligence and corporate security, according to Nolan (1997: 58), lies in the following difference in the managing of vulnerabilities: "Security would close the vulnerability as if it were a hole in the fence; counterintelligence would seek to find opportunities these vulnerabilities present." Although not phrased as such by Nolan (1997: 53-61), the notion of corporate counterintelligence involving a certain degree of intra-organisational (internal) environmental scanning to ascertain organisational vulnerabilities is implicit to his proposition.

While exploratory in nature, some more recent works within Competitive Intelligence endeavour to integrate the whole of corporate defensive intelligence (i.e. corporate counterintelligence as well as security measures) with positive business intelligence. Serving as an example is a proposition by Brouard (2004) which builds on the works of Nolan (1997), Pattakos (1997), Nolan & Quinn, (2000) and Francq (2001) on an "intelligence gathering and protection intelligence process". As suggested by the title of the model and as depicted by the following graphic illustration, Brouard's (2004) model consists of a "gathering process" (geared towards positive corporate intelligence) and a "protection" process (dealing with the defensive corporate intelligence process):

Figure 25: Intelligence gathering and protection intelligence process



Source: Brouard, 2004: 5.

In the explication of the above model, Brouard (2004: 2-3, 8-9) stresses the importance of environmental scanning including both an internal environmental (organisational context) and an external, macro-environmental dimension.

4.3 SUMMARY AND IMPLICATIONS FOR THE OPEN-SOURCE COUNTERESPIONAGE ENVIRONMENTAL SCANNING PROCESS

In contrast to Business Intelligence which draws extensively on Intelligence Studies' thinking, Intelligence Studies appears to be largely self-isolated and self-impoverished from enrichment by the discourses within Business Intelligence. Regrettably, Business Intelligence has not escaped the dominance in thinking insofar as the rigid circular structuring of the intelligence process is concerned. Business Intelligence, however, is clearly more developed in the conceptual structuring of the defensive/counterintelligence process, and the integration thereof with the positive intelligence process.

Given previously noted fundamental contextual differences, Business Intelligence thinking cannot be summarily applied to Intelligence Studies and statutory intelligence practice. Despite these differences, Business Intelligence propositions on the counterintelligence process and the integration thereof with the positive intelligence process, render the following that are useful to the conceptualisation of open-source counterespionage environmental scanning in the statutory intelligence milieu:

- Environmental scanning, consisting of both internal and external dimensions, is not a separate phase in the intelligence and protective processes, but is performed throughout these processes (Brouard, 2004: 2-3, 8-9).
- "Key intelligence needs" serve as the premise of the positive and protective/defensive processes (DeGenaro, 2005: 12-15; Brouard, 2004: 1, 5; Nolan, 1997:57; Muller, 2002: 4-5, 8; Francq, 2000: 85). In the case of 'protective corporate intelligence', the postulation of key requirements has the identification of critical information as an imperative precondition.
- With reference to Nolan's (1997:53-61) postulation as depicted in Figure 24, the centre that drives and symbiotically integrates the positive and protection processes consists of the client ("decision-maker"), the "strategists" (practically, the line-functional leadership of the competitive intelligence structure), and the analysis function.

The subsequent section endeavours to incorporate the above-mentioned contentions, as well as aspects that emerged from the examination of the discourse within Intelligence Studies, in the forwarding of propositions on intelligence and counterintelligence processes that are germane to the requirements of the CE framework.

5. A PROPOSITION ON A REDUCTIVE, CONCEPTUAL NEXUS FOR THE ALL-DISCIPLINE INTELLIGENCE PROCESS

While the theoretical discourse within Intelligence Studies and statutory intelligence was shown in Chapter Two to have gained significant momentum since 9/11, an agenda for the development of a truly all-disciplinary intelligence process has, figuratively speaking, not been set as yet. On the contrary, deliberations on such a process that involved eminent scholars and seasoned practitioners - during a conference hosted by the Office of the US Director of National Intelligence and the RAND Corporation in June 2005 and with the theme *Toward a Theory of Intelligence* – suggest that clarity in this regard will require extensive research and further debate (Treverton *et al*, 2006: 25).

An attempt to forward even a tentative model on an all-disciplinary intelligence process as part of this study would consequently be both overambitious and premature. To partially compensate for the void in a viable overarching proposition, the study could nevertheless endeavour to propose a reductive, conceptual nexus toward an all-discipline intelligence process. It must be emphasised that, whether narrative or schematic, this study's proposition in this respect should not in any way be construed as an attempt to construct an overarching all-discipline process. This conceptual nexus is comparable with the 'contour' towards a grand theory of intelligence forwarded in Chapter Two and is inevitably 'abstract' in certain respects. Since theoretical approaches on an abstract level ultimately condition intelligence practice, such a nexus is - in addition to other aspects mentioned - indisputably relevant and pivotal to the design of the CE framework.

Chapter Two also referred to Johnson's (in Gill, 2006: 5) assertion that progress in theorisation on intelligence compels the laying out of "what we know in such a manner as to suggest next steps in theory construction." Equally important in the view of this study is to be forthright about 'what we do not know' and re-examine 'what we think we know'.

'What we think we know' includes certain axioms in Intelligence Studies. One such axiom is the contention of statutory intelligence as consisting of four principal subdisciplines, namely, 'analysis', 'collection', 'counterintelligence' and 'covert action'. For reasons of clarity and consistency with the Intelligence Studies' lexicon, this study has thus far also used the concept 'intelligence subdiscipline' in this conventional sense.

It is unclear how the common acceptance of 'analysis', 'collection', 'counterintelligence' and 'covert action' as the principal intelligence subdisciplines originated or evolved. Future studies by Intelligence Studies historians and historiographers might well find that the four-subdiscipline division coincided with the organisational structuring of some post-World War II, Western statutory intelligence services. What is murky, but in this instance based on purely argumentative-logical grounds, is the inclusion of two subdisciplines ('analysis' and 'collection') as phases in depiction of the intelligence process (Figures 17-20), while the other two ('counterintelligence' and 'covert action') are conspicuous in their absence.

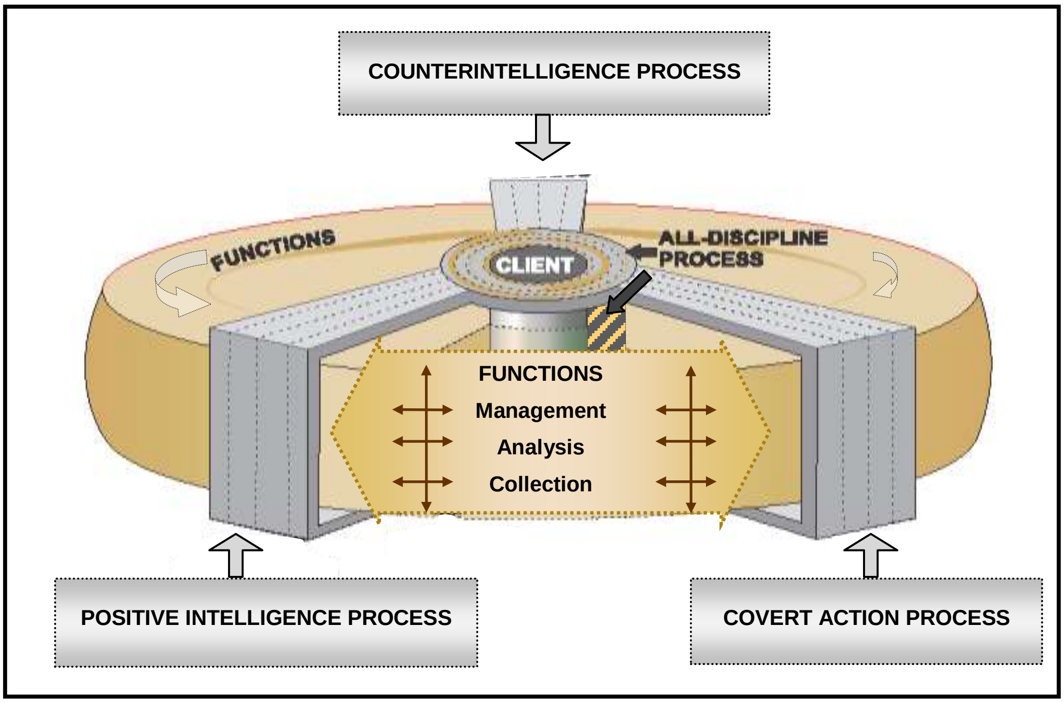
In the light of the evaluation of the discourse within Intelligence Studies and Business Intelligence views on intelligence processes, a different perspective is called for. An all-discipline intelligence nexus, it is argued, should be underpinned by the following unequivocal distinction between subdisciplines, functional areas and practicalities:

- As a central contention towards the proposition of the nexus, the axiom of intelligence consisting of the said four principal subdisciplines is contested. Statutory intelligence, this study argues, consists of *three principal sub-disciplines*, namely, 'positive intelligence', 'counterintelligence' and 'covert action'. There is no compelling reason why Hulnick's (2007) assertion that each of 'counterintelligence' and 'covert action' which follows a unique methodology and distinctive "pattern" of activities, cannot be extended to 'positive intelligence'. To reiterate, an all-discipline intelligence process should coherently integrate and bind these three subprocesses.
- 'Analysis' and 'collection' are *functional areas* of activity that are performed within all three subdisciplines. These functional areas are obviously not limited to 'analysis' and 'collection'. The identification of further functional areas would require dedicated research and this study suffices with proposing 'intelligence management' as an addition. Apart from its typical connotations, 'intelligence management', as used in the context of the proposed nexus, also includes the coordination of the activities between the different intelligence structures of a particular nation state. Supported by analysis, intelligence management is in reality the interface with the client (decision maker). In an alternative proposition, the functional areas of analysis and management can be positioned as that which synergistically binds the three subdisciplinary processes.

- Arguably the most confounding axiom reflected in propositions on the intelligence process reviewed is the inclusion of 'dissemination'. The latter deals with *practical and procedural issues* such as the types of intelligence products ("product line") and the delivery thereof to consumers (Lowenthal, 2003: 48-49). It is doubtful whether an all-source model, which is at a macro-theoretical level and inherently abstract, should include practical and procedural matters of such a nature.

Existing notions, as Figures 17 to 20 demonstrate, blend 'subdisciplines', 'functional areas' as well as practical issues into an overarching intelligence process without conceptual distinction and on equal footing. Based on the assertions above, the following is proposed:

Figure 26: A reductive, conceptual nexus toward an all-discipline intelligence process



The proposition, admittedly, requires much further refinement as well as substantiating research and is indicated as such in Chapter Eight. At the very least, indications are that the nexus aids to conceptually clarify the relationship between counterintelligence and transnational security concerns such as counterproliferation (of WMD), organised crime and counterterrorism. While some scholars consider counterterrorism as part of counterintelligence, others assert counterterrorism to have "developed" into a "separate intelligence discipline" (Hulnick, 2007: 10; Wettering, 2000: 266). Counterterrorism is neither a separate intelligence discipline nor is it part of counterintelligence. Instead, it is a security concern that involves facets of ‘positive intelligence’, ‘covert action’ as well as ‘counterintelligence’.

6. A PROPOSAL ON THE COUNTERINTELLIGENCE PROCESS

As depicted above, counterintelligence is an integral part of the all-discipline intelligence process. Similar to other subdisciplines, it was argued, counterintelligence has a distinctive role that is executed by means of a unique ‘pattern of activity’. It is this pattern of activity that constitutes the counterintelligence process. The subsequent proposal on an all-source counterintelligence process is submitted within the parameters of preconditions. These qualifications are in part a recapitulation and an extension of assertions made in the earlier appraisal of existing intelligence and counterintelligence models. The *caveats* are not similar in nature to the growing number of qualifications employed in defence of the intelligence cycle, but rather explanatory comments accompanying the postulation of an alternative proposal.

First and foremost, the counterintelligence process is forwarded, and qualified, as a model. Therefore, it is, to requote Berkowitz & Goodman (2000: 72-73), a simplification and idealisation of a reality that is “more subtle and more complex”. Even though a simplification, the model should not be construed as an attempt to offer a ‘skeleton’ for the compilation of a ‘fast recipe’ counterintelligence ‘cookbook’. Scholars proposing or seeking a counterintelligence model wherein all activities fit neatly and that serves as a ‘formula’ for ‘shortcutting’ the tedious work of counterintelligence, are in all probability searching in vain. Analogically phrased, most seasoned practitioners who have toiled in the heat of the counterintelligence kitchen would advise ‘easy recipe’ proponents to conjure up their broths in alternative locations. Consequently, the counterintelligence model endeavours to simplify without oversimplification.

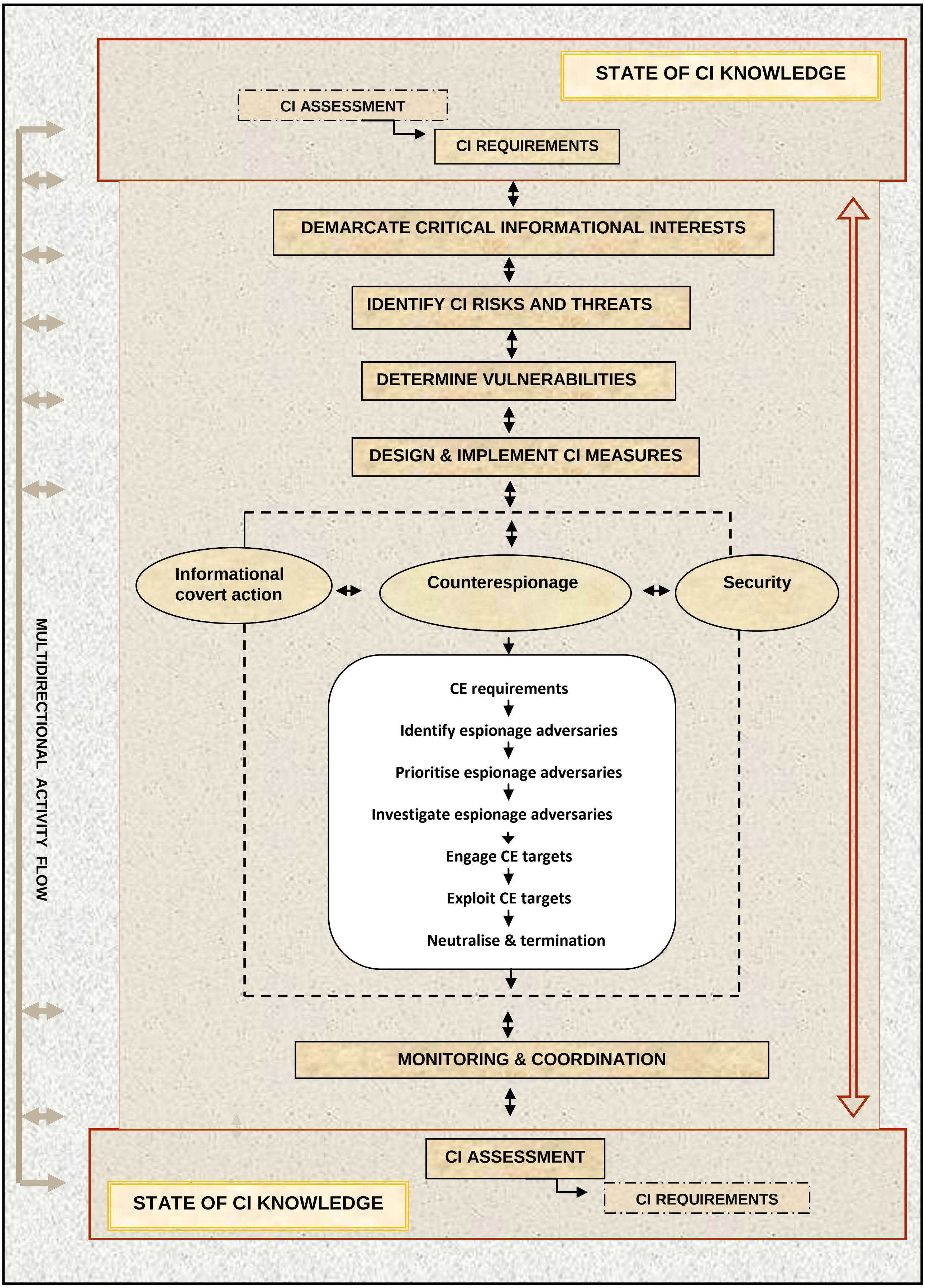
To this end, the counterintelligence model clusters (counterintelligence) activities according to stages that, in order to aid easier conceptualisation, are presented as a consecutively ordered process. This consecutive phasing is, however, not a rigid chronological compartmentalisation. Phases are interlinked and rarely neatly completed before moving to the next. The multidirectional activity flow proposed by Lowenthal (2003: 52) is therefore applied, *mutatis mutandis*, to the counterintelligence processes. Counterintelligence phases and the activity flow are at the same time linear, circular, open-ended and in continuous interaction (Lowenthal, 2003: 52).

The qualification on the multidirectional flow of, and within, the counterintelligence process, extends to two further aspects. Firstly, at a practical level, some activities are not limited to a specific phase but recur throughout the counterintelligence process. Serving as examples are intelligence management functions and environmental scanning (in both its collection and analysis dimensions). Secondly, and at a macro-level, the counterintelligence process links with the positive intelligence and covert action processes through a continuous multidirectional flow. Although the narrative explication of the counterintelligence model selectively reflects on the multidirectional flow between the principal intelligence subdisciplines, such references do not in any measure replicate the full extent of this symbiotic interaction.

The counterintelligence model is furthermore qualified in focus. Dimensions of the counterintelligence model to be used later in the design of the CE scanning process are highlighted at the inevitable expense of others. As various aspects that form part of the counterintelligence process are also incorporated as part of the open-source CE scanning process, a too detailed explication of such aspects (in the presentation of the counterintelligence model here) would result in excessive repetition. Consequently, the counterintelligence model is in some respects cursory in its narrative description and relies on the more detailed explication of the CE scanning process for further elucidation.

Within the parameters of the stated preconditions, the proposition on a counterintelligence model can schematically be depicted as follows:

Figure 27: The all-source counterintelligence process


STATE OF CI KNOWLEDGE
CI ASSESSMENT
CI REQUIREMENTS
DEMARCATE CRITICAL INFORMATIONAL INTERESTS
IDENTIFY CI RISKS AND THREATS
DETERMINE VULNERABILITIES
DESIGN & IMPLEMENT CI MEASURES
Informational covert action
Counterespionage
Security
CE requirements
Identify espionage adversaries
Prioritise espionage adversaries
Investigate espionage adversaries
Engage CE targets
Exploit CE targets
Neutralise & termination
MONITORING & COORDINATION
CI ASSESSMENT
CI REQUIREMENTS
STATE OF CI KNOWLEDGE
MULTIDIRECTIONAL ACTIVITY FLOW

6.1 FORMULATION OF COUNTERINTELLIGENCE REQUIREMENTS

In its broadest sense, counterintelligence requirements refer to that ‘intelligence’ (information) and those ‘services’ (actions) the client expects from its counterintelligence apparatus in order to optimally pursue its vital interests and objectives. Counterintelligence requirements are thus all about the direction and prioritisation of the effort of statutory intelligence in accordance with the needs of the client.

Especially within counterintelligence, such requirements are for the most part not contained in a neatly packaged ‘wish list’ received from the client. Even would a utopian relationship have existed between a statutory counterintelligence structure and its client, it would be unrealistic to expect the latter to provide clear-cut, all-encompassing requirements and priorities. It is surely incumbent on the counterintelligence structure to propose such requirements and priorities. Although there are exceptions, the policymaker’s decisions or guidance in this regard is mainly on a strategic level and pertains to (broad) principal intelligence requirements.

Hence, counterintelligence requirements are mostly derived and not received. They are derived from the intelligence service’s assessment of the policymaker’s national and national security objectives, and information collected by the intelligence service itself. In practice, this appraisal is contained in a national counterintelligence assessment which considers four key counterintelligence questions, namely:

- What are the vital informational interests of the nation state that warrant the expending of significant resources to advance and protect?
- Which significant threats and risks exist in relation to the vital informational interests?
- How, and in what respects, are the vital national interests vulnerable to such risks and threats?
- What counterintelligence measures are required to further determine risks and threats against vital national informational interests, effectively safeguard the said interests, and exploit the opportunities presented by risks and threats?

Essentially, the said assessment reflects the existing ‘state of counterintelligence knowledge’. The ‘state of knowledge’, as elaborated upon in Section 8.2 with specific reference to the CE framework, entails clarity on what the counterintelligence structure 'knows', 'what it does not do not sufficiently know' and 'what it needs to know'. In the linear facet of the multidirectional activity flow, the counterintelligence assessment is simultaneously at the beginning, performed throughout, as well as at the end of the counterintelligence process. Consequently, the aforesaid four key counterintelligence questions are also building blocks in the process. Considering its intricacy and dispersion throughout the counterintelligence processes, Figure 27 depicts counterintelligence assessment as well as the formulation of counterintelligence requirements as a continuous phase. Based on the principal counterintelligence requirements contained in the national counterintelligence assessment, more specific requirements are generated throughout the counterintelligence process.

6.2 THE DEMARCATION OF CRITICAL NATIONAL INFORMATIONAL INTERESTS

The demarcation of information vital to the nation's present and future stability and prosperity constitute the subsequent phase of the counterintelligence process. Chapter Six will show that not all information vital to national prosperity is necessarily of counterintelligence relevance. Counterintelligence needs to ascertain information of such critical value and nature that if it were compromised in integrity and/or content, national prosperity and security would be detrimentally affected. This delineation pertains to the *substance* of the information (namely the subject matter), the *location* of the information (practically the custodians thereof); and (c) the *repositories* (systems) in which this information resides.

The substance of, as well as the clandestine activities undertaken to procure secret, positive intelligence is deemed as being part of the state's critical informational interests. Since counterintelligence must know what it is supposed to protect, interaction with positive intelligence is of obvious importance in this regard. Interfacing with positive intelligence, moreover, aids counterintelligence in the delineation of national informational interests. The interaction between counterintelligence and covert action is of the same dualistic importance at this stage of the counterintelligence process.

6.3 IDENTIFICATION AND DESCRIPTION OF COUNTERINTELLIGENCE RISKS AND THREATS

The counterintelligence process is rarely conducted *ad novo*, and the body of existing counterintelligence information is utilised in the identification and description of counterintelligence risks and threats. While such risks and threats are addressed in the counterintelligence assessment at a strategic level, this phase of the counterintelligence process adds a tactical and operational focus.

The identification and description of risks and threats involves all three counterintelligence fields. From a counterespionage perspective, the risk and threats that espionage adversaries pose to critical informational interests are appraised. Interlocked with the counterespionage assessment, the risks and threats in relation to hostile informational covert action are examined. Equally important are risks emanating from the security field. Examples of such risks could include security breeches, a high level of non-adherence to security regulations on information control, as well as breeches in relation to INSYSEC (as explained in Chapter Three).

6.4 IDENTIFICATION AND APPRAISAL OF VULNERABILITIES

Following, and in various respects overlapping with the preceding phase, the counterintelligence process progresses to the assessment of the vulnerabilities of the nation state’s informational interests to the identified risks and threats. Concurrently, the effectiveness and pertinence (i.e. the ‘appropriateness’ in view of the nature of risks and threats) of existing countermeasures – offensively as well as defensively – are evaluated. Since critical national informational interests are not limited to the state apparatus, the assessment of vulnerabilities and protection also include entities of national security relevance such as corporate enterprises.

6.5 DEVISING AND IMPLEMENTING COUNTERINTELLIGENCE MEASURES

The foregoing appraisal enables a decision on which counterintelligence measures are obsolete, which require modification, and in which areas are they lacking or insufficient. Informed by the deficiencies in the ‘counterintelligence picture’ identified during preceding phases, areas for directing the analysis and collection effort are prioritised. This stage of the counterintelligence process is thus focused on ‘what are we going to do to procure information required and rectify weaknesses in offensive as well as defensive counterintelligence protection?’

The decisions taken in this regard are embodied in an overall strategy for the execution of counterintelligence measures. Within the ambit of the overall strategy, and without negating the importance of continuing interaction, the specialised design of the counterintelligence measures are conducted within the respective counterintelligence fields.

‘Counterespionage’, ‘security’ and ‘informational covert action’ are specialisation fields, each with its own ‘logic’ and methodology. Simplified for purposes of a counterintelligence model, the description of the counterintelligence process has so far focused on the commonalities in patterns of activity that these fields share. Extending such a generalisation to the design and implementation phase of the counterintelligence process would, however, be an oversimplification and distortion of reality. Deliberating on the distinctive processes of designing and implementing measures within the security and informational covert action fields, will distract from the counterespionage emphasis of the study.

Given the importance of the process followed in the design and implementation of counterespionage measures, Section Seven is devoted to a more detailed discussion thereof, and the listing of the following seven phases of the counterespionage process will suffice here:

- Formulation of counterespionage requirements;
- identification of espionage adversaries;
- prioritisation of espionage adversaries;
- investigation of espionage adversaries;
- engagement of counterespionage targets;
- exploitation of counterespionage targets; and
- neutralisation and termination.

6.6 MONITORING AND COORDINATION

Although monitoring and coordination are more a part of the preceding phase than representing a separate stage of the counterintelligence process, such a conceptual clustering provides the simplification and clarification central to the construction of a counterintelligence model. Monitoring and coordination are performed at two levels, namely, within the respective fields, and secondly, at an integrated counterintelligence level.

Integrated monitoring and coordination are obvious prerequisites for effective counterintelligence. Both counterespionage and informational covert action are inherently deceptive. Deficient coordination in the implementation of activities within, and between these fields increases, *inter alia*, the risk of self-deception. The intelligence service could, in other words, fall victim to initiatives aimed at deceiving adversarial espionage actor(s). As part of an informational covert action programme, for example, an 'asset' (human source or agent) could be established with the aim of feeding disinformation to an espionage adversary. The contact between the asset and the espionage adversary is detected by the counterespionage function. Unaware of his/her actual status, counterespionage recruits the asset under a false flag. As a result, disinformation provided by the covert action structure is fed 'unfiltered' to the counterespionage structure.

Coordination between counterespionage and security is equally imperative. In the coordination of the measures instituted within these two counterintelligence fields, a balance needs to be maintained between, to paraphrase Nolan (1997: 58), security's mission to 'close holes in the fence', and counterespionage that seeks to exploit the offensive opportunities that vulnerabilities present. Exposed vulnerabilities in security measures could, for example, be left apparently weak to entice suspected hostile espionage.

6.7 COUNTERINTELLIGENCE ASSESSMENT

Although a continual activity, an intelligence service will additionally schedule comprehensive appraisals of the effectiveness of counterintelligence measures at regular intervals (e.g. annually or bi-yearly). In respect of counterespionage, this appraisal will consider 'new' information on espionage risks and threats generated throughout the counterintelligence process. Such an appraisal is indispensable toward a revision of the comprehensive counterintelligence assessment conducted earlier in the counterintelligence process. The latter, on its part, is likely to result in a revision of counterintelligence requirements.

This section forwarded a proposition on the all-source, statutory counterintelligence process. Given the critique levelled against purported all-disciplinary proposals that are in effect positive intelligence 'stove-piped' processes, the counterintelligence model intentionally highlighted the interdependence between, 'positive intelligence' 'covert action' and 'counterintelligence'. The continuous interaction within the counterintelligence process between the fields of 'security', 'counterespionage' and 'informational covert action' were also emphasised. In addition to being a theoretical imperative, the interdependence between the intelligence subdisciplines and the counterintelligence fields respectively was accentuated because it has direct implications for the design of the CE framework. Within the CE scanning process, analysis and collection are performed parallel to the all-disciplinary intelligence and the all-field counterintelligence processes. Yet, perspectives emanating from positive intelligence, covert action and the other counterintelligence fields are required for successful open-source, counterespionage environmental scanning. In order to offset its 'isolation' from the all-source endeavour, the CE framework will be shown to include aspects that would conventionally be associated with positive intelligence, covert action as well as counterintelligence fields other than counterespionage.

7. A PROPOSITION ON THE COUNTERESPIONAGE PROCESS

In outlining the counterintelligence process, the preceding section re-asserted and illustrated qualifications previously expressed regarding the process within the statutory milieu in general. It is also within the context of these *caveats* that a proposition for an all-source, seven-phased counterespionage process is presented. These seven phases designate, in ascending order, the progressive increase in the aggressiveness of statutory counterespionage methods. In this respect a further qualification needs to be added. Some of the counterespionage methods can serve more than one purpose. The variety of HUMINT sources[2], for example, can simultaneously be employed as instruments of collection, exploitation and neutralisation. In the interest of simplicity, the illustration of the counterespionage process by means of examples relies mainly on the HUMINT aspect of counterespionage. This should not be construed as negating the importance of TECHINT within counterespionage as was discussed in Chapter Three.

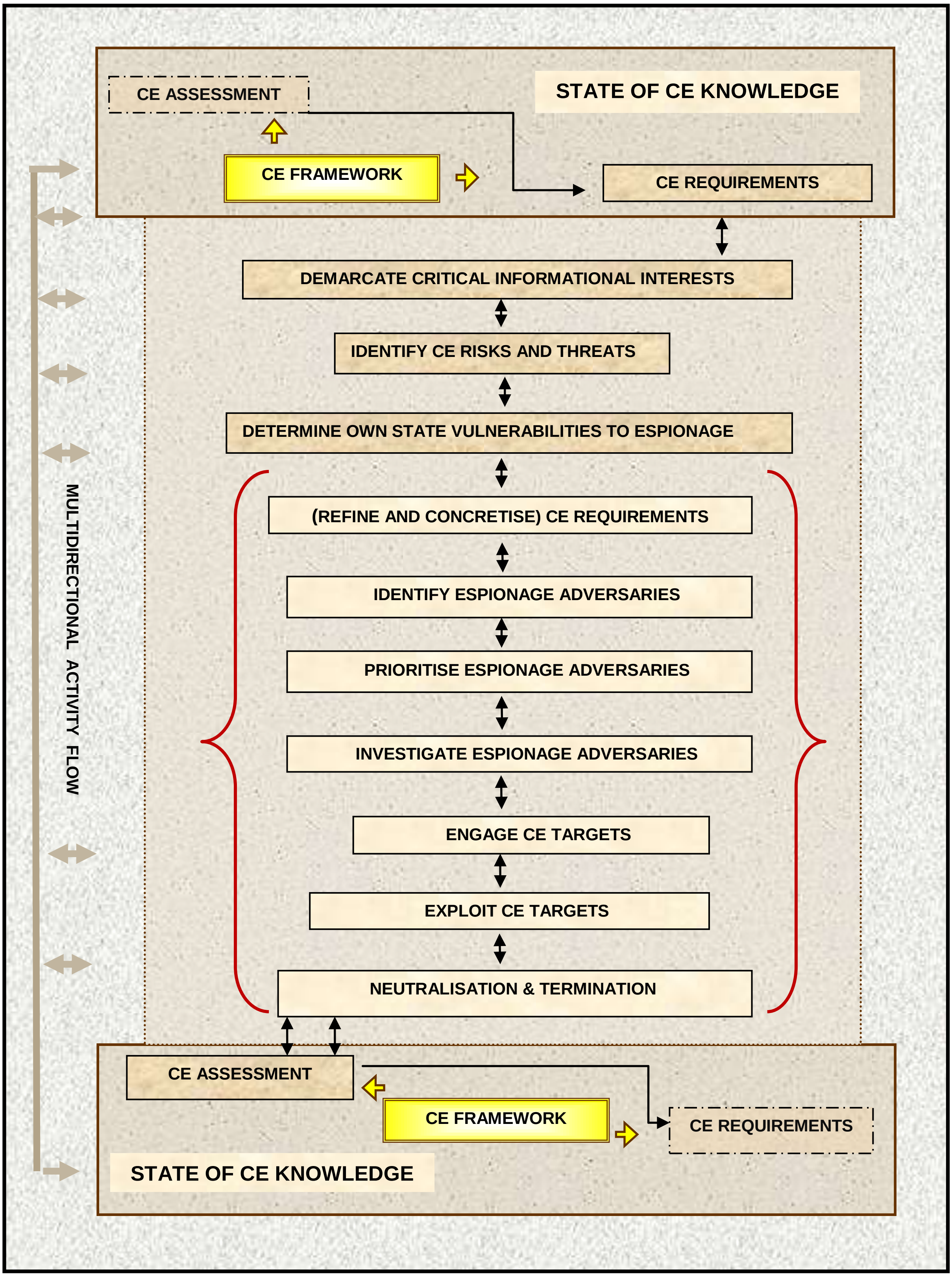
7.1 FORMULATION OF COUNTERESPIONAGE REQUIREMENTS

The formulation of counterespionage requirements is based on the outcome of preceding stages of the counterintelligence process. Should the counterespionage process have been presented autonomously – in other words not as part of the broader counterintelligence process as per Figure 27 – the said

[2] As noted in Chapter Three, HUMINT in the counterespionage context includes, but is not limited to peripheral agents, agents-in-place, access agents, moles, defectors, double agents, multi-turned agents (such as triple, quadruple agents), agent provocateurs, walk-ins, agents of influence, unwitting agents, penetration agents, infiltration agents, false flag agents, witting agents and 'sleepers'.

stages would thus need to have been adapted. Such an adaptation can graphically be depicted as follows:

Figure 28: The all-source counterespionage process


CE ASSESSMENT
STATE OF CE KNOWLEDGE
CE FRAMEWORK
CE REQUIREMENTS
DEMARCATE CRITICAL INFORMATIONAL INTERESTS
IDENTIFY CE RISKS AND THREATS
DETERMINE OWN STATE VULNERABILITIES TO ESPIONAGE
(REFINE AND CONCRETISE) CE REQUIREMENTS
IDENTIFY ESPIONAGE ADVERSARIES
PRIORITISE ESPIONAGE ADVERSARIES
INVESTIGATE ESPIONAGE ADVERSARIES
ENGAGE CE TARGETS
EXPLOIT CE TARGETS
NEUTRALISATION & TERMINATION
MULTIDIRECTIONAL ACTIVITY FLOW
CE ASSESSMENT
CE FRAMEWORK
CE REQUIREMENTS
STATE OF CE KNOWLEDGE

Since the counterintelligence process was already presented, this section examines only the stages of the counterespionage process as red bracketed in Figure 28.

7.2 IDENTIFICATION OF ESPIONAGE ADVERSARIES

From a counterespionage perspective the prior phases ascertained the ‘state of knowledge’ in relation to the following:

- Known and suspected espionage adversaries;
- deficiencies in the own state’s counterespionage measures through which critical informational interests are under- and unprotected and thus rendered vulnerable to hostile espionage endeavours; and
- deficiencies in the intelligence picture regarding adversarial espionage directed against critical information interests.

The ‘state of knowledge’ is of course not static and is consistently updated throughout the counterespionage process. Indispensable in this regard is a formalised counterespionage ‘indications and warnings’ (I & W) mechanism to guide the open- and secret source scouting of the environment. The I & W mechanism functions in symbiosis with the positive intelligence and covert action disciplines, as well as with the counterintelligence field of security.

Since adversaries of the state, in general, are potentially also hostile espionage actors, a multidirectional interaction between counterespionage and positive intelligence is maintained. Positive intelligence advises counterespionage on the emergence of ‘new’ adversaries and pertinent developments in relation to known opponents of the own state. Positive intelligence furthermore informs counterespionage of adversarial conduct that is incongruent with ‘what would have been expected’. The unfolding of extraordinary, pre-emptive tactics by an opponent during negotiations could, for example, suggest that the own state’s strategy is being compromised through adversarial espionage. It is counterespionage’s self-evident task to determine the concomitant espionage risk and threats.

Continuous interaction with covert action is equally essential. The relationship between counterespionage and covert action is highly complex and this section suffices with an example pertinent to the identification of espionage adversaries. Sound covert action depends on contingency planning for difficulties experienced during the execution of such programmes. This planning expects the unexpected.

A covert action initiative that runs inexplicably ‘smoothly’ might suggest that the initiative has been comprised and that the targeted adversary has ‘turned’ the operation to its own advantage. Since the compromising of an own state covert action operation could be the result of hostile espionage penetration, information on such developments could aid in the identification of espionage adversaries.

The fact that security breaches and suspicious conduct, reported by the security structures of intelligences services, aid in the identification of espionage adversaries, is well-documented and elaboration by means of examples unnecessary.

7.3 PRIORITISATION OF ESPIONAGE ADVERSARIES

Intelligence services have finite resources and few, if any, counterespionage structures are afforded the luxury of being able to focus on all known and suspected espionage adversaries. Using the criteria set out in Chapter Four, espionage adversaries are consequently prioritised for further scrutiny according to the risks and/or threats they pose to national security.

7.4 INVESTIGATION OF ESPIONAGE ADVERSARIES

The further ‘scrutiny’ of espionage adversaries can, by lack of a more apt term, be described as the investigation phase. ‘Investigation’ in the context of its use here, denotes the analysis and collection of information by means of overt and secret methods regarding prioritised espionage adversaries. Secret methods of collection vary in risk and resource implications. Depending on the particular circumstances, the recruitment of a high-ranking member of an adversarial intelligence service as an agent would be deemed as a high-risk counterespionage measure. Very high risk and cost measures would typically only be employed after the ‘investigation’ phase has been concluded.

The aim of investigation is, in short, to enable prioritisation within prioritisation. Even though tentatively prioritised in the preceding phase, not all such espionage adversaries would at the outcome of the investigation phase be ranked as espionage targets. A counterespionage target can be described as an espionage adversary of such significance that the employment of counterespionage measures carrying a high risk and with sizeable resource implications is warranted. Although sizable, the cost and risk implications of measures employed during the ‘investigation’ phase are generally lower – when compared with those utilised during the next (‘engagement of espionage targets’) phase. As part of the investigation phase, by way of illustration, the redirection of existing agents or the recruitment of peripheral agents, would be preferred over the recruitment of a high-ranking member of an adversarial intelligence service. During the investigation phase, in more practical terms, existing (direct and/or indirect) access to a target would mostly be utilised. Should there not be existing access to a target, lower risk TECHINT and HUMINT methods (such as the recruitment of a peripheral agent and surveillance) would be instituted.

7.5 THE ENGAGEMENT OF COUNTERESPIONAGE TARGETS

At its core, counterespionage is about the waging of informational warfare against the espionage enemies of the nation state. During the preceding phases of the counterespionage process these enemies (‘espionage targets’) were identified and ‘sized-up’. Identification and ‘sizing-up’ without the engagement, exploitation and the eventual neutralisation of espionage targets would contradict the very nature of counterespionage.

The engagement of espionage targets entails the establishment of the *instrumentality* (‘access channel’) through which aggressive collection, exploitation and neutralisation can be conducted. The engagement phase is comparable with what in Hulnick’s (2007: 10-17) counterintelligence model is defined as “penetration”. Penetration can be achieved through TECHINT and HUMINT measures. The aptness of the study’s use of ‘engagement’ instead of ‘penetration’ as describing this phase is validated by the fact that HUMINT access can also be achieved by means of ‘infiltration’. In the case of infiltration, an asset (agent) is obtained that is not as yet directly involved in the espionage target’s structure. On direction of the (own state’s) intelligence service, the asset is, often gradually and through a protracted course of action, guided to become part of the espionage adversary’s intelligence structure.

7.6 EXPLOITATION OF COUNTERESPIONAGE TARGETS

Subsequent to establishing the instrumentality, the exploitation of an espionage target ensues. The forms of exploitation are diverse and, to list but a few, include aggressive collection, manipulation, deception, repression of espionage activities, disinformation as well as the disruption and prevention of espionage activities (Zuehlke, 1980: 17-21). Exploitation is achieved through a wide range of countermeasures which were discussed and conceptually ‘pigeon holed’ in Chapter Three by means of definitions and descriptions. In their practical execution, however, the respective measures are dimensions of a converged and multifaceted entirety.

7.7 NEUTRALISATION AND TERMINATION

While the neutralisation of espionage adversaries can partially be accomplished through exploitation, counterespionage operations would typically have a 'neutralisation and termination' phase at the end of their 'life-cycle'. The termination of counterespionage operations can either be opted for (at the initiative of the intelligence service) or imposed by circumstances. The Ames and Hanssen cases, discussed in Chapter Three, serve as examples. From a Russian perspective, the termination of the Ames and Hanssen cases was – insofar as can be surmised from open sources – imposed by events following the detection of these moles by the US. From a US point of view, counterespionage operations were conducted against Ames and Hanssen. Subsequently, and upon having gathered sufficient evidence, the US opted for the termination of its counterespionage operations and did so by means of prosecution.

The Ames and Hanssen cases illustrated prosecution as a form of 'acclaimed' termination and neutralisation. Other measures of a similar nature are expulsion, public exposure and publicised diplomatic protest. It is perhaps the visibility of these neutralisation and termination measures that prompted Hulnick (2007: 15-16) to assert "claim success" as the final stage of his counterintelligence model. Hulnick (2007: 15), however, adds the following vital qualification in his introductory remark:

> Finally, in the last step of the counterintelligence process, authorities often make public claims of success, a rare step in intelligence work. Normally intelligence managers try hard to keep successes secret so that they might be repeated. An oft-quoted CIA saying is, "The secret of our success is the secret of our success." In cases in which intelligence has been gathered successfully, it is critical to protect sources and methods. In counterintelligence, however, the claim of success, when the case has ended, could be used to convince the public that the government is ever watchful and actually doing something with the billions of dollars spent on intelligence.

As opposed to the acclaimed category, 'protected' termination and neutralisation therefore have their own distinctive advantages. If executed skilfully, protected termination and neutralisation could provide the 'seeds' for a subsequent 'generation' of counterespionage operations.

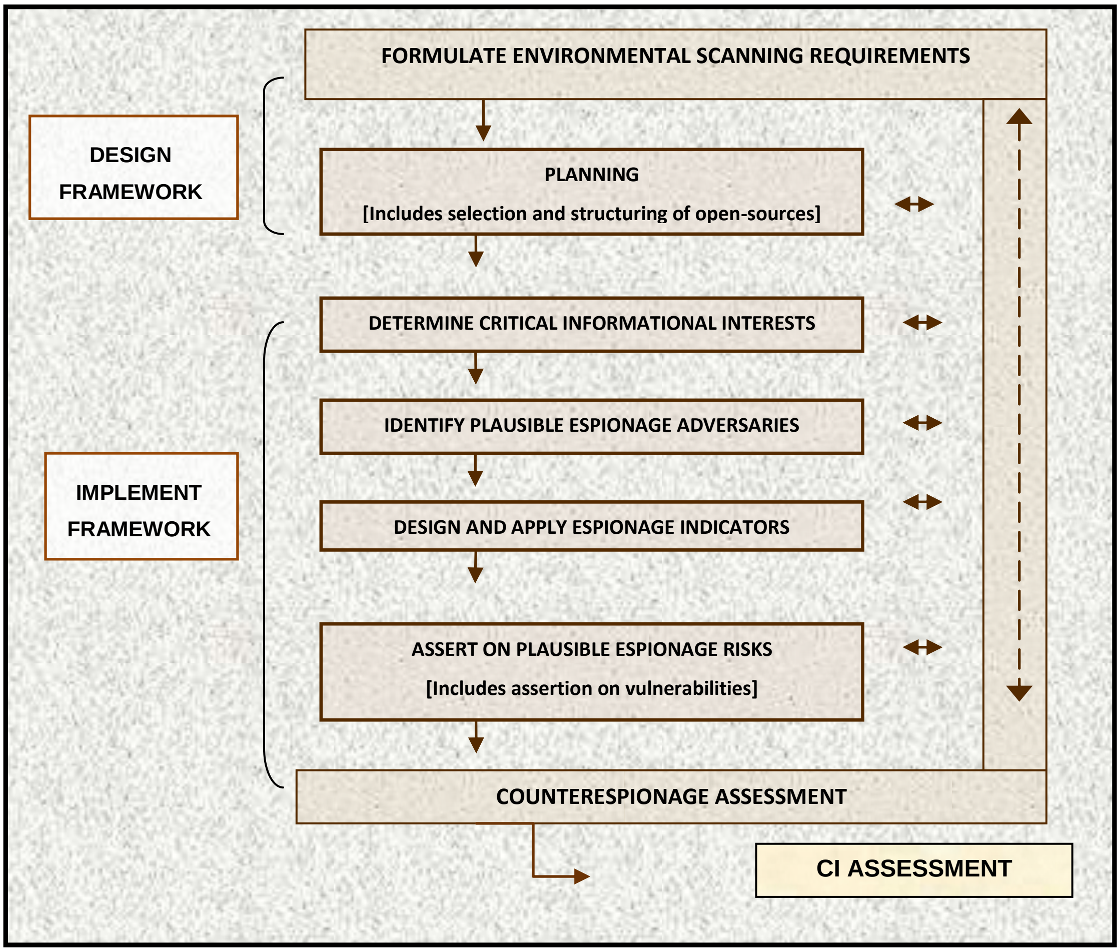
8. OPEN-SOURCE INTELLIGENCE AND THE COUNTERESPIONAGE FRAMEWORK AS PART OF THE ALL-SOURCE COUNTERESPIONAGE PROCESS

This section presents the CE framework as an open-source environmental scanning instrument within the context of the all-source counterespionage process. To this end, a structural outline of the CE framework as process is provided. This is followed by a distinction between, on the one hand, the role of OSINT within the counterespionage process in general and, on the other hand, the specialised function fulfilled by the CE framework. Subsequently, the CE framework is aligned with the all-source counterespionage process.

8.1 A STRUCTURAL OUTLINE OF THE OPEN-SOURCE COUNTERESPIONAGE SCANNING PROCESS AND FRAMEWORK

Similar to other processes within the statutory intelligence environment, the CE framework as process is subject to the same qualifications in relation to the multidirectional activity flow, the recurring and overlapping nature of stages and activities, as well as the fact that models are reductive idealisations of a complex process. Chapters Six and Seven will show the intricacy of the CE scanning process and framework even if simplified to a micro- theoretical construct. Consequently, the following graphic depiction of the CE scanning process and framework is in certain respects an oversimplification and purports to be no more than a broad structural outline:

Figure 29: A broad structural outline of the open-source counterespionage environmental scanning process and framework


FORMULATE ENVIRONMENTAL SCANNING REQUIREMENTS
DESIGN FRAMEWORK
PLANNING
[Includes selection and structuring of open-sources]
DETERMINE CRITICAL INFORMATIONAL INTERESTS
IDENTIFY PLAUSIBLE ESPIONAGE ADVERSARIES
IMPLEMENT FRAMEWORK
DESIGN AND APPLY ESPIONAGE INDICATORS
ASSERT ON PLAUSIBLE ESPIONAGE RISKS
[Includes assertion on vulnerabilities]
COUNTERESPIONAGE ASSESSMENT
CI ASSESSMENT

As is clear from the preceding graphic depiction, the CE framework mirrors the activity flow in certain respects, and some of its stages are akin to that of the all-source counterintelligence and counterespionage processes. What is not depicted is the location of the CE framework within the all-source counterespionage process. What needs to be determined, in other words, is the manner in which the CE framework is synergistically aligned with the all-source counterespionage process.

8.2 THE ROLE AND LOCATION OF OPEN-SOURCE INTELLIGENCE IN RESPECT OF THE ALL-SOURCE COUNTERESPIONAGE PROCESS

Since the CE framework is an OSINT instrument, the role and location of OSINT relative to the all-source counterespionage process in general, offers a point of departure for aligning the CE framework. OSINT's role and location within the counterespionage process is related to the limitations and advantages of open sources in the statutory intelligence milieu. These advantages and limitations were discussed In Chapter Four, and further observations in this regard are limited to aspects essential for contextual purposes.

OSINT *per se* is not a parallel process within the all-source counterespionage endeavour. Instead, Chapter Four contended OSINT to be interwoven with the whole counterespionage process. Consequently, there are no specific nodal points that link OSINT with all-source counterespionage. Broadly speaking, and with progression of the all-source counterespionage process, however, there are shifts in the demands made on OSINT. This shift pertains to the type of intelligence required from OSINT.

At the early stages of the counterespionage process (such as the identification and prioritisation of espionage adversaries), OSINT's role is mainly, but not exclusively, of a strategic nature. Its function in "strategic counterintelligence", Steele (2007: 109-111) asserts, is the identification of "emerging threats". It is on the strategic level, Steele (2007: 109) states, where "OSINT should, but does not shine."

During later stages of the counterespionage process the demands on OSINT are more, but also in this instance not exclusively related to the delivery of tactical and operational intelligence. During the 'engagement', 'exploitation' and 'neutralisation' phases, OSINT's focus is on detailed information regarding multifarious aspects such as the profiling of espionage targets and their individual operatives, adversarial *modus operandi*, the establishment of cover for (own state) countermeasures and the 'testing' of suspected adversarial cover, the monitoring of mass media to detect informational covert action around specific issues, as well as the provision of information to, for example, double agents in response to the intelligence requirements posed by the adversarial counterespionage actors. The detection of informational covert action and the provision of information to double agents could include aspects of a strategic nature and serve as examples of instances where OSINT (also at the later stages of the counterespionage process) could include strategic aspects.

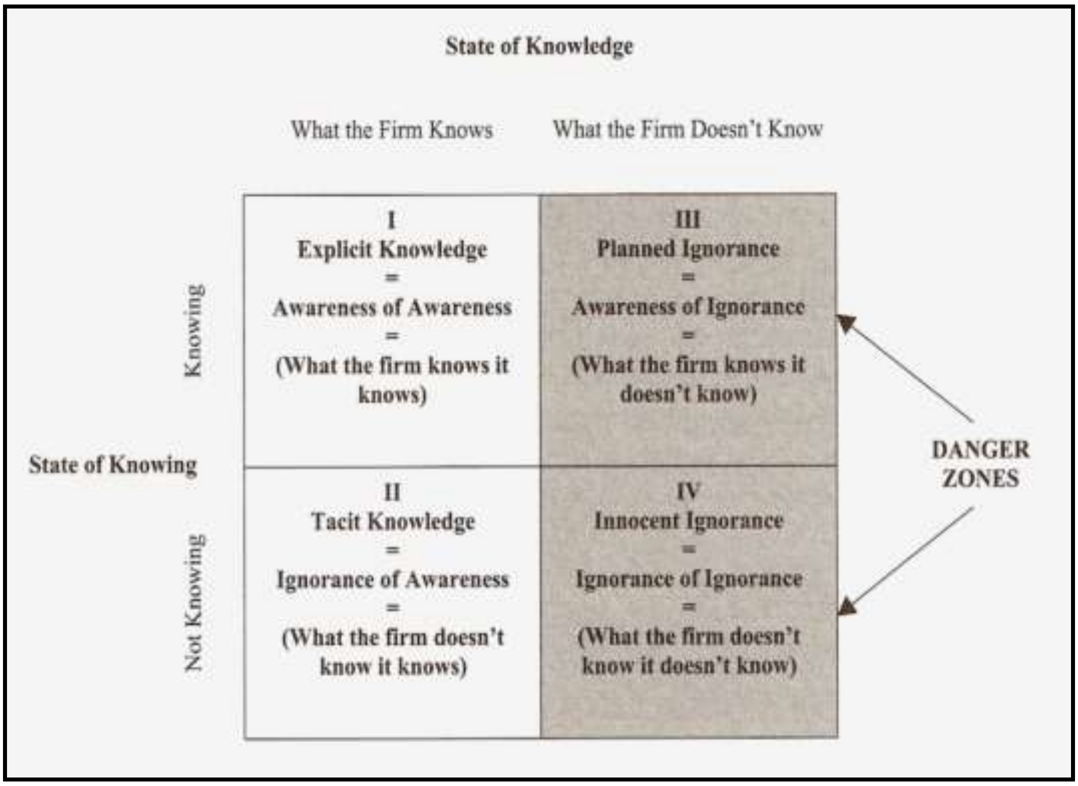
8.3 THE ROLE AND LOCATION OF THE OPEN-SOURCE COUNTERESPIONAGE FRAMEWORK IN RELATION TO THE ALL-SOURCE COUNTERESPIONAGE PROCESS

Similar to the role of OSINT in relation to the all-source counterespionage process, the CE framework's focus progressively moves from the strategic to the tactical and operational. This is illustrated by the refinement of the CE framework's resolution from a contextual focus, to focus areas and eventually to focal points (Figure Six, Chapter Three).

Unlike OSINT in general, however, the CE framework is interlocked with but, in so far as its execution is concerned, not interwoven with the all-source counterespionage process. Chapter Four presented the CE framework as a parallel instrument that should contribute to the moderation of counterespionage failure. Furthermore, the degenerative counterespionage spiral was linked to various factors contributing to such failure. This degenerative spiral 'contaminates' the all-source counterespionage state of knowledge and the continuous refinement of counterespionage requirements throughout the counterespionage process. In the interest of elucidation, a previously used hypothetical example is worth recapitulating. On the strength of the existing 'state of knowledge', foreign intelligence service X is prioritised in the formulation of counterespionage requirements. In most instances, this produces more information on service X, leading to the continued or higher prioritisation of this service in subsequent counterespionage requirements. Since resources are limited, this self-feeding cycle results in the operational and analysis effort, as well as other resources, being converged to certain areas while the espionage risks posed by other espionage adversaries go undetected.

The CE framework should be positioned and interfaced with the all-source counterespionage process at a point where it has the greatest impact in respect of the 'state of knowledge' and the breaking of this spiral. In practical terms, the questions arises as to where within the all-source counterespionage process the CE framework's outcome or end product should be delivered? In order to determine this, cognisance ought to be taken of the dimensions that constitute the 'counterespionage state of knowledge'. The following matrix emanating from the Competitive Business Intelligence field offers a useful premise in this regard:

Figure 30: Dangers of knowledge management without competitive intelligence



Source: Knip, 2003: 308

Knip's (2003: 308) proposition can potentially be adapted comprehensively, and be applied to the whole of the multifaceted statutory counterintelligence and counterespionage 'body of knowledge'. The following cursory and selective application is adequate for purposes of pronouncing on the location of the CE framework as part of the all-source counterespionage process:

Figure 31: Matrix for mapping the counterespionage ‘state of knowledge’ – a cursory application in respect of espionage adversaries

QUADRANT 1	QUADRANT 3
EXPLICIT KNOWLEDGE & REQUIREMENTS	**PLANNED IGNORANCE**
What the intelligence service knows it knows and wants to know.	What the intelligence service explicitly does not see as being a priority to know.
Espionage adversaries are known and the intelligence service is clear on further information required on these adversaries. Based on existing information, and during the ‘requirements’ and ‘identification’ phases of the all-source counterespionage process, these espionage adversaries are prioritised for further actions.	Espionage actors in the macro-environment were methodically assessed and can, beyond reasonable doubt and for the foreseeable future, be discarded as national security risks and threats. In order to focus resources on areas of high counterespionage concern, espionage actors in this category are explicitly excluded from further counterespionage attention in the ‘requirements’ phase of the all-source counterespionage process.
QUADRANT 2	**QUADRANT 4**
TACIT KNOWLEDGE	**INNOCENT IGNORANCE**
What the intelligence service does not know it knows.	What the intelligence service does not know, it does not know.
As a result of factors leading to intelligence failure, as discussed in Chapter Four, ‘signals’ of adversarial espionage are lost in the ‘noise’. Relevant information is gathered, but the ‘legible images’ are not forthcoming. Adversarial espionage actors that could be posing national security risks and threats are not addressed in the ‘counterespionage requirements’ and ‘identification of espionage adversaries’ phases of the all-source counterespionage process.	‘Signals’ of adversarial espionage are ill-defined and/ or the all-source counterespionage environmental scanning is too narrow in scope. This situation is the result of factors contributing to intelligence failures such as received opinion, groupthink and stagnation. Adversarial espionage actors who could pose national security risks and threats are not contained in the ‘counterespionage assessment’, addressed in the formulation of ‘counterespionage requirements’ and consequently do not feature in the ‘identification of espionage adversaries’ or sub-sequent phases of the all-source counterespionage process.

DANGER ZONES

While the CE framework is pertinent to both the indicated 'danger zones', it is mainly geared towards the moderation of 'innocent ignorance'. The narrative explication of the latter in the matrix above (Figure 31), points to the counterespionage process's 'assessment' and 'formulation of requirements' phases as at the root of 'innocent ignorance' and the degenerative, self-feeding spiral. As depicted *per* Figure 28, the CE framework's outcome (product) would probably be most beneficial to the all-source CE process, if considered in the compilation of the comprehensive counterespionage assessment typically compiled by statutory intelligence services annually or bi-annually. The counterespionage assessment, augmented by the CE framework's outcome, provides the basis for the formulation of counterespionage requirements and the setting of priorities. Should these priorities include espionage risks identified through the application of the CE framework, a contribution would have been made been toward bridging the aforementioned degenerative spiral.

9. CONCLUSION

This chapter contextualised the CE framework as part of a process located within higher order intelligence processes. This was done from the premise that the CE framework needs to be presented as part of a multilayered unison of intelligence, counterintelligence and counterespionage processes.

To this end some propositions within Intelligence Studies purporting to represent the all-discipline intelligence process were appraised. The traditional intelligence cycle, contemporised versions thereof as well as other intelligence process propositions reviewed, were found to be deficient in accommodating 'counterintelligence'. Furthermore, and with the exception of a model by Hulnick (2007), propositions on the counterintelligence process *per se* were ascertained to be vague and unreflective of the range of activities performed within this subdiscipline. Business Intelligence transpired to be more developed in the conceptual structuring of the counterintelligence process, and the integration thereof with the positive intelligence process. Business Intelligence thinking, however, cannot be summarily applied to Intelligence Studies and statutory intelligence practice. Conceptualisations of the intelligence and counterintelligence processes in consulted literature were thus concluded to be insufficient in serving as foundational or contextual constituents for the design of open-source CE environmental scanning.

With the categorical qualification that it should not be construed as an attempt to construct an overarching all-discipline process, a reductive conceptual nexus toward an all-discipline intelligence process was proposed. This conceptual nexus advocates a clear distinction between ‘intelligence subdisciplines’, ‘functional areas’ and ‘practicalities’. In contradiction of one of Intelligence Studies’ axioms, statutory intelligence was argued to consist of three principal subdisciplines, namely, positive intelligence, counterintelligence and covert action. Analysis and collection were forwarded as functional areas of activity that are performed within all three subdisciplines.

Subsequently, a proposition on the all-source, statutory counterintelligence process was submitted. Within the parameters of the counterintelligence model, the chapter proceeded to present a proposal on the all-source counterespionage process. This was followed by a broad structural outline of the process of open-source, counterespionage environmental scanning. Based on a distinction between, on the one hand, the role of OSINT within the counterespionage process in general and, on the other hand, the specialised function fulfilled by the CE framework, the latter was subsequently aligned with the all-source counterespionage process.

Propositions made on the all-source counterintelligence and counterespionage processes as well as on outlining of the CE framework, contoured the methodical structuring of the open-source CE scanning process. Expounding on this contour, the subsequent chapter comprehensively addresses the methodology of open-source environmental scanning in the counterespionage milieu.

CHAPTER SIX

AN INTEGRATED PROCESS FOR OPEN-SOURCE, COUNTERESPIONAGE ENVIRONMENTAL SCANNING AND RISK ASSESSMENT: METHODICAL APPROACH, DESIGN AND THE DEMARCATION OF THE REFERENT OBJECTS

1. INTRODUCTION

This chapter, by expanding on the structural outline provided in Chapter Five, introduces the CE framework as part of a broader scanning process consisting of phased, open-source environmental scanning activities. The chapter commences with an outline of the CE scanning process's methodological logic. Pursuant to this outline, the initial phases of the CE scanning process which deal with the conceptualisation, design and planning thereof are presented. The chapter proceeds with explicating the first phase in the execution of CE environmental scanning *per se*, namely the delineation of the environmental scanning's referent objects. The latter will be shown to comprise the 'secrets' valued by the own state and sought by espionage adversaries. Subsequent phases of the CE environmental scanning process are addressed in Chapter Seven.

In their chronological presentation of the CE environmental scanning process's phases, and although structurally separated, Chapters Six and Seven are thus conceptually a unit. Both chapters are primarily focused on addressing, in considerably more detail than thus far, the following research question: 'Given the voluminous extent of overt information, how can the CE environmental scanning process be methodically structured?' In addressing the methodology of CE environmental scanning, the chapters are simultaneously 'theoretical-integrative' and 'pragmatic-utilitarian' in their approach.

On a theoretical level, various conceptual constructs forwarded in the course of the study are integrated into a cohesive process for open-source CE environmental scanning and risk assessment. Such theoretical compositions comprise definitional elements (such as espionage risk, counterespionage, and environmental scanning) as well as the propositions made on conceptual approaches about several aspects of CE environmental scanning. The latter include, but are not limited to, the assessment and prioritisation of counterespionage security concerns (Figure 12, Chapter Four); open-source collection subdisciplines (Figure 15, Chapter Four); the uses and limitations of open-source intelligence in the statutory counterespionage milieu (Chapter Four); and the outline of the open-source counterespionage environmental scanning framework (Figure 29, Chapter Five).

On a pragmatic-utilitarian level, Chapters Six and Seven concretise the process for open-source identification and assessment of espionage risks within the statutory intelligence milieu. This concretisation should be viewed in the context of Chapter Five, which placed open-source CE environmental scanning as a process within higher order processes. This study is, to reiterate, neither primarily located at the praxis level (Figure Three, Chapter Two) nor does it purport to offer a 'practical manual' for conducting the arduous work of CE environmental scanning. These qualifications, however, do not negate its necessity to have practical application and use. In line with this requisite, this chapter is "pragmatic" in that it engages "real-life difficulties" regarding the use of open-source information in the counterespionage environment (Mouton, 2005: 137-145; paraphrased).

Without compromising the study's overall micro-theoretical orientation, Chapters Six and Seven address the CE framework, and the pragmatic utility of the broader CE environmental scanning process in four respects. Firstly, the presentation of the CE scanning, which as a structured process in itself, serves a practical utility purpose. The micro-theoretical structuring of the CE environmental scanning process provides the methodological 'skeleton' (outline) around which the praxis of CE environmental scanning can be refined. Secondly, and complementary to the methodological outline, matrixes are advanced for directing exigent facets of the open-source CE scanning process. While some of these matrixes might be refined to *pro forma*, it is prudent to emphasise that they are presented in the form of conceptual guides as part of the CE scanning process. Differently phrased, and in line with its lexicographical meaning, a matrix in the context of Chapters Six and Seven should be seen as a notional aid from which assertions on espionage risks "originate, develop, or take form" (*Merriam-Webster Online Dictionary:* 2008/06/23; verbs in quotation adapted from singular to plural). Matrixes should thus not be construed as having the exactness of 'filling-in-the-missing-words' questionnaires, but rather as beacons that structure open-source collection and assessment activities.

Thirdly, the chapters also address the practical feasibility of executing environmental scanning that – to paraphrase Meyer (1987: 97) – has as a ”proper focus” the ”total environment”. Should this have been a purely abstract theoretical study, the extensive and intensive scanning of the ‘total environment’ could have been presented as the ideal aiming point. Statutory counterespionage is, of course, not conducted in an ideal milieu with infinite resources. A recurring theme in the chapters is therefore directed at finding the equilibrium between the ideal of the scanning of the total environment, and the practical resource constraints of statutory counterespionage practice.

Fourthly, and in what might seem as a contradiction of the earlier qualification in respect of its micro-theoretical nature, the presentation of the CE environmental scanning process does (ostensibly) venture into the praxis domain in certain respects. Specific sources deemed as useful to scanning are mentioned. The intention, however, is not to provide a comprehensive open-source inventory as would be required from a study at the praxis level. Examples provided in this regard are illustrative and are not in any measure representative of the wide array of open-sources available for utilisation in CE environmental scanning. ‘Real-life’ examples are furthermore provided as elucidation of the CE framework. These highly-selective examples lack the comprehensiveness, detail and balance demanded from case studies included in praxis studies. Such a balance would, *inter alia*, entail proportioned emphasis on all categories of espionage role players. While other categories of role players are not disregarded in the course of the chapters, examples used frequently pertain to the US, Germany and the PRC and are thus biased toward nation states as espionage and counterespionage actors. Lastly, the chapter’s initial sections confront the real-life management of the CE environmental scanning as a parallel, statutory intelligence project. This is done at notional level and predominately limited to aspects impacting on the design and configuration of the CE scanning process.

2. THE METHODOLOGICAL LOGIC OF THE OPEN-SOURCE COUNTERESPIONAGE ENVIRONMENTAL SCANNING PROCESS

In forwarding a structural contour of the open-source counterespionage environmental scanning process, Chapter Five referred to the intricacy of the process – even if presented as a simplified outline in this chapter. In their explication of the CE scanning process, Chapters Six and Seven are – measured against preceding chapters - not only the most extensive but also the most complex. This complexity is inherent to counterintelligence. Echoing similar observations by other authoritative scholars (cited in Chapter Five, Section 3.1), Miler (1980: 40) remarks as follows:

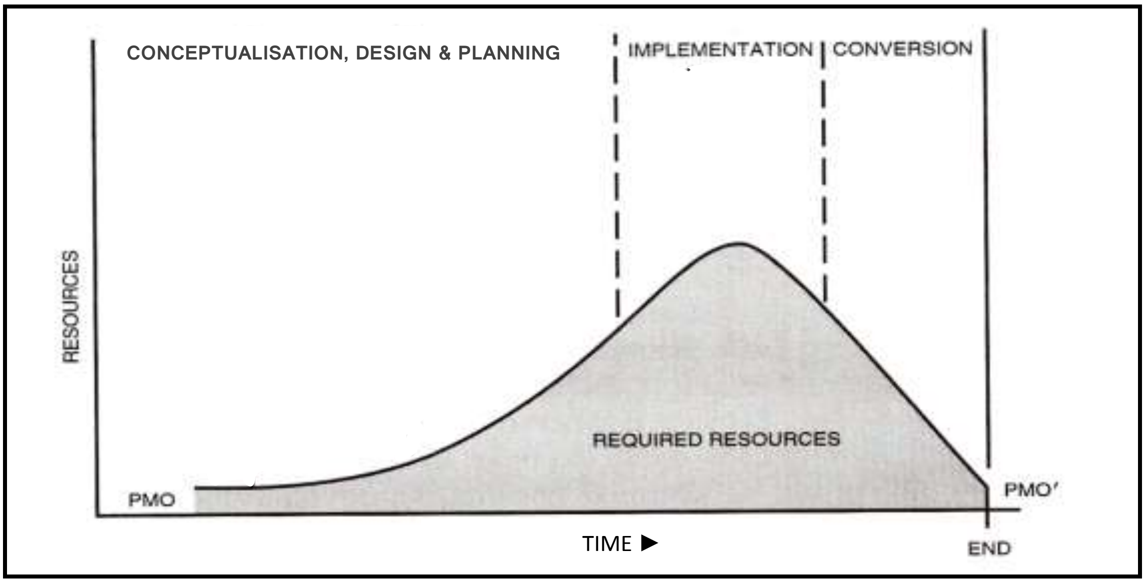
> It is not easy, nor can one feel confident, to re-enter this world where, it has been said, the tortuous logic of counterintelligence prevails ... Unfortunately, there seems to be no easy way to explain counterintelligence ... Because effective counter-intelligence is a combination of so many aspects of the intelligence business and other political, military, economic and societal factors ....

To aid in ‘navigating’ this “tortuous logic”, this section serves as a referential, conceptual guide. It presents a cursory overview of the ‘argumentative logic’ behind the methodology of CE environmental scanning and risk assessment. The cursory overview comprises a synthesis of some previously made contentions and additional key contentions. To this end, a narrative explication as well as a graphical depiction of the CE ‘methodological logic’ of the environmental scanning process is provided.

The methodological logic of the CE environmental scanning is shaped by its composite dimensions of being a *parallel*, *open-source counterespionage* instrument. Chapters Four and Five illustrated the *parallel* dimension of CE environmental scanning as an institutional solution to an institutional predicament of failure. The solution entails conducting a collection and assessment project ‘independently’ from the all-source counterintelligence endeavour. As a parallel *project*, the CE environmental scanning process derives some of its argumentative logic from Project Management as it is practised within the private and public sectors. Projects typically have a “life cycle” consisting of the sequential progression in the five main stages, namely conceptualisation, planning, definition and design, implementation, and conversion (Kerzner, 1988: 73-84). These stages also correspond with the rise, peak and decline in the appropriation of resources. Each main stage normally consists of several phases. A phase in turn represents a clustering of steps and activities.

Kerzner (1988: 81) appropriately remarks that not all projects – especially those in the research and development domain – follow a five-stage life cycle. The demarcation of stages is customised to suit the peculiarities of each project. In the case of the CE open-source environmental scanning process conceptualisation, planning, as well as definition and design, are intertwined and for all practical purposes constitute a single main stage. Kerzner’s (1988: 81) proposition can be applied to the CE environmental scanning process as indicated in the following graphic illustration:

Figure 32: The life cycle of the open-source, counterespionage environmental scanning process



Source: Kerzner, 1988: 81(adapted).

Narratively, the main stages depicted above can concisely be explained as:

- *Conceptualisation, design and planning*. Albeit generic and on a micro-theoretical level, the 'design' of a phased, open-source CE environmental scanning process is the previously stated primary focus of this chapter. While administrative and logistical matters are by and large excluded from the focus of the study, some aspects pertaining to the 'conceptualisation', 'planning' and 'management' that influence the 'design' of the process are addressed. The CE framework is the structural 'blueprint' for the execution of the scanning process, and its design – in the course of the conceptualisation, design and planning stage – contours the phases of the 'implementation' and 'conversion' stages to follow.
- *Implementation*. The implementation of the CE environmental process entails the execution of the collection and assessment of information in line with the CE framework as designed.
- *Conversion*. The collection and the assessment of information during the implementation stage culminate in the submission, and probably the verbal presentation, of an open-source counterespionage environmental scanning report to the intelligence service's executive management. The report has at

its core actionable findings which include plausible espionage risks, concomitant opportunities as well as recommendations on reducing own state vulnerabilities to espionage. These findings are actionable in that they are 'converted' into action through the ensuing pursuance by the all-source counterespionage effort.

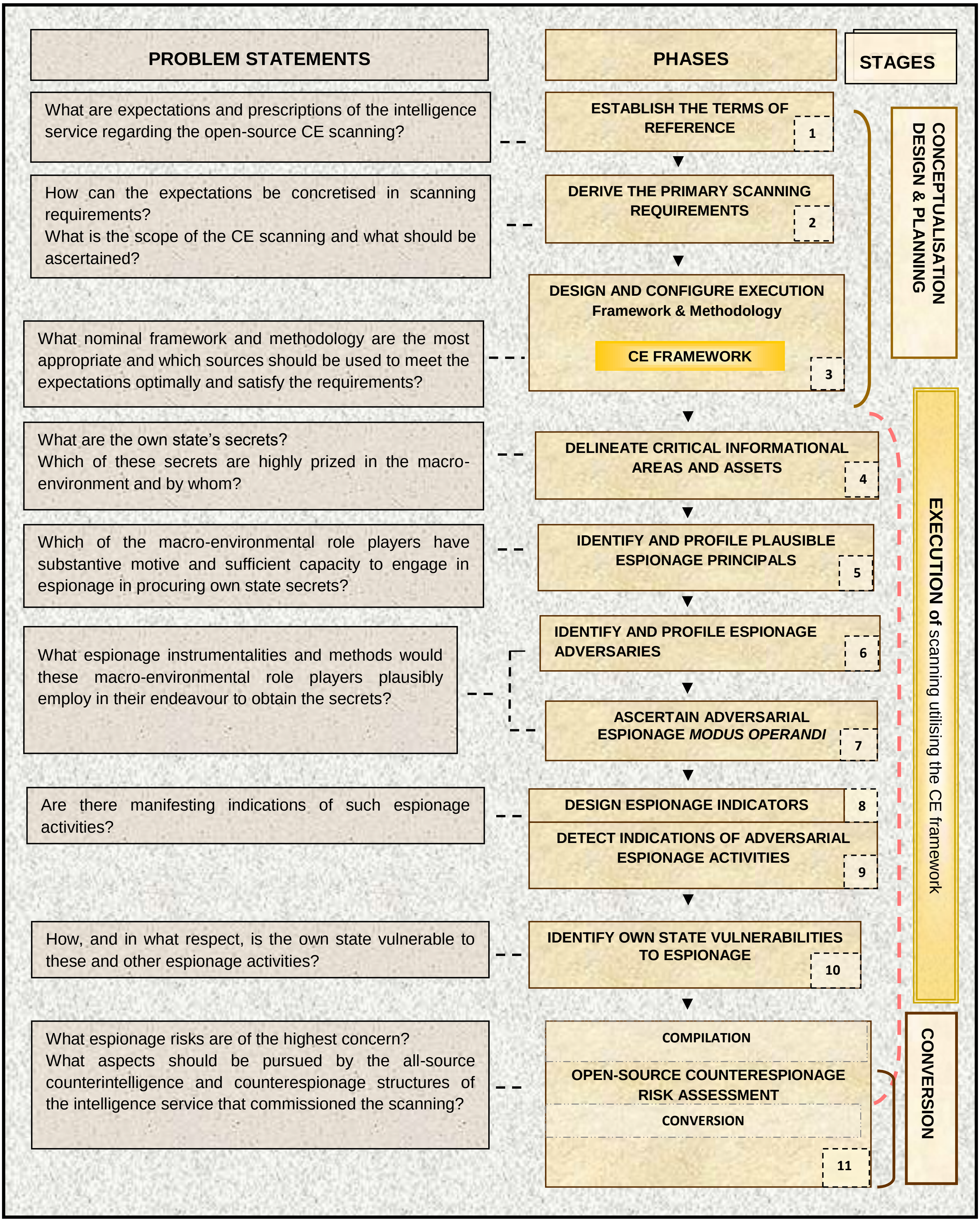
Supplementary to its dimension as a parallel (statutory intelligence) *project*, the methodological logic of the CE environmental scanning process is determined by its status as an *open-source counterespionage* instrument. Attempting to reflect on all facets of counterespionage as part of an exploratory proposal on an open-source environmental scanning process would be overambitious. Moreover, it would defeat the intention to conceptually simplify a complex process. With the provision that it is a simplification, the proposal on the CE scanning process accentuates the role conventionally ascribed to counterespionage. Accordingly, counterespionage is predominantly (but not exclusively) portrayed as the 'battle' between espionage role players in the informational arena over 'secrets'.

Within this arena, much of the all-source counterespionage effort is concentrated on determining espionage risks and threats through information gathered on the espionage targets *per se* (Godson, 1989: 17-19). The secret operational access to espionage adversaries is thus often the 'default starting point' for further 'unravelling' the espionage risk and threat picture. Through the gathering and assessment of information on the espionage adversaries, the all-source counterespionage endeavour determines other facets of espionage risks and threats. One of these is the identification of those own state secrets adversaries want to procure. The self-feeding cycle of prioritisation this approach results in was extensively discussed previously.

More so than in the all-source counterespionage domain, the CE framework is compelled to rely on inferring, deducing and projecting espionage risks through the collection and assessment of information that is significantly more circumstantial than conclusive. Its open-source dependence denies the CE framework of an espionage-adversarial centric 'default starting point'. Instead, the CE scanning process follows a long-routed, 'indirect' approach and has an argumentative-logic which moves from the general to the specific. This indirect approach has as its point of departure the notion of establishing the referent objects of espionage and counterespionage, namely the secrets valued by the own state and sought by other actors. Some secrets are of such a nature that even their existence is not ascertainable through open sources. Arguably, for the larger part the existence of secrets can be determined by means of open sources. Through the use of open sources the broad ‘topics’ or ‘areas’ of which secrets exist can be determined, but the content thereof most likely not. These secrets are not necessarily apparent and are in relation to both the own state and macro-environmental role players inferred through an exacting, yet pivotal, process. The outcome of this process is indispensable in informing the subsequent CE environmental scanning phases. These include the identification of espionage principals as well as adversaries, determining adversarial *modus operandi*, detecting indications of adversarial espionage activities, and asserting on own state vulnerabilities to such espionage.

Graphically, the argumentative logic underpinning the CE environmental scanning process – which proximates the different phases with problem statements – can be depicted as follows:

Figure 33: The methodological logic of the open-source, counterespionage environmental scanning process



PROBLEM STATEMENTS

What are expectations and prescriptions of the intelligence service regarding the open-source CE scanning?

How can the expectations be concretised in scanning requirements?
What is the scope of the CE scanning and what should be ascertained?

What nominal framework and methodology are the most appropriate and which sources should be used to meet the expectations optimally and satisfy the requirements?

What are the own state's secrets?
Which of these secrets are highly prized in the macro-environment and by whom?

Which of the macro-environmental role players have substantive motive and sufficient capacity to engage in espionage in procuring own state secrets?

What espionage instrumentalities and methods would these macro-environmental role players plausibly employ in their endeavour to obtain the secrets?

Are there manifesting indications of such espionage activities?

How, and in what respect, is the own state vulnerable to these and other espionage activities?

What espionage risks are of the highest concern?
What aspects should be pursued by the all-source counterintelligence and counterespionage structures of the intelligence service that commissioned the scanning?

PHASES
ESTABLISH THE TERMS OF REFERENCE
1
DERIVE THE PRIMARY SCANNING REQUIREMENTS
2
DESIGN AND CONFIGURE EXECUTION
Framework & Methodology
CE FRAMEWORK
3
DELINEATE CRITICAL INFORMATIONAL AREAS AND ASSETS
4
IDENTIFY AND PROFILE PLAUSIBLE ESPIONAGE PRINCIPALS
5
IDENTIFY AND PROFILE ESPIONAGE ADVERSARIES
6
ASCERTAIN ADVERSARIAL ESPIONAGE MODUS OPERANDI
7
DESIGN ESPIONAGE INDICATORS
8
DETECT INDICATIONS OF ADVERSARIAL ESPIONAGE ACTIVITIES
9
IDENTIFY OWN STATE VULNERABILITIES TO ESPIONAGE
10
COMPILATION
OPEN-SOURCE COUNTERESPIONAGE RISK ASSESSMENT
CONVERSION
11
STAGES
CONCEPTUALISATION DESIGN & PLANNING
EXECUTION of scanning utilising the CE framework
CONVERSION

This section provided a cursory overview of the argumentative logic of the CE environmental scanning process. A few key assertions submitted in preceding chapters were recapitulated and brief reference was made to some contentions advanced in the rest of the chapter. In the subsequent sections these contentions are restated, expanded on, and supplemented with additional propositions.

3. ESTABLISHMENT OF THE TERMS OF REFERENCE

As would have been surmised from the preceding section, the envisaged CE environmental scanning process is of such a magnitude that it would require the allocation of substantial resources. Consequently, CE environmental scanning is unlikely to be initiated *ad lib*. Depending on the organisational structuring of an intelligence service, the project would probably need approval from the executive management of the intelligence service. Sound intelligence practice dictates that the sanction of the executive management should be documented as a pivotal part of the project's 'Terms of Reference' (ToR).

3.1 CLARIFICATION OF THE CONCEPT TERMS OF REFERENCE

The establishment of the project's Terms of Reference (ToR) thus constitutes the launching phase of the CE environmental scanning process. Comparable to a "Statement of Work" (SOW) in the corporate project management milieu (Kerzner, 1998: 535), the ToR of the CE scanning process articulate the client's (executive management's) expectations. In addition, the ToR authorise the assignment of resources to, and determine the modalities of, the environmental scanning to be performed. Similar to other complex projects in the statutory intelligence milieu, effective CE environmental scanning presupposes a ToR that clearly stipulates the following:

- The project purpose and objectives;
- the legal, regulatory and procedural mandate for the project;
- the benefits to the organisation, which are concretised in project deliverables and envisaged outcome(s);
- project risks;
- the allocation of resources such as information bases, information sources, personnel, technology and equipment, facilities and funds;
- a project organisational chart which stipulates the project sponsor and project manager; prescribes the reporting channels and mechanisms, and prioritises

the CE scanning project in relation to other projects/priorities within the intelligence service; and

- the time frame for the design, execution and conclusion of the project.

3.2 THE TERMS OF REFERENCE AS THE BASIS FOR THE DERIVATION OF PRIMARY SCANNING REQUIREMENTS

It needs to be emphasised that the ToR are not mere bureaucratic technicalities. The ToR direct the CE scanning process and are indispensable for ensuring the desired synergy between the outcome of the latter and the all-source counterespionage effort. Typically, under the heading *project purpose and objectives,* the ToR document the client's needs and provide the parameters within which primary scanning requirements will be formulated later on. While this study describes the CE scanning process as a comprehensive, multi-sectored process, the needs of the client might in some instances be more limited. The client could, for example, instruct the CE scanning to be restricted to determining espionage risks only within a sector (such as economic/technological or political/diplomatic) or even a certain aspect within a sector (for example a specific diplomatic initiative). Excessive limitations in the scope of the CE framework, must however be heeded, as this would detract from the benefits to be derived through this open-source instrument.

Further foundational toward the formulation of primary scanning requirements, are instructions contained in the ToR under the heading *project deliverables and envisaged outcome(s)*. Based on the project purpose and objectives, the envisaged outcome(s) describes the end product and in so doing determines the emphasis to be placed on the different types of intelligence in the course of the CE scanning process. In addition to the end product, under this subheading of the ToR, provision can also be made for secondary products during the process. These can firstly take the form of 'milestone' reports. One such example is a 'probing report' and is explained in Section 5.4 (Chapter Six). Secondly, products are typically required on aspects that emerged during environmental scanning that are of such a nature that the issuing of warning intelligence reports is warranted. Examples pertaining to these are cited in Figure 36 (Subsection 5.4.3, Chapter Six).

3.3 ALLOCATION OF RESOURCES TO THE COUNTERESPIONAGE SCANNING PROCESS

Seeing that managerial and logistical particularities associated with CE environmental scanning fall outside the focus of this study, only brief observations regarding such aspects emanating from the ToR are made. The latter address two managerial and logistical aspects that influence the execution of the CE scanning process on a conceptual level; thus warranting mention. These are *resource allocation* and *project risks*. The implications of these aspects in relation to the sources for utilisation in CE scanning and the composition of the project team are highlighted.

The parallel nature of CE environmental scanning – combined with the complexity of counterespionage – includes factors that should be considered in the allocation of human resources to the project. A project team without a core of practitioners seasoned in counterintelligence, as well as positive intelligence, is unlikely to succeed.

Chapter Four indicated that, in the statutory intelligence context, OSINT is not risk free and open sources not *gratis.* Under the headings *resource allocation* and *project risks*, the ToR sanction and prescribe resources for utilisation in the CE scanning process. The selection and structuring of open sources are fairly unambiguous and this aspect is addressed in Section 5.3. More complicated is the matter of the project team's prior knowledge of, and continued access to, secret information. While the envisaged CE scanning relies on open-source collection, the ToR will determine whether, and if so, the degree to which the project team will be allowed access to existing secret intelligence as background for open-source environmental scanning. The question as to whether open-source (counterespionage) scanning can be optimally executed without familiarity with the existing classified informational base, will undoubtedly elicit a response from counterespionage practitioners as wide ranging as the positions on OSINT's role within intelligence and counterespionage (as explained in Chapter Four).

Flowing from the contention of OSINT as an auxiliary and subservient function, 'secret-information supremacists' would probably argue that the role of the CE framework is restricted to the gathering of the "outer pieces" of the espionage risk "jigsaw puzzle" (Jardines, 2002: 10). The "outer pieces" in this regard can only be procured with a clear view of the secretly procured "precious inner pieces" (Jardines, 2002: 10). This position would pose familiarity with, and constantly updated knowledge of, secret information as a precondition for effective open-source CE scanning. More practically, 'secret-information supremacists' would favour ToR that sanction the project team's access to existing all-source information prior to and/or during the scanning process. ToR of such a nature would in certain respects defeat a primary purpose of parallel, open-source CE scanning. This degree of exposure to the existing all-source information base would nearly inevitably 'contaminate' the CE scanning process and perpetuate the (previously discussed) myopic self-feeding cycle. In so doing, one of the primary benefits of the CE framework as a parallel OSINT instrument would be severely impeded. Chapter Four, will be recalled, advanced the gaining of fresh insights from an objective distance as a primary *rationale* for open-source, CE environmental scanning.

As an opposing view, 'OSINT zealots' could advocate the feasibility and merits of the CE framework as a 'puristic' open-source instrument. Open-source CE environmental scanning, some 'OSINT zealots' might argue, is thus possible without prior knowledge of, and access to, classified information. In order to maintain an objective distance, the project team is assumed as being able to detach itself cognitively from prior knowledge of classified counterespionage information.

While an objective distance is at the heart of parallel statutory intelligence projects, detachment to the extent of a cognitive *tabula rasa* is neither practically possible nor a prerequisite for obtaining optimum benefits from the CE scanning process. Simultaneously, an objective distance would hardly be achievable should the project team be exposed to the existing all-source counterintelligence information base throughout the scanning process. This study favours a pragmatic compromise between these two positions that is in tune with the reality of statutory counterespionage practice. The 'middle-ground position' forms part of the generic assumptions in relation to the ToR of the CE scanning process and is explored in the subsequent subsection.

3.4 GENERIC PRESUMPTIONS OF THE TOR

The nature of, and the directions contained in the ToR, ultimately depend on the needs and context of the intelligence service commissioning the CE environmental scanning. Consequently, the scope and nature of CE scanning, as derived from the ToR, can also vary considerably. A discussion of the possible multiple variations in the CE scanning process would be more confusing than fruitful and this study is limited to outlining a general framework. This generic process is rooted in the following presumptions on which subsequent phases are built:

- The CE scanning is to comprehensively identify, describe, assess and prioritise espionage risks against the nation state. The spectrum of the scanning is macro-environmental and multi-sectoral. While multi-sectoral, the objective of the scanning is to identify espionage risks relevant to the mandate of the civilian intelligence service (commissioning the environmental scanning).
- The key deliverable of the CE scanning process is an open-source counterespionage risk assessment. Drawing on the collective knowledge and experience of the project team as well as inferences from open sources, the assessment should include postulations on own state vulnerabilities and proposals on countermeasures.
- The project team is mandated to use all open sources – as defined in Section 5.3 of this chapter – available to the intelligence service.
- The collective knowledge and expertise of the experienced project team are assets to the CE scanning. Such 'knowledge' refers to general familiarity with the statutory counterintelligence field and the broad espionage risk and threat picture. Categorically excluded, however, is the purpose-specific perusal of classified information with a view, or during the execution of, the CE open-source environmental scanning process. The project team is, in other words, denied access to classified information at the onset, and for the duration of, the CE scanning process.

In summation, this section, examined the establishment of the ToR as the launching phase of the CE environmental scanning process. Like OSINT in general, CE scanning was neither intended to be 'easy' nor 'cheap'. The ToR govern the allocation of information as well as human resources and are therefore key to the successful execution of the project. The ToR, moreover, are foundational to the derivation of primary scanning requirements and thus determine the directional focus of the CE environmental scanning.

4. THE DERIVATION OF PRIMARY SCANNING REQUIREMENTS

The derivation of primary scanning requirements entails the concretising of the directions of the ToR on the principle objectives and scope of the scanning into 'what is required to be determined'. Essentially, primary scanning requirements are a type-specific form of statutory intelligence requirements and are akin to 'research questions' in the academic realm. Based on the indicated presumptions of the ToR, primary scanning requirements would typically include the following:

- What are the own state's counterespionage-relevant informational interests and assets?
- Which of the own state's informational assets are at risk to adversarial espionage?
- Who are the espionage adversaries that pose risks to the own state's informational interests?
- What are the capabilities and *modus operandi* of espionage adversaries?
- Are there indications of these adversaries engaging in espionage activities?
- What is the conceivable impact (the type and nature of adverse consequences) that could result from adversarial targeting, or through espionage of the identified informational assets?
- To what degree is the own state vulnerable to, and what countermeasures can be instituted to mitigate, espionage risks?

Different from other levels of scanning requirements generated later on in the process – namely key and particularised scanning requirements – primary scanning requirements are determined at the inception of the CE scanning process with a broad and fixed resolution. These requirements are fixed in the sense that they constitute the cornerstones of subsequent phases of CE environmental scanning and are unlikely to be subject to recalibration as the scanning process progresses. Key and particularised scanning requirements which pertain to the information gaps emerging in the course of the scanning are, however, refined throughout the process.

5. THE DESIGN AND CONFIGURATION OF THE EXECUTION STAGE

Figuratively, the envisaged open-source counterespionage risk assessment – as described in the ToR and as 'deconstructed' in the primary scanning requirements – is the analogical 'destination' of the CE environmental scanning process. The allegorical 'route' to be followed in arriving at the destination, as well as the manner in which it should be navigated, still needs to be plotted. This phase, in more concrete terms, sets out to design the methodological schema (CE framework), structures the means (open sources) through which espionage risks are to be identified, and stipulates realistic parameters within which this is achievable.

5.1 THE FORMULATION OF A CONCEPTUAL VIEW OF THE ENVIRONMENT TO BE SCANNED

The prospect of scanning the expansive and amorphous ‘environment’ could be overwhelming. Within the design and configuration of the execution stage, the first step aims to establish a notional grasp of, and imposes some cognitive ‘order’ on, the environment to be scanned. Since it involves a notional and cognitive ‘think pattern’, the step itself defies easy description. In this instance, the outcome of the step possibly best conveys the various actions performed (in the execution of the step). Figure Six (Chapter Three) provides a visual presentation of a possible outcome of the step (cognitive structuring). As illustrated in the figure, the structuring pertains to the ‘deconstruction’ of the macro-environment into its main ‘elements’ and the project’s approach to the scanning of these.

This notional ordering serves a number of utility purposes of which the sectoring of the macro-environment serves as example. The following sectoring of the macro-environment was motivated in Chapter Three as apposite to the needs of the CE framework: political, military, social, technological, economic, ecological (environmental) and informational. As will transpire during the explication of further CE environmental scanning phases, this sectoral segmentation is useful as a conceptual tool with practical application.

5.2 THE DESIGN OF THE COUNTERESPIONAGE FRAMEWORK – THE IDENTIFICATION AND SEQUENTIAL ARRANGEMENT OF METHODICAL BUILDING BLOCKS

The practical value of the notional ordering described above, is demonstrated in the second step in the design and configuration of the execution stage, namely the design of a methodological schema in the form of the CE framework. Together with the primary scanning requirements, the notional ordering guides in the identification of the methodological buildings blocks required in the execution of the CE environmental scanning process. An example of what these building blocks could be is depicted in Figure 33 (Chapter Six) as the phases of CE environmental scanning bracketed as execution stage. The building blocks advanced are only a proposition and, depending on the preference of the project team and the particular circumstances, various alternatives are possible.

Subsequent to their delineation, these building blocks are sequentially arranged as phases in the execution of CE environmental scanning. On the basis of a motivation provided later in this chapter; this study proposes the identification of ‘critical informational assets and areas’ as the inception phase. Likewise, several variational alternative sequential arrangements are possible. In summation, and again with reference to Figure 33 (Chapter Six), the study proposes that the CE framework consists of the following sequential phases:

- Delineation of critical informational assets and areas;
- identification and profiling of espionage principals;
- identification and profiling of espionage adversaries;
- ascertainment of adversarial *modus operandi*;
- detection of indications of adversarial espionage;
- identification of own state vulnerabilities to espionage; and the
- compilation of an open-source, counterespionage risk assessment.

5.3 THE SELECTION AND SYSTEMISATION OF OPEN SOURCES

Of equal importance for clarification, is the purposeful selection and systemisation of the means to be used at arriving at the destination, namely open sources. Attempting to rely solely on a progressive identification of sources along the route, in a haphazard fashion, invites entrapment in the “information glut” (Meyer, 1987: 28).

Chapter Four cautioned against an over-reliance on the Internet and underscored the requirement for a balanced approach in the selection of open sources. A balance in the diversity of open sources would include – to name but a few in re-capitulation – the use of journals, books, reputable websites, information services, the attendance of seminars and conferences as well as personal interaction with academia and other experts. A balance in approach, however, extends further than the mere diversity in the types of sources. As indicated in Figure Six (Chapter Three), it also pertains to the topical selection of sources that enables scanning which varies from the ‘scouting’ of the macro-environment (contextual focus) to the ‘scrutiny’ of adversarial espionage actors (focus areas) and indications of their activities (focal points).

Sources useful in environmental scouting are, in a topical sense, concerned with the drivers of, and multi-sectoral trends in, the international security environment. Chapter Three cited as examples comprehensive and ongoing initiatives within the UK and US statutory security establishments to describe and project the transformation of the global environment and the implications thereof for international and national security (UK, 2007; US, 2004*b*; US, 2004*c*; UK, 2003; US, 2003; US, 2000*b*). Mention was also made of research projects conducted by institutions such as the UK-based Institute for Public Policy Research and the RAND Cooperation in the US (Kearns & Gude, 2008; Treverton, 2005; Karoly & Panis, 2004).

The selection of sources informing the 'focus areas' and 'focal points' of the CE framework can benefit substantially from taking due cognisance of 'Comparative Intelligence'. The latter is a field within Intelligence Studies only recently having regained prominence. It centres on the comparative assessment of statutory intelligence communities and services globally, and parallels aspects such as structures, oversight, *modus operandi* and priorities (O'Connell, 2004: 191, 198-199). Following exploratory work in this field by Godson (1988), Hastedt (1991) and Bozeman (1992), more recent works leading the re-emergence of this field include those by Johnson (2003) Todd & Bloch (2004), O'Connell (2004), Gendron (2005) and Henderson (2007). The importance of CE scanning heeding developments within Comparative Intelligence is, however, not limited to open-source selection. This field is invaluable in the execution of all the subsequent phases (namely Phases Four to Ten, Figure 33). The contribution of Comparative Intelligence to CE environmental scanning is also not restricted to opposing statutory intelligence services as own state adversaries. Albeit still limited, the espionage risks and threats non-state espionage actors pose to the nation state are some of the budding areas of enquiry of Comparative Intelligence.

Sources thus far discussed in this section conform to the narrow definition of open sources. For purposes of the CE framework a broader classification of open-sources, which include certain grey sources, was motivated in Chapter Four. In line with the broader definition, sources that the ToR allocate to the CE scanning process should preferably include premium, 'on-request' information services that provide analysed products on subjects ranging from country risk profiles to assessments of developments in relation to crime, the economy, the technological sphere, and so forth. Products such as these, as would rightly be observed, are conventionally associated with positive intelligence. Effective counterespionage, Chapter Five affirmed, presupposes the symbiotic interfacing with positive intelligence. The latter, for example, generates information on the own state's competitors and adversaries in general. Assessed through the counterespionage prism this positive intelligence is information assessed with the aim of establishing whether such competitors and adversaries are or could engage in espionage against the own state.

As a parallel process, and unlike the all-source counterespionage endeavour, CE environmental scanning is in this respect conducted in ‘isolation’ from the positive intelligence effort of the intelligence service. This isolation can partially be compensated for by the efficient use of the type of open sources mentioned. In addition, some information services provide current-reportorial as well as (on request) in-depth products on a multitude of espionage actors. Understandably, statutory intelligence services tend to protect full details on the identity and exploitation of information services from public disclosure. The precondition of this study on the non-disclosure of sensitive information therefore limits the citing of such sources to the near self-evident (Figure 34).

The subsequent outline of open-source structuring for CE environmental scanning purposes is therefore highly selective and would in practice be much more comprehensive. Given the centrality of Comparative Intelligence to the CE scanning process the outline emphasises, but is not limited to, sources useful in Comparative Intelligence.

Figure 34: The structuring of initial open-source selection – a selective illustration

PERIODIC PUBLICATIONS	
Intelligence and National Security	London, Frank Cass & Co Limited.
International Journal of Intelligence and Counterintelligence	London, Taylor & Francis.
Studies in Intelligence	Washington Center for the Study of Intelligence (Central Intelligence Agency). Also available online at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi/publications/.
ELECTRONIC JOURNALS, PREMIUM INFORMATION SERVICES AND SUBSCRIPTION DATABASES	
Jane’s Intelligence Review	London, Jane’s Information Group.
Jane’s Intelligence Digest	London, Jane’s Information Group.
Intelligence Online	Paris, Indigo Publications.
Africa Intelligence	Paris, Indigo Publications.

<table>
<tr><td colspan="2">Factiva</td><td colspan="3">http://factiva.com</td></tr>
<tr><td colspan="2">Dialog</td><td colspan="3">http://www.dialog.com</td></tr>
<tr><td colspan="2">Datastar</td><td colspan="3">http://www.datastarweb.com</td></tr>
<tr><th colspan="5">REFERENCE WORKS (BOOKS)</th></tr>
<tr><td>Henderson, R.</td><td>Brassey's International Intelligence Yearbook
(Remark: Indispensable work and highly recommended in respect of comparative intelligence. Country profiles and the outline of the intelligence apparatus of more than fifty countries. These profiles and outlines cover foreign, domestic, military, and technical intelligence branches. Some entries extend to the inclusion of organisational charts that depict the relationship between the national intelligence services and the executive branch of government.</td><td>2007</td><td>London</td><td>Brassey's International.</td></tr>
<tr><td>Chapman, B.</td><td>Researching national security and intelligence policy. (Remark: The work is likewise highly recommended. As claimed by Chapman (2004: xxi) the reference guide is indeed “global” in its scope. It details multiple research institutions and “public accessible English-language governmental publications” from various countries (on all continents) as well as intergovernmental bodies.</td><td>2004</td><td>Washing-
ton</td><td>CQ Press</td></tr>
<tr><td>Johnson, L.K. (ed.).</td><td>Strategic intelligence - counterintelligence and counterterrorism: defending the nation against hostile forces. Volumes 1 to 4.</td><td>2007</td><td>Westport</td><td>Praeger Securities International.</td></tr>
<tr><td>Carlisle, R. P (ed.).</td><td>Encyclopedia of intelligence and counter-intelligence. Volumes 1 and 2.</td><td>2004</td><td>New York</td><td>Sharpe Reference</td></tr>
<tr><td>Polmar, N Allen, T, B.</td><td>Spy book: the encyclopedia of espionage.</td><td>1996</td><td>New York</td><td>Random House</td></tr>
<tr><th colspan="5">GENERAL INTERNET SITES (ON STATUTORY INTELLIGENCE AND RELATED ASPECTS)</th></tr>
<tr><td colspan="2">CI Centre</td><td colspan="3">http//www.cicentre.com/</td></tr>
<tr><td colspan="2">Federation of American Scientists</td><td colspan="3">http//www.fas.org</td></tr>
<tr><td colspan="2">Cryptome</td><td colspan="3">http://cryptome.org/</td></tr>
<tr><td colspan="2">Global Security</td><td colspan="3">http://www.globalsecurity.org/</td></tr>
<tr><td colspan="2">Strategy Page</td><td colspan="3">http://www.strategypage.com/</td></tr>
</table>

WEBSITES OF RESPECTIVE STATUTORY INTELLIGENCE SERVICES
A comprehensive list of such sites in Henderson (2007).
EXPERTS, ACADEMIC AND OTHER INSTITUTIONS
As determined by the nature of the own state. Discussed in subsequent sections of this chapter.
SEMINARS AND CONFERENCES
As determined by the nature of the own state. Discussed in subsequent sections of this chapter.

It would be rare, if at all possible, at this juncture to identify all sources to be utilised in the CE scanning process. Nonetheless, numerous sources will be added as the scanning progresses. It is precisely the anticipated expansiveness of additional sources emerging in the course of the CE scanning process that underscores the necessity of establishing a structured core of sources at the onset. The soundness of this core is tested, and additional sources added, as early as the next step, namely the alignment of the execution of the CE scanning process with reality.

5.4 THE CONFIGURATION OF NOTIONAL DESIGNS IN ACCORDANCE WITH REALITY

At this point in the CE scanning process, it is not only the open-source base that is ‘untested’. The conceptual view of the macro-environment and the CE framework are prototypical designs figuratively ‘plotted’ on the conceptual ‘drawing board’. Prior to proceeding to the execution stage of environmental ‘scouting’ and ‘scrutiny’, these designs are ‘tested’, and where necessary, configured in accordance with reality.

5.4.1 Conducting an environmental probe

Functionally, this is achieved by an environmental probe which culminates in the submission, to the intelligence service’s management, of a pilot document entitled: *An exploratory overview of international security, intelligence and counterintelligence in the 21st century*. The report, comparable to the content of Chapter Three of this study, serves as a referential document throughout the execution stage, and could have the following format:

Figure 35: Probing the macro-environment – an exploratory overview of international security, intelligence and counterintelligence in the 21st century

- International and national security in the 21st century
  - – Drivers of change
  - – Strategic trends affecting international security and insecurity
  - – Implications of the strategic trends for national security
- 21st century espionage threats, risks and challenges to the nation state
  - – Adversarial espionage actors as focal points of CE environmental scanning
  - – Adversarial espionage collection: sources and methods
  - – The nature and categories of information collected by espionage adversaries
  - – Other aspects relating to adversarial espionage *modus operandi*
- Statutory counterintelligence methods and measures
  - – Physical security
  - – Information and technological systems security
  - – Personnel security
  - – CI collection methods
  - – Neutralisation, deception and exploitation
- Challenges to statutory counterintelligence and counterespionage
- Implications for open-source CE environmental scanning

As reflected by the subthemes included in the proposed format, the pilot document is intended to provide a 'panoptic' and – in comparison with the outcomes of 'scouting' and 'scrutiny' – a largely superficial overview of the terrain to be scanned. Experience has taught that some practitioners may doubt the necessity of a pilot document and, citing reasons such as time-constraints, opt for the omission of this step. The price for this omission will undoubtedly be paid in time and by the resources squandered through intensive re-planning and redesigning during the execution stage. It will also become apparent by the disappointment of both the project team and management in failing to meet unrealistic expectations from this OSINT instrument. The considerable effort expended in the probing of the environment is by and large outweighed by the dividends it pays.

5.4.2 Aligning the counterespionage framework with the 21st century espionage and counterespionage reality

These dividends pertain, amongst others, to the seemingly contradictory notion of the 'broadening' and 'limiting' in the configuration of the focus and outcome of the CE framework. While the project team is assumed to have a general (all-source) familiarity in respect of statutory counterintelligence and the macro-environment, the exploratory probe and the resultant overview acquaint it with the scanning terrain through a *parallel OSINT* prism. A previously noted primary *rationale* for *parallel* CE scanning is the broadening and enrichment of the view of the intelligence service on espionage risks. Espionage risks, or aspects thereof, not purposefully sought, could go undetected during the execution of the CE environmental scanning.

A configuration based on the questionable notion of nation states predominating the espionage arena, for example, may result in 21st century espionage risks emanating from the activities of other categories of actors not detected in the scanning process. In presenting the 'reality' according to which the focus of the CE framework should be configured, Chapter Three posited the fact that the nation state is confronted with convoluted espionage risks posed not only by other nation states but also by entities within private enterprise; NGOs; entities within the mass media; terrorist and extremist groupings; as well as unaffiliated individuals and groups. A more detailed view of the scrutiny in the execution stage, the focal and focus points of the CE scanning process (Figure Six, Chapter Three) should thus pertinently provide for the variety of espionage actors. A knowledgeable and 'fresh' configuration to this effect is hardly attainable without the insights derived from an environmental probing.

5.4.3 Configuration of the counterespionage scanning process in line with the reality of the limitations of open-source intelligence

The configuration of the CE scanning process, as suggested, also pertains to the setting of parameters in tempering expectations in line with the reality of open-source limitations. Chapter Four, as will be recalled, was dedicated to the extensive examination of such expectations and limitations. Emphasis was also drawn to the fact that the CE framework as an OSINT tool, in itself and by itself, is unlikely to assert concerns on counterespionage beyond the level of plausibility. The 'answers' the CE framework can provide to the scanning requirements are thus tentative assertions. Even with the qualification of their tentative status, the description of espionage risks would not consistently conform to all the essential elements of intelligence, (namely the who?, what?, when?, where?, why? and how?).

While a general consciousness of the limitations of the CE scanning process is important, awareness alone is abstract and insufficient. Parameters should demarcate in clearer terms 'what is knowable' through open sources. Also in this instance, the necessity of environmental probing is underscored. An informed judgement of 'what is knowable', after all, follows on insights obtained in the course of the probing process. These parameters on the 'knowable' are included in the probing report – under the heading *Implications for open-source CE environmental scanning* – and convey to the executive management of the intelligence service the limits in meeting the expectations contained in the ToR. Ideally, configurations of open-source limitations are first done generically (that is in respect of the CE framework as a whole), and then particularised in respect of each of the phases of the CE framework. This section suffices with an example of a generic configuration entitled *A typology of own state counterintelligence information – the assumptions and role of open-source counterespionage scanning.* Contrary to what impression might be garnered from its title, this is not an abstract and notional construct, for it is quintessentially practical.

Without compromising its primary counterespionage focus, but rather supplementing it, CE environmental scanning therefore maintains a peripheral, yet vigilant view which considers defensive counterintelligence. All-source counterespionage is charged with identifying espionage risks and threats to protect all relevant classes of counterintelligence information offensively. The pragmatic calibration of the offensive-defensive focus and role of the CE framework to what 'what is knowable in open-source scanning' is underpinned by a typological view of the classes of own state counterintelligence information. The composition of a typology is axiomatically determined by the purpose of its compilation. In the case of CE environmental scanning, this typology needs to provide clarity on two aspects. Firstly, and given the varying degrees of secrecy inherent to the work of counterintelligence, what categories of information can the project team presume to be familiar with and/or infer from open-sources? This categorisation, as will be explained, needs to distinguish between the 'secrecy of the existence' and the 'secrecy of the substance' of information. Secondly, what should the role of the CE scanning process be in relation to the respective classes of information?

Based on the assumptions in respect of the ToR regarding sources availed to, as well as the collective counterintelligence knowledge and expertise of the project team, the following typology of counterintelligence information can serve as a guide in calibrating the focus of the CE scanning:

Figure 36: A typology of own state counterintelligence information – the assumptions and role of open-source counterespionage scanning

A TYPOLOGICAL CLASSIFICATION OF CI INFORMATION	DESCRIPTION OF INFORMATION CLASS	OPEN-SOURCE SCANNING: ASSUMPTIONS AND ROLE
EXISTENCE: **Highly classified and compartmentalised** **SUBSTANCE:** **Highly classified and compartmentalised**	Information deemed of such importance and nature that the existence (of the information) as well as the substance (information content) are afforded a high level of classification and compartmentalisation. An example would be information relating to a nation state's endeavours to establish chemical, biological, radiological, and/or nuclear (CBRN) capabilities in contravention of treaties to which the state is a signatory. The existence of such projects, as well as the information related to the programmes, is highly classified and privileged.	The project team is assumed not to be familiar with information in this category. Generally, these secrets are also not inferable through open sources. Nevertheless, CE scanning could detect indications, or the actual compromising, of information reasonably deemed to be of such a nature. Indicators (such as trends in media reporting) could, for example, suggest the risk of CBRN programme(s) being exposed. The project team was, in other words, not aware of the existence of the programme(s) prior to the scanning, but through open sources could detect the possible existence (of such information) and find indicators indicating the compromise thereof. While an appraisal of such developments is included in the *Open-source counterespionage risk assessment* at the project's conclusion, their importance warrants immediate reporting by means of secondary products in the form of intelligence-warning reports as envisaged in Section 3.2 (Chapter Six).
EXISTENCE: **Known** **SUBSTANCE:** **Classified**	The existence of the information ('topic') is not sensitive. The substance is in part, or in its entirety, protected. An example would be information pertaining to research into cost-effective nuclear fusion as an electric power source.	The project team has general familiarity with and/or can infer from open sources the existence, but not the content, of these secrets. CE scanning is required to identify, and report on, espionage risks to such information.

<u>EXISTENCE</u>: **Known** **<u>SUBSTANCE</u>:** **Partially or entirely unclassified** **[Counterintelligence protection required]**	Information on aspects falling into this category is in the public domain (not classified or privileged). Based on its collective counterintelligence expertise, as well as insights derived during the scanning process, the project team considers the information of such a nature that it should be classified. The unprotected status of the information can be the result of either oversight or of new trends. In some instances it is imperative that 'damage containment and prevention' be done and warning intelligence reports issued. One of the own state's parastatals, by way of illustration, is involved in the development of ceramic materials for industrial and domestic use. In the course of the CE scanning it emerges that this technology has a dual-use application in the military field (armour protection) and is highly prized by other macro-environmental role players.	CE scanning is required to demarcate (counterintelligence relevant) information falling into this category, as well as the other two categories discussed below. Depending on the information category, espionage risks thereto should be identified and/or recommendations on defensive counterintelligence protection made. Findings in this regard will be contained in the open-source *counterespionage risk assessment* at the project's conclusion (see Section Eight, Chapter Seven). If warranted, intelligence warning reports should be submitted.
<u>EXISTENCE</u>: **Known** **<u>SUBSTANCE</u>:** **Partially or entirely unclassified** **[Counterintelligence protection obsolete]**	On the basis of the project team's collective knowledge and the appraisal of open sources it is ascertained that counterintelligence protection afforded to certain bodies of information is redundant. Changes in the macro-environment render counterintelligence safeguarding obsolete. Precious counterintelligence resources are thus dissipated. During the CE scanning process the project team could, for example, establish that the counterintelligence protection the state affords to aspects of satellite-imagining technology is redundant, given current commercially available technical 'know-how' in this field.	As described above.

EXISTENCE: **Known** **SUBSTANCE:** **Mostly unprotected**	Information that does not necessarily require classification in respect of the existence or content, but that is of such a nature that the integrity of the information and/or the systems in which it resides needs to be ensured. Information in this category varies from the more concrete (the information network underpinning infrastructure such as transport systems and electricity distribution) to the more 'intangible' (e.g. government's reputational integrity and communication strategy). While the information *per se* could be unclassified and be available in the public domain, knowledge of the informational security measures safeguarding the integrity of systems (in which the information resides) would typically be deemed as privileged.	As described above.

5.4.4 Additional benefits derived from the environmental probing

The collection and assessment process by which the probing report is produced, serves as a 'trial run' for synergism in the personal interaction between, and the counterintelligence-practice acumen of, the respective project team members. At least at the time of writing, this project team will consist of humans and not predictable androids programmed with equivalently cloned counterintelligence skills. However soundly conceptualised, designed and planned, the execution of CE environmental scanning could stumble over the 'human factor'. If necessary, the composition of the project team, other aspects of resource allocation and the project's organisational flow can be rectified at this relatively early juncture of the environmental scanning process.

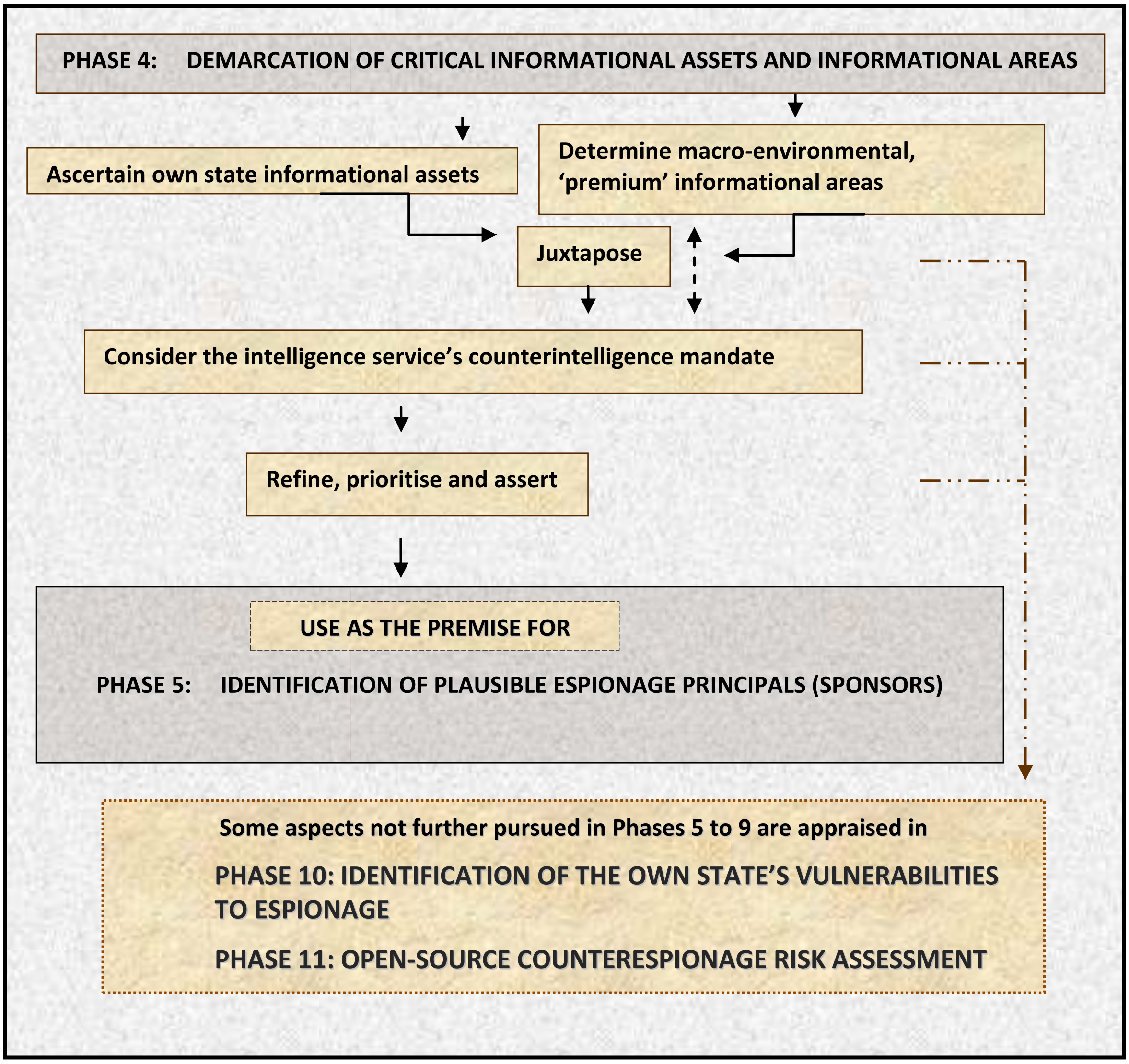
The preceding sections demonstrated the conceptualisation, design and planning stage as more than a mere routine, administrative 'formality' prior to the commencement of the 'actual work'. The establishment of the ToR, the derivation of primary scanning requirements, and the design and configuration of the CE framework, are not mere phases that precede the actual environmental scanning process. Instead, they are an integral part of the CE environmental scanning process. This stage, as depicted in Figure 32, is not as resource intensive as it is time consuming. The execution stage will show the considerable time allocated to conceptualisation, design and planning is justified.

6. THE DETERMINATION OF CRITICAL INFORMATIONAL ASSETS AND PREMIUM INFORMATIONAL AREAS

The effort expended on sound design, planning and conceptualisation is nowhere more apparent than at the inception phase of the execution of the CE scanning process, with the demarcation of critical informational assets and the premium informational areas. Informational assets and areas, in essence, refer to the referent objects of espionage and statutory counterespionage. Although it will emerge in the course of the section as a definitional oversimplification in certain respects, the term ‘secrets’ is in some instances used interchangeably in the discussion that follows with ‘critical informational interests’ and/or ‘premium informational areas’.

The phase commences with the identification of the own state’s secrets. From a counterespionage perspective, these ‘bodies of information’ are secret because they are highly prized (‘at premium’) in the macro-environment. Consequently, the phase proceeds to delineate the macro-environmental ‘informational areas’ in which secrets are most at premium. Juxtaposed, and refined in accordance with the mandate of the civilian intelligence service, the convergence of own state secrets and premium informational areas establishes the premise for the identification of espionage principals (sponsors) further on in the CE scanning process. Graphically, Phase Four can be illustrated as follows:

Figure 37: The open-source identification of critical informational assets and premium informational areas


PHASE 4: DEMARCATION OF CRITICAL INFORMATIONAL ASSETS AND INFORMATIONAL AREAS
Ascertain own state informational assets
Determine macro-environmental, 'premium' informational areas
Juxtapose
Consider the intelligence service's counterintelligence mandate
Refine, prioritise and assert
USE AS THE PREMISE FOR
PHASE 5: IDENTIFICATION OF PLAUSIBLE ESPIONAGE PRINCIPALS (SPONSORS)
Some aspects not further pursued in Phases 5 to 9 are appraised in
PHASE 10: IDENTIFICATION OF THE OWN STATE'S VULNERABILITIES TO ESPIONAGE
PHASE 11: OPEN-SOURCE COUNTERESPIONAGE RISK ASSESSMENT

6.1 THE DEMARCATION OF THE OWN STATE'S CRITICAL INFORMATIONAL ASSETS

Several variations, it was previously asserted, are possible in the sequential structuring of the phases of the CE scanning in general, and in the selection, in particular, of the commencement phase of the execution stage. Given the open-source orientation of this study, the question arises: Why is the selection of the 'demarcation of critical informational assets and areas' deemed as the most apposite start for the execution of CE open-source scanning? Furthermore, what is the *rationale* for positing the identification of own state secrets as the first subphase of Phase Four? Lastly, on what grounds is such a substantial part of this chapter devoted to this phase?

Few would be more perplexed by the sequential-structuring of the CE framework and the prominence afforded to the demarcation of informational assets and areas than protagonists of the indicators-at-the-centre approach to open-source environmental scanning. Chapter Four (Section Six) and subsequent sections of this chapter recognise the invaluable role of indicators in open-source CE scanning. This role is not in dispute. What the study does contest, if only then from a counterespionage perspective, is the view of indicators at the predominating nucleus of the design and execution of open-source environmental scanning. Used out of proper context, especially in inexperienced hands, the employment of espionage indicators is more of a hazard than an aid. A set of indicators, by way of analogy, is not a stand-alone, espionage-detecting radar device. If not 'deployed' as part of other 'systems', 'chaff and 'flares' [4] might be construed as enemies, while 'stealthier' opponents will not show on the 'screen' at all. Reliable espionage indicators are designed as part of, and not prior to, the execution of the CE scanning process. These indicators are furthermore employed, and for good reason, (in Phase Eight – Chapter Seven, Section Six) within the context of preceding scanning phases.

In previewing the argumentative logic of the CE scanning process (Section Two, Chapter Six) brief reference was made to the *rationale* for positioning the identification of informational assets and areas at the inception of the execution phase. Its open-source dependence, it was argued, denies the CE framework of the espionage-adversary-centric 'default starting point' that frequently prevails in the all-source counterespionage practice.

6.1.1 The *rationale* behind the positioning of the identification of own state informational assets at the inception of the execution stage

There is, however, an additional and more compelling reason for this positioning. Within counterintelligence in the main, an 'adversary-centric default' is not the ideal 'starting point'. In describing the latter, deGraffenreid (1989: 151) asserts that:

> A country must first know what it is trying to protect. What are those values, secrets and institutions that it needs to protect? In a free society there are lot of them. Given the finite nature of its CI

[4] In the military, the terms 'chaff' and 'flares' indicate radar countermeasures used by aircraft.

> resources, what are its most precious secrets? This requires analysis and decision.

With explicit reference to counterespionage, Godson (2001: 188) endorses this standpoint and advises as follows: “Ascertaining what really needs protection is the right place to begin”. Although the offensive dimension of counterintelligence, effective counterespionage thus has as a prerequisite a clear understanding of what information needs to be protected. Within the all-source counterintelligence context, the ‘adversary-centric default’ of counterespionage can in part be justified by its (counterespionage’s) offensive mission. The task of demarcating and classifying own state secrets rests mostly with the defensive counterintelligence function. In performing this task, defensive counterintelligence draws on various types of information of which that generated by counterespionage is but one. The ‘adversary-centric default’ of all-source counterespionage, it can be argued, is justifiable if informed by the defensive demarcation of own state secrets of counterintelligence.

The CE scanning process was explained as an *ad novo* process which, unlike all-source counterespionage, cannot build on existing counterintelligence appraisals of critical information assets. Being a parallel open-source instrument, the demarcation of these assets is – contrary to what should (ideally) be the case in all-source counterintelligence – not a ‘given’ within CE environmental scanning. Critical informational assets therefore have to be inferred from – and within the pre-decided limits (Subsection 5.4.3, Chapter Six) of – overt information. Hence, the execution of the first subphase of CE environmental scanning is set at the “right place” as it determines “what needs protection”, namely the own state’s secrets.

6.1.2 The challenge of the open-source demarcation of the own state’s critical informational assets

Although ideally the “right place to start” in all-source counterintelligence, the identification of “what needs to be protected” is a mammoth, and for this reason, an often neglected task (Godson, 2001: 188-190;1989: 18-20). Within the context of the CE framework, this task is conceptually even more challenging. Prior to advancing practical steps in this regard, the challenge needs to be ‘unpacked’. It is this ‘unpacking’ – practically and notionally – that holds the key to the formulation of practical steps. In presenting this challenge, the characteristics of critical informational assets are taken as the points of departure.

6.1.2.1 The entirety of critical informational assets is seldom clearly demarcated

Some of the critical informational assets of the own state are self-evident, and albeit shaped by the particular circumstances of a respective country, not uncommon to other comparable nation states. For a "powerful, technologically advanced country", these assets, in the view of Godson (2001: 188-190), are the secret information in relation to, *inter alia*, strategic command and control systems, "details of the government's relations with scores of regimes around the world", the "plan[s] one state uses in negotiations with others", the activities of organised crime syndicates and "proprietary technology". The complexity and extensiveness of the task lie in adding some detail to the description of generic 'secrets' and in identifying informational assets that are less obvious.

Notably, in the US (2006*c*, 2006*d*), enviable strides have been made in demarcating critical informational assets in the technological-scientific field. Yet, the search in consulted literature for a nation state claiming that all its multi-sectoral critical informational assets have been precisely defined has been in vain. Indeed, such a claim would be conceited and reflect oblivion to reality. Against the backdrop of the informational and technological explosion of the 21st century, particularly nation states with substantive national interests are faced with an exponential increase in the 'bodies of information' of actual or potential critical importance. The fast changing macro-environment has as a consequence that critical informational assets have to be identified, assessed and re-assed continuously. The sheer extent of information relevant to the national interests makes the full identification of critical assets an unachievable ideal.

6.1.2.2 'Critical informational assets' are subjective designations assigned to purposely identified 'bodies of information'

As implied, bodies of information do not necessarily emerge with a tag stating 'critical informational assets – protection required'. Such a classification and typification is an assigned label. The bodies of information, in other words, firstly need to be delineated and then appraised as to whether they warrant the designation of own state secrets. Who then, performs such a delineation and designation?

6.1.2.3 Critical informational assets are identified and delineated by the statutory security apparatus

Blessed be the intelligence statutory intelligence service which receives an encyclopaedic, multi-voluminous inventory from its political master listing national critical interests and assets warranting protection and advancement. In practice, this is the function of, and one of the reasons why nation states possess, statutory security apparatuses in general and counterintelligence structures in particular. Within all-source counterintelligence, dynamic and continuous interaction with the client could aid in this task, but it is not a substitution thereof. The degree to which open-source CE scanning could interact with the client is dependent on the ToR. The resources allocated to CE scanning are only a fraction of that at the avail of all-source counterintelligence. Consequently the exposure of CE scanning to the client – if actually allowed by the ToR – would be markedly more limited. As a result, CE scanning would frequently be challenged to determine less self-evident informational assets through conventional open-source collection and assessment.

6.1.2.4 Critical informational assets are located in a multi-sectoral web of own state, national interests

The success with which the challenge is practically met depends foremost on the underlying (micro-) theoretical approach. Theoretically, all critical informational assets are located in the multi-sectoral web of the own state's national interests. Within this web some informational interests are, as suggested, rather self-evident. Others, however, are opaque, imbedded and need to be inferred, be it in an all-source counterintelligence endeavour or in open-source CE scanning. The process of 'uncovering' opaque informational assets presupposes conceptual clarity on the locality of these assets in the multi-sectoral web of interests of the own state. Phrased as a simplified question: where do informational assets 'fit in' on a conceptual level? Although the 'answer' to this question revolves around definitional relationships and is inevitably theoretical, it will shortly transpire to have very real practical ramifications.

Notionally, the concept 'critical informational assets' is related to the broader constructs of 'national security perception', 'informational power', the 'informational sphere' as a category of state power, 'informational warfare', 'national interests', 'national security interests' and 'informational interests'. These concepts were discussed in previous chapters and the recapitulation below is restricted to those aspects with direct implications for open-source CE scanning – notably insofar as the identification of steps is concerned.

The state pursues its national security interests based on its ultimately subjective national security perception. The latter is embodied in the government's national policy, objectives and strategy as well as the political leadership's *Weltanschauung* (Buzan, 1991: 6, 16, 18, 102-103, 132-139; Hough, 2006: 1-6, 15-16; Johnson, 2003: 640). The national security interests are pursued in the political, social, technological, economic, military, ecological (environmental) and informational sectors. These sectors, to re-quote Buzan (1991: 20), "do not operate in isolation from each other. Each defines a focal point within the security problematique, and a way of ordering priorities, but [they] are woven together in a strong web of linkages." Like other national interests, the informational interests of the state are focal points in the web. Informational interests can thus not be pigeon-holed as being purely limited to the informational sector, but transverse across the entirety of the 'web' of national interests. Informational interests are, in other words, inseparable from national interests in the political, social, technological, economic, military, and ecological (environmental) sectors.

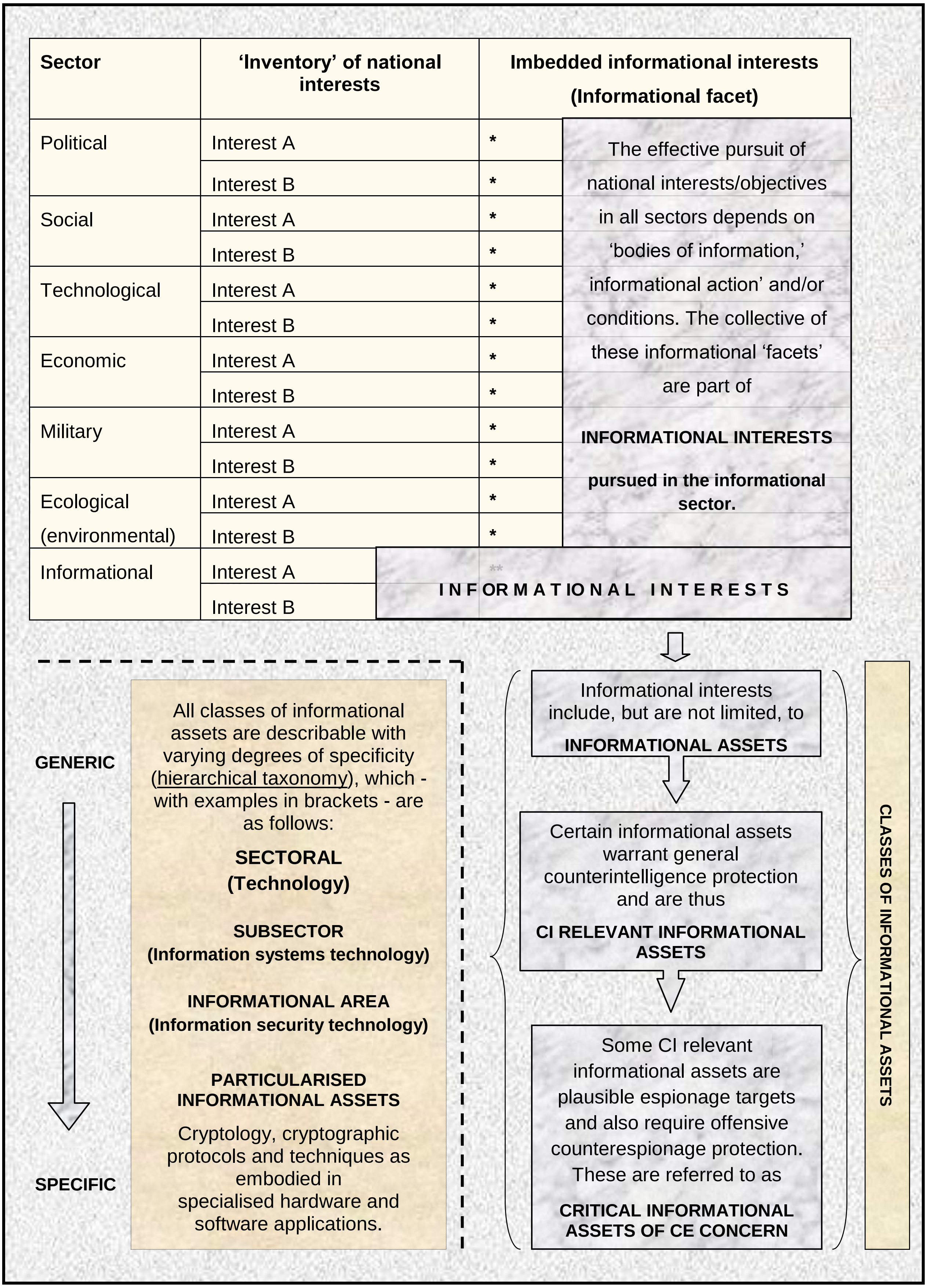
With the qualification of their interwoven nature, the informational interests of the state consist of three interrelated facets. Firstly, informational interests encompass the *informational assets* which the state possesses, values and protects. The latter encompass the whole body of information at the nation state's avail necessary for its survival, prosperity as well as the expansion of its national interests. These informational assets are of both a tangible and intangible nature and denote the systems, institutions and people that gather, store, process, communicate and otherwise utilise information. In a broader sense, the reputational integrity of the state (the international and domestic public image) is also an informational asset. Secondly, informational interests denote the (informational) assets the state *aspires to procure* (such as the secrets of adversaries). Thirdly, informational interests pertain to the *conditions* the state seeks to realise (for example, the gaining of a competitive edge over an adversary through obtaining such secrets, augmenting its own informational integrity through counterintelligence measures or undermining the informational integrity of an adversary).

Certain informational assets are of such a nature that they require counterintelligence protection. The extensive range of counterintelligence protective measures was discussed in considerable detail in Chapter Three

(Section Six) and will therefore only be synoptically referred to here for purposes of contextualisation. Counterintelligence, in a nutshell, comprises a defensive shield and an offensive sword. Defensive measures range from access control and perimeter security to INSYSEC. As part of information security, the content and, sometimes, knowledge of the existence of certain informational assets are protected through the assignment of classified designations (namely, confidential, secret and top secret – collectively referred to as 'secrets') and privileged access to information through compartmentalisation (the so-called 'need-to-know' principle). Defensive measures aim to protect the integrity and content of informational assets in general. Some, but not all defensively-safeguarded informational assets, are of such a nature that they also warrant offensive protection by means of the offensive counterespionage 'sword'. These informational assets are of counterespionage concern since they are plausible targets for adversarial espionage collection. It is these counterespionage-relevant informational assets which – for purposes of this study – are referred to as 'critical informational assets'. The qualifier 'critical' is a free adaption of the equivalent term employed in the US national security community as referring to such information and technology which, being compromised through for example espionage, would significantly impede the country in optimally pursuing its national security objectives (US, 2008*d*; US 2007*g*; US, 2006*c*; US 2006*c*; US, 2005*e*; US, 2005). The term 'critical' is used within defensive business intelligence too, in categorising what the information companies regard as warranting protection by defensive competitive intelligence programmes (Vibert, 2004: 43-44).

With a view of advancing concrete steps for the open-source identification of critical informational assets (in Subsection 6.1.3), and as a background to a practical example presented later in Figure 39, the preceding micro-theoretical explication is summarised in the following matrix:

Figure 38: Critical informational assets within the context of multi-sectoral national interests



Sector	‘Inventory’ of national interests	Imbedded informational interests (Informational facet)	
Political	Interest A	*	The effective pursuit of national interests/objectives in all sectors depends on ‘bodies of information,’ informational action’ and/or conditions. The collective of these informational ‘facets’ are part of **INFORMATIONAL INTERESTS** **pursued in the informational sector.**
	Interest B	*	
Social	Interest A	*	
	Interest B	*	
Technological	Interest A	*	
	Interest B	*	
Economic	Interest A	*	
	Interest B	*	
Military	Interest A	*	
	Interest B	*	
Ecological (environmental)	Interest A	*	
	Interest B	*	
Informational	Interest A	**	INFORMATIONAL INTERESTS
	Interest B		

GENERIC

SPECIFIC

All classes of informational assets are describable with varying degrees of specificity (hierarchical taxonomy), which - with examples in brackets - are as follows:

SECTORAL
(Technology)

SUBSECTOR
(Information systems technology)

INFORMATIONAL AREA
(Information security technology)

PARTICULARISED INFORMATIONAL ASSETS

Cryptology, cryptographic protocols and techniques as embodied in specialised hardware and software applications.

Informational interests include, but are not limited, to **INFORMATIONAL ASSETS**

Certain informational assets warrant general counterintelligence protection and are thus **CI RELEVANT INFORMATIONAL ASSETS**

Some CI relevant informational assets are plausible espionage targets and also require offensive counterespionage protection. These are referred to as **CRITICAL INFORMATIONAL ASSETS OF CE CONCERN**

6.1.2.5 Deficient clarity on notions pre-conditional to the optimal identification of critical informational assets

At least conceptually then, clarity on the state's national security perception, policy, objectives and priorities would enable the delineation of the own state's critical informational assets. Herein, to paraphrase Johnson (2003: 639, 641; 2001: 188) "lies the rub"; the "seemingly simple" notions of national security objectives and priorities are "frequently" unclear – especially in non-authoritarian regimes. In a similar vein, Hough (2006: 1) observes that "a lack of clear [national security] policy guidelines" in some instances compels the formulation of a national security strategy "based on an interpretation of certain (and often fragmented) elements of national security policy that may exist."

The ensuing course of action followed in CE environmental scanning is determined by the degree of equivocality in national security priorities (and related concepts). Matters, having inadequate open-source information for even generalised (broad) inferences, are stated as such and the counterespionage implications stipulated (Section 6.3). On other issues, further collection and appraisal may enable general inferences from informational assets. General inferences from the latter will inevitably lack specificity. In open-source scanning it would, in fact, at times not be possible to describe the informational assets as such but only the informational area within which they resort.

6.1.3 Steps in the open-source demarcation of own state critical assets

Although not pertinently indicated as such, most steps for the identification of critical informational assets will have crystallised in the course of unpacking the challenge and the notional clarification of concepts.

6.1.3.1 Decide on a detailed systemised approach

As a first step a detailed, systemised approach is designed. The latter consists of deciding on subsequent steps (on which a proposal is advanced below in Subsections 6.1.3.2 to 6.1.3.5) as well as the 'format' of the execution (as illustrated in Figure 39).

6.1.3.2 Refine the selection of open sources to be used

Building on the initial selection in Phase Four (Section 5.4, Chapter Six), open sources that are of value to the identification of national interests and assets are selected. These include unclassified governmental information such as policy statements, scheduled (such as annual reports) and *ad hoc* official government reports, legislation and legislative debates, public speeches, press conferences, media reporting as well as publications by academic institutions, institutes and 'think-tanks'. Since national security interests span wider than the public sector, comparable information sources stemming from parastatals, the corporate sphere and civil society also need to be consulted. Within the confines noted earlier (Subsection 6.2.2.3, Chapter Six), the information sources mentioned can be supplemented by HUMINT in the form of interaction with relevant stakeholders such as governmental office bearers, corporate leaders, academia and other independent experts.

6.1.3.3 Plot the state's multi-sectoral national interests

The ensuing steps move from the general to the specific, and commence with the plotting of the web of the own state's multi-sectoral national interests. Depending on the preferences of the project team and the particular circumstances within which the scanning is conducted, the matrix in Figure 38 can serve as a conceptual guide and the proposal in Figure 39 as a further refinement.

6.1.3.4 Ascertain the national interests' informational facets and derive the collective of informational interests (and assets)

National interests in the respective sectors are subsequently appraised in order to determine their informational facets. These 'facets' are used to infer informational interests and imbedded informational assets. Phrased as a question – the central criterion for this inference is as follows: Is there a 'body of information' crucial to maintaining and advancing the interest in question, and if so, what is the informational subject matter ('topic')? These 'bodies of information' are deemed as informational assets.

6.1.3.5 Determine the counterintelligence relevance of 'informational assets' and assert which of these are 'critical' (informational assets)

In practice, the distinction between, on the one hand, an informational asset's broader counterintelligence relevance and, on the other hand, its more pertinent counterespionage significance, is blurred. Although conceptually two steps, functionally the appraisals of an informational asset's counterintelligence and counterespionage relevance, are performed as concurrent activities. Interrelated criteria that the project team would typically consider are the degree:

- To which the confidentiality ('secrecy') of an informational asset is important for the effective pursuit of a national interest/objective;

- of negative ramifications on the pursuit of the interest/objective should the information be compromised;
- to which the integrity of the information – whether or not the content warrants secrecy – is important in the pursuit of the interest/objective in question; and
- to which the content of the information is of such a nature that it is a plausible target for adversarial espionage.

It must be emphasised that the counterespionage relevance of informational assets is not determined as a 'once-off' step of the execution of the CE environmental scanning at this stage. The tentative appraisal made at this point is subject to revision and more definite assertions later on in the scanning process.

6.1.3.6 Determine the custodians of the informational assets

The informational assets are usually within the primary custody of more than one own state entity. These entities include structures within the state apparatus, parastatals as well as and corporate entities (deemed as of national security relevance). While it features more prominently at relatively advanced phases of the CE environmental scanning process (notably Phases Ten and Eleven), the identification of custodians of information is done at this juncture.

6.1.3.7 Compile an inventory of findings

Lastly, the outcome of the preceding steps is recorded in an inventory. The latter normally comprises the detailed 'worksheets' as well as a summary thereof. A practical indication of what the 'worksheet' should approximate is provided in the next subsection (6.1.4).

6.1.4 The identification of critical informational interests and assets - opportunities and being proactive

In setting out the requirements with which the CE framework should concur, Chapter Four indicated the necessity of a proactive approach and a future directed time-orientation in the identification of espionage risks. The requirement of being proactive is moreover reflected in the definition advanced (in Chapter Four, Subsection 2.1.3; emphasis added) for an espionage risk as a "credible plausible situation, resulting from the activities of an opposing intelligence structure(s), which exists or may develop in a manner which significantly impedes a government's optimal pursuit of its national security strategy and the realisation of its objectives." Open-source CE scanning performed diligently thus enters the realm of estimative intelligence, forecasting and scenario building. One of the advantages, and requirements of the CE framework, it was also noted, is the delivery of “by-products from the counterespionage activity that are of the highest concern to positive intelligence” (Kent, 1949; 1966: 216). To concretely demonstrate the meeting of these requirements, and simultaneously practically illustrate notions advanced in this section (6.1), a scenario from the perspective of the hypothetical own state is used.

The scenario has as context the macro-environmental trends of growing demand and dwindling oil reserves which propel energy security to the centre of the security agenda of various nation states. The project team ascertained the own state’s self-reliance on oil supply as a national strategic security. [5] In the course of open-source collection and appraisal, indications emerged of significant Antarctic oil reserves as well as technological advancements that may enable the financially viable extraction thereof. Moving from the premise that the ‘tapping’ of these reserves would benefit the national strategic objectives of energy self-reliance, the project team formulates specific objectives and derives informational interests and assets. Although it would be provided in greater detail in actual counterespionage practice, the following example nevertheless conveys the outcome of this process:

[5] Note is taken of the definitional distinction between ‘national interests’, ‘national objectives’ and ‘national strategy‘ (Hough, 2006: 1-6, 15-16) and that – measured against strict definitional criteria – the use of the terms in the scenario sketching provided in Figure 39 could be contested. In the interest of simplification, the terms are employed without deliberating the definitional differences.

Figure 39: The proactive derivation of own state critical informational assets – a practical illustration

SECTOR	'INVENTORY' OF SPECIFIC OBJECTIVES	RELATIVE VALUE OF NATIONAL INTEREST [5]				INFORMATIONAL FACETS	CRITICAL INFORMATIONAL ASSETS
		I	V	M	P		
POLITICAL	International acquiescence on oil and mineral exploration and exploitation in the Antarctic, through a revision of the 1959 Antarctic Treaty and the 1991 Madrid protocol. Remark: In the interest of brevity, the term 'exploitation' is subsequently used in the table to denote exploration (geological surveying to determine resources), the commercial mining of minerals and commercial oil extraction.		**X**			Information on the own state's position and strategy, discussions with multi-state institutions, key nation states as well as other major international and domestic role players. Information on the position of multi-state institutions (e.g. United Nations – UN), key nation states as well as other major international and domestic role players. International law and conventions.	Information on the strategy and the negotiation 'bottom lines' of the own state and other role players. Information supporting and regarding the confidential negotiations between the own state and other role players.

[5] Key: Indispensible (I), vital (V), major (M) and peripheral (P).

SOCIAL	Support of the national populace for the exploitation of Antarctic resources.		X			Information on the sentiment of the national populace regarding Antarctic exploitation. Information on the position of opposition parties and lobby groups. Trends in media reporting.	The plans and activities of radical lobbying groups opposed to natural resource exploitation in the Antarctic region. The existence and substance of own state informational covert action to mobilise support. Adversaries' use of lobbying groups and the media for purposes of espionage and influencing (informational covert action).
TECHNOLOGICAL	Financially viable capacity to extract oil in unfavourable Antarctic conditions (such as the geographical source-rock structuring and reservoir maturation). Longer-term, non-fossil based energy-generation alternatives.	X	X			Open and secret information concerning technological advances by other nation states and the private sector in mining and oil extraction in conditions comparable to those in the Antarctic. Information (open and secret) relating to the own state's research programmes into mining and oil extraction in conditions comparable to those in the Antarctic. Macro-environmental infomation on viable studies into non-fossil based energy-generation	Information obtained by the own state through espionage on leading-edge technology being developed by other role players for viable mining and oil extraction in the conditions mentioned. Information on the unique technology being developed in this regard as part of own state research programmes.

						alternatives. Information emanating from (an own) state-sponsored academic research into hydrogen production.	
ECONOMICAL	Energy self-sufficiency and a longer-term positive balance of payments.	**X**				Data and information with a bearing on the own state fiscal and monetary status and planning for the improvement thereof. Information central to successful negotiations in securing preferential loans in financing the own state current account deficit. Information on the strategic energy (oil and uranium) reserves of the own state.	Own state negotiation strategy as well as sensitive ‘trade-offs’ (such as the sharing of strategic weapons technology) for preferential-rate financing from other nation state(s).
MILITARY	Combined armed forces, expeditionary capacity able to project offensive combat power internationally in general. Expeditionary capacity able to project military power specifically in Antarctica.	**X**	**X**			All-source information required by the military to prepare, deploy and sustain a military presence in the protection of supply routes to as well as potential (future) national interests in Antarctica.	Strategic and military assessments on the protection of supply routes and Antarctica as a military theatre of operation. Plans of deployment and operation in Antarctica as well as the size and the capacity of a rapid deployment force.

						Information regarding military readiness, contingency planning, adjustment in weaponry (for effective use) in Antarctica.	
ECOLOGICAL	Expanding national mineral and energy resources.		X			Open and secret information on the mineral resources and oil reserves within the Antarctic region.	Privileged information obtained through secret methods on mineral resources and oil reserves in Antarctica.
	Limiting the ecological impact of mining and oil exploitation.			X		Open and secret information regarding the ecological impact of mineral and oil exploration in the Antarctic region.	Secret information not in the public domain on the extensive detrimental impact of mineral and oil exploitation in Antarctica

INFORMATIONAL	Effective informational systems/ repositories and the integrity thereof.	X				All of the above.	All of the above.
	The own state's reputational integrity and communication strategy.		X				
	Open and secret intelligence and counterintelligence capabilities and activities (HUMINT & TECHINT)	X					
	Informational covert action capacity and initiatives.		X				

6.2 THE IDENTIFICATION OF PREMIUM INFORMATIONAL AREAS IN THE MACRO-ENVIRONMENT

Whereas the preceding subphase of CE environmental scanning involved the introspective scanning of the own state, this subphase focuses on the macro-environment retrospectively. Notwithstanding the differentiation between 'informational assets' and 'informational areas', the intricacy and the extent of the process followed in relation to one role player (the own state), combined with the prospect of scanning the macro-environment with its multiplicity of actors, bring to the fore the recurring theme of reconciling the theoretically conceivable with the practically attainable.

6.2.1 A motivation for premium informational areas as focal point

A theoretical 'ideal-type approach' [6] would hold the process of delineating premium informational areas in the macro-environment as concurring in logic with that followed in ascertaining own state critical informational assets. Premium informational areas would thus be ascertained by the outcome of a process that considered the security perceptions of macro-environmental role players, their multi-sectoral interests and objectives as well as inferences made from 'imbedded' informational facets. Environmental scanning modelled on this constructed ideal of the theoretically conceivable would require the scrutiny of multiple macro-actors and widen the spectrum of open-source CE scanning to an unattainable proportion. Resources required for such scanning would exceed not only those typically assigned to parallel projects, but also the (all-source) resource capacity of many an intelligence service.

A micro-theory is the intermediary between theories of higher abstraction and praxis. It is therefore on this level that a feasible approach should be proposed. Although the external environment was superficially probed (in Phase Three), it is during this subphase that the 'door' to the scanning thereof is 'opened'. Since the choice of a 'point of entry' will decisively influence subsequent phases, options should be weighed. One such option – and perhaps the one most frequently used – is the 'entry' of the macro-environment through the selective scanning of a limited number of macro-environmental role-players. The posing of macro-environmental role-players as the focal points, at this juncture, would be nothing more than transposing

[6] The term 'ideal-type' is used here as referring to an idealised construction of the 'achievable' and not in its sociological (Weberian) definitional connotation.

the earlier contested adversary-centric default to open-source environmental scanning. As a further alternative, the already determined own state's critical informational assets can be considered as an angle of approach. This position has two distinct disadvantages – both stemming from the particularised nature of own state critical-informational assets. Firstly, if used as a point of entry, this approach carries an unacceptably high risk of compromise. Secondly, the particularised nature of informational assets could 'tunnel vision' the focus of the CE scanning and distract from the requirement to provide fresh insights and a broader perspective.

The option favoured by this study in 'entering' the external environment, through the notional prism of the 'informational areas', presents the following advantages:

- It is guided, but not blinded or 'tunnel-visioned', by the nature of the own state and its informational assets;
- although dovetailed with the preceding subphase, its focus on external (macro-environmental) informational areas carries a low risk of compromise; and
- the approach is sufficiently wide in providing fresh insights, yet not so broad in spectrum that it borders on the unattainable.

6.2.2 The methodology for ascertaining premium informational areas

The discussion of the execution stage of the CE scanning has thus far mainly been conducted on a notional level. In some instances (such as contained in the next subsection – 6.2.2.1) micro-theoretical clarification and recapitulation would still be necessary. In the main, however, the methodology in ascertaining premium informational areas, as well the discussion of the subsequent phases of the execution of the CE framework progressively relies more on the illustration of the process by means of examples. Such elucidations should not be construed as purporting to be case studies. The demonstration of the CE framework by a credible case study would require specialised knowledge and extensive research of several nation states, non-state actors and societal sectors. In addition, a case study would restrict the flexibility in the generic application of the CE framework. Most importantly perhaps, a case study that complies with answerable academic criteria, would add complexity, rather than aid in simplifying the further explication of the CE environmental scanning process.

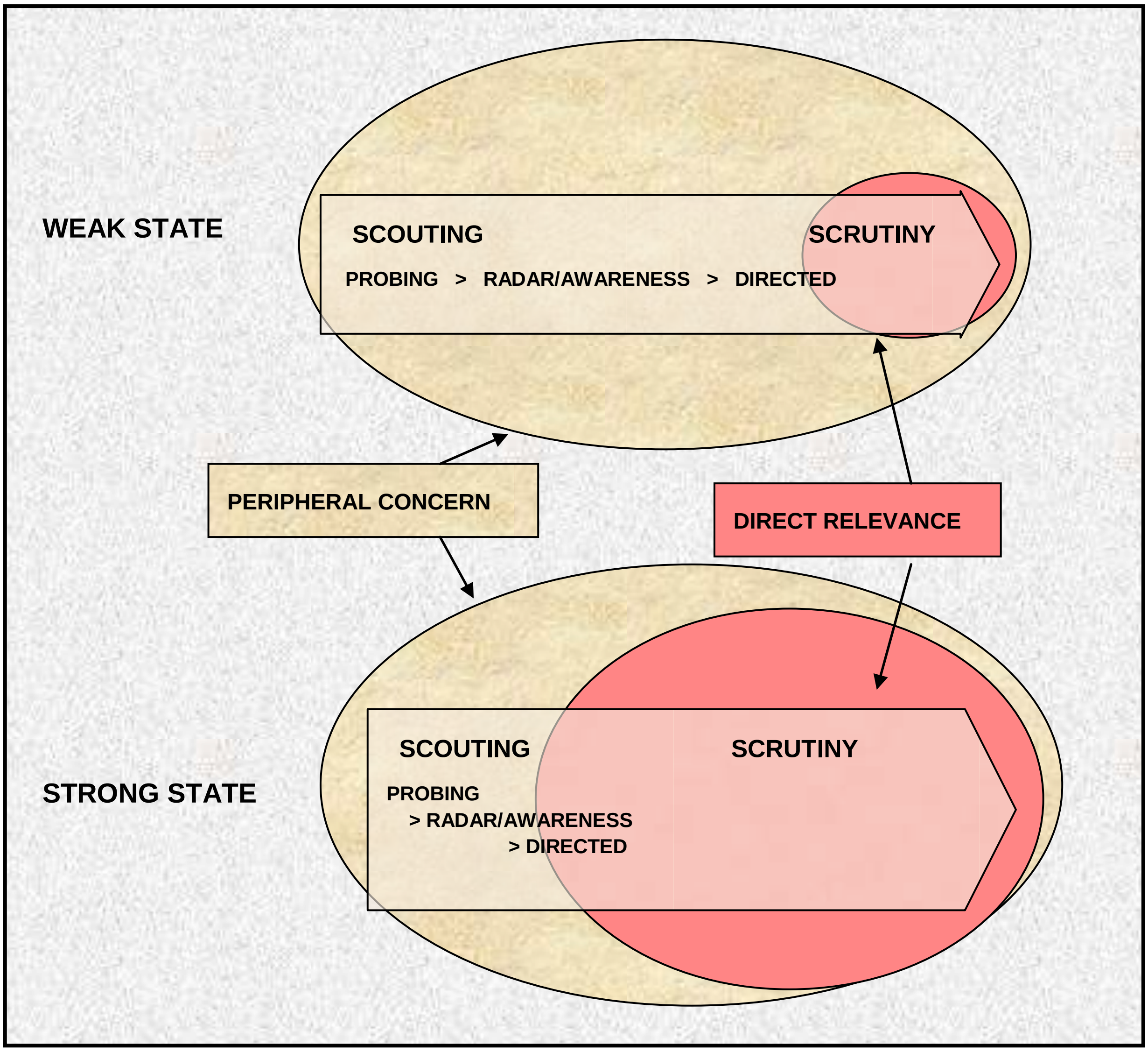
6.2.2.1 *Consider the nature of the own state and its interests*

The methodology of ascertaining premium informational areas, as was noted, is interlocked with the preceding subphase. The delineation of premium informational areas sets out with the calibration of the resolution of the CE framework in accordance with both the nature of the own state’s interests and the stratified macro-environment.

For purposes of CE environmental scanning the ‘total environment’ is not an absolute and constant entirety. It can be stratified in line with the nature of the own state, and the resolution (intensity of scanning) of the CE framework can be adjusted accordingly. While more nuanced in practice, the distinction made in the stratification of the macro-environment for CE scanning is simplified into the two main spheres respectively: ‘direct security relevance’ and ‘peripheral concern’. With reference to Buzan (1991: 6, 16, 18,102-103, 134) and Johnson (2003: 638-641), Chapters Two and Three showed the ’nature of the own state’ as determined by the interplay of variables that, to name but a few, include: geographic location, domestic homogeneity and social-political cohesion, natural resources, technological advancement, infrastructure, economic wealth, international presence and involvement. These variables were furthermore examined and a distinction was made between ‘weak’ and ‘strong’ states. These differences between states and their influence on national security were discussed earlier and are thus not further elaborated on. Important here are the implications of these differences to this phase (Four) of CE environmental scanning which centres on the area of convergence between the own state’s multi-sectoral interests and those of other role players. A strong state, such as the US, has interests that are expansive in various respects. These interests are geographically vast, physically extensive (i.e. measured strategically as well as being ‘financially quantified’) and substantive in all sectors (political, military, social, technological, economic, ecological and informational). At the other end of the continuum, the interests of a weak, undeveloped state such as Swaziland are vastly more limited.

For strong states with vast interests, the macro-environment of the ‘direct security relevance’ area is extensive and ringed by a narrow zone of ‘peripheral concern’. Conversely, for weak states, the core of ‘direct security relevance’ is small, but the band of ‘peripheral concern’ proportionally much wider. The stratification of the macro-environment and the implications thereof on the CE scanning focus resolution can be illustrated as follows:

Figure 40: The stratification of the macro-environment in accordance with the nature of the own state



Given the globalised security order, even weak states cannot afford to be oblivious of the whole of the macro-environment in the demarcation of informational areas at premium in the macro-environment. CE scanning calls for a pragmatic balance, but not a compromise, between generality and specificity in the calibration of its focus. ‘Scouting’ employed in determining premium informational areas is already less granulated than ‘scrutiny’ employed in ascertaining own state informational assets. In addition, ‘scouting’ is an umbrella term for, in ascending order of intensity: ‘probing’, “radar/awareness” and “directed” viewing” (Pollard, 1999: 13, 65). While ‘probing’ and ‘radar/awareness’ are maintained in terms of the peripheral zone, ‘directed’ scouting, for the identification of premium informational areas, is reserved for the segment of direct, national-security relevance.

Since the nature of the own state decisively influences the identification of premium informational areas, some assumptions are required for further elucidation. The hypothetical own state is a strong, economically prosperous and technologically advanced country. While substantive, and relative to its techno-economic interests, its own (interests) in the socio-political and military spheres are more limited. In this, the own state is reminiscent of a country such as Japan – but since this is hypothetical it should not be construed as such. Using the same qualification, the own state's technological interests and assets resemble those of the US. Accordingly, most of the specific examples mentioned, and various inferences drawn, are based on US primary sources (US, 2007*e*: 1-7; US, 2007*g*: 2-18, 26; US, 2006*c*; 2006*d*, 2004*c*: 34-35, 75,111-116), but freely adapted to the needs of the study. Insofar as opposing espionage-relevant role players are concerned, the own state proximates typical prosperous Western nation states that, in addition to the US, include the UK, Germany and Canada.

Adding to the state's hypothetical nature, and for practical considerations, the secondary sources used in the 'construction' of the own state are biased towards, but not limited to, the national security perspective of Western powers in general. Secondary sources utilised to inform this generalised view include the following: Burgess, 2008 (1-10); Mena, 2003 (xv-xvi, 15, 37-38, 301-302); Nasheri, 2004 (8-9, 16-21); Edwards, 2006 (1-22); Hoffmann, 2007 (2-4); Kitfield, 2007 (1-7); and Rennstich, 2003 (1-18.) Because of its hypothetical construction, the examples subsequently provided do not always refer in detail to the sources from which inferences (regarding the own state and its national security context) were derived at. Lastly, the hypothetical examples should be interpreted against the backdrop of the '21st century reality of espionage and counterespionage' outlined in Chapter Three.

6.2.2.2 *Appraise and prioritise sectors*

The interwoven nature of sectors, previously indicated in relation to the own state, is naturally equally applicable to the macro-environment. Since sectors are interlinked the appraisal of one sector will inform the identification of premium informational areas in one or more. Although all relevant sectors need to be appraised, finite resources dictate that those with the highest priority need to be scouted first, and with a sharper resolution. The prioritisation of sectors is guided by three criteria, namely:

- The relative premium attached to sectors in the macro-environment. There would be little opposition to the assertion that there is no sector in which espionage does not manifest. However, a generalised perspective of nation states being comparable to the own state requires that the sectors in which espionage is most prevalent need to be identified. To this end, the sources and methodology of Comparative Intelligence are (Section 5.3, Chapter Six), as with other steps and phases, indispensable.

- The importance of a sector gauged against the own state's national security and prosperity. Chapter Four indicated 'plausible impact' as the pivotal prioritisation criterion from a counterespionage perspective. In this instance, the project team, which at this juncture has already established the own state's multi-sectoral interests and assets, considers the following criterion: In which sector(s) are those critical informational assets predominately located, which, if compromised through espionage, would have the most detrimental impact on national security and prosperity?
- The mandate of the intelligence service. Based on the assumption of this being a civilian intelligence service, the military sector, although not negated in its entirety, is not a foremost priority. Information emerging during the scanning, in relation to the military sphere will in practical terms be noted for utilisation later (Section 6.4.3, Chapter Six) but not fleshed out in detail.

Guided by the above criteria, the project team can proceed with the appraisal and prioritisation of sectors. Sources consulted (by the project team) are in agreement that foreign intelligence services continue to aggressively target the political, military and economic spheres, but also that the prominence of the technology sector is increasing exponentially. This trend is reflected in the US's (2007*g*: 5; emphasis added) assertion that: "[t]he most critical areas include future military and political intentions, military capabilities and vulnerabilities, economic and commercial policies, and foreign policy initiatives. *Increasingly, however, technology ranks high in foreign collection priorities*."

In the prioritisation of sectors, the CE framework considers not only foreign intelligence services but takes a panoptic view that considers the importance attached to information by other categories of actors also. From this 'all-actor' perspective, the project team concurs with the following assertion by Nasheri (2004: 19): "Now, espionage activities have largely shifted to concentrate on technology, manufacturing processes, and other trade secrets that sometimes have dual use, but often only civilian application." The civilian intelligence mandate of the intelligence service conducting the CE environmental scanning process, moreover, reinforces a tentative proposition of the technological sector as the foremost priority. This tentative assertion is subsequently benchmarked against, and found to be reinforced by, the assessments of civilian intelligence services of nation states comparable in nature to the own state (Burgess, 2008: 1-10: UK, 2008: 10-24; UK, 2007: 57-66; US, 2004c: 34-35, 75, 111-116; Canada, 2003: 3-7; Germany, 2005: 264-285). In addition, the technological sector, together with the economic sector, is gauged as pivotal to the own state's national security and prosperity. These two sectors, as all others, are symbiotically linked with the informational sector. Consequently, the top three priorities opted for are the technological, economic and informational sectors.

Although substantive, the own state's interests in the socio-political and military spheres are more limited. On this basis, and in order of declining primacy, the prioritisation of sectors decided on for further CE scanning is as follows: technological, economic, informational, political, military, social and ecological (environmental). The technological sector as the leading priority is hypothetically used as an example in further illustrating the ensuing subphase of determining and prioritising subsectors.

6.2.2.3 *Determine and prioritise categories (subsectors)*

The technological sector is wide-ranging and multifaceted. CE environmental scanning therefore needs to ascertain the specific subsectors within which information is prized. The own state's technological interests in certain respects concur with those of the US, and open-source collection includes the procurement of applicable official sources emanating from this country. The project team establishes the US (2006*d*, 2006*e)* as regarding the following twenty subsectors (in alphabetical order) as at premium from a counterespionage perspective: aeronautics technology; armaments and energetic materials technology; biological technology; biomedical technology; chemical technology; directed and kinetic energy technology; energy systems technology; electronics technology; ground combat systems technology; information systems technology; lasers and optics technology; manufacturing and fabrication technology; marine systems technology; materials and processing technology; nuclear technology; positioning, navigation, and time technology; sensors technology; signature control technology; space systems technology, and weapons effects technology.

Although all at premium, subsectors are not equal within the context of the CE framework. They are neither equal to the degree to which they are prized in the macro-environment nor in relevance to the own state. Considering both these criteria the subsectors are thus to be prioritised by the project team. According to a recent

US official survey (2006*c*: 7), the information system technology was targeted “at a rate almost twice that of any other technology category”. The other nine technologies constituting the ‘top ten’, in order of declining frequency of targeting are, according to the US (2007*g*: 4-5; 2006*c*: 2-27):

- Lasers and optics technology;
- aeronautics technology;
- sensors technology;
- armaments and energetic materials technology;
- electronics technology;
- space systems technology;
- marine systems technology;
- materials and processing technology; and
- signature control technology.

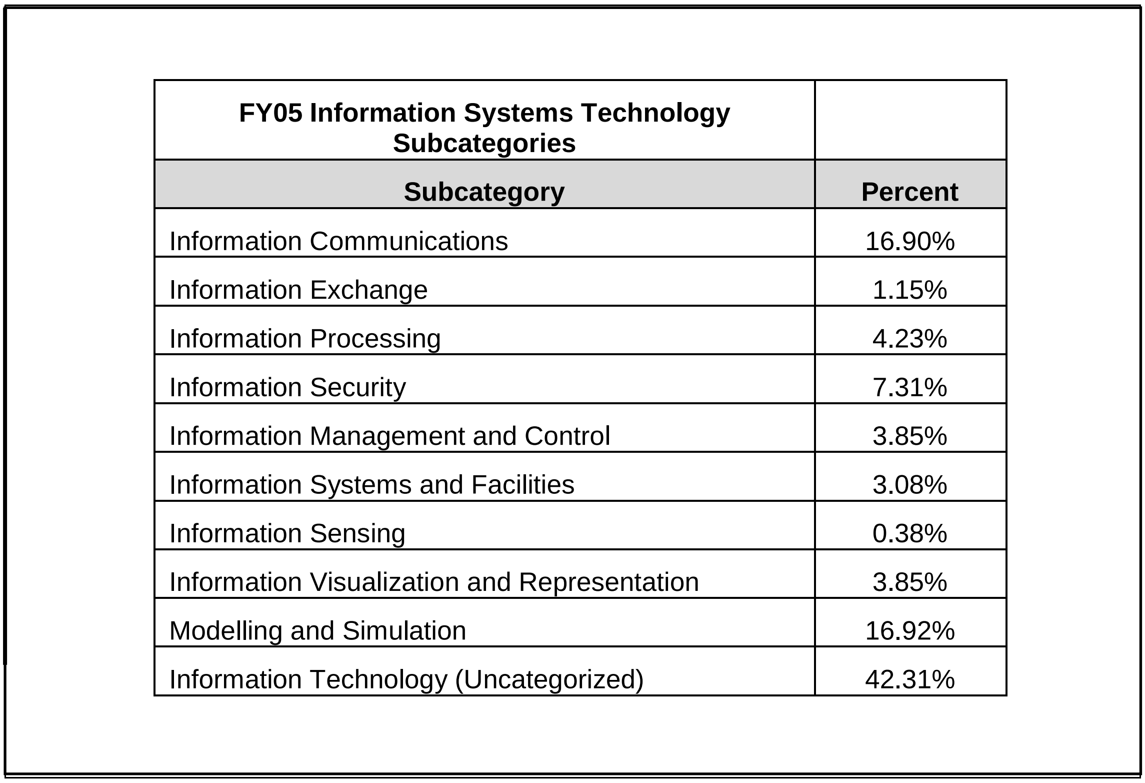
Although not as detailed or quantified, the assessments of various other prosperous nation states echo the views of the US in the importance it attaches to the informational system technology as a cluster of critical informational assets and concur that this subsector is increasingly targeted by adversarial espionage actors (Burgess, 2008: 1-11; UK, 2007: 37, 57-67; UK, 2008: 20-21; Germany, 2005: 264-285). The own state is no exception and the project team identified ‘information system technology’ as the foremost priority. The remainder of the US ‘top ten’ can, however, not summarily be applied to the own state. The technological specialisation within the own state’s economy differs in certain respects from that of the US. Military-related technology, for one, does not feature as prominently. Employing both criteria mentioned the following are regarded as the five most crucial priorities: information system technology, electronics technology, manufacturing and fabrication technology, lasers and optics technology, and energy systems technology.

6.2.2.4 *Ascertain informational areas at premium in the macro-environment*

Starting with the ‘top five’, the CE scanning process proceeds to dissect the subsectors in order to identify the specific aspects within subsectors that are at premium in the macro-environment. For illustrative purposes the discussion is limited to ‘information systems technology’.

Open-source information gathered to inform the projects team’s appraisal of the ‘information systems technology’ subsector include the following extract from a US (2006*c*: 1, 7) official publication that lists the informational areas most frequently targeted by “foreign entities”:

Figure 41: Premium informational areas – information technology sub-categories



FY05 Information Systems Technology Subcategories	
Subcategory	**Percent**
Information Communications	16.90%
Information Exchange	1.15%
Information Processing	4.23%
Information Security	7.31%
Information Management and Control	3.85%
Information Systems and Facilities	3.08%
Information Sensing	0.38%
Information Visualization and Representation	3.85%
Modelling and Simulation	16.92%
Information Technology (Uncategorized)	42.31%

Source: US, 2006c: 7 (adapted).

The information contained in the table is, as during preceding steps, assessed against the background of the own state's national security context, its civilian intelligence service's mandate, as well as other open-source information in the macro-environment. Information procured suggests 'information security technology' as the informational area which is currently and for the foreseeable future, most at premium in the macro-environment (Mena, 2003: xv-xvi, 15, 37-38, 301-302, 423; US, 2007*e*: 1-7; US, 2004*c*: 38-42, 97; Hoffman, 2007: 2-4; Burgess, 2008: 1-10; Rennstich, 2003 1-18). In this hypothetical scenario, 'information security technology' is, judged against the macro-environmental premium, followed by 'information communications', 'modelling and simulation technology', 'information systems and facilities technology', 'information systems and facilities', and 'information management and control technology'. 'Modelling and simulation technology' is closely associated with weapon development programmes (US, 2006*c*: 7) and is thus excluded from in-depth CE scanning. The following are thus concluded to be the top five informational areas (within the information systems subcategory):

- Information security technology;
- information communications;

- information systems and facilities technology;
- information systems and facilities; and
- information management and control technology.

6.2.2.5 *Particularise the prioritised premium informational areas*

Although the objective to identify premium informational areas has been met, the project team could opt to particularise informational areas. Referring to information security technology, the following simplified question could be asked: From a counterespionage premise, what precise elements of information security technology are at premium? At this juncture of the CE scanning process, the 'picture' would be incomplete and fragmented. A decision to proceed with the particularisation of informational areas (as part of Phase Four) will thus largely depend on the nature and extent of open-source information collected up to this point.

Depending on the resources, time allocated to, and the expertise of the project team, two options are possible. The first involves the identification as well as the detailed description of particularised technologies. The project team could embark on the compilation of data sheets on particular technologies that would have the following as some of their main themes: technological parameters, critical materials, unique software, major commercial and other applications, as well as technological affordability (US, 2006*d*: v). The development of such datasheets is on a praxis level, and this study suffices with listing the following tabulated examples of technologies on which they would be compiled in relation to informational security:

Figure 42: Information security technology – listing of particularised technologies on which data sheets are compiled

CRYPTOLOGY	CRYPTOGRAPHIC PROTOCOLS AND TECHNIQUES
• Mathematics • Distributed key generation • Elliptic curve system security • Deterministic random number generation • Message integrity and non-repudiation • Stream ciphers • Quantum cryptography	• Electronic money transfer • High-speed encryption • Key management • Key recovery system failure mode and effects analyses • Secret sharing schemes • Zero-knowledge proofs • Digital data stenography

<u>Source</u>: US, 2006*d*: 1-5, 7, 11, 29 (adapted).

As a second option, the project team could suffice with the mere listing of particularised technologies. In the case of information security technology, the table above will be deemed to be adequately detailed.

6.3 THE IDENTIFICATION OF MACRO-ENVIRONMENTAL ROLE PLAYERS

The information located within sectors, subsectors and areas is – to restate the obvious – sought by certain macro-environmental role players. The identification of these role-players is not a sequential step from, but performed in conjunction with, the steps outlined above (Subsection 6.2.2, Chapter Six). The importance of and *rationale* behind this indirect approach in identifying macro-environmental role players was discussed in Subsection 6.2.1 (Chapter Six). The exclusion of macro-environmental role players in entitling this phase and subphase is intentional, and underscores the aim to use informational areas as the point of entry into the macro-environment. This emphasis is also reflected in the graphical outline of this phase (Figure 37, Chapter Six).

6.3.1 Open-source limitations in determining macro-environmental role players

Since the identification of macro-environmental role players is a concurrent subprocess, it is performed in the indicated order of ascending specificity, namely sector level, subsector level and finally on the level of informational areas. While the identification of macro-environmental role players – like the demarcation of informational sectors, subsectors and informational areas – draws on Comparative Intelligence, open-source limitations (relative to those faced in the demarcation of informational areas) are more marked.

In open societies, the counterintelligence programmes of statutory intelligence services endeavour to establish an awareness of the national security relevance of certain bodies of information. To this end, and as it transpired in the preceding discussion, these bodies of information obviously need to be (partially) described and disclosed. Counterintelligence awareness programmes, the annual and *ad hoc* reports of the statutory intelligence service as well as secondary sources informed by such information, thus provide a substantive open-source base for the identification of informational areas with a degree of relatively high specificity.

Open-source literature on the ‘linking’ of informational areas with specific macro-environmental role players is markedly and understandably more limited. In the US, for example, freely available and voluminous compendiums exist in which critical informational areas are demarcated in detail. These compendiums and other official documentation, however, do not divulge adversarial espionage actors with a degree of detail propositional to the specificity with which the informational areas are described. Instead, a document such *as Technological collection trends in the U.S. defence industry* suffices with general references to the categories of adversarial espionage actors and a geographic breakdown of regions where adversarial collection efforts originated from (US, 2006*c*).

The parsimony in linking espionage actors with pertinent informational areas and assets is not only understandable but also sound counterintelligence practice. Detailed 'interconnection' could jeopardise a state's investigations and CE operations. In some instances, even if it were not for operational considerations, public exposure may have negative ramifications for the state's broader (and predominantly beneficial) relationship with certain actors. Should it be deemed as not being detrimental to their own broader interests, nation states do cite some macro-environmental role players' targeting of their informational assets in publicly available documentation. In line with the tortuous logic of CE, the public disclosure of espionage actors, their activities and targets could, under certain circumstances, as discussed in Chapter Four (Section 6.6), also be a counterespionage neutralisation method. In the main, however, public disclosures of espionage actors and their pertinent targets (i.e. on the 'informational area' level of specificity) represent only a small fraction of detected espionage cases.

For the larger part, such 'linking' in documentation in the public domain is done mostly at the sectoral and subsectoral level. However, regarding the technological and economic sectors, and while still parsimonious, open-source identifies opposing nation states mostly by name. While the prominence of corporate entities as espionage actors is widely noted, the exposure of the identities of specific role players is in short supply. Insofar as liberal democracies are concerned – from which most of the sources used in this study emanate – this tendency can safely be assumed as ascribable to legal considerations. Should a nation state not have compelling evidence of a corporate entity (or other non-state actor) engaged in espionage it will not be prepared to submit such evidence, as claims to this effect could result in litigation (against the state). It is also for this reason that examples, provided at a later stage in the study, mostly refrain from identifying specific companies and/or other non-state actors.

The aforementioned limitations do, however, not imply that determining the interconnectedness of macro-environmental role players with informational areas as being entirely out of the reach of the open-source ambit. Grey sources – earlier noted as being part of open sources for purposes of CE scanning – are exceptionally helpful but, for reasons discussed in (Section 8, Chapter Six), cannot be used in illustration. The linking of macro-environmental role players with informational areas is also partly achievable through the use of 'pure' (in other words conventionally defined) open sources. Although possibly incomplete, certain pieces of the 'jigsaw puzzle' can be constructed through meticulous gathering, exacting analysis and astute inferences.

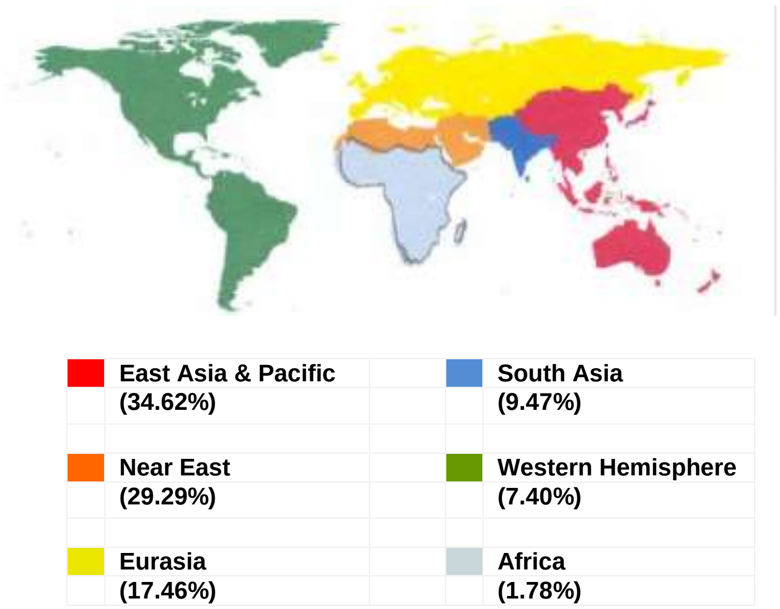
To ensure that focusing on espionage risks of the highest concern remains paramount, the CE environmental scanning project team could opt for the identification of macro-environmental role players on the sectoral and subsectoral level during this phase (Four), and reserve the linking of informational areas with 'informational areas' to prioritised actors. In practical terms, interlinking espionage actors with particularised informational areas would thus be performed in Phase Five ('identification and profiling of plausible espionage principals'). The illustration of the CE scanning process in the subsequent subsection and phases is based on the assumption that the project team indeed opted for this alternative insofar as the technological sector is concerned.

6.3.2 A selective illustration of determining macro-environmental role players

Moving from this assumption, the project team continues with identifying macro-environmental role players that place a high premium on information in all the sectors and subsectors prioritised in the course of the process described in Subsection 6.2.2 (Chapter Six). In keeping with earlier examples, the illustration of the identification of macro-environmental role players is restricted to the information system technology subsector.

The information collected by the project team includes the specifics represented in the following figure that proximates espionage collection attempts against the US with the geographic regions from where they originated:

Figure 43: Information systems technology: collection activity by region



Source: US, 2006*c*: 8.

In the appraisal by the project team it is revealed that the figure (map) reveals a deficiency in two respects. Firstly, it is presented from a US counterespionage perspective and therefore does not reflect the US as the principal espionage actor in the information system technology subsector. Secondly, and validating the contentions made in the preceding subsection, the figure is not sufficiently granulated in that no specific actors are identified.

Cognisant of the ToR's stipulations that require the CE framework to consider all categories of macro-environmental role players, the project team continues with further scanning. Additional sources consulted in this scanning process, to name but a few, include: Nasheri, 2005: 4-5, 9-10, 16-48; Wettering, 2000: 269-294; Burgess, 2008: 1-16; Canada, 2003: 2-7; Germany, 2005: 264-285; US, 2007*b*: 1-3; US, 2007*g*: 2-18, 26; US, 2005*b*: 486-488; US, 2004*c*: 97, 51-52, 111-116; Williams, 1997: 321, 327, 333; Kitfield, 2007: 1-7. The outcome of the further scanning can be summarised in tabulated format:

Figure 44: Subsector (information system technology): macro-environmental role players

ROLE PLAYER CATEGORY	ACTORS IDENTIFIED
Nation states	US, PRC, Russia, France, Japan, India, Germany, the UK, Pakistan, Cuba, Italy, Belarus, Israel, North Korea, South Korea, the Ukraine, Libya, Egypt, Georgia, Iran, Iraq, Libya and Syria,
Corporate entities	US-based information technology company 'X'. French parastatal 'Z'. PRC state-owned company 'Q'. Japanese multinational companies: Mitsubishi, Toshiba, Ishikawajima-Harima and Nissan (US, 2007*g*: 26: Nasheri, 2005: 20).
Criminal groupings	Russian organised crime syndicates 'X' & 'Y', Japanese yakuza – syndicate 'Q'; Columbian cartel 'R'; Nigerian criminal organisation 'Z' and La Cosa Nostra 'T' grouping.
Terrorists and extremists	Hizbollah and al-Qaeda

This subphase of the CE environmental scanning process centred on ascertaining the counterespionage-relevant bodies at premium in the macro-environment. It was found that open sources allow for the relatively detailed delineation of the bodies of information *per se*. The subphase proceeded to juxtapose the information prized in the macro-environmental with specific actors. Given open-source limitations, the degree of specificity to which this is practicably attainable varies and would generally require CE environmental scrutiny of prioritised macro-environmental role players. This prioritisation is among the aspects addressed in the next section.

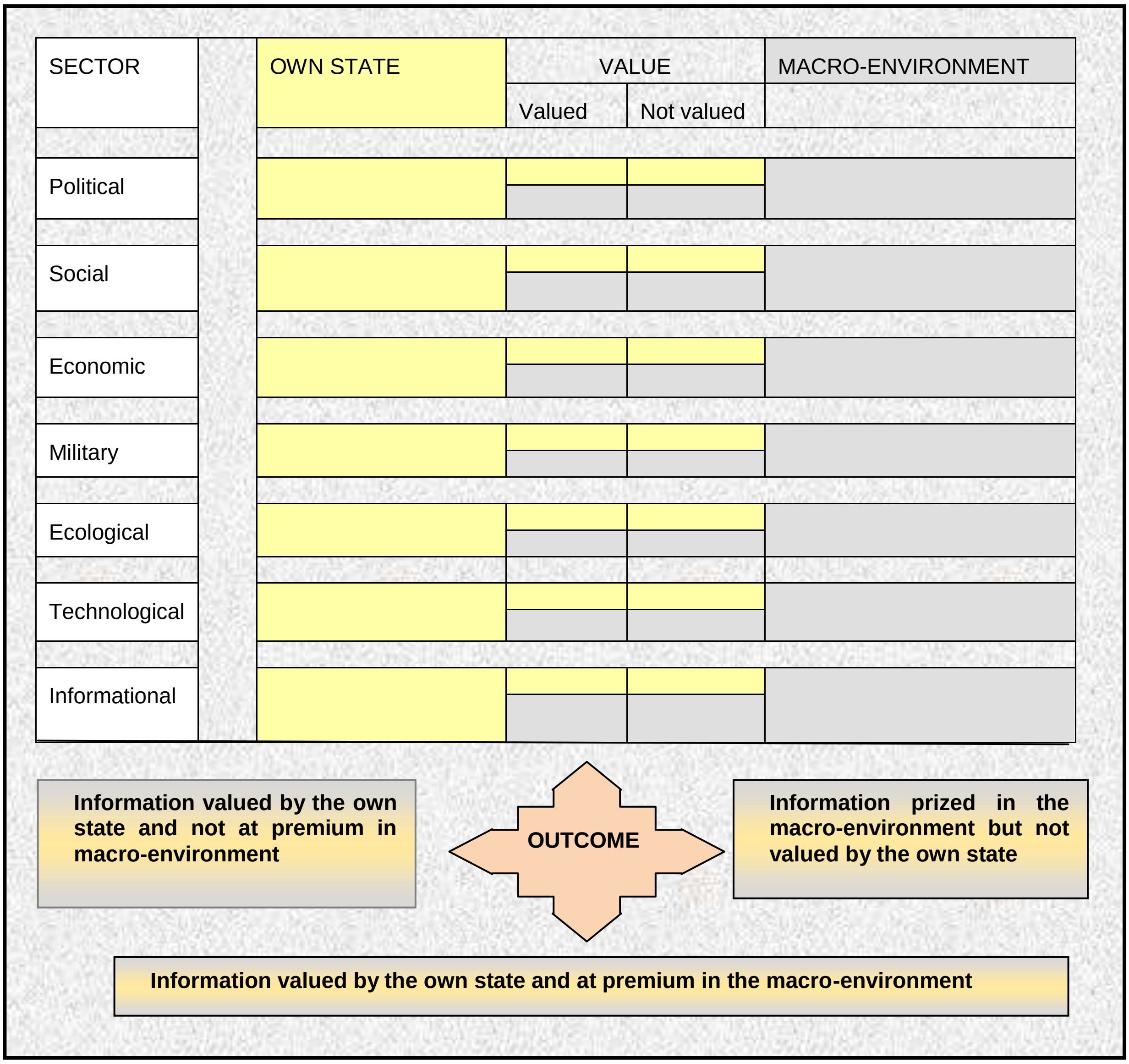
6.4 THE CONDUCTING OF AN INTEGRATED APPRAISAL

Through the preceding subphases two extensive sets of counterespionage-relevant bodies of information were demarcated, namely those valued by the own state and those at premium in the macro-environment. The utility of each respective set (individually), in general, and the reasons for asserting on own state informational interests to the 'fine resolution' of particularised informational assets, specifically, will transpire in the subsequent phases of the CE scanning. During this subphase, the considerable effort expended in demarcating these bodies of information is justified by the benefits derived from a comparative appraisal The outcome of this comparison not only informs the prioritisation of macro-environmental role players for scrutiny (during Phase Five), but also lays the foundation for an appraisal of the own state's vulnerabilities to adversarial espionage.

6.4.1 The prioritisation for the scrutiny of macro-environmental role players through open-source counterespionage environmental scanning

The prioritisation of macro-environmental role players, as suggested, is primarily informed by the outcome of a comparative appraisal. The following is proposed as a matrix for the conceptual structuring of this comparison:

Figure 45: Conceptual matrix: juxtaposing own state informational assets and macro-environmental premium-informational areas (sectoral)



SECTOR	OWN STATE	VALUE		MACRO-ENVIRONMENT
		Valued	Not valued	
Political				
Social				
Economic				
Military				
Ecological				
Technological				
Informational				

Information valued by the own state and not at premium in macro-environment

OUTCOME

Information prized in the macro-environment but not valued by the own state

Information valued by the own state and at premium in the macro-environment

In line with the matrix, the own state's informational assets and bodies of information are at premium in the macro-environment. This task will of course be performed by a sizable project team that benefits from sources not available to this study. A comprehensive illustration of the comparison is thus clearly not achievable within the confines of this academic study, therefore the following illustration of the application of the matrix is hypothetical and highly selective:

Figure 46: Selective illustration of the comparative appraisal of own state informational assets and premium macro-environmental informational areas – technological subsectors

SUBSECTOR	OWN STATE	VALUE		MACRO-ENVIRONMENT
		Valued	Not valued	
Information system		✔		US, PRC, Russia, France, Japan, India, Pakistan, South Korea, the Ukraine. Companies 'X', 'Y', 'Z'. Russian organised crime syndicate 'X'. Japanese yakuza' X'.
		✔		
Electronics		✔		US, PRC, Japan, India, Germany, Italy, Indonesia, South Korea, Ukraine. Companies 'Q', 'R', 'T'. Japanese yakuza 'X'.
		✔		
Nuclear			X	US, PRC, Russia, France, India, Pakistan, Cuba, Israel, North Korea, Libya and Syria. Companies 'Q', 'Y'. Russian organised crime syndicate 'X'.
		✔		
Lasers and optics		✔		US, France, Japan, Germany, Italy, South Korea, Ukraine, Egypt, Georgia. Companies X', 'W', 'V'.
		✔		
Energetic materials			X	US, PRC, Russia, France, India, UK, Pakistan, Cuba, Israel, North Korea, Libya, Egypt, Iran, Iraq, Libya and Syria. Companies 'Q', 'T', 'W'. Russian organised crime syndicate 'X'.
		✔		

In addition to being highly selective, the comparison above is a micro-theoretical elucidation and simplification of the intricate process conducted in counterespionage practice. In practice, to name one example, the value assigned to bodies of information could vary from indispensable and vital, to major and peripheral. Albeit in relation to the ranking of the interests, this nuanced distinction was demonstrated in Figure 39 (Chapter Six). On a micro-theoretical level, the implications of the comparison take precedence over such a nuanced distinction. These relate to the clustering of bodies of information in line with the following outcomes:

- Information valued by the own state and at premium in the macro-environment;
- information prized in the macro-environment but not valued by the own state; and
- information valued by the own state and not at premium in the macro-environment.

While all three clusters have implications for the CE scanning process, the prioritisation of macro-environmental role players takes as premise 'information valued by the own state and at premium in the macro-environment'. To enable such prioritisation, the bodies of information ascertained as prized by the own state and in the macro-environment are restructured on a role player *per* role player basis. The following (once again highly selective and hypothetical), serves as an example:

Figure 47: Prioritisation of macro-environmental role players

		BODIES OF INFORMATION VALUED BY THE OWN STATE AND IN THE MACRO-ENVIRONMENT **(Described to highest level of specificity as ascertained in relation to specific actors/sectors)**			
		POLITICAL	**TECHNOLOGICAL**	**ECOLOGICAL**	**SOCIAL**
ROLE PLAYERS	**PRC**	Strategy and position (of the own state) *re* "One China" (Taiwan).	Materials and processing technology. Information security technology. Information communications technology. Information systems and facilities technology.	Own state strategy and intentions: Exploitation of Antarctic resources. Own state strategy and 'bottom lines': Carbon emissions restrictions.	Chinese émigré community: Radicalisation of lobby groups on Tibet.
	Company 'X'	Intention (of own state political leadership) on the expansion nuclear power generation.	None identified.	Own state current and projected strategic energy reserves.	Intelligence on extremist opposition to nuclear power generation.

	Organised crime group ‘Z’	State’s intentions (legislative and governance) on the curbing of organised crime. Intelligence databases on organised crime grouping Z.	Information security technology. Information systems and facilities technology.	None identified.	None identified.
	NGO ‘Y’	Intention (of own state political leadership) on the nuclear expansion power generation.	None identified.	Own state strategy and ‘bottom lines’: Carbon emissions restrictions. Own state strategy and plans: Exploitation of Antarctic resources.	Government’s informational covert action initiatives to lobby support for nuclear power generation.
	Extremist grouping ‘Z’	Intelligence databases on extremist grouping ‘Z’.	Information security technology.	None identified.	None identified.

Several quasi-quantitative and ‘easy-step’ methods can be conjured up for prioritising the macro-environmental role players so listed for further CE scanning. In keeping with the previously expressed reservations in this regard, the study advances the above as a conceptually structured basis which, if viewed holistically, informs a qualitative judgement on the selection and prioritisation of macro-environmental role players for scrutiny in the subsequent phase of the CE environmental-scanning process (Phase Five: the identification and profiling of plausible espionage sponsors).

6.4.2 The assessment of discrepancies between the relative values of own state informational assets and macro-environmental informational areas

Whereas the ‘information valued by the own state and at premium in the macro-environment’ cluster centred on similarities and was used as a premise for prioritising macro-environmental role players, the other two clusters have a bearing on the appraisal of incongruences between the two sets of counterespionage-relevant information.

Reduced to its essence, the incongruences are no more than differences in the values assigned to certain bodies of information by the own state and the (generalised) collective of macro-environmental actors respectively. While the project team would strive to be objective, the demarcation of the own state's informational assets was predominantly informed by the state's subjective perception of its interests. Similarly, the values macro-environmental role players attach to bodies of information are based on their subjective perception of security. Since the latter, and therefore premium informational areas, are generalised collectives, they do however, offer a (relatively) 'impartial' benchmark in the twofold assessment of discrepancies.

The said discrepancies are appraised firstly with the view of assessing the 'accuracy' of the project team's delineation of premium informational areas and own state informational assets. Are these discrepancies in other words 'actual' discrepancies or merely the result of oversights in the work of the CE environmental scanning process thus far? Secondly, and as a concurrent action, the discrepancies are reviewed with the aim of pronouncing on possible vulnerabilities in the own state's counterintelligence protection of its informational assets. The requirement of the CE framework to fulfil an offensive-defensive function through conducting such an assessment is derived from the ToR (Section 3.4) and was concretised in Section 5.4 earlier in this chapter. While a vulnerability assessment is performed as part of Phase Ten and Eleven (to be discussed in Chapter Seven), the foundational work is done here (in Phase Four). At this juncture, the emphasis of the foundational work on own state vulnerabilities is not on providing 'answers', but rather on posing problem statements/hypotheses which are subjected to further examination in subsequent phases of CE scanning.

The one cluster of incongruences centres on *information prized in the macro-environment but not valued by the own state*. In the project team's appraisal, these discrepancies are ascribable to one or (more likely) a combination of the following:

- The project team's demarcation of some of the own state's informational assets and/or premium informational areas are deficient and need to be reviewed.
- The process followed in the demarcation *per se* was sound, but the own state's informational asset(s) is(are) of such a sensitive nature that information in the open source realm does not reflect the value it attaches thereto (Figure 36, Chapter Six). Alternatively, the value was erroneously judged because of deficient clarity on pre-conditional notions (Subsection 6.1.2.4, Chapter Six). In

both instances guidance is requested from the client in the progress report to be discussed shortly (Section 6.5, Chapter Six).

- The state's perception of its critical informational interests, and thus the counterintelligence protection afforded to certain informational assets are incongruent with macro-environmental trends. Alternatively, the unprotected status of the information can be the result of an oversight. Whatever the reason, critical informational assets could be unprotected. An example in this regard was provided *per* Figure 36 (Chapter Six).

The other cluster of incongruences revolves around *information valued by the own state and not at premium in the macro-environment*. The project team appraises these discrepancies as resulting from one or more of the following:

- The delineation of the own state's informational assets and/or premium informational areas done as part of the CE scanning process is lacking and needs to be re-examined.
- Particular bodies of information are valued by the own state and one or a few other macro-environmental role players. Since 'premium informational areas' are a generalised and collective designation, the value attached to these bodies of information by one or a small number of macro-environmental role-players could have been overlooked in the CE scanning process thus far. Discrepancies of this nature are clarified through further open-source collection and assessment.
- The fact that the own state regards some bodies as critical and warranting counterintelligence protection, while such information which is not at premium in the macro-environment may necessitate a re-evaluation of the own state's view. Changes in the macro-environment could have rendered counterintelligence safeguarding obsolete and state resources are thus dissipated. (Refer to Figure 36 [Chapter Six] for a practical example.)

6.4.3 The submission of interim products

Flowing from the preceding appraisals – as envisaged and described earlier (Section 3 and Subsection 5.4.3, Chapter Six) – interim warning products, if so warranted, are submitted to the client on possible counterintelligence vulnerabilities in the protection of own state informational assets.

Furthermore, a progress report on the CE environmental scanning process is compiled. In addition to matters relating to the management of the project, the client's guidance is requested on the aspects mentioned above. The progress report will furthermore be accompanied by appendices containing national-security relevant information that emerges during the CE scanning process, but falls outside the civilian service's mandate or the ToR.

This section addressed – from an open-source, counterespionage perspective – the demarcation of own state informational assets, and those bodies of information at premium in the macro-environment. The outcome of a comparative appraisal of these two 'sets' of information was advanced as the basis for the qualitative prioritisation of macro-environmental role players for the purpose of further CE environmental scanning. Moreover, the outcome of the comparative appraisal offers some cornerstones for the assessment of own state vulnerabilities to espionage further on.

7. CONCLUSION

This chapter's primary aim was to address the following research question: 'Given the voluminous extent of overt information, how can the CE environmental scanning process be methodically structured?' It was emphasised that the integrated response to the research problem spans two chapters (Chapters Six and Seven). Chapter Six's specific objectives were to provide a methodologically structured outline of the CE environmental scanning process as a whole, and to explicate the initial phases of this process.

Since the CE scanning process is envisaged as parallel *project*, reference was made to a five-stage project life-cycle categorisation ascribed to within Project Management. It was further noted that each stage typically comprise of several phases, while a phase in turn is divided into subphases and activities. The layered distinction between stages, phases and subphases was found to be useful in the methodological structuring of the CE scanning process. Instead of the conventional five-stage approach, however, a three-stage division was concluded to be more apposite to the CE scanning process's needs. The three main stages thus proposed for the clustering of the various phases of the CE scanning process were the following; namely conceptualisation, design and planning; implementation; and conversion. In outlining the CE scanning process's methodological logic, these phases and stages were linked to specific problem statements (Figure 33).

In accordance with the chapter's stated objectives, the conceptualisation, design and planning stage was subsequently examined more comprehensively. It was emphasised that this stage should not be viewed as a mere bureaucratic necessity. Scant attention to this stage will translate in the squandering of time and resources further on in the CE scanning process. The assertion on its importance, is attested to by the following key findings on the respective phases of this stage:

- *Phase One: establish the Terms of Reference (ToR)*. The ToR govern the allocation of information as well as human resources and are therefore pivotal to the successful execution of the project. The ToR are also foundational to the derivation of primary scanning requirements and determine the directional focus of the CE environmental scanning.
- *Phase Two: derive the primary scanning requirements*. The derivation of the primary scanning requirements involves the concretising of ToR into 'what is required to be determined'. Primary scanning requirements were ascertained as a type-specific form of statutory intelligence requirements and as the analogical 'destination' of the CE environmental scanning process.
- *Phase Three: design and configure the execution of environmental scanning*. This phase emerged as the plotting of the allegorical 'route' to be followed in arriving at the 'destination', as well as the manner in which the 'route' should be navigated. During this phase, in functional terms, the methodological schema (CE framework) for the execution of the scanning is designed, the means ('open sources') through which espionage risks are to be identified structured, and realistic parameters within which this is achievable are stipulated. It was concluded that, prior to proceeding to the execution stage, the practical feasibility of notional constructs - such as the CE framework - should be tested by means of a probing report.

The chapter proceeded to explicate the launching phase (Phase Four) of the CE environmental scanning's execution. Of all the phases of the CE environmental scanning process, *Phase Four* was by far the one the most extensively discussed. The comprehensiveness of its discussion is proportionate to its importance. It is also proportionate to the effort allocated to this phase in the practice of open-source CE environmental scanning.

The 'adversary-centric default', frequently and erroneously resorted to in all-source counterintelligence, was found as not the ideal starting point for the CE environmental scanning's execution. Instead, the execution stage should commence with the identification of espionage and counterespionage's referent objects ('secrets'). From a counterespionage perspective, certain 'bodies of information' are secret, in part, because they are valued by the own state and highly prized ('at premium') in the macro-environment. The chapter advanced separate subphases for demarcating two 'sets' of counterespionage-relevant bodies of information, namely ‘own state secrets’ and ‘premium informational areas’. Propositions were made for the methodological structuring of both of these subphases by means of specific steps and the employment of conceptual matrixes. Juxtaposed, and refined in accordance with the mandate of the civilian intelligence service, the convergence of own state secrets and premium informational areas was proposed as the premise for the qualitative identification of macro-environmental role players that may pose espionage risks to the own state.

In line with the study’s reservations regarding quasi-quantitative and ‘easy-step’ methods, also the prioritising of macro-environmental role players for further CE scanning is found to be qualitative in nature. During subsequent CE environmental scanning phases, macro-environmental role players so prioritised are further scrutinised. These, as well as other, phases are explored in the next chapter.

CHAPTER SEVEN

AN INTEGRATED PROCESS FOR OPEN-SOURCE, COUNTERESPIONAGE ENVIRONMENTAL SCANNING AND RISK ASSESSMENT: ESPIONAGE ADVERSARIES, OWN STATE VULNERABILITIES AND COUNTER-ESPIONAGE ASSESSMENT

1. INTRODUCTION

While fundamental to the CE scanning process, the coincidence of informational interests ascertained through the phases described in the previous chapter, is insufficient for credible assertions on espionage actors hostile to the own state. Not all macro-environmental role players (hereafter referred to as 'role players') with converging informational interests can, in other words, summarily be deemed as adversarial espionage actors.

Therefore, and in a continuation of addressing the earlier mentioned research question on the CE environmental scanning process's methodological structuring, this chapter's first objective is the design of an open-source based subprocess for establishing justifiable grounds for asserting - or where applicable discarding - role players as espionage actors adversarial to the own state. It is contended that this subprocess spans the following five phases of the CE environmental scanning process: the identification and profiling of plausible espionage principals (Phase Five); the identification and profiling of plausible espionage adversaries (Phase Six); determining adversarial espionage *modus operandi* (Phase Seven); the design of open-source detectable espionage indicators (Phase Eight); and the application of these indicators (Phase Nine). On conclusion of these phases credible pronouncements are possible on the plausible existence of situations whereby adversaries are exploiting, or intend to exploit, own state vulnerabilities in procuring own state informational assets through espionage.

Espionage efforts however aggressive against a state with, *per absurdum,* impenetrable counterespionage barriers, are just that – espionage efforts and not necessarily espionage risks. Micro-theoretically phrased, and as will be demonstrated in the course of the chapter, 'vulnerability' is *sine qua non* to a postulation on the existence of an espionage risk. The chapter therefore has as second objective to advance a phase (Ten) centred on ascertaining own state vulnerabilities to espionage.

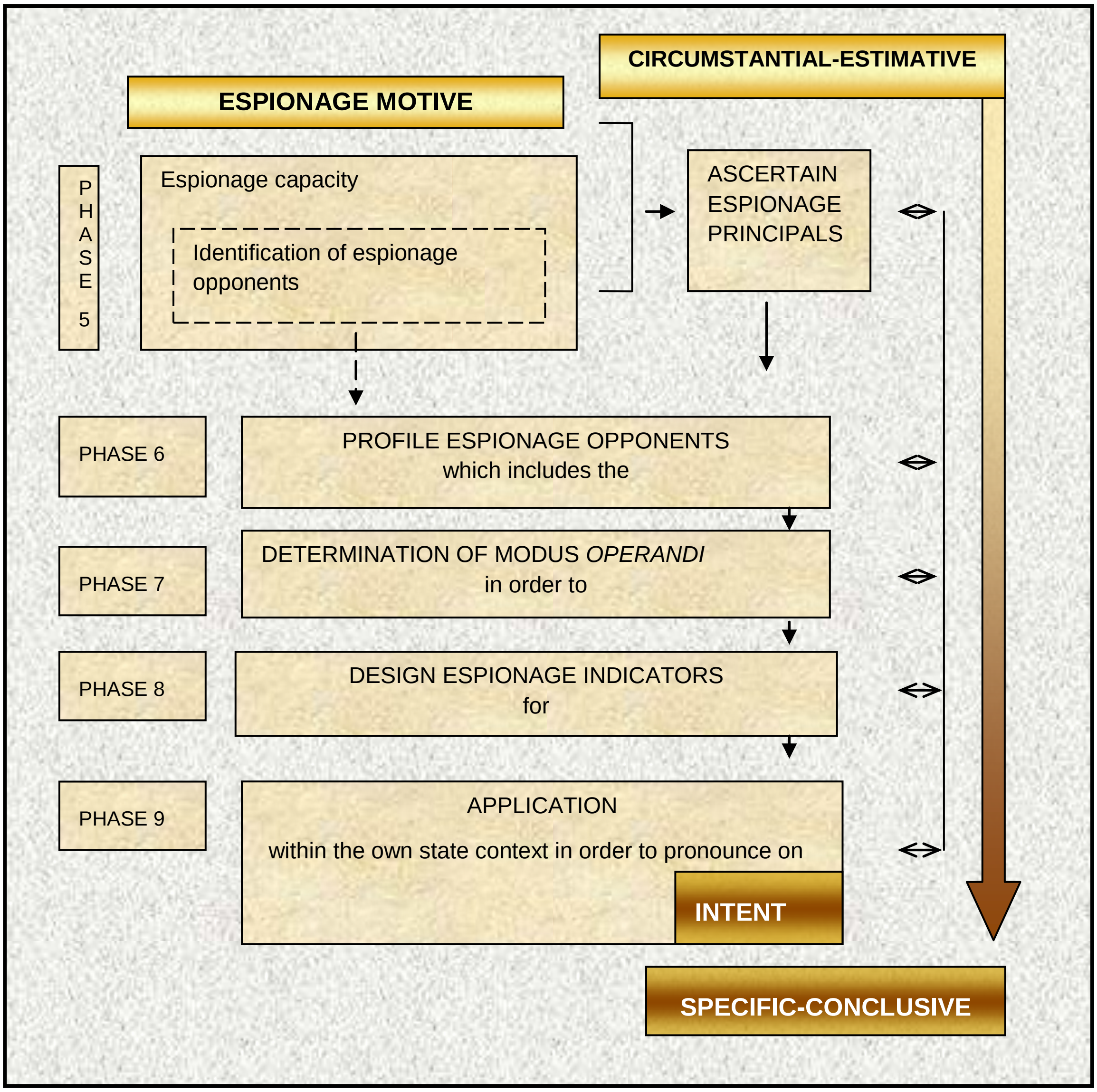
The chapter's third objective is the postulation of a proposition on the CE environmental scanning process's final phase, namely an open-source counterespionage risk assessment. Emphasis is placed on the format of the product submitted to the intelligence service that commissioned the project.

In addressing the methodology of CE environmental scanning, Chapter Seven is simultaneously 'theoretical-integrative' and 'pragmatic-utilitarian' orientated. This orientation was explicated in Chapter Six (Section One) and is therefore not elaborated upon here. Similar to Chapter Six, this chapter also relies mainly on the use of the hypothetical 'own state' and the PRC for illustration purposes.

2. A CONCEPTUAL APPROACH TO THE OPEN-SOURCE DETERMINATION OF ESPIONAGE PRINCIPALS, OPPONENTS, *MODUS OPERANDI* AND INDICATORS

As implied in the introduction to this chapter, Phases Five to Nine of the CE scanning process are a notional and practical 'unit'. Notionally, and albeit with emphasises varying from phase to phase, all five phases are focused on potential or actual espionage adversaries. These phases' notional unison is mirrored in the practical execution of CE environmental scanning. Although presented as five distinctive clusters of activities, these phases are in practice not executed in a strict linear-sequential fashion. Indications of espionage activities (Phase Nine), for example, may lead to the identification of an espionage principal (Phase Five). The notional and practical unison of the phases necessitates the inclusion of this section which advances an overarching conceptual approach. Graphically the structuring of the five phases can be depicted as follows:

Figure 48: The open-source determination of espionage principals, opponents, *modus operandi* and indicators


CIRCUMSTANTIAL-ESTIMATIVE
ESPIONAGE MOTIVE
PHASE 5
Espionage capacity
Identification of espionage opponents
ASCERTAIN ESPIONAGE PRINCIPALS
PHASE 6
PROFILE ESPIONAGE OPPONENTS which includes the
PHASE 7
DETERMINATION OF MODUS OPERANDI in order to
PHASE 8
DESIGN ESPIONAGE INDICATORS for
PHASE 9
APPLICATION
within the own state context in order to pronounce on
INTENT
SPECIFIC-CONCLUSIVE

Whereas secret counterespionage collection avails information for ‘directly’ identifying hostile espionage actors and describing their activities, the open-source dependent CE scanning process is - as was the case in the identification of CE-relevant informational interests - reliant on an ‘indirect’ approach. In the case of Phases Five to Nine, the indirect approach entails a focus that progresses from broad, estimative inferences to specific-indicative assertions on adversarial espionage activities.

As depicted in Figure 48, Phase Five aims to establish credible grounds for a *plausible* assertion on the status of a role player as an espionage adversary. Credible grounds, in the view of this study, comprise of substantive motive and sufficient espionage capacity. Without purporting to concur with the legal definition of the term, 'motive' as used here denotes a compelling "reason" for a "certain course of action" – in this case espionage (*thefreedictionary.com*: 2008/10/17). Inferences made solely on the existence of espionage motive (*vis-à-vis* the own state) and adequate capacity, are admittedly more circumstantial than conclusive. Often such generalised assertions are 'as good as it gets' within open-source scanning.

With the qualification that it would be attainable in relation to all role players, the CE framework nevertheless endeavours to move beyond circumstantial inferences and ascertain 'espionage intent'. Applied to the study's context, 'intent' denotes a "directed", "fixed" and "strong" adversarial resolve that precedes and/or accompanies the act of espionage (*YourDictionary.com*: 2008/11/17). As suggested in the foregoing definition, intent has the connotations of both 'intend' (planning of espionage) as well as the present or past resolve in the execution of espionage. Whereas 'motive' is *per* definition circumstantial, a credible pronunciation on the presence of adversarial 'intent', requires specific information on adversarial espionage activities or at least conclusive indications thereof. With rare exceptions, the procurement of direct (unequivocal) information on espionage planning and activities, against the own state, is the reserve of secret and intrusive collection. "[S]ecret intelligence", in the words of Gendron (2005: 398-399), is generally "needed against adversaries who themselves operate secretively."

In extending the CE indirect approach to a tactical level, and rather than over-ambitiously setting out to identify *adversarial espionage activities as such,* the CE framework surveys the environment with the main aim to detect *indicators (*of adversarial espionage activities). The design and application of espionage indicators, Section 6.1 (Chapter Six) cautioned, should be approached with circumspection. The proper design of espionage indicators is informed by a profound understanding of espionage opponents and their *modus operandi*. To this end, and as may have been surmised from Figure 48, a definitional distinction should be drawn between an 'espionage principal' and an 'espionage opponent'.

The term 'espionage principal' is used as an abbreviated designation for the concept of 'the principal sponsor of adversarial espionage activities, foreseen or conducted, in respect of the own state'. The espionage principal is the primary initiator, the ultimate beneficiary and - as suggested by the term 'sponsor' – the ultimate bearer of the costs and risks of adversarial espionage activities.

Espionage principals, however, could sponsor espionage without themselves being the perpetrators of espionage. In the case of nation states, for example, espionage is typically conducted on behalf of the state by means of statutory security intelligence services. Similarly, corporate entities contract “private security ‘consultanc[ies]’ ” for purposes of industrial espionage (Todd & Bloch, 2004: 6; Chapter Three, Subsection 5.5.1.2). It is actors such as these that the own state’s statutory counterespionage structure faces in the informational warfare trenches and that are henceforth collectively referred to as espionage opponents. Since espionage opponents execute actual espionage, it is their *modus operandi* that informs the design of espionage indicators.

As with Phase Four, the elucidation of phases Five to Nine is presented from the view point of the hypothetical own state. The latter, for purposes of the phases to be discussed, is deemed as a typical Western nation state and relies especially on perspectives derived from official US and Germany documentation. The PRC is posited as the hypothetical own state’s adversary and this country (the PRC) is used in illustration of CE environmental scanning activities performed in relation to espionage principals, opponents, *modus operandi* and espionage indicators.

The reliance on examples relating to the PRC as a nation state, does not negate the insistence of the study to configure the CE framework in accordance with the 21st century reality of the multiple categories of various espionage adversaries. The PRC is utilised due to practical considerations. Primary sources on categories of role players other than nation states are, for one, in considerably shorter supply. Even should such literature have been abundant, an equal emphasis on all role player categories would have rendered the study so extensive as to be impracticable. In addition, the espionage conducted by nation states shares similarities with that of other role player categories. Moreover, the discussion of the PRC intelligence’s *modus operandi* does include references to other categories of role players. Consequently, postulations on the PRC and its intelligence apparatus as espionage adversaries provide a useful premise for postulations on other types of actors.

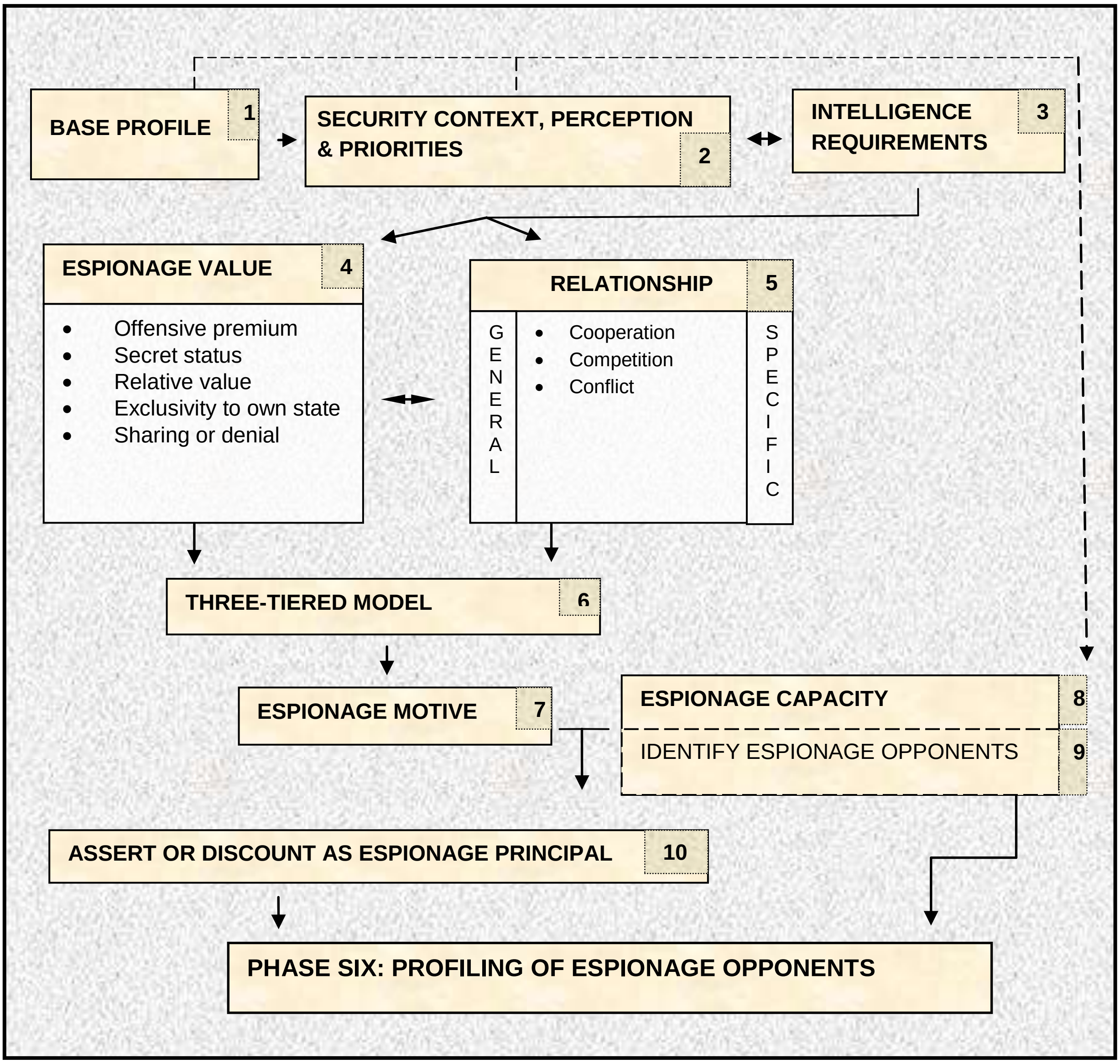
3. DETERMINING ESPIONAGE PRINCIPALS AND OPPONENTS

As noted in the preceding section, the primary objective of Phase Five is to determine which amongst the role players identified (in Phase Four) can be asserted as plausible espionage principals posing an espionage risk to the own state. A central contention forwarded was that a credible assertion on a role player's status as espionage principal rests on two preconditions namely substantive motive and espionage capacity. Espionage capacity, it was further contended, is dovetailed with this phase's second objective namely to identify a role player's plausible espionage conduits (espionage opponents).

3.1 AN OUTLINE OF THE COUNTERESPIONAGE ENVIRONMENTAL SCANNING PROCESS FOR DETERMINING ESPIONAGE PRINCIPALS AND OPPONENTS

Based on these central contentions, the process for the open-source determination of espionage principals and espionage opponents can graphically be presented as comprising of the following clusters ('steps') of CE environmental scanning activities:

Figure 49: The open-source determination of espionage principals and espionage opponents



For easier reference, the various steps in foregoing figure are numbered from 1(one) to 10 (ten). As with the numbering of phases, enumeration of steps should not be construed as suggesting a sequential-linear execution of steps. Figure 49 depicts a multidirectional activity resembling Lowenthal's (2003: 52) proposal in respect of the intelligence process as a whole (Figure, 20, Chapter Four). Because this CE environmental scanning phase's steps intersect, with some recurring at various junctures of the process, a comprehensive discussion of each respective step as well as the inter-connective multidirectional activity flow, would result in excessive repetition. Furthermore, a detailed step-by-step dissection would fragment both the argumentative logic of the highly theoretical three-tiered relationship, and the practical elucidation of the process by means of PRC-related examples. In order to limit repetition and illustrative fragmentation, this section proceeds with firstly advancing, at a micro-theoretical and generic level, a three-tiered relationship model as an instrument for appraising espionage motive (Section 8.2). Pursuant to the model's presentation, key aspects of the process (for determining espionage principals and opponents) are illustrated with specific reference to the PRC (Section 8.3).

3.2 A THREE-TIERED MODEL FOR APPRAISING ADVERSARIAL ESPIONAGE MOTIVE

The discussion of Phase Five thus far highlighted the centrality to the phase of the concepts 'espionage motive' and 'espionage capacity'. Whereas espionage capacity will transpire later on to be relatively objectively determinable, espionage motive is inherently a subjective notion.

3.2.1 The challenge of the open-source determination of espionage motive

Kalaris & McCoy's (1989:130) description of counterintelligence as "above all about" the understanding of adversarial thinking and "behaviour", is arguably no more apt than if applied to the concept of adversarial 'espionage motive'. Within all-source counterespionage, an appraisal on espionage motive demands of intelligence practitioners to 'empathetically' view the own state and its secrets through other role players' eyes. Chapter Four (Section 4) pointed out mindsets lacking this empathetic view of adversaries as one of the reasons for intelligence failures. These mindsets include an own-state centric view which refers to the assumption that adversarial entities 'think and act' in the same manner as the own state. Counterintelligence failures occur despite the all-source endeavour's access to secret information (on for example 'inner-circle' deliberations) widely regarded as central to the understanding of an opponent's thinking and conduct (Gendron, 2005: 398-399). Adding to the challenge to the *parallel* open-source based CE framework as a process, is its deprival of such 'inner-circle' information. The following trilogy is central in meeting the dualistic challenge to open-source CE scanning of compensating for the void of secret 'inner-circle' information and moderating failures stemming from non-empathetic mindsets:

- The meticulous scrutiny of prioritised role players that involves the gradual development of an understanding which starts with the 'basics'. Typical counterespionage matters such as adversarial intelligence requirements and *modus operandi* are preceded by the compilation of base profile and clarity on an opponent's security perception and priorities (Section 8.3, Chapter Six).
- A balanced approach to the utilisation of open source which purposely includes HUMINT. Experience has taught that the latter, in the form of interaction with experts, is invaluable in forming an understanding of a role player.
- A notional structure for viewing the own state and its secrets through other role players' 'eyes'.

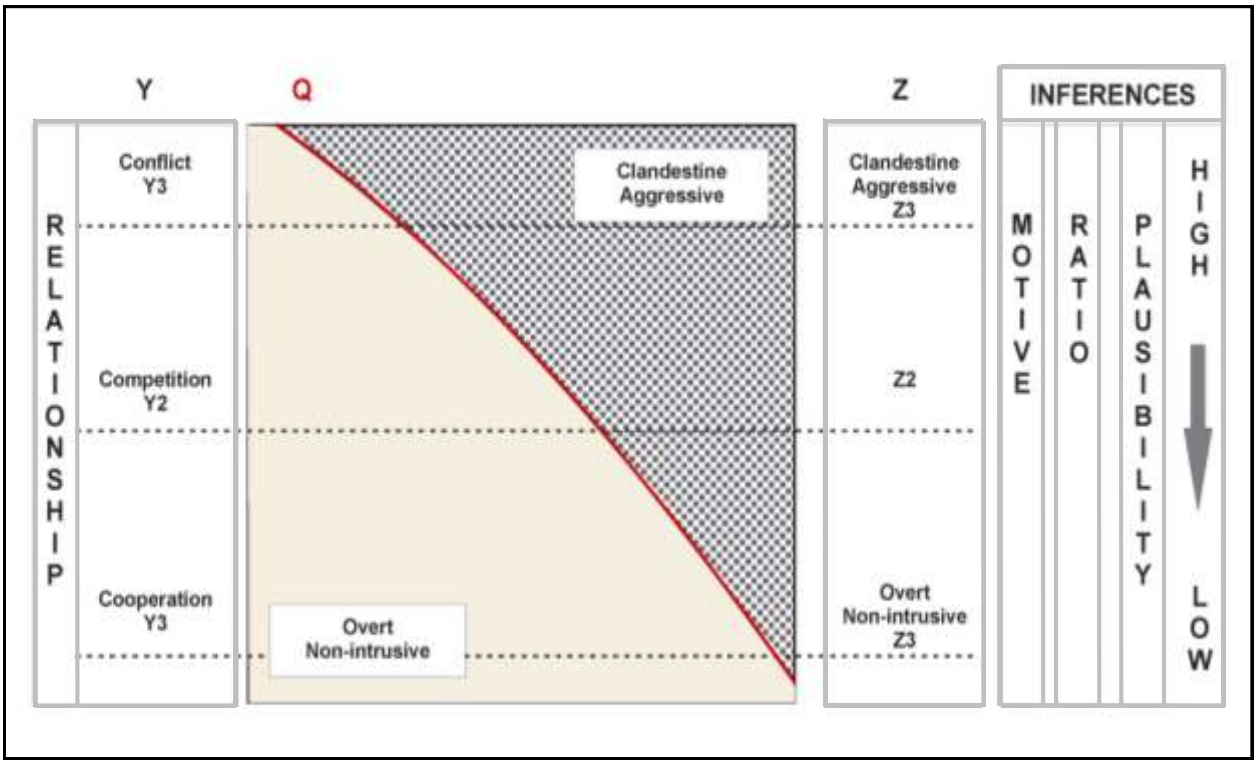
3.2.2 An ideal-type model as a conceptual aid in the qualitative assessment of espionage motive

The notional structure proposed for guiding open-source collection and appraisal in this regard, is not a 'precision instrument'. Instead, it should be viewed as a "rule of thumb" model which is "a method of procedure based on experience and common sense" *(Merriam-Webster Online Dictionary:* 2008/06/16). The conceptual approach advances "general principle[s] regarded as roughly correct but not intended to be scientifically accurate" *(Merriam-Webster Online Dictionary:* 2008/06/16). It is reminiscent of, but does not necessarily comply in every sense with, a Weberian ideal-type model which is a:

> [M]ental construct ... derived from observable reality although not conforming to it in detail because of *deliberate simplification and exaggeration*. It is not ideal in the sense that it is excellent, nor is it an average; it is, rather, a *constructed ideal* used to approximate reality by selecting and accentuating certain elements. (*Britannica Online Encyclopaedia* : 2008/09/09; emphasis added).

The model which is subsequently explained can graphically be depicted as follows:

Figure 50: An ideal-type, three-tiered relationship model for inferring espionage motive



The model rests on five suppositions some of which, if viewed in isolation, might appear to be self-evident. When synthesised into a model, however, these suppositions attain significance that extend beyond the obvious.

3.2.3 Supposition One: The three-tiered relationship between the own state and a macro-environmental role player

As first contention, the aggregate relationship between the own state and a role player is posited as varying on spectrum from conflict, at the one end, to cooperation, at the other end. As a midpoint on this relationship scale (tiers) a relationship of competition exists. The relationship scale is represented in Figure 50 by the left vertical axis Y.

3.2.4 Supposition Two: The secret-overt collection ratio

The model has as second supposition the distinction between the intelligence collection modes of clandestine-aggressive intelligence gathering (espionage) and open-source collection. This is represented in Figure 50 on right vertical axis Z.

Effective intelligence gathering, Chapter Four argued, comprises of a balance between clandestine and overt collection methods. While views were highlighted on the clandestine-overt ratio in the statutory intelligence milieu, the predominance that clandestine collection takes over overt methods, and *vice versa*, is unique from situation to situation. Under which circumstances then would a role player be inclined – in other words 'has a motive' - to favour clandestine collection? Whether or not such a condition exists, is determined by the correlations which constitute the model's third and fourth cornerstones.

3.2.5 Supposition Three: The relationship tiers and correlative inferences

The model's third cornerstone, represented by the correlation curve (Q), postulates a correspondence between, on the one hand, the aggregate 'relationship tiers' and, on the other hand, three interlinked derivates namely, a role player's mode of intelligence collection; the level of adversarial motive for resorting clandestine intelligence collection; and the degree of plausibility of espionage being planned or executed against the own state.

It is contended that a high level of conflict in the aggregate relationship would mostly signal a strengthening of a role player's motive to employ clandestine aggressive espionage measures. Conversely, a relationship of cooperation suggests depreciation in espionage motive and increases the propensity towards overt non-aggressive intelligence gathering. Technically, both 'espionage motive' and the 'overt-secret ratio' are thus correlative inferences expressible in variable terms (such as 'very low', 'medium' and 'very high'). By conjecture - and since the *degree* of 'espionage motive' as well as *variable ratio* of intelligence collection methods are deducted - the *level* of the plausibility of espionage manifesting, follows as a third, correlative variant. The relationship tiers, in practical terms, provide bases for the following projections:

Figure 51: The correlation between relationship tiers and derivatives

RELATIONSHIP TIER	INFERENCES		
	INFERRED SECRET-OVERT COLLECTION RATIO [MODES OF INTELLIGENCE COLLECTION]	INFERRED LEVEL OF ESPIONAGE MOTIVE	INFERRED DEGREE OF PLAUSIBILITY
Cooperation (Y1 - Z1)	Predominantly non-aggressive, overt.	Very low	Very low
Competition (Y2 - Z2)	Mostly overt, but with an element of clandestine collection.	Medium	Medium
Conflict (Y3 - Z3)	Predominantly clandestine and with a high level of aggressiveness.	Very high	Very High

These generalised projections serve as the three-tiered model's baselines and are depicted in Figure 51 as the horizontal lines Y1 - Z1, Y2 - Z2 and Y3 - Z3. It would have been noticed that neither the graphical depiction (Figure 50) nor the narrative explication excludes substantive espionage motive (and other derivatives) on any one of the respective baselines.

Few would dispute the propensity towards espionage in relationships of conflict and competition. Similarly, it is widely accepted that espionage traverses the boundaries of alliances (US 2005*b*: 488; Lowenthal, 2003: 114; Kalaris & McCoy, 1989: 130). Viewed superficially, the latter axiom could be interpreted as contradicting one of the model's central contentions, namely that - as a 'general rule' (ideal-type) - a relationship of cooperation has as a corollary a decrease in espionage motive and the plausibility of espionage. Is the assertion that the existence of cooperation indeed decreases the propensity towards espionage then at all valid? Are incidences of espionage in relationships of cooperation 'exceptions to the rule' or do they rather constitute the 'rule? If 'exceptions' are the rule, then not only the postulated model's veracity, but also its usefulness is questionable. Although an exaggerated simplification, an ideal-type model should after all be consistent with reality.

These 'exceptions', however, will be shown to be not only congruent with the model but as supporting its credence. The model presented thus far is configured in accordance with the aggregate relationship and is thus 'rudimentary'. The model's conceptual refinement, its interpretation as well as its practical application consider both the multifaceted intricacy of the relationship between the own state and a role player, and the model's yet to be discussed fourth cornerstone.

3.2.6 Supposition Four: The espionage value of an informational asset as the determinant of correlation

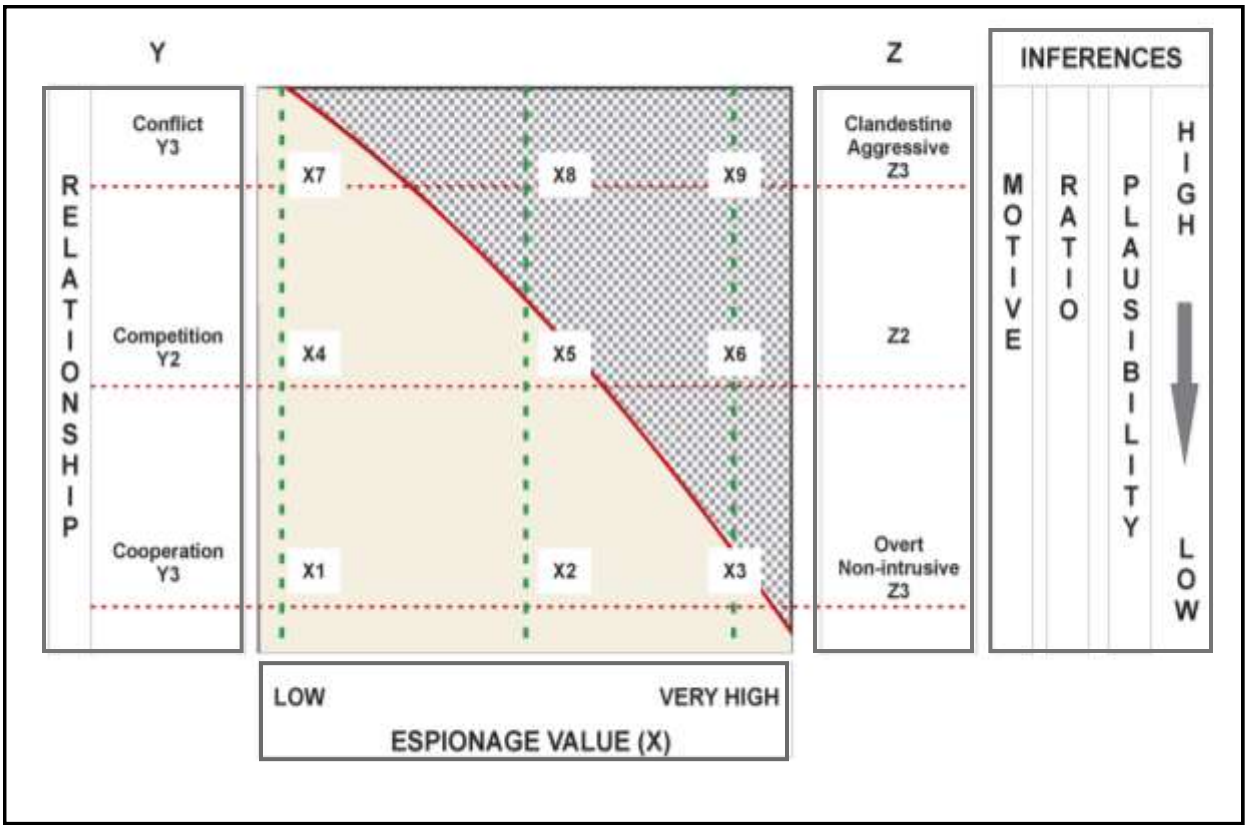
The relationship between the own state and a role player is seldom homogenous and rarely pertains to one aspect only. The relationship is an aggregate of subrelationships. Although the general relationship between the own state and a macro-environmental role-player could be one of cooperation, competition and conflict over some issues are not precluded. In the case of the CE framework, these 'issues' are informational interests and assets. It is a role player's perception of pertinent informational interests/assets, within the context of its relationship with the own state, that holds the key towards clarifying the above-mentioned 'exceptions' and refining the model.

3.2.6.1 The concept and application of 'espionage value'

For the larger part 'exceptions' are not random. There is, in other words, a pattern to these 'exceptions' – a 'rule' to the 'exceptions to the rule'. Whether or not espionage motive can be inferred from, for example, the cooperation tier is depended on 'espionage value'. Espionage value can be defined as the relative importance a role player would plausibly assign to procuring a specific informational asset (in possession of the own state) through espionage.

The model posits 'espionage value' as a co-variable (represented in Figure 52 as the correlation determinant 'X') in gauging 'espionage motive', 'espionage plausibility' and the 'secret-overt collection ratio'. The addition and application of the vertical correlation determinant result in points of intersection with the correlation curve. It is from such points of intersection that inferences are made on espionage motive; espionage plausibility and the secret-overt collection ratio. The addition of the espionage value as correlation determinant, which for elucidation purposes provides for three vertical intersection lines, can graphically be depicted as follows:

Figure 52: Three-tiered relationship model – addition of espionage value as a co-variable ('correlation determinant')



As is clear from the graphical depiction, the points of intersection (and the resultant inferences) do not contradict the generalised correlations drawn from the relationship tiers. On the contrary, the inclusion of the espionage value determinant results in a sharper calibration of the model. In further explication, the following inferences are drawn from the model with reference to the some intersection points:

- In an aggregate relationship of cooperation, a role player would for the overwhelming part have negligible motive to engage in espionage against the own state around most aspects. Concomitantly, collection around these issues will therefore be mostly overt and non-aggressive. On informational assets deemed by the role player as of an exceptionally high espionage value, the presence of an espionage motive is however plausible (X3).
- Within a general relationship of competition, the collection is inferred to be for the most part of an overt nature (X4 to X5). On informational assets of high (X5) and very high value (X6), the plausible motive for clandestine collection, supplementary to open-source gathering, is nonetheless substantial.

- Within a relationship of conflict, the propensity towards secret intelligence gathering generally endears. Should a role player not attach major importance to an informational asset, the plausibility of an espionage motive weakens in step (X7).

3.2.6.2 Variables pertaining to the espionage value of an informational asset

The 'scouting' during Phase Four broadly identified those certain informational assets in possession of the own state which other role players deem valuable. During Phase Five, however, specific role players and the informational assets they value are 'scrutinised'. These informational assets are viewed pertinently through the 'eyes' of a specific role player; within the context of the relationship with the own state; and with the aim to ascertain such assets' espionage value. The weighing of an informational asset's espionage value is a qualitative appraisal and no single criterion or litmus test is advanced. The following variables are thus employed as a collective and not in a specific sequential order.

(a) The nature of the premium attached to informational assets – 'hunter', 'protector' or both?

A role player could place a premium on an informational asset as a 'hunter', 'protector' or both. The CE framework is concerned with those informational assets a role player seeks to offensively procure. It was ascertained in Phase Four that role players value particular informational assets and may seek to procure these assets through espionage. Since the 'scouting' (in Phase Four) took a broad view of the macro-environment, the sometimes blurred distinction between a role player's offensive and defensive premium may have been misjudged. During Phase Five, it is verified whether the premium a role player's attaches to an informational asset is indeed related to the offensive procurement, and not merely the protection, of an asset it already possesses.

(b) Is the 'secret', in fact, secret?

In what is an obvious, yet imperative proposition, a role player would resort to high risk and cost espionage only if the information sought is not obtainable through open sources (Gendron, 2005: 423-424). Assuming own state information assets as secret and privileged when they are not, invalidates subsequent propositions on the existence of espionage risks. Two of the CE framework's earlier noted signature roles, namely to determine whether what are deemed as 'secrets' are in fact 'secret' and whether perceived 'secrets' warrant a 'secret' designation, are thus underscored (Subsection 5.4.3, Chapter Six). For this reason, the CE environmental scanning process does not suffice with the tentative assertions in this regard made during the forgoing phase. Instead, the tentative assertions on 'informational assets' as 'secrets' are scrutinised and verified or refuted. The scrutiny entails an attempt to procure the assumed secret content of a topic through integrated open-source collection as explained in Chapter Four (Figure 15).

In certain respects the verification of the status of 'secrets as secrets' emulates the OSINT collection initiative presumed to have been conducted by the opposition. Depending on the time and human resource capacity allocated to the project, this task can be conducted by the project team in its entirety. Alternatively, or preferably as a supplementary initiate, information service(s) can be used selectively (Section 5.3, Chapter Six). While the tasking of information services does carry the peril of the own intelligence service requirements being compromised, creativity in tradecraft (tasking) would mostly enable the reduction of the prospect to an acceptable degree.

(c) The relative value of the secret to a role player

Information gathered and assessed to verify or refute an informational asset's secret status is also utilised to assess the relative value of its procurement to a role player. The relative value of the 'secret' to a role player comprises of two aspects. Firstly, the value of the secret in relation to role player's security interests. Phrased, as question, how important is the 'secret' if measured holistically against the role player's security interests – indispensible, vital or major?

The second dimension of a secret's relative value, juxtaposes the benefit a role player could derive from obtaining it, against the espionage procurement cost thereof. Be it in all-source or open-source counterespionage, procurement cost would for the larger part evade exact expression in financial terms. Qualitatively, though, the procurement cost of an asset comprises of a combination of the following:

- The "opportunity cost" should there be opted for espionage. Since resources are limited, the expending of thereof on one target implies the foregoing of the opportunity to target other secrets (Gendron, 2005: 413-414; 417-419; 421-425);

- the resources and know-how required for the collection of an informational asset if measured against the sum of the role player's espionage resources, technology and capabilities; and
- the reputational risk and the impact on its relationship with the own state and/or other role players, should the espionage be exposed.

(d) The degree to which the secrets are exclusive to the own state

From a macro-environmental role player's perspective, the attractiveness of specifically the own state's informational assets as espionage targets would increase *pari passu* with the uniqueness thereof. The question which needs to be answered is whether the own state is a primary (or possibly the sole) custodian of a particular secret or whether there are other role players that posses similar information? The more unique such secret information is to the own state, the higher the espionage value thereof tends to be from an opposing role player's perspective.

(e) The sharing or denial of secrets

Even should it have been established that a role player would benefit extensively from procuring a secret unique to the own state, surmising a role player to attach a high espionage value to an informational asset solely on these grounds would be flawed. Espionage value is decisively influenced by whether or not a role player is denied authorised access to the secret in question. With consideration of its national interests, the own state opts to share or deny other role players access to a particular secret. Although there are exceptions, intelligence sharing between the own state and a macro-environmental role player would subtract from the latter's motive for espionage. Conversely, should the own state opt to exclude a role player from such sharing, the latter's motive for resorting to espionage is reinforced.

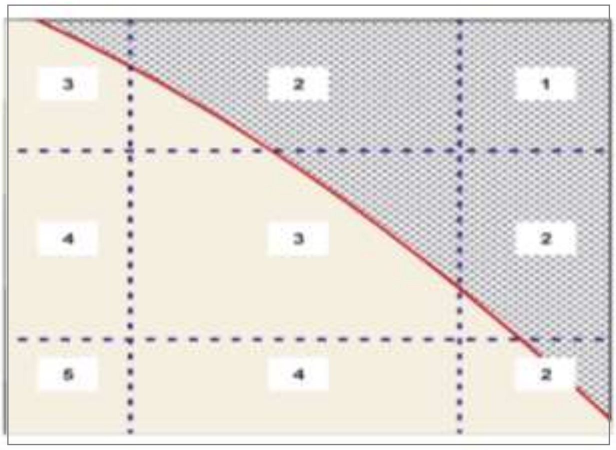
Nation states typically formalise the sharing of secrets in memoranda of understanding. Depending on the ToR, this poses a further challenge to the CE framework as a *parallel*, open-source instrument in ascertaining espionage motive – the particulars and sometimes the existence of intelligence sharing agreements are in themselves secret. In the presumed absence of access to secret intelligence sharing agreements, the project team would consider two factors in reaching a justifiable open-source judgement. Firstly, the relative value of the informational asset to the own state. The latter would be averse to the sharing of some types of secrets seen as indispensible to national security and prosperity.

Secondly, the relationship between the own state and a role player on interests broader than, but linked to, an informational asset.[8]

3.2.7 Supposition Five: Prioritisation grid

It is evident from the outlining of the model's cornerstones thus far, as well as from the discussion of preceding phases and steps, that the CE framework would in some instances generate an extensive net of converging informational interests and assets. Prioritisation throughout the CE scanning process is imperative and the model is no exception. The three-tiered model's practical utility would thus be significantly enhanced by the incorporation of a 'mechanism' through which the deduced implications are prioritised for purposes of subsequent scanning steps and phases. To this end, the model provides for the following superimposition of a 'prioritisation grid':

Figure 53: Three-tiered relationship model – superimposition of a prioritisation grid



With the categorical qualification that numeric figures (1 to 5) are used here to denote points on a continuum scale and should be construed as an attempt to forward a quantitative-*cum*-numeric formula, the prioritisation grid consists of a matrix that ranks deduced implications from the area of highest priority (1) to the area of the lowest priority (5). In tabulated format, the matrix used can be summarised as follows:

[8] The linkage between broader interests and informational assets was explained earlier (Chapter Six, Section 6.1)

Figure 54: A matrix for prioritisation with the three-tiered relationship model

		PRIORITISATION		
		Very low	Medium	Vey high
Relationship	Conflict	3	2	1
	Competition	4	3	2
	Cooperation	5	4	2

This section proposed a three-tiered relationship model for guiding the open-source collection and appraisal of information in order to credibly pronounce on a role player's espionage motive as well as the concomitant derivatives of espionage plausibility and a projection on the overt-secret collection ratio an opponent could be expected to employ. These inferences were emphasised as an exaggerated simplification of a much more complex reality. It is precisely this simplification which enables the model to concretise the cognitive process (the appraisal of an opponent's espionage motive) that counterintelligence practitioners conduct 'intuitively'.

3.3 THE OPEN-SOURCE PROCESS OF IDENTIFYING ESPIONAGE PRINCIPALS AND OPPONENTS

The three-tiered model advanced in the preceding section was presented as a cognitive aid in the counterintelligence-orientated understanding of an opponent's thinking and behaviour. In itself and by itself the model is thus not a key for instantaneously unlocking the riddle of adversarial thinking. Figure 49 shows the model to be part of a process through which such understanding is progressively developed. The application of the model depends on information collected and appraisals done during preceding steps.

3.3.1 The compilation of a base profile

Kent's (1949, 1966: 7) assertion that the "the first class of information to be acquired" in the identification of role players posing an actual or potential risk/threat to the own state "is essentially descriptive and reportorial", remains valid in the contemporary era. Accordingly, the phase commences with the open-source collection of 'basic intelligence'. This information is compiled into a 'base profile'. The format of a base profile varies according the category of role player. The format of a base profile compiled on an organised crime syndicate would, for example, differ from that followed in relation to a nation state, corporate entity or an NGO. Despite these differences, the base profile typically contains descriptive information on the *raison d'être* of an entity, its primary objectives, organisational structure, the scope and geographical manifestation of its activities, its size (for example personnel strength in the case of businesses, or support base should it be an NGO) and resources at its avail.

Within statutory intelligence a 'base profile' in relation to a nation state is commonly referred to as a 'country profile'. *The CIA World Fact Book* (US, 2009*a*) - which covers 266 "world entities" and is updated on line bi-monthly - serves as a generic example of the format used in country profiling. Although the template (the document's organising structure in headings and subheadings) of a country profile varies according to the envisaged application of the product, the aspects of content would in most instances be congruent with those contained in *The CIA World Fact Book*. Aspects covered typically included, to name a few, a country's history, geography, climatology, natural resources, people (demographics, ethnical composition, health and education standards), a multitude economic and infrastructure aspects, the political dispensation as well as governance and administrative practices. The base profile could also include reference to salient national and "transnational" security "issues" (US, 2009*a*).

The purpose of the compilation of a base profile in the CE scanning process is the same as what is the case in statutory intelligence in general, namely to provide the holistic context for the security-focused collection and assessment to follow. National and transnational security issues are therefore addressed briefly and on a descriptive-reportorial level. Since the base profile, within the CE scanning process is compiled with a view on establishing a broad factual foundation for security and (own state) counterespionage-directed collection and appraisals later on, it would, however, be more detailed in its covering of the following aspects concerning the role player and the own state:

- Political, economic, technological, trade, techno-scientific and other cooperation agreements;
- declared disputes;
- the nature and extent of bi-lateral trade and economic interaction; and
- a role-player's diplomatic and other formalised representation in the own state such as government-sponsored NGOs.

Seeing that *The CIA World Fact Book's* readily accessible country profile on the PRC (US, 2009*a*) sufficiently demonstrates the format and content of a base profile, the study refrains from illustrating this document by means of an example.

3.3.2 Ascertaining an opponent's security context, perception and priorities

Expanding on the reportorial-descriptive foundation of the base profile, security-directed profiling gathers and assesses information on matters with a direct bearing on a role-player's security milieu, objectives and priorities. Unlike the base profile, security-directed profiling is not a 'distillation of facts'. Even in relation to the own state and in the all-source intelligence endeavour, it was previously mentioned, the notions of national security objectives, policy as well as priorities are frequently unclear (Johnson, 2003: 639, 641). As a result, the open-source profiling of a role player solely consisting of reportorial-descriptive intelligence is unlikely to be of much utility. This step of the CE scanning process therefore places high demands on the project team's estimative and interpretive skills.

A repetition of the extensive endeavour followed in determining the own state's security perception, policies and objectives - in respect of all prioritised role players - is neither practical nor necessary. What is necessary is a balance between the holistic view of a nation state's security interests in general, and those with a bearing on the own state, in particular. The latter entails ascertaining a role player's *de facto* leadership's perception of matters of national security/insecurity and the role of the own state in this regard. Essentially the problem statement the project team addresses is: What is a role player's perception of its security interests and where does the own state 'fit into picture'? The outlines of the 'answer' to this question is briefly illustrated by reference to the PRC and the own state.

The PRC's central leadership's perception of the protection and advancement of this country's national interests is underpinned by the dualistic vision of, on the one hand, restoring the 'Third Kingdom' to its former glory and, on the other hand, concurrently maintaining the one-party political system. There are growing indications that this notion translates in the intent of eventually surpassing the US as the predominating superpower – economically, politically and military. In pursuing this vision the PRC's national security strategy has the following primary objectives: maintaining 'domestic stability'; the expansion of economic power and technological know-how; raising the PRC's political and diplomatic stature; achieving the ideal of a geographical united 'one China'; increasing the PRC's military might and projection of power; and safeguard the PRC from transnational security threats.

The PRC views sustained economic growth of “key importance when it comes to maintaining stability in the People’s Republic” (Germany, 2008: 267). The country’s rapid economic growth is rooted in a state-driven economic modernisation that is export-orientated and is shifting from labour-intensive to higher-level technological production (US, 2009*e*: 4). Technological advancement and know-how are seen as critical to the PRC’s economic, military and thus ultimately its political prowess. This security perception is manifested in “863 Program” (US, 2009*e*: 158). Launched in 1986, the programme is coordinated by the Ministry of Science and Technology (MOST) and is designed to fast track China's long-term high-level technology development (PRC, 2008). The acquisition and development of civil, military and multi-use technologies are of the programme’s key aims. Specific technologies prioritised include the following: biotechnology; space technology; information technology; laser technology; automation technology; energy technology and advanced materials; agriculture developments and manufacturing processes. The programme is executed *inter alia* through the fostering of joint research and development initiatives with technological advanced countries such as the own state. It is estimated that in the past decade, multinational research and development centres of which the PRC forms part increased from less than 50 to well over 700 (Kitfield, 2007: 3). The programme also facilitates the enrolment of vast numbers of PRC students in developed countries.

In the political and diplomatic arena, the PRC strives to obtain a “larger voice” in “international organizations ranging from the International Monetary Fund and the G-20 Group of industrialized nations to the United Nations” (US, 2009*e*: 3, 15-17). The PRC’s growing political stature is matched by the continuing priority being attached to the modernising of its armed forces (Germany, 2008: 267).

Politically, diplomatically and if needs be through the projection of military force, the PRC remains committed to achieve a ‘truly’ united China. One of the PRC’s key “near-term” national security priorities is “[d]etering Taiwan from declaring independence” and to “impede other nations … from intervening on Taiwan’s behalf” (US, 2009*e*: 6-7). Civil groups and individual supporters, inside and outside the PRC, of an independent Taiwan are seen as a national security threat and as one of “Five Poisons” (Germany, 2008: 267). A similar view is taken of, and the label ("poisons") assigned to two other movements perceived to be eroding the united China idea, namely the Uyghur separatists and those advocating Tibetan independence. A further priority linked to the united China ideal, is the outright incorporation of the Hong Kong Special Administrative Region. This priority is visible in Beijing's growing influence in, and the "chipping away incrementally at [,] the legal support for Hong Kong's domestic autonomy" (US, 2009*e*: 10).

As suggested earlier, PRC leadership views domestic stability and the Communist Party's control of China as an "absolute priority" (Germany, 2008: 266). In addition to those already mentioned, pro-democracy advocates and the Falun Gong movement are perceived as the other two "poisons" posing a threat to the PRC's national security.

The expansion and internationalisation of the PRC's national interests coupled with the effects of globalisation are resulting in the PRC's leadership affording increasing priority to transnational security threats. In addition to conventional transnational security issues (such as terrorism), there is a "growing appreciation" for non-traditional threats" that could negatively affect China's national interests (US, 2009*e*: 6). The latter is "evidenced by … the increasing allocation of resources towards missions such as peacekeeping, counterpiracy, and disaster relief" (US, 2009*e*: 6).

Within the context of the security perception and priorities, the PRC's leadership's view of the own state – that is assumed for the purposes of the discussion in this section to be a prosperous, technologically advanced and influential Western state – can be summarised as follows:

- In the economic sphere the own state is seen as a major competitor in the export market. This intense competition does not preclude joint business ventures or selective partnerships in techno-scientific research and development. The acquisition of the own state's technological and scientific expertise is perceived as of significant importance to the PRC's economic advancement. The PRC government encourages and directly sponsors techno-scientific interaction between the two countries.
- The PRC is cognisant of differences in opinion in the own state's political and security thinking over whether the PRC is a strategic partner or adversary. This division opens up the possibility of lobbying the own state's political

leadership in support of the PRC's aspirations to increase its influence in the International Monetary Fund and the G-20 Group.

- The own state's is perceived as supporting the causes of Taiwan, Tibet, Uyghur separatists and pro-democracy advocates.
- In the view of the PRC's leadership, the own state - like other Western governments - manipulates the media to unfairly portray China's domestic political dispensation and practices. This is viewed as detrimental to the PRC's national security interests (US, 2009*e*: 10-11).
- Cooperation with the own state on the countering of some forms of organised crime (such as piracy, Russian syndicates and the Japanese *yakuza*) is deemed as in the PRC's national interest.

3.3.3 The open-source ascertainment of intelligence requirements

A role player's security perception determined in the previous step manifests in, and provides the contours of, its intelligence requirements. Johnson (2004: 639) posits this correlation as follows: "Thus, the contours of a country's perceived information needs are a function of the extent to which its leaders sense the presence of threats to, or opportunities for, the advancement of their national (or, in some regimes, merely personal) interests."

3.3.3.1 Intelligence requirements ?: A fundamental counterespionage problem statement

Earlier in the chapter (Section 6.1) "What needs to be protected?" was posed as arguably counterintelligence's most fundamental problem statement. Equally imperative in counterintelligence's offensive dimension (counterespionage), was previously argued, is providing an answer to the question: "What secrets do actual and potential adversaries seek?" During Phase Four some of a role player's intelligence requirements were of course established and considered in the prioritisation of role players for scrutiny. This was, however, done not only with a 'coarse' scouting resolution, but focused on premium informational areas in general and not a specific role player and its intelligence requirements *per se*. Consequently, information on a role player's intelligence requirements is, at this juncture of the scanning process, still superficial and fragmented.

The scrutiny in Phase Five is geared towards comprehensively determining a role player's intelligence requirements – in the main and in relation to the own state. The comprehensive picture of role player's intelligence requirements enables the following:

- The offensive premium a role player attaches to secrets seeks can be confirmed or refuted;
- additional secrets a role player values (not already determined in Phase Four), and of which the own state is a custodian, could emerge;
- a holistic and detailed inventory of intelligence requirements provides the context for appraising a role player's comparative valuation of procuring specific secrets through espionage; and
- since intelligence requirements are scrutinised, the secret status of informational assets on which the intelligence requirements are centred can be refuted or confirmed.

3.3.3.2 Approaches to the open-source ascertainment of intelligence requirements

A balanced methodology for the open-source ascertainment of an opponent's intelligence requirements purposely accounts for the following three angles of approach:

- What others report a role player's intelligence requirements to be. In the case of the PRC this method would be informed by for example: official, publically availed counterintelligence appraisals by states such as the US, Canada, the UK and Germany; media reports and/or the records of court proceedings implicating the PRC; and publications within academic disciplines such as Security, Strategic and Intelligence Studies, as well as Business Counterintelligence .
- What the role player says its intelligence requirements are. With varying degrees of specificity, several nation states declare their principal intelligence requirements (in the form of intelligence priorities) and as part of statutory intelligence communities' annual reports, budget speeches, *ad hoc* statements and reports, as well as on websites. Understandably, publically declared intelligence priorities are mostly limited to the nearly self-evident. While open-source CE scanning should not negate this method, its value relative to the other two methods is more limited – especially when the focus is on a totalitarian state such as the PRC.
- Intelligence requirements can be inferred. Of the three approaches, the inference of intelligence requirements is the most intricate and resource intensive. Since this approach could lead to the open-source exposure of the less obvious, it is also potentially the most rewarding. Various variants of this methods are possible, two of which are elaborated on below.

The conventional variant of inferring intelligence requirements is encapsulated in Johnson's (2004: 639) above-quoted assertion of intelligence requirements as a "function" of role player's leadership's perception of threats and opportunities. A role player's security context, perception and priorities are thus used to extrapolate intelligence requirements. The scanning activities described in Subsection 8.2.3 (Chapter Six) are therefore not only pre-conditional to understand a role player's 'thinking', but also useful in deducing intelligence requirements in broad. However, should the objective be to proceed beyond "contours" to detailed intelligence requirements (particularised informational assets), the extent of the effort required - notably in the economic and techno-scientific sectors - is not proportionate to the benefits derived.

The range of possible alternative methods in inferring an opponent's particularised intelligence requirements is vast and perhaps limited only by the project team innovativeness. This study limits itself to illustrating one such method. The aim thereof is to ascertain the PRC's intelligence requirements in the techno-scientific field. Attesting to the CE scanning process's multidirectional activity flow this method, on the one hand, presupposes a sound knowledge of informational assets sought in the macro-environment (Phase Four) as well as the centralised coordination of the PRC's political, economic, military and technological sectors (previous steps in Phase Five). Given centralised coordination within the PRC, research and other publications can be assumed to reflect the 'real demand' for such knowledge in the sectors mentioned. At least in part, this real demand constitutes intelligence requirements.

On the other hand, the method presupposes an understanding of the PRC intelligence community's ethos and functioning (subsequent steps of Phase Five and Phase Six) as well as its *modus operandi* (Phase Seven). The utilisation of students and institutions, under the banner of *bona fide* research and exchanges with foreign (non-Chinese) entities, is a central feature of the PRC's espionage *modus operandi*. Academic research publications are of obvious importance in establishing 'credentials' for such interaction. The practical implication of the two-fold premise to open-source CE scanning obvious - a comparative appraisal trends in PRC research and (counterintelligence relevant) information at premium in the macro-environment will, by inference, provide indications of particularised information assets sought by this country and its intelligence apparatus.

The following observation in the most recent *Report to Congress of the U.S.-China Economic and Security Review Commission* (US, 2009*e*: 170) by implication validates the study's assertion on the symbiotic link between research (and other) publications and the contention that the latter can be utilised for inferring particularised intelligence requirements:

> These journals have engaged in a surprisingly open discussion of the need to develop greater capabilities for computer network operations and have even provided details as to what form these capabilities should assume ... some determined western open-source researchers have been able to gain insights into the institutional developments of China's cyber capabilities through studying the debates in these journals.

Serving as an example of detailed appraisal of PRC research trends through a dissection of publically available (PRC) publications is Kostoff *et al*''s (2006: 1 - 503) voluminous study, entitled *The structure and infrastructure of Chinese science and technology.* Amongst other aspects addressed, the study identifies the most prominent research topics and presents these in the form of multi-level, hierarchical taxonomies. Viewing sections of Kostoff *et al's* (2006: 43, 114-115, 119, 136, 168-169, 172, 175-176, 349, 393, 401-402, 426) work through a counterintelligence prism, the project team could have inferred PRC intelligence requirements in the information system technology field to include the following: search algorithms, recognition algorithms (face, speech and typed character characterisation), computer networks and the various nodes in such networks, system and protocol security, artificial neural networks, microwave circuits and amplifiers, grid computing, compression of encoding/decoding and proxy signature schemes for data encryption.

3.3.3.3 The compilation of an inventory of intelligence requirements

A role player's intelligence requirements, ascertained through a combination of approaches, are compiled in the format of an inventory. The inventory provides for the following:

- A listing and description of the informational assets a role player seeks. The specificity with which such informational assets are describable in the inventory will vary in accordance with hierarchical taxonomies discussed in Section Six (Chapter Six). In the practical execution of CE scanning it would, in other words, seldom be possible to describe all the secrets an opponent seeks with equal specificity. In some instances the description of particularised informational assets would be achievable, while in other case such description would be limited to a subsectoral level. Ideally, an inventory of intelligence requirements will in its formatting accommodate hierarchical taxonomies in respect of all the sectors. In the interest of simplicity the illustration provided per Figure 55 is less complex in format.

- Entities targeted for the acquisition of the secrets. Under this heading entities targeted for the acquisition of a secret are listed. From this information, the own state's 'allure' as an espionage target for procuring such secret can be deduced. Should nation states comparable to the own state have been targeted the risk to the own state increases. The risk also increases in instances where the own state is in alliance with, or cooperate with an entity known to have been targeted. Australia has, for example, reportedly established through technical interception the PRC espionage interest not only this country's (Australia) position *vis-á-vis* Taiwan, but also "wants to know what Australia knows about what the US is really thinking about North Korea and Taiwan" (Daley, 2005).
- The presumed value of the 'secret' to an opponent measured against its security perception, priorities and other intelligence requirements. This value is expressed on an one-to-ten scale, with one (1) denoting minor importance and ten (10) indispensable. The value of what are ostensibly 'trivial' informational assets should be gauged within a broader context. The Italian domestic intelligence service (*Agenzia Informazioni e Sicurezza Interna*), by way of illustration, reported fashion designs of leading Italian fashion houses to have been compromised through PRC-based cyber espionage (*The Washington Times,* 2007-05-12). While some states may deem this incident as trivial, it should be interpreted against the backdrop of the clothing and textile industry constituting a significant portion of the global export market, the PRC as a major producer in this regard and its objective to increase its share of the lucrative high-end segment.
- Relevance of, and relationship with, the own state. Information under this heading, in conjunction with that contained under *Entities targeted for the acquisition of the secrets* relates to the relevance and 'attractiveness' of the own state as a target for the acquisition of a secret. Amongst the aspects considered is whether the own state is seen as possessing a particular secret as well as the issue-specific relationship with the own state.

The following serves as a selective illustration of an inventory of a role player's intelligence requirements:

Figure 55: Inventory of intelligence requirements – the Peoples' Republic of China (a selective illustration)

SECTOR	**REQUIREMENT**		**TARGETED ENTITIES**	**VALUE**	**OWN STATE: RELEVANCE & RELATIONSHIP**
	Topic/area	**Description**			
POLITICAL	**Taiwan**	Influential nation state's political thinking, strategies regarding, and actual support to Taiwan. The identification and profiles of influential "politicians and bureaucrats" that could be lobbied in support of the PRC's position (Daley, 2005: 1-2).	United States, Australia, Germany, UK, Russia, Canada, Russia and Japan.	8	The PRC and the own state's current political leadership is in conflict over Taiwan's status. The own state is seen as a key player in preventing the PRC's to realise its aim of incorporating Taiwan. Critical to the PRC is information on (a) the conditions under which the own state would intervene on Taiwan's behalf and (b) the own state's contingency planning in this regard.
	Textile and clothing (economic subsector).	Clothing manufacturing technology, fashion designs and proprietary information of international major players.	Corporate enterprises based in South Korea, Italy, France and Malaysia.	3	The clothing and textile industry is not a prioritised (own state) economic subsector.

TECHNOLOGICAL/ECONOMIC	**Information system and security technology**	Leading edge software and hardware developments. In relation to the following: search algorithms, recognition algorithms (face, speech and typed character characterisation), computer networks and the various nodes in such networks, system and protocol security, artificial neural networks, microwave circuits and amplifiers, grid computing, compression of encoding/ decoding and proxy signature schemes for data encryption	Governments, parastatals, corporate entities as well as research and academic institutions of technologically advanced countries that, to name a few, include the US, Japan, Germany, France, South Korea and Canada.	10	Although limited joint ventures between companies exist, the own state and the PRC are in intense competition in the commercial informational technology market. The PRC and the own state (similar to other highly developed countries) are effectively in a 'cyber state of war' (intense conflict). The concomitant information technology 'arms race' has leading edge soft and hardware development at its core. The PRC and the own state deems information security technologies, implemented and those being developed, as indispensable to national security.
SOCIAL	**Organised crime**	Piracy - especially along the East African waters (US, 2009*e*: 15). Japanese yakuza and Russian organised crime syndicates.	Organised crime groups as well as states suspected of cooperating with these.	6	The PRC and the own state view cooperation and (presumably sharing of secret intelligence) as beneficial to their respective national interests.

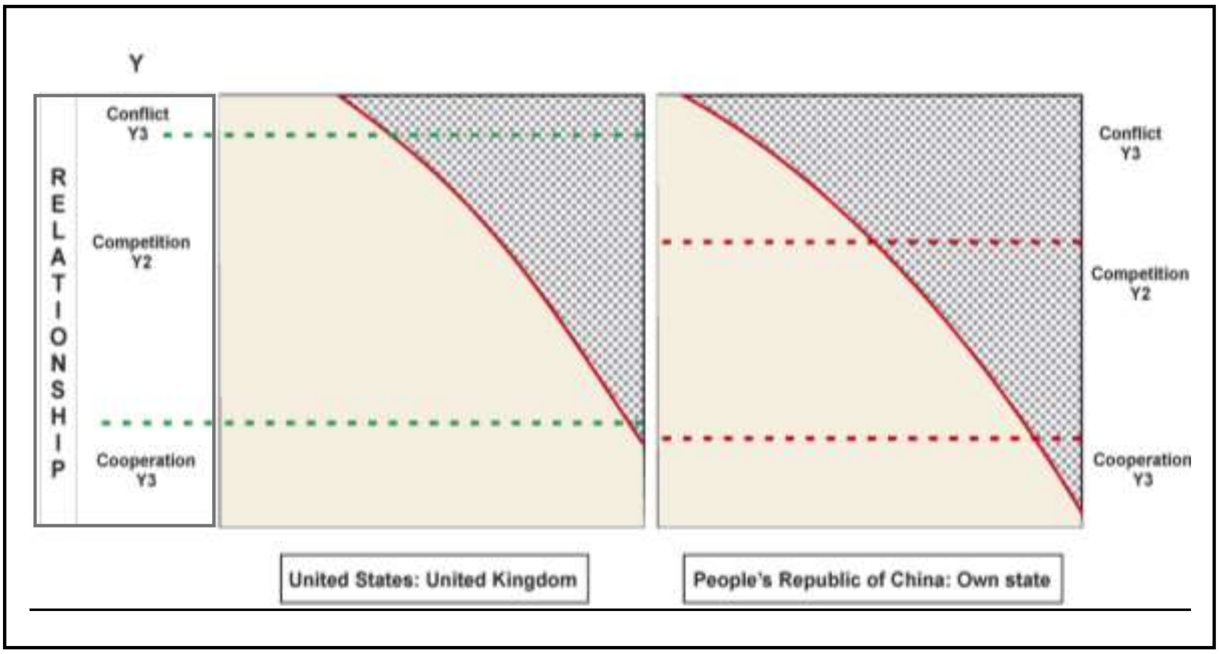
3.3.4 The application of the three-tiered model

Since it is intended as a selective illustration, the inventory above contains limited examples which are counterintelligence wise unambiguous, and from which the espionage motive in relation to the different intelligence requirements is thus readily inferable. On the basis of the examples used, the necessity of a conceptual model as an aid in deducting espionage motive and other derivates could rightly be questioned. In practice, open-source CE scanning generates an extensive number of intelligence requirements – some of which are considerably more complex than the examples advanced. The employment of conceptual guides, such as the three-tired model, would therefore be well advised. In line with the study's orientation, the model's demonstration is also done at a micro-theoretical level. Prior to its actual employment in counterespionage in a project, it needs to be emphasised that the model would require considerable praxis-directed refinement.

3.3.4.1 Configuration of the model

On a micro-theoretical level, the model's application commences with its alignment in accordance with the aggregate relationship between the own state and another role player. The variance in configuration is shown by contrasting the own state relationship with the PRC, with a close-cooperation relationship existing between the US and the UK.

Figure 56: Configuration of the three-tiered relationship model



3.3.4.2 Determining espionage value and issue-specific relationships

On the basis of the intelligence requirements inventory, the espionage values of information assets sought by a role player are subsequently determined. This value can be determined qualitatively or by means of quantitative-cum-numeric formula. Although the study favours a qualitative approach, the following table accommodates both methods:

Figure 57: The assessment of the espionage value a role player attaches to an informational asset

ROLE PLAYER: PEOPLE'S REPUBLIC OF CHINA		
INFORMATIONAL ASSET: X		
		SUBRATING
SECRET AND PROTECTED NATURE		**A**
Qualitative description		
NATURE OF PREMIUM		**B**
Qualitative description		
COMPARATIVE VALUE		**C**
Qualitative description		
UNIQUENESS TO THE OWN STATE		**D**
Qualitative description		
CONCLUSION		
Qualitative appraisal		
RATING	**A + B + C + D = E**	**TOTAL**

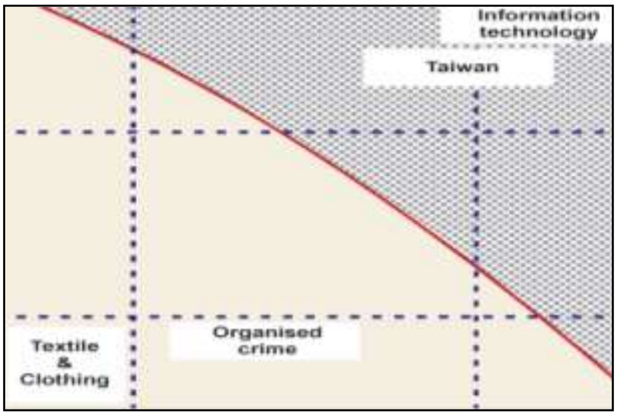
Should the qualitative method be followed, the areas shaded in grey are discarded and the listed aspects are qualitatively described and a conclusion reached. Chapter Four expressed reservations over the practice – in statutory intelligence and Business Intelligence – of quantifying variables by means of quantitative-*cum*-numeric formula. Numeric values are useful to indicate points on a continuum (e.g. a 1 to 10 scale) and are employed as such in this study. However, the application of such numbers in formulae distorts a complex reality. The table above, is a case in point against the use of formulae. Formulae protagonists would most likely have assigned and added up factor values (A + B + C + D) to arrive at the total value

'E'. The chapter amply showed these factors to be interlinked. Furthermore, the equation places the various factors numeratively on an equal footing. In illustrating the near absurdity of such formulae, the question can be posed whether 'uniqueness to the own state' would not in some instances outweigh 'secret and protected nature'. If so, the pursuant question would be by how much – a factor of 2 or perhaps 3,12? If the latter, would the formula then read A + B + C + 3,12(D) = E ? Disconcerting then is that the role of formulas is not restricted to that of conceptual guides for practitioners, but that outcomes are conveyed to the client. "Such numerical formulas", to re-quote Lowenthal (2003: 101), "may be more satisfying than words, but they run the risk of conveying to the policy client a degree of precision that does not exist." The three-tiered models 'outcome', in contrast, is not contained in the product to the client. Its intended application as a conceptual guide to the project team, its qualitative-based nature, as well as its limitations, were sufficiently explained and require no further elaboration.

3.3.4.3. The plotting of informational assets sought

Also previously explained were the application of issue-specific relationships and espionage values in the plotting of informational assets (Section 8.2, Chapter Six). This subsection therefore suffices with the following illustration:

Figure 58: The plotting of informational assets sought by the People's Republic of China *vis-à-vis* the own state



3.3.5 Assert on espionage motive

The three-tiered model visually presents conclusion of a role player's espionage motive. On the basis of the example per Figure 58, it is concluded that the PRC has substantive motive to engage in espionage against the own state. Considering the value of the assets to the own state, ascertained in Chapter Six (Section 6.1), it is clear that the compromising of some informational assets depicted above would have a significant, and others (particularised assets in the information system and security technology field) a potentially catastrophic, impact on the own state's national security interests.

3.3.6 Establish espionage capacity and identify of espionage opponents

While a role player could have substantive motive to engage in espionage against the own state, whether or not it poses an espionage risk is depended on its capacity to actual execute espionage in acquiring the secrets it seeks. This CE environmental scanning's subphase consequently aims to ascertain a role player's capacity to engage in espionage in fulfilling its intelligence requirements in respect of the own state.

3.3.6.1 The advisability of including 'espionage capacity' as a distinctive variable

It is widely acknowledged that the PRC possesses an imposing 'espionage capacity', capable of aggressively pursuing its intelligence requirements. Although not as extensive, also considerably less powerful nation states possess sufficient resources to pose a significant espionage risk the own state in attempting the procurement of some of the informational assets noted above. Chapter Three, will be recalled, posited the accessibility of TECHINT collection methods - notably CYBINT - to a widening array of espionage actors as the 'equaliser' in the international espionage arena. In substantiation, examples were provided of unaffiliated individuals penetrating the informational networks of statutory security establishments. Given open-source limitations and the 21st century espionage reality, there are thus justifiable grounds for – instead of including 'espionage capacity' as a distinctive variable – opting for the use of 'presumed capacity' as part of the CE framework.

This study's inclusion of 'espionage capacity' as a distinctive variable is based on practical and micro-theoretical considerations. Despite the availability of collection methods previously the reserve of more powerful nation states, the gathering of some secrets (through for example MASINT and CYBINT) still demand a degree of sophistication and resources that a limited number of countries posses. Consequently, the methodical scrutiny of 'espionage capacity', *albeit* from open sources, remains important. A properly designed, micro-theoretical structured appraisal of espionage capacity as a distinctive variable, furthermore, provides insights invaluable to related processes such as the identification, profiling and the determining of the *modus operandi* of espionage opponents.

3.3.6.2 The process of establishing espionage capacity and the identification of espionage opponents

In the case of a nation state as opposing actor, the subphase has as its first step the identification of the role player's institutionalised security and intelligence apparatus. To this end, information pertaining the following are collected and assessed:

- The "legal and administrative structure" which forms the basis for the statutory intelligence function (O'Connel, 2004: 195);
- the identification and description of state organs specifically charged with intelligence – be it *de jure* or *de facto*; and
- the identification and description of other state organs fulfilling a supporting role in performing the statutory intelligence function.

Since it has a bearing on the effectiveness with, and the manner in which, espionage is performed, the state's 'security *ethos*' as well as the relationship between the political leadership and the intelligence apparatus are secondly examined. Aspects for consideration include the following:

- The level of integration between governance and the intelligence community. Put as a question: Is the intelligence community interwoven with the fabric of the national decision making process and policy execution? (O'Connel, 2004: 195-196).
- The degree and nature of intelligence structures' subordination and accountability to the state's political leadership (O'Connel, 2004: 195).
- The country's security *ethos* which denotes *inter alia* whether 'security' is seen as the government's most "compelling mission" (Gendron, 2005: 400). The ethos manifests in the measure to which "intelligence gathering" as the "derivative moral obligation of a state", is emphasised over - or in the case of authoritarian regimes at the cost of - "democratic values, human rights and civil liberties" (Gendron, 2005: 400-402, 412, 417-419).

The security *ethos* and the relationship between the political leadership and the intelligence apparatus decisively influence the third yardstick in appraising an opposing state's espionage capacity, namely resource allocation. The latter, more practically, takes into account the intelligence structures' "organisational size and budget" relative to not only the other governance machinery of the state in question, but also in comparison to that of intelligence services internationally (O'Connel, 2004: 195).

The "size and budget" of opposing intelligence services, O'Connel (2004: 196) rightly observes, are frequently and incorrectly, alleviated to the predominating "measure of importance." Size and budget are important, but should be part of a holistic appraisal. In addition to factors already mentioned, the holistic appraisal fourthly considers the*"[b]readth and diversity of intelligence requirements*: what emphasis...[do]... the political leaders place on their intelligence services? Do they rely on intelligence for unique information on a small number of problem sets or targets, or do they expect coverage of events and activities around the world?" (O'Connel, 2004: 195; emphasis in the original).

Size and budget furthermore do not necessarily directly translate into the fifth - and most difficult to concretely define – factor in gauging espionage capacity. The latter pertains to the effectiveness and prowess of an opposing state's espionage structures. One has to look no further for substantiation of this factor than the extent of espionage perpetrated against the US by the relatively small and moderately resourced, yet effective and aggressive, intelligence services of Cuba and Israel (US, 2009*d*).

As suggested above, the project team would undoubtedly have concluded that the PRC has the espionage capacity and prowess to aggressively pursue its (the PRC's) intelligence requirements. The project team's appraisal was in part informed by comparative intelligence analysis and drew on open-source obtainable statements and assessments of other nation states. In US counterintelligence circles, the PRC is reported to be "the most aggressive country conducting espionage against the United States" (US, 2009*e*: 7,148). The FBI rates the PRC as the "biggest" espionage threat facing the US (US, 2009*e*: 148). The PRC is rated as a primary espionage actor also by other Western states such as Germany, France, the UK, the Netherlands and Belgium. This view is shared by various non-Western powers. A report by the Russian FSB, for example, lists Chinese intelligence as one of the three most active foreign countries in Russia (*Novoye Vremya*, 2005: 16-18).

The PRC leadership perceives security as the state's most "compelling mission" (Gendron, 2005: 400) and statutory intelligence as central to the pursuance thereof. Statutory intelligence is interwoven with the political and state apparatus. Strategically, intelligence is coordinated through the General Office of the Central

Committee of the Communist Party. The primary line-functional responsibility rests with the Ministry of State Security, the Ministry of Public Security and departments within the People's Liberation Army (PLA) (US, 2009*e*:151). Various other ministries, government departments, state-owned enterprises, 'private' enterprises, research and development institutions as well as news agencies are inextricably linked with the espionage effort (US, 2009e:151-154). Of these the Ministry of Science and Technology (MOST), the Ministry of Commerce (MOFCOM) and Xinhua (frequently referred to in English literature as the New China News Agency - NCNA) have particularly pivotal intelligence functions. The PRC's primary intelligence organs and the other entities mentioned are deemed as espionage opponents which the own state's counterespionage function engages.

3.3.7 Concluding on, and the prioritisation of, espionage principals

Based on the outcome of the subprocess of ascertaining espionage motive and espionage capacity, a qualitative assessment is reached on whether plausible grounds exist for ascertaining a role player as an espionage principal. Depending on the resources allocated to the project team, a prioritisation of actors that are to be further scrutinised in the next phases would be required. 'Impact', motivated in Chapter Four (Subsection 2.1.3) as the principle prioritisation criterion, is also applied in this instance. Since espionage capacity has been ascertained, the project team will consider the impact on the own state's national security should the informational assets sought by the respective principle's be compromised.

4. THE PROFILING OF ESPIONAGE OPPONENTS

During the preceding phase the entities an espionage principle would plausibly employ in the execution of espionage have been identified. Phase Six of the environmental scanning process sets out to profile these espionage opponents. In the case of nation states, this profiling focuses on the intelligence community (and other institutions with 'secondary' intelligence functions) collectively; as well as on the respective opponents individually. This profiling aims to establish in considerable detail the following aspects:

- The respective responsibilities of the institutions which fulfil a primary or secondary intelligence function.
- The level of cohesion within and between the respective organs. Is the "competition" between both the intelligence structures and other institutions beneficial to, or does it weaken, the espionage effort? (O'Connel, 2004: 195).

- The “overall approach to [intelligence] collection” (O’Connel, 2004: 196).
- The “collection emphasis” and the “relative propositions” between HUMINT and the various TECHINT subdisciplines (O’Connel, 2004: 196).
- The competence in the use of the collection methods and the astuteness in intelligence analysis (O’Connel, 2004: 195-197).

In determining the respective responsibilities of the organs constituting the PRC’s ‘formal’ intelligence community, the project team utilises the following as a starting point:

Figure 59: The People's Republic of China's intelligence community

PRC SECURITY, FOREIGN INTELLIGENCE & TECHNOLOGY COLLECTION AGENCIES	INSTITUTIONAL SUBORDINATION	PRIMARY MISSIONS
CIVILIAN ENTITIES		
Ministry of State Security	PRC State Council/ CCP Politburo Politics and Law Committee	• Foreign intelligence collection • Intelligence analysis • Counterintelligence • Suppression of dissident groups
Ministry of Public Security	PRC State Council/ CCP Politburo Politics and Law Committee	• Domestic security operations/law enforcement • Counterintelligence
CCP International Liaison Department	CCP Central committee	• Liaison with foreign political parties • Influence operations • Intelligence collection
CCP United Front Work Department	CCP Central committee	• Liaison with non-communist Chinese Groups • Influence operations • Intelligence collection
Various Civilian Scientific Research & Development Institutions	Chinese Academy of Sciences (primary)	• Technology acquisition
MILITARY ENTITIES		
Second Department, PLA General Staff Department (Military Intelligence)	PLA General Staff Department	• Foreign intelligence collection (especially military data) • Intelligence analysis • Technology acquisition
Third Department, PLA General Staff Department (Signals Intelligence)	PLA General Staff Department	• Signals intelligence collection and analysis • Cyber intelligence collection and analysis
Fourth Department, PLA General Staff Department (Electronic Warfare)	PLA General Staff Department	• Electronic warfare (jamming, etc.) • Computer network attacks
International Liaison Department, PLA General Political Department	PLA General Political Department	• Foreign intelligence collection • Political/psychological warfare
Various Defense Industrial Firms	11 Different state-owned defense enterprise group companies	• Technology acquisition

Source: US, 2009*e*:152 (adapted).

In line with the phase's objectives the project team proceeds to also profile other institutions that *per* strict definition are not statutory intelligence bodies. One of several profiled is the news agency *Xinhua* which maintains more than 100 bureaus internationally (Peng, 2010: 1). *Xinhua*'s workforce of over 10 000 individuals significantly exceeds that of well-known news agencies such as *Associated Press* and *Agence France-Presse* (Peng, 2010: 1-2). The agency plays a central role in the Chinese's intelligence community. It gathers information from informants, foreign diplomats, foreign journalists and news services and compile and distribute and produce classified reports for the country's political and bureaucratic leadership (US, 2009*e*: 153). Further PRC media entities identified as closely linked with the PRC political-state security apparatus and thus profiled, include *Renmin Ribao, Guangming Ribao*, *Jingji Ribao*, *Zhongguo Qingnian Bao* and *Gongren Ribao* (US, 2007*j*: 3-10).

The project team found the PRC's intelligence community's as highly competent in all the TECHINT collection subdisciplines. Within the cyber sphere this country is seen by several nation states as *the* primary threat to national security. Competence in TECHINT, does not translate in less emphasis on HUMINT. Traditionally, the PRC's approach to HUMINT was governed by the 'actuarial' (also called the 'grains of sand') principle. The latter involved the 'vacuuming' of vast bits of information - frequently by civilians. Analysed and integrated, these bits of information rendered useful intelligence. This approach relied, to a large extent, on the efforts of civilian PRC citizen's visiting foreign countries or individuals with a historic-ethnic link to China residing in foreign countries. The ethnic-historic link rather than financial remuneration was used as method of gaining such civilians' cooperation. Although probably not replacing the "scattershot" approach in its entirety, there are recent indications of more focused HUMINT collection gaining favour (US, 2009*e*: 154-155). Sources outside the ethic-historic Chinese community - with access to specific secrets sought - are being recruited, handled and financially rewarded (US, 2009*e*: 7, 148-150, 156-158). As illustrated by this example, and in stating the obvious, collection approaches determine *modus operandi*. While aspects relating to the latter emerge during Phase Six, the subsequent phase is dedicated to a detailed scrutiny of espionage opponents' *modus operandi*.

5. DETERMINING AN ESPIONAGE OPPONENTS' *MODUS OPERANDI*

The interconnection between 'collection approaches' and *modus operandi* substantiates anew the study's insistence on phases being notional and methodological constructs, rather than rigid procedural compartments. *Modus operandi* is essentially about the detailed dissection and the 'fleshing out' of collection approaches.

5.1 ADVERSARIAL MODUS *OPERANDI* WITHIN THE ALL-SOURCE COUNTER-INTELLIGENCE PRACTICE

In the all-source counterintelligence endeavour, this dissection takes the form of *modus operandi* [9] memoranda and checklists (hereafter collectively referred to as 'checklists'). These are copious documents. It is not uncommon for a checklist on a single espionage opponent or community, which in some instances have been developed over decades, to consist of several volumes. Checklists are 'living' and 'growing' documents which are continuously updated in accordance with changes in adversarial *modus operandi*. While open-source information is used for this purpose, a checklist is for a substantial part based on secretly collected information.

Its sheer extent, puts an attempt to forward a *modus operandi* checklist comparable to that within the all-source environment outside the realistically achievable bounds of this study. In addition, the content and the format of a checklist ('headings 'and 'subheadings'), in certain respects, reflect the own state's *modus operandi* in the identification and countering of adversarial espionage – especially in so far as TECHINT is concerned. The forwarding of a condensed version mirroring the all-source checklist could unintentionally be in breach of the previously noted precondition that the study should not in any manner compromise secret information or insights derived from classified information.

[9] According to strict definitional criteria, *modi operandi* is the plural form of *modus operandi*. Since these checklists deal with various methods of operation, the term *modi operandi* would technically be correct. In consulted literature and it intelligence practice, *modus operandi* is used as the singular and plural noun. In line with the prevailing custom, and with the exception of Section 6.2.2 (Chapter Seven), the study employs the term *modus operandi* as a singular and plural noun.

5.2 ADVERSARIAL *MODUS OPERANDI* IN THE OPEN-SOURCE SCANNING CONTEXT

The fact that checklists are developed over long periods of time and commonly compiled at the hand of prescribed formats, heightens the risk of ‘growing’ digressing into institutional ‘inbreeding’. Such digression may bear the fruits of ‘stagnation’, ‘received opinion’ and ‘groupthink’. These ‘fruits’, Chapter Four (Section 4.1) showed, increase the propensity toward intelligence failures. As during other junctures of the scanning process, the CE framework is charged with meeting the requirement of providing fresh perspectives from an objective distance.

Open-sources in the hands of a skilled project team of can, however, render a surprisingly ‘legible image’ of adversarial *modus operandi.* Reduce to its essence, the open-source identification of *modus operandi* hinges on three aspects namely ‘espionage method’, ‘espionage instrumentality’ (means) and ‘espionage style’.

Contrary to a popular misconception, espionage has not as its only features the adventurous exploits of highly-trained human spies, physical surveillance and high-tech interceptions. The US (2008:2) counterintelligence community lists the foremost and “[e]nduring [espionage] methods” by which this country is targeted as namely, “requests for information; solicitation of marketing and services; acquisition of technology and companies; official foreign visitors; exploitation of joint research and cont[r]acts[10]; conferences, conventions [and] trade shows; cyber attack and exploitation; and foreign collection against US travellers abroad.” In the same report (US, 2008: 2) the US’s Counterintelligence Center (ACIC) disclosed that 85 percent of “targeting incidents” involved “direct [information] request[s] in person or via e-mail, telephone, or fax.” This estimation should of course be interpreted with the necessary qualifications. The figure is based on reported/detected incidents within a specific field, namely “foreign economic collection and industrial espionage” (US, 2008). In addition, some of the ‘best’ spies are the ‘best’ because they evade discovery, and certain TECHINT collection operations are so ‘good’ that they are probably not detected. Nonetheless, the foregoing citations from the report (US, 2008:2) illustrate the diversity in espionage methods.

[10] The report (US, 2008: 2) use the term “contacts”, but the probable intention was reference to ‘contracts’.

These methods are executed through the use of instrumentalities (the ‘means’) that include various types of human agents (discussed in Chapter Three); entities and TECHINT collection platforms. An espionage opponent’s ‘style’ and practices in employing espionage instrumentalities constitutes its tradecraft.

Considering the three elements (espionage method, espionage means and espionage style) individually, and as a collective, the CE scanning proceeds to the compilation of a general overview of espionage *modus operandi*. The document reviews, in more detail than the probing report (Subsection 5.4.1, Chapter Six) current trends in *modus operandi* in the macro-environment - with reference to all categories of role players. Flowing from these trends, a generic *modus operandi* checklist for each of category of role players is compiled and these accompany the overview as appendices. With the qualifications stated (Section 5.1, Chapter Seven), a generic *modus operandi* checklist list for statutory intelligence opponents (namely foreign intelligence communities and services) which mostly addresses HUMINT, could contain the following elements:

Figure 60: Generic *modus operandi* checklist for statutory intelligence communities and services [11]

COVER AND INSTRUMENTALITIES
Official cover and instrumentalities Embassy and missions.
‘Semi-official’ cover and instrumentalities • Government- supported foundations and aid organisations. • Parastatals or state-owned enterprises. • State-owned and national news agencies. • Government affiliated entities that include “research institutes, laboratories, government-funded universities [and] contractors representing governments” (US, 2005*c*:5). • Academic and techno-scientific exchange programmes and visits.

[11] The cursory ‘bulleted’ checklist relies on preceding parts of the study as well as the rest of this chapter for elucidation.

Other instrumentalities employed for cover and/or intelligence gathering

- Corporate entities (not state owned or controlled).
- Private security companies.
- Criminal groupings and syndicates.

RECRUITMENT AND HANDLING PRACTICES (HUMINT)

- Cultivation, cold and combined recruitment approaches.
- False and own flag recruitment and handling.
- Witting and 'unwitting' recruitment and handling. Unwitting utilisation refers to the exploitation of a subject without the latter being aware of the actual intention behind interaction. Examples of unwitting utilisation include requests for information, foreign visits to and from other countries, solicitation of marketing services, as well as interaction during conventions and trade shows.
- Predilection for the use, or not, of double and multiple 'turned' agents. The use of penetration or/and infiltration agents.
    - Communication
    - Personal meetings - frequency, location (e.g. 'third country') and procedures.
- Methods of communication other than personal meetings.
- Remuneration and the use of coercion.
- Operational support which includes the use of false identification and other documentation.
- Agent evaluation and training practices.
- Operational security methods (such as counter-surveillance measures and the concealment of information).
- Practices regarding the termination of agents' services.

TECHINT METHODS

- The use of missions abroad as TECHINT collection platforms.
- TECHINT collection on foreign missions and other targets in the own country.
- Practices in relation to "reverse engineering" and "copying" (Nasheri, 2005: 68-70).
- "Netspionage" conducted by the intelligence service itself and/or through the use of "techno-criminals" (Nasheri, 2005: 39).

Adversarial *modus operandi* is important to CE scanning for various reasons. Information collected and appraised in this regard, for one, enables a more precise description of the espionage risks posed by opponents. In doing so, the assessment of adversarial *modus operandi* informs the CE scanning process's recommendations on the own state's countering of risks. *Modus operandi*, as was previously explained, is furthermore central to the formulation of espionage indicators. The specificity with which *modus operandi* is described is clearly then in direct correlation with the benefits to be derived in the describing of espionage risks, the own state's counterespionage actions and the design of espionage indicators. Consequently, generic *modus operandi* checklists are intermediate products. They are the bases for the formulation of the phase's final products – finer calibrated *modus operandi* checklists on prioritised espionage opponents.

6. THE DESIGN AND APPLICATION OF OPEN-SOURCE ESPIONAGE INDICATORS

Within the confines of open-source limitations, the preceding phase endeavoured to describe opponents' *modus operandi* as comprehensively as possible. *Modus operandi* as defined by Carl (1996: 375, 658-659) is an adversary's "signature". Although some 'lines' and 'dots' of this "signature" will be missing, open sources were previously argued to often provide a 'legible image.' Inevitably more fragmented is the open-source detection of this *modus operandi* manifesting in adversarial espionage activities against the own state. Micro-theoretically phrased: not all aspects of *open-source describable modus operandi* are convertible to *open-source detectable* indicators of espionage activities; and the application of not all of these (open-source espionage indicators) will render results. Despite these limitations, espionage indicators are invaluable to effective CE environmental scanning. Notionally and in CE environmental scanning's execution, the 'design' and 'application' of open-source espionage indicators are separate phases (Figures 33 and 48, Chapter Six). For reasons of coherency, this section addresses both of these in an integrated explication.

6.1 ESPIONAGE INDICATORS IN THE ALL-SOURCE COUNTERINTELLIGENCE MILIEU

Operational espionage indicators are used in the offensive, and mostly secret, countering of adversaries. Like the detailed *modus operandi* checklist from which they are derived, these target-specific indicators are in themselves secret and knowledge thereof within a statutory intelligence service is strictly compartmentalised. The highly privileged access to the information on these types of indicators is normally limited to the counterespionage line-functionary structures and the executive management. While a significant portion of operational espionage indicators would be deemed by intelligence services as protected information, not all espionage indicators (if described in general terms) are, or should be, treated as secrets. Effective counterintelligence intelligence requires public awareness in general, and the vigilance of individuals and institutions dealing with sensitive information in particular. To this end statutory intelligence services conduct counterintelligence awareness programmes of which the sharing of some (broadly formulated) espionage indicators are an integral part.

Consequently, counterintelligence awareness programmes and research aimed at informing such programmes form the bulk of open-source literature in relation to espionage indicators. Aimed at individuals and institutions with actual or potential access to national-security relevant information, awareness programmes have the following elements:

- Counterintelligence procedures, prescriptions and procedures on information and communication security.
- Indicators of “insider espionage” which are presented as a listing of suspicious activities that could suggest an individual being exploited by a hostile intelligence entity.
- Indicators suggesting an “insider’s” susceptibility to hostile intelligence exploitation. These indicators relate to personal and behavioural traits as well as lifestyle patterns.
- Generic indicators of hostile espionage activities. Hostile espionage indicators contained in counterintelligence awareness documents are for a substantial part derived from general adversarial *modus operandi*. Frequently overlapping with “insider espionage” indicators, hostile espionage indicators are more directed towards detecting the ‘external entities’ that attempt to procure information from unsuspecting individuals/institutions through, for example, requests for information, the solicitation of marketing services, and so on.
- Counterintelligence prescriptions and procedures on countermeasures which include the requirement to report, on the basis of the afore-mentioned indicators, “suspicious” conduct /activities.

Of the aspects listed above, ‘hostile espionage indicators’ are of immediate relevance to the section. The following extracts from the US (2006*c*: 22-29) awareness programmes are provided as background for a postulation on open-source espionage indicators:

Figure 61: Espionage indicators in the all-source, statutory counterintelligence environment

SOLICITATION AND MARKETING OF SERVICES	
Indicators	**Countermeasure**
• Offers to provide offshore software support for defence-related projects • Invitations for cultural exchanges, individual-to-individual exchanges, or ambassador programs • Offers to act as a sales or purchasing agent in foreign countries • Internships sponsored by a foreign government or foreign business	• Implement a technology control plan • Request a threat assessment from the industrial Security Representative or DSS CI Office • Scrutinize employees hired at the request of a foreign entity or business partner • Report the contact to the Facility Security Officer
REQUEST FOR INFORMATION (RFI)	
Indicators	**Countermeasure**
• Technology is ITAR controlled • Cleared defence contractor does not normally conduct business with the foreign requester • Request originates from an embargoed nation or represents unidentified third party • Request is unsolicited or unwarranted • Requester claims to represent an official government agency but avoids proper channels to make the request • Initial request targets an employee who does not know the sender and is not in the sales or marketing department • Requester is fishing for information or asking for highly technical information in a field in which she is not conversant • Requester is located in a country known to target the U.S. cleared defence industry	• Educate employees about the threat • On company websites, include a notice that products and technologies are export controlled to screen out requests from foreign entities • Ask who the requester represents and why they seek the requested information • Incorporate security into web design and advertising and initiate an active monitoring solution website • Report the contact to the Facility Security Officer, Industrial Security Representative, and DSS CI Office because other cleared defence contractor facilities may have also been targeted for similar technologies
ACQUISITION OF TECHNOLOGY	
Indicators	**Countermeasure**
• Foreign individuals or competitors seek a position in the U.S. company that affords access to restricted technology • Statements that licenses are unnecessary • Foreign company requests a U.S. company send information/products to another U.S. based company for foreign transfer or via	• Perform due diligence on the buyer and the end user • Ask about the end use of the solicited technology or information • Scrutinize employees hired at the request of a foreign entity/business partner • Request a threat assessment from the

email to foreign addresses • Requester appears to be skirting controls • Multiple similar requests made over time • Foreign competitors purchase U.S. defense firms	Industrial Security Representative or DSS CI Office

Source: US, 2006c: 22-29 (extracts).

6.2 ESPIONAGE INDICATORS WITHIN OPEN-SOURCE COUNTERESPIONAGE ENVIRONMENTAL SCANNING

The all-source detection of adversarial espionage activities, on the basis of the indicators provided above, relies on reports by individuals and institutions to the statutory counterintelligence apparatus. It also involves an institutional network of formalised cooperation between the counterintelligence structures and relevant institutions. Neither this network nor the 'results' of this interaction is at the avail of *parallel* open-source scanning. Theoretically, it is conceivable that open-source CE scanning can partially compensate for this void through conducting comprehensive surveys. Few intelligence services, however, have the capacity to allocate resources to a parallel project enabling indicator-based surveys of this magnitude. More likely, the ToR would limit the project's mandate to selective interaction with individuals and institutions.

6.2.1 Factors for consideration in the definition and the design of open-source espionage indicators

A perusal of all-source indicators contained in Figure 61 validates the earlier assertion (Section 6.1, Chapter Six) on the need for modesty in the design, and expectations regarding the results obtained through the application, of open-sources espionage indicators. The mere duplication of all-source indicators for open-source CE scanning is idealistically over-ambitious. Espionage indicators should be defined and applied in accordance with open-source and resource limitations.

In-all source counterintelligence, the notion 'indicator' denotes a specific, pertinently described activity that could *per se* constitute espionage (Figure 61). These are thus direct indicators. Given open-source and resource limitations, CE scanning takes a broader (less-specific) and indirect view in defining an espionage indicator. In refining the propositions advanced in this regard in Chapter Four (Section Six), an espionage indicator is defined as an open-source ascertainable aspect (situation, event or trend) of a particular *modus operandi* which provides plausible grounds for surmising the possibility of adversarial espionage activity. A situation, event or trend – so defined – is *indicative of the plausibility of an espionage activity*, but (with some exceptions that are explained later on) not a direct indicator thereof. In a puristic definitional sense, in other words, CE scanning aims to detect 'indications of hostile espionage activity' and not 'espionage indicators'. Nonetheless, and since the looser interpretation of the term is qualified, the study continues to use 'espionage indicators' as denoting, and sometimes interchangeable with, 'indications of espionage activities'.

Whether in the all-source or open-source CE scanning environment, Chapter Six (Section 6.1) cautioned on circumspection in the design and application of indicators. Indicators are designed pursuant to, and are applied in the context of, a thorough knowledge of a particular espionage principal and espionage opponent(s). An indicator is also employed within the context of other indicators. Although there are exceptions, surmising plausible espionage activity solely on the basis of a single indicator is normally an unsound counterespionage practice.

6.2.2 Methodological problem statements for the design of open-source espionage indicators

The need for proper context is underscored in the methodology for open-source espionage indicators' design. Phrased as syllogistic problem statements, the methodology consists of the following steps:

- What is the general *modi operandi* employed by a category of role players?
- The manifestation of which of these *modi operandi* are at least partially detectable through open-sources?
- What aspects of a particular *modus operandi* are open-source ascertainable and can these be converted to 'espionage indicators'?
- Is it plausible that an espionage adversary employs this *modus operandi* for the procurement of informational assets valued by the own state? As reflected by this problem statement, preceding CE scanning phases' outcome – such as the demarcation of the own state's critical informational assets and premium informational areas, the convergence of informational interests as well as an adversary's intelligence requirements – direct the employment of espionage indicators to those matters of the highest concern. So doing, the design and application of open-source espionage indicators are narrowed down to a scope realistically manageable within a parallel project's confines.

- Which open sources can be utilised?

It is beyond the scope of an exploratory, micro-theoretical study to advance a comprehensive catalogue of open-source espionage indicators regarding one or all of the different categories of espionage role players. The illustration to follow in the rest of this section is limited to the 'nation-state' category and reviews only some of the multiple open-source espionage indicators. Of these, and because it is the first example that illustrates the methodological logic, the 'exploitation of diplomatic cover and missions for secret HUMINT intelligence gathering' is discussed in some detail. Since the methodological logic applies *mutatis mutandis* to other examples, these are more concisely explained. These examples are furthermore limited in reference to the PRC.

6.2.3 The exploitation of diplomatic cover and missions for secret HUMINT gathering

Chapter Three further observed that, amid the 21st century convergence in the secret collection activities of different categories of actors, some clandestine collection methods remain within the prerogative of the nation state. Given its status as a sovereign geopolitical authority, most nation states maintain foreign missions (High Commissions, embassies, consulates or diplomatic offices) in, and engage in diplomatic relationships with other countries deemed appropriate. Part of a mission's activities is the *bona fide* collection of information through official liaison with the own state (US, 1996: 9-10). The attributes of - and the internationally recognised privileges accompanying - diplomatic relationships and missions, however also afford substantive protection, credible cover and convenient platforms for espionage. Chapter Three further noted that diplomatic status and diplomatic missions are widely exploited by statutory intelligence services for, *inter alia*, HUMINT collection. To this end use is made of 'declared members', 'undeclared members' and other diplomats.

6.2.3.1 Relevant open sources

Diplomatic missions are typically charged with visibly promoting the interests of their sponsor countries. In the execution of this function, the foreign country publically avails official information on topics ranging from the composition of its mission (e.g. the official designations and identities of diplomats) to activities in the host country. Similar unclassified, official own-state information varies from 'diplomatic lists' (individuals attached to foreign missions granted diplomatic status) to communiqués and press releases on interaction. Depending on the relative importance of the diplomatic relationship, the domestic and international media report on significant developments in this regard. Owing to their sensationalist value, reciprocal diplomatic actions in relation to alleged and actual espionage (such as the expulsion of diplomats) are often cited in the popular media. Sources earlier mentioned as useful in comparative intelligence, not only report on such incidents, but also provide overviews of the exploitation of diplomatic relations and missions for espionage purposes.

Excluding its representation to the UN and other international bodies, the PRC maintains more than 150 embassy-level missions abroad. Determined by the nature of the PRC's relationship with other nation states, consular offices have also been established in support of embassies in states deemed as high priorities. Out of a total of 61 consular offices, five are located in the US, four in Japan and three in each of the UK, Germany, France, Australia, South Africa and Canada (*The Guardian*, 2006/03/04). The PRC's intelligence apparatus makes extensive use of both embassies and consular offices missions in the execution of espionage (Germany, 2008: 266-26; US, 2009*e*: 151; US, 2007*g*: 9; US, 1996: 9-10).

6.2.3.2 Espionage indicators relating to diplomatic missions

Espionage indicators in relation to diplomatic missions require clarity on the following open-source determinable facets:

- The organisational structure of the mission.
- The generally accepted, *bona fide* responsibilities conventionally allocated to the various posts within this structure. These posts include, to name a few, ambassador; political and economic consuls; first, second and third secretaries (political, economic and cultural); military attachés; and various consular officers.
- The identities of the individuals occupying these posts as well as their diplomatic careers (reflecting previous posting in other countries and the duration of thereof).
- The activities of individuals (as far as are reasonably ascertainable through open-sources).
- The positions an adversary typically exploits for espionage. In the case of the PRC, political and economic positions as well as military attachés are known to be favoured for espionage purposes (Germany, 2008: 268-270; US, 2009e: 151; US, 2007*g*: 8-10). In the US (2007*g*: 9), also PRC consular officers

dealing with "émigrés who contact the consulate to surrender their passport or renounce their citizenship", reportedly play a key role in the HUMINT collection effort.

On the basis of the facets listed above, open-source detectable espionage indicators include the following:

- The focus and nature of open-source collection – especially by diplomats occupying the positions characteristically exploited for espionage. According to the German domestic intelligence services (Germany, 2008: 268) the PRC's "intelligence staff" under diplomatic cover "mainly analyse open sources of information. To that end they analyze press reports and technical literature or go to lectures and industry fairs." The "diverse events" attended by PRC officials are, however, simultaneously used for the soliciting of information ('unwitting' handling) and the cultivation of contacts for subsequent recruit (Germany, 2008: 268). As reflected in the German intelligence service's appraisal, the distinction between open-source and secret collection is often blurred. Through open sources, the CE scanning project team can establish (in part) the PRC's officials' specific areas of interests and the nature thereof. The procurement of attendance lists and the selective attendance of seminars, conventions and the like, by the project team is mandated by the ToR. In addition, distribution lists of publications by the own state's government departments, parastatals as well as academic and research institutions are useful – especially if measured against the individuals supposed *bona fide* functions.[12]
- Activities of diplomats, as mentioned in the discussion of the preceding indicator, that are incongruent with their official position (declared to the own state) may be indicative of intelligence gathering.
- In a similar vein*,* responsibilities and tasks that are discrepant with the seniority of a post may signal involvement in espionage.
- Career paths of diplomats which, are suspicious from a counterintelligence perspective, serve as a further open-source ascertainable indicator of an individual(s) possibly be an undeclared intelligence officer under diplomatic cover. It is not uncommon for missions to avail diplomats' *curriculum vitaes*.

[12] Attendance and distribution lists are conventionally categorised as grey sources. The inclusion of the latter in the CE scanning process was discussed in Chapter Four and earlier in this chapter.

Past and current diplomatic lists from other nation states (that catalogue foreign missions and diplomats) are in most instances also publically available. These lists can be used to verify or 'construct' suspicious diplomats' career paths. Aspects regarded as suspicious include the following:

- Previous postings in other countries that were of an unusually short duration. This may suggest the expulsion of the diplomat from another country (without 'public exposure') or the recalling of the diplomatic officer by his/her own intelligence service.
- The diplomatic post held in the mission or consulate is incongruent with previous experience and postings.
- The seniority of the posting is drastically different from the directly preceding posting.

6.2.4 Indicators pertaining to the use of front companies for espionage purposes

Notwithstanding diverse methods of execution, the use of front companies features in the espionage *modus operandi* of virtually all effective intelligence services.[13] The PRC serves as a case in point. From the mid-1980s onward, front companies have started to take centre stage in this country's intelligence apparatus's *modus operandi* for industrial and techno-scientific intelligence gathering (Lunev, 1997: 1, 3). Such companies in the US are estimated to be in excess of 3 500. Their presence in Canada is put between 300 and 500, while numerous front companies have been publically cited and identified by German counterintelligence authorities (US, 2009*e*: 151, 158-161: Kitfield, 2007: 2).

[13] In line with the convention in consulted Intelligence Studies' literature the term 'front companies' is used here with relatively wide connotations. In Intelligence Studies, the concept 'front companies' is employed as an umbrella term that denotes corporate entities exploited by statutory intelligence services for espionage and other intelligence purposes. As opposed to its looser interpretation in Intelligence Studies, the term ('front companies') carries more specific connotations in statutory counterespionage practice. The qualifier 'front' is typically employed in reference to a business enterprise that is under the direct control of; frequently owned *via* 'cut-outs' (entities that buffer the identities of the actual controllers) by; and commonly has on its staff compliment undercover members of, the particular intelligence service. The term 'company' is also more exactly used in reference to an enterprise that concurs with the legal criteria for such a juristic entity and is thus distinguishable from, for example, a 'proprietorship', 'close cooperation', 'corporation', 'partnership' and so forth.

The prevalence of the exploitation of front companies by the PRC and other espionage actors, is in part ascribed to front companies' utility in establishing and maintaining both of the two main categories of espionage cover, namely 'cover for action' (the concealment of espionage activities) and 'cover for status' (the concealment of the identities of some of an intelligence service's members/agents). In the techno-scientific field, the dualistic cover provided by front companies is employed for the following intelligence gathering (espionage) actions:

- The soliciting of information through information requests, the offering of marketing services and the visiting of targeted companies or other facilities possessing the technology desired (Wettering, 2000: 267-270).
- The purchasing of high-technology equipment - which in some instances are in contravention of the targeted country's legislation.
- The procurement of sensitive information through mergers and acquisitions (US, 2008*d*: 23).
- The entering into joint ventures which are exploited for technological procurement outside the agreed parameters of the venture.
- 'Head hunting' and recruitment drives to obtain services for the front companies of own state experts in various techno-scientific areas. In some instances, the mere interviewing of knowledgeable applicants keen to secure a position advertised with exceptionally lucrative benefits can in itself be exploited for the solicitation of sensitive information.

The qualification advanced in Section 6.1 (of this chapter), namely that the detection of some espionage indicators - such as information requests and the solicitation of market services - is mostly out of parallel, open-source CE scanning's reach, also applies to adversaries' exploitation of front companies. As with the design of indicators in general, the nature and extent of open-source material at the project team's avail should be computed. Applicable open-sources that are at the project team's disposal include freely accessible (own state and other states) databases on companies; 'due diligence' checks and company profiles (outsourceable by the team to private information services); statutory and business intelligence publicised information; as well as a multitude of local and international business, techno-scientific and industrial publications, websites, and the like. Utilising these sources, the following can serve as open-source espionage indicators:

- The presence in the own state of front companies;

- mooted and actual interaction between front companies and entities regarded by the own-state as of national-security relevance;
- joint ventures planned or already established;
- mergers and acquisitions involving own-state based business and front companies;
- personnel recruitment advertisements by known or suspected front companies; and
- personnel recruitment, even if by reputable staffing agencies, that raises counterintelligence concern since invitations for applications are suspiciously vague in details on the employer; pertain to expertise in critical technologies; offer exceptionally lucrative remuneration; and/or stipulate frequent travel or placement in a foreign country as post requirement.

Even with open-source ascertainable espionage indicators in hand, the scrutiny of the expansive (local and international) business environment to detect the exploitation of front companies to the detriment of the own state may appear as a mammoth, if not insurmountable task. It is for this reason that espionage indicators are designed and applied at an advanced phase of the CE scanning process. Guided by preceding phases, the CE framework at this juncture is sharply focused on specific adversaries and their espionage instrumentalities. In the case of the PRC, the project team would take as point of departure front companies identified by the intelligence communities of various nation states as suspected or confirmed (PRC) espionage instrumentalities. The latter, to name a few, include (Elroy, 2006: 1-5; *WorldNetDaily.com*. 2003; Lunev, 1997):

- Poly Technologies Corporation - owned by the China International Trust and Investment Corporation (CITIC), but effectively under control of the PRC Military Intelligence (General Staff Department);
- China National Precision Machinery Import and Export Corporation;
- Great Wall Industry Corporation (CGWIC);
- SICO Microsystems Incorporated;
- China National Electronics Import and Export Corporation;
- China National Aero-Technology Import and Export Corporation;
- China Nuclear Energy Industry Corporation;
- China State Shipbuilding Corporation (COSCO); and the
- Yuanwang Group.

Adding to the feasibility of executing the seemingly mammoth task, is the fact that the CE scanning's scope is at this juncture calibrated in accordance with the informational assets determined earlier in the scanning process as being valued by the own state and pertinent adversaries. Moreover, and as during other phases, comparative analysis adds to narrow the CE environmental scanning's focus to areas of the highest concern. Given the similarities between the own state and the US, for example, the project team would in the application of indicators in respect of front companies take cognisance of the US's (2008*d*: 23) evaluation of the PRC as the principal role player in foreign mergers and acquisitions of "U.S. critical technology companies". Of these, the US (2008*d*: 23) states, "all but a handful" were "friendly" and "60 percent involved US firms in advanced materials, computers - including software and peripherals - and biotechnology; areas of relative US technical strength". The remaining transactions involved "US firms in electronics and semiconductors, professional and scientific instrumentation, communications equipment, advanced manufacturing, and aircraft and spare parts." (US, 2008*d*: 23).

6.2.5 Open-source espionage indicators in the techno-scientific field

It is also through this sharply calibrated focus that two further open-source detectable espionage indicators should be viewed. Both indicators pertain to unexpected 'innovations' and 'breakthroughs' by entities linked to an espionage principal.

6.2.5.1 Products plausibly resultant from espionage

The first of these indicators is a competitor's unexpected innovation of a product (item or service) closely resembling that which is already manufactured, prototyped, being developed or patented by the own state or an own-stated base industry. With certain provisions the item's emergence may be the 'fruits' of adversarial espionage. The fact that the emergence of a resembling item is not posed as an unconditional espionage indicator, is in line with the study's earlier noted insistence on the necessity for circumspection and proper context in the indicators' application. Prior to inferring adversarial espionage, other plausible explanations for the opponent's unexpected innovation need to be considered. This contextual appraisal would consider inter-related aspects such as the item type; whether the technological know-how is indeed as exclusive to the own state as was previously assumed; the opposing producer's level of research; an opponent's development and expertise in the area item's invention; as well as the opponent's cooperation with other role players in this regard.

Rapid strides in the PRC's manufacturing of "high-tech products" - notably in the weapon/military, aerospace, nanotechnology, bio-technology and pharmaceutics, information technology, telecommunications and automotive areas – are for example not solely the fruits of espionage (US, 2008*f*: 1-6; The Task Force on the future of American innovation, 2005: 5-14). Innovations can in part be ascribed to an immense state-driven investment in research and development (Kostoff *et al*, 2006: 6-9; US, 2008*f*: 1-6; The Task Force on the future of American innovation, 2005: 5-14). Nevertheless, the 'leaps' made in the production of some PRC 'inventions' are so 'ingenious' that they are not consistent with this country's research and development 'trajectory' and/or the resemblance these items bear to those developed by other role players too close to be coincidental. It is such instances that provide plausible grounds for inferring espionage. The majority of such examples cited in consulted literature pertains to PRC military equipment and weapons which on appearance and/or from performance characteristics are judged as "knockoff copies" (Cooper, 2006: 1-7; *India-defence*, 2009-01-08: 1-2; US, 1999: ii- xxxvii). PRC military equipment and weapons reportedly copied from countries such as the US and the Republic of South Africa (RSA) include technology related to: the *Luyang II* naval guided-destroyers' battle management system, the PL-ASR air-to-air missile, the ZW-10 attack helicopter's systems and the DF-31 intercontinental ballistic missile's (ICBM's) thermo-nuclear warhead (*India-defence*, 2009-01-08: 1-2; Cooper, 2006: 1-7; US, 1999: ii-xxxvii).

In general, the timeous identification and the assessments of whether military products have resulted from espionage is an all-source effort requiring secret information and expertise. Not only is secret information excluded from open-source scanning, but the CE scanning process was previously qualified as conducted from a civilian intelligence premise.

In as far as 'products as espionage indicators' are concerned, the CE scanning process is, therefore more focused on the commercial/civilian market. If the US intelligence community's changing view on the "Chinese espionage problem" is taken as a measuring rod (Eringer, 2008: 1-2), the need for the open-source scanning of segments, besides the military, in order to detect products pirated through espionage is rising sharply. In contrast to the perception less than a decade ago when, in the words of Eringer (2008: 1-2), the "Chinese espionage problem was thought to be focused on military technology", the "problem" is increasingly raising its commercial head in multi-use and 'purely' commercial products related to, amongst others, information system technology, telecommunication, as well as the automotive industry (Eringer, 2008:2). The US experience is of course shared by other nation states and their industries. At the 2006 Beijing car show, for example, South Korea's Hyundai Motor Company representatives observed new models displayed by the Chinese manufacturers Liaoning SG Automotive and Tianma Auto to be "shockingly " similar in appearance to Hyundai's Santa Fe and its affiliate Kia Motors' Sorento vehicles (Jung-a, 2007: 1-2). The following year (2007), some of Kia's employees were arrested for "stealing crucial information on the Sorento" and "selling car technology to China" (Jung-a, 2007: 1-2).

In the information age, items that can serve as espionage indicators in open-source scanning are no longer limited to physical products. They also extend to sophisticated services underpinned by advanced technology. The Canadian-based Research-in-Motion company, by way of illustration, scheduled the launch in the PRC of its "iconic Blackberry" wireless e-mail service and mobile phone device for the end of May 2006 (Hesseldahl, 2006: 1). Pre-empting this launch, the PRC state-controlled telecommunications operator China Unicom Limited "surprised" with the introduction in China of a "Redberry" service in April 2006 (York & Avery, 2006: 1-2; Hesseldahl, 2006: 1). China Unicom did not put on the market a 'new' "proprietary handset" resembling the "Blackberry" instrument and linked the service to China Unicom's existing instruments. The "Redberry service" and the technology on which it depended, however, was a "brazen" copy of the service pioneered by Research-in-Motion (Hesseldahl, 2006: 1; York & Avery, 2006: 1-2).

6.2.5.2 The publication of breakthroughs in techno-scientific research

Without detracting from their importance, the detection of unexpectedly 'innovative' physical items or services are, in certain respects, inevitably re-active, and their use in open-source CE scanning as early warning indicators is limited. The second indicator in this field, namely the nature and content of articles in techno-scientific publications, is more apposite to an early warning role. From a positive intelligence premise, a US (1996:10; emphasis added) *Operations security intelligence threat handbook* remarks as follows:

> Open source information can often provide extremely valuable information concerning an organization's activities and capabilities. Frequently, *open source material can provide information* on organizational dynamics, *technical processes*, and *research activities* not available in any other form. When open source data is compiled, it is often possible to derive classified data or trade secrets. *This is particularly true in the case of studies published in technical journals*.

Within open-source counterespionage, “technical journals” are equally invaluable. Depending on an opposing nation state’s socio-political fabric and dynamics these journals - Section Three (Chapter Seven) demonstrated - can be used for deriving adversarial intelligence requirements (*vis-à-vis* the own state). The familiarity and insights gained through the scrutiny of such journals in inferring intelligence requirements have an added benefit in that articles in these publications serve as open-source detectable espionage indicators. The articles are evaluated with a view to determine whether aspects of published research may have been informed by own-state secrets compromised through espionage.

Similar to items and services, incidents such as the above are admittedly reactive in the sense that they implicate retrospectively espionage that has already occurred. This similarity ostensively contradicts the assertion on the techno-scientific publications as early warning espionage indicators. The pro-activity of publications-as-indicators, as opposed to the predominantly reactive role of products-as-indicators, lies in differences in the nature and extent of information compromised.

Products-as-indicators typically involve the compromise of coherent, substantial bodies of information at an advanced development stage. The opposition concluded its espionage operations in procuring these bodies of information and considers it opportune to, by way of analogy, show its hand. The examples provided on whole vehicle designs and an integrated mobile phone service offer sufficient proof of this. In contrast, and while the study’s precondition on the exclusion of secret information prevents the citing of cases in corroboration, experience has taught techno-scientific articles suggesting adversarial espionage to pertain to techno-scientific research at an early or at most an intermediary development stage. Moreover, articles generally would reflect the author to have been *priveé* to aspects, but not the entirety of the own state’s research programmes. Consequently, the detection of signals of adversarial espionage and the subsequent issuing of interim CE scanning products in the form of alerts, enable all-source counterintelligence to institute proactive measures in the protection of the applicable related research programmes. Seeing that the compromise of own-state secrets has been detected relatively early, offensive actions that are in various respects, also pro-active, may also be possible. Examples of possible offensive actions include ‘dangles’, double agent operations and disinformation.

These pro-active benefits justify the considerable complexity attached to, and the effort the project team would expend on identifying espionage indicators in techno-scientific publications. Unlike products-as-indicators, espionage indications in publications are decidedly more opaque. As attested to by the PRC-related examples provided in the preceding subsection, products *per se* are commonly clearly perceptible espionage indicators. In contrast, the signals of espionage in publications are faint and dispersed. Instances of articles containing information blatantly ‘pirated’ from and ‘traceable’ to the own state are relatively limited. Experiments, tests, trials and hypotheses reflected on in techno-scientific articles, for example, can be roughly comparable to, but not identical to those of the own state. The project team would probably find that the articles’ content might not even afford the basis for comparisons on experiments, trials and the like. Inferences on espionage thus rely on appraising publications with the research and development ‘trajectory’ yardstick. As suggested earlier, the employment of this yardstick requires a thorough knowledge of the techno-scientific know-how of the opposition in general, as well as of individual researchers and institutions specifically. In so far as the PRC is concerned, works such as Kostoff *et al* (2006) – elaborated on in Subsection 3.3.3 of this chapter – offer a point of departure.

6.2.6 Open-source espionage indicators employed in respect of the mass media

Whereas techno-scientific publications characteristically have a limited distribution, the popular media or mass media is aimed at a “relatively large, heterogeneous” audience and include mass-circulation newspapers and magazines, television, radio and the main stream Internet (De Beer 1998: 7, 10-12). The mass media is scrutinized and selectively monitored throughout the project’s execution stage to different ends. Context vital for the subsequent explication of mass media espionage indicators was provided in Chapter Three (Subsection 5.1.5) under the heading *Mass media as focal point of CE environmental scanning*.

In statutory counterespionage practice, a wide array of espionage indicators are employed in as far as the mass media is concerned. The confines of a micro-theoretical study allow for a brief explication of only three of these.

6.2.6.1 Media leakages as reactive espionage indicators

As with techno-scientific publications, the compromise of own-state secrets in mass media reporting acts as espionage indicator. In sharp contrast to techno-scientific publications, however, the compromise of own-state secrets in the popular media is less complex to identify. On the contrary, explicit journalistic reference to secret documentation and/or sources adds to the sensationalist value of a 'scoop'. Chapter Three quoted a US (2005*b*: 381) report on the detrimental impact of "serious press leaks" on statutory collection capabilities and national security. This concern was shown to be shared by the statutory intelligence communities of other nation states. Chapter Three furthermore commented on the relationship between the mass media and other categories of espionage role players. Suffice to state here then that 'leakages' of this nature are an important, yet by and large a reactive, espionage indicator.

6.2.6.2 Pro-active espionage signals in relation to the mass media

In the all-source counterintelligence endeavour, measures to pre-emptively limit or prevent leakages of own-state secrets range from the engagement of, and secret collection on, high risk media entities, up to litigation (for instance interdicts preventing the publishing of information) and the monitoring of the mass media reporting to detect early warning signals of impending compromise. The emphasis of open-source environmental scanning in this regard is on the detection of early warning signals. The latter could provide plausible grounds to infer espionage activities being conducted or the possibility of such activities being initiated in the near future.

It would have been observed that this subsection favours the term 'signals' over 'indicators'. In the context of its use here, the term 'signals' includes, but is not limited to, what is customarily deemed as 'indicator(s)'. In addition to 'indicators', 'signals' encompass aspects that would conventionally be classified as aggravating, mitigating and contextual risk factors. With this qualification, 'signals' suggesting an increase in the plausibility of espionage risk(s), are as follows:

- The topic of media coverage nature deals with an issue of high national security relevance. In determining such relevance, the critical informational assets ascertained in previous phases can serve as beacons. Given the relationship between adversarial espionage and informational covert action discussed later on in the section, the impact of reporting on a topic on the own state's reputational integrity is also considered in assessing national security relevance.

- The frequency and prominence of reporting on topics relevant to CE scanning are increasing – thus suggesting intensifying mass media interest in the topic.
- Reporting based on sensitive or classified information would add to the perceived news ('scoop') value.
- Sensitive information regarding the topic or related topics has been compromised previously.
- The media coverage is predominantly informed by investigative journalism. Practically, a publication attributes an article's content to its own journalists and sources rather than relying on news agencies such as *Reuters*, *Associated Press* and *Agence France-Presse*.
- The reporting entity's (such as the journalist and/or publication) sentiment *vis-à-vis* that of the own *state* or national-security relevant institution is generally negative.
- The reporting entity has links with, or is sympathetic toward, an own-state opponent.

Viewed collectively, the detection of such signals could, under the conditions stipulated in Chapter Six (Section 3.2 and Subsection 5.4.3), prompt the project team to submit interim, warning intelligence products.

6.2.6.3 Mass media propaganda as a concomitant espionage indicator

Contrary to a misconception, the mass media is but one of the instruments used in propaganda. Propaganda can assume various forms such as public demonstrations, petition drives and the orchestrated circulation of rumours through strategically placed agents of influence (Godson, 2001: 156). In the contemporary era, however, "most" propaganda is spread through the use of the mass media (Godson, 2001: 156). Propaganda messages disseminated through the mass media are naturally in the open. Mass media propaganda (hereafter referred to as 'propaganda'), in other words, manifests in open sources and is thus within CE environmental scanning's reach.

The explication of propaganda as open-source detectable, concomitant espionage indicator, requires a conceptual clarification supplementary to that provided in the study thus far. Propaganda essentially is about the influencing of perceptions through the conveyance of a message to a target audience, through a medium (in this case the mass media), and to the sponsor's benefit. A distinction can be made between white (overt), grey and black propaganda. The latter two are part of informational covert action. Godson (2001: 151-152) explains these concepts as follows:

> [O]vert propaganda identifies the sponsor, and it is usually truthful. If it is not, that fact will eventually come to light, to discredit the sponsor … Covert propaganda refers to information, ideas, and symbolic actions whose sponsor remains unknown … Covert propaganda can be black (well hidden) or gray (disseminated with a thin veil of cover). The propaganda itself may be truthful or intentionally false. The current term for the latter is "disinformation". Gray propaganda hides its source from the uninitiated public, but not from sophisticated observers.

Albeit with a lower level of certainty than would be the case in white and grey propaganda, a sophisticated project team would also be able to identify instances of plausible black propaganda. Assertions beyond reasonable doubt on the latter, however, require information secretly obtained and are listed as such for pursuance by an intelligence service's all-source counterintelligence structures in the counterespionage risk assessment (Phase 11).

The CE framework regards, by default and unless found otherwise through scrutiny, all incidences of propaganda as espionage indicators. The positing of propaganda as a default espionage indicator rests on the following suppositions:

- Similar to espionage, grey and black propaganda are high cost and/or risk endeavours, which a role player enacts on aspects deemed of matching importance to its security and prosperity. Depending on the nature of the issue, these aspects are often also prioritised for espionage. In a similar vein, and while they do not carry the risk of exposure, white propaganda campaigns could entail a sizable financial expenditure. An experienced project team will therefore appraise the themes, subjects and dissect the nature of white propaganda campaigns in order to ascertain concomitant espionage risks they may pose.
- Grey, and especially black, propaganda frequently involves the utilisation of suitable opinion-shaping assets of which journalists are well-known examples.

It is rare for the successful talent-spotting, cultivation, recruitment and exploitation of such assets not to be dependent in some way or the other on information obtained through espionage.

- Assets are not necessarily acquired for a single purpose. Assets useful for propaganda commonly have access useful to espionage and *vice versa*.

A thorough open-source identification of propaganda builds on, and is interlocked with, the media monitoring described earlier. The detection of propaganda will therefore also take into account signs such as the propaganda's theme, the sourcing of information, and so forth. While these signs partially guide the CE environmental scanning process to plausible and actual propaganda campaigns, supplementary criteria are considered. The latter include whether the perceptions the propaganda strives to influence are to the own state's disadvantage; the role player(s) entities that stands to benefit from the propaganda (to the own state's detriment); and whether the propaganda message contains elements of misrepresentation or disinformation.

6.2.7 Open-source indicators of cyber espionage

The increasing reliance on information technology over the last few decades for the storage and exchange of information in the private and public sectors world-wide have led to an unprecedented interconnection of the networks and related technology that facilitates these services. It follows that intelligence information is also vulnerable to cyber espionage and other related forms of hostile cyber-intelligence activities. Therefore, the postulation of open-source detectable espionage indicators requires conceptual clarity on the relationship between (cyber) espionage and other cyber activities of counterintelligence relevance.

6.2.7.1 Conceptual clarification

Helpful in this regard is the US Department of Defense's (as cited in US, 2009*e*: 170; emphasis in the original) definitions of the following concepts:

> *Computer Network Operations*: Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations.
> *Computer Network Exploitation*: Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.

> *Computer Network Attack*: Actions taken through the use of computer networks to disrupt, deny, degrade or destroy information resident in computers and computer networks, or the computers and networks themselves.

The definitions above, in short, suggest that network operations are both the object and the means to a cyber attack. Whereas the effects of cyber attacks are often visible, most intrusive and exploitation actions are done in such as way as to avoid detection. Exploitation assumes different forms and of which cyber espionage and certain types of cyber crime are examples. Cyber espionage is both an 'enabler' (for disruptive- destructive action and cyber crime) and an end in its own right (covert TECHINT information collection). Consequently, cyber espionage typically, but not always, precedes disruptive cyber action.[14] The manifestation of disruptive action could thus be a reactive indicator that cyber espionage has been conducted. Disruptive action can, under certain conditions, also be a concurrent (real-time) indicator of espionage in progress.

6.2.7.2 Cyber-espionage indicators in the all-source statutory counterespionage milieu

Apart from conceptual clarity, appreciating the challenge of the design of open-source cyber-espionage indicators necessitates brief reference to the statutory counterintelligence endeavour in this field. Within the statutory counterintelligence milieu, the timeous detection and exploitation of cyber-espionage attempts relies on offensive counter-CYBINT techniques.[15] For counter-CYBINT to be effective, offensive techniques function in synergy with, and are part of an integrated meta-system that incorporates, defensive measures. The offensive and defensive configurations generate massive amounts of counterintelligence relevant data. The data is processed through physical devices, and software tools which generate automated alerts based on preconfigured indicators. However

[14] Although no examples were found in literature consulted, a HUMINT asset ('agent') can provide information on system weaknesses exploitable for disruptive action. In these cases HUMINT and not CYBINT precedes disruptive action.

[15] 'Fish bowling' was described in Section 6.6 (Chapter Three) as an example of offensive measures. Depending on the application or combination of applications used, this measure contains the intrusion within pre-set perimeters, while at the same time ascertaining the intrusion's origin, signature, information acquisition profile (intended espionage objectives) and disruptive aims.

sophisticated the digital system is, the attribution of intrusive cyber activity to an identifiable originator, such as the actual espionage actor, remains notoriously difficult. Two complimentary methods are used in this respect. Firstly, the "forensic analysis" of an intruder's signature and footprints can "sometimes reveal the affiliation of the responsible actor" (US, 2009*e*: 169). Secondly, an analysis of the "nature" of the intrusion according to criteria such as the information, networks and entities targeted may in some instances aid in surmising the identity of the originator and/or its sponsor. (US, 2009*e*: 169). An appraisal of this kind is referred to by this study as 'circumstantial analysis'.

Since the cyber space for a significant part comprises of a vast interconnected global web and commonly used technologies, the own state's counterintelligence endeavour is not dependent solely on self-generated data and information. The latter is augmented by data, information as well as assessments obtained through selective interaction with other nation states and corporate entities – such as information technology and security service providers as well as information security associations, organisations and professionals.

6.2.7.3 Cyber-espionage indicators as part of open-source counterespionage environmental scanning

The system, data and information as described above are classified and not at the CE framework's avail. Consequently, the project team faces the dualistic challenge of alternative sources and alternatives to conventional, system-based cyber-espionage indicators. Two micro-theoretical suppositions underpin meeting this challenge. Firstly, the construct 'cyber-espionage indicator' needs to be employed with connotations broader than its conventional system-based meaning. Within open-source CE scanning, the term 'espionage indicator' also pertains to cyber activities that are not strict definitional sense 'espionage'. In another difference from its conventional meaning, 'cyber-espionage indicator' furthermore includes not only specific incidents, but also trends and patterns derived from the appraisal of multiple incidents. Secondly, and given the CE framework's isolation from the own state system-based data, cyber-intrusion incidents and trends reported by other role players are central to inferring cyber-espionage risks to the own state. Flowing from this micro-theoretical positioning, the three open-source detectable cyber-espionage indicators are subsequently discussed.

(a) Incidents of cyber intrusions publically reported and relevant to the own state

The conceptual clarification earlier in the section showed cyber espionage as intertwined with various other forms of cyber intrusions. If reported in open sources, and subject to an appraisal of relevance to the own state, other forms of intrusion could directly or indirectly serve as indicators of cyber espionage. To be of optimal use, CE scanning self-evidently needs to identify intrusive incidents as soon as possible and when warranted issue interim warning products. Open sources are thus monitored mainly on-line and on a continuous basis for recent reports on not only cyber-espionage incidents but also the latest cases of detected malware (including viruses, worms, Trojan horses); Denials of Service (DoS) attacks; phishing; vandalism (for example site defacement and data corruption); cyber fraud and so forth. Such incidents are widely reported in sources ranging from popular media to specialised websites.

These reports do not necessarily link incidents to perpetrators. Within the open-source milieu, the attribution of actions to perpetrators is done mainly through circumstantial analysis. In other words, based on its knowledge of specific adversaries, the project team could make plausible assertions on the originator of malicious cyber activity. A recent "study" commissioned by the US government (as cited in US, 2009*e*: 169-170), for example, advances the following as the characteristic signature of PRC-sponsored malicious cyber activity:

- The extra-ordinary wide scope of the "computer network exploitation" that targets "many countries" around the world is beyond the capabilities of "virtually all organized cybercriminal enterprises and is difficult at best without some state sponsorship".
- The "depth of resources" required to sustain the scope, duration and focus of the exploitation suggests probable state sponsorship.
- The exploitation is executed with an exceptionally high degree of sophistication.
- The "type of information targeted" is congruent with the PRC's intelligence requirements (such as US "China-policy related information") and "has no inherent monetary value to cybercriminals".
- The exploitation is primary spearheaded towards governmental networks and those of high national-security relevance.

Information derived from widely-reported incidents of cyber intrusions could be insufficient for credible inferences on a plausible sponsor's signature. In such instances, the project team would be compelled to also utilise data as subsequently described under the second open-source indicator of cyber espionage.

(b) Emerging patterns of malicious cyber activities

Whereas the preceding indicator deals with *information* refined to, by lack of a more apt term, 'news item' format, the second indicator has as a supplementary source *data* on malicious cyber activities. While CE scanning is deprived of own state system-based data, Mena (2003: 326) correctly remarks that "data about cracker activity from all over the Internet" is freely available and "can be used to discover intrusion trends". Mena (2003: 326) continues with mentioning *DShield.org* and *Incidents.org.* as examples of such websites.

Varying from website to website, data is availed in various formats and levels of processing. In some instances, the data is relatively 'raw' and the project team's effective utilisation thereof would require data mining and analysis software. Other websites - such as *Messagelabs intelligence* hosted by the well-known cyber-security provider Symantec – avails data in processed format and furthermore offer a data content analysis. The following extract from *Messagelabs intelligence's* (2010: 1-17) monthly edition for March serves an example of data content analysis:

Figure 62: *Messagelabs intelligence: March 2010 report*

TARGETED ATTACKS		**MOST FREQUENTLY TARGETED INDIVIDUALS**	
Country of origin (Based on sender location)	**Percentage**		**Percentage**
PRC	**28.2%**	**Expert: Asian Defense Policy**	**15.3%**
Romania	**21.1%**	**Diplomatic Mission**	**15.2%**
United States	**13.8%**	**Expert: International Finance**	**7.9%**
Taiwan	**12.9%**	**Expert: Asian Foreign Policy**	**5.0%**

Source: *Messagelabs intelligence – March 2010*: 3, 5 (adapted extract).

With the *caveat* that it is an oversimplification, the project team could have surmised from the data analysis above, that trends in malicious cyber activities internationally indicate a heightening in the risk of the PRC's cyber-espionage targeting of the own state's foreign missions. Information pertaining the own state's Asian foreign policy as well as its defence and economic strategy, would have been concluded, is particularly at risk.

(c) Trends in relation to the hacking community

Provided that it is executed in a secure manner, the monitoring of trends in relation to hacking community could provide indications of developing cyber-espionage risks. On certain hacker websites, "hacking tips" are openly shared and the "latest state-of-the-art software hacking tools" offered free of charge (Wettering, 2000: 276). Appraised through knowledgable eyes, the nature of the "tips" and the vulnerabilities in counter-CYBINT measures "hacking tools" target, could offer pre-emptive warning of nascent espionage risks to the own state.

Depending on the *modus operandi* of espionage opponents prioritised during earlier phases of the CE environmental scanning process, the monitoring of hacker sites may render signs of adversarial recruitment of freelance hackers. Chapter Three (Subsection 5.2.) mentioned North Korea's alleged recruitment of a team of 500 computer hackers. The PRC intelligence community is a further case in point. In addition to "patriotic" hackers (so called "red hackers"), unaffiliated, "freelance" hackers driven by "entrepreneurial" considerations are also used (US, 2009*e*: 175-176, 178).[16]

This section focused on the design and application of open-source espionage indicators. For contextual reasons brief reference was made to the use of espionage indicators in the all-source counterintelligence milieu. Subsequently, a definition of, and a proposal on the methodology for designing, open-source espionage indicators were advanced. The section proceeded with an outline of some open-source detectable indicators relating to the exploitation of diplomatic cover and missions for secret HUMINT intelligence gathering, the techno-scientific

[16] It must be cautioned that the identification of recruitment drives, and even more so the recruiter, is no easy feat. Offensive actions (such as solicitation and 'dangles') executed with a high-level of operational (cyber) security measures are generally required. Consequently, the intelligence service that commissioned the CE scanning, could deem such initiates as the prerogative of secret counterespionage and not within a parallel, open-source project's Terms of Reference (ToR).

field, the mass media and the cyber sphere. In line with assertions in Chapter Six, the section cautioned on the need for circumspection in the design and application of indicators. It was emphasised that indicators are design pursuant to, and are applied in the context of, a thorough knowledge of a particular espionage principal and espionage opponent(s).

Nevertheless, the design and application of open-source detectable espionage indictors in certain respects represent the culmination of the CE environmental scanning's focus on adversaries. Whereas the focus on adversaries is 'externally' orientated, the subsequent phase is 'introspectively' directed towards the own state. During this phase, which is discussed in the next section, the own state's vulnerabilities to espionage are ascertained.

7. THE OPEN-SOURCE IDENTIFICATION OF OWN STATE VULNERABILITIES TO ESPIONAGE

Espionage indicators determined during the preceding phase, however, are of direct relevance to the open-source identification of own state vulnerabilities to espionage. The latter are also linked with two other environmental scanning phases. Prior to addressing the interconnectivity between these phases, the chapter's theoretical-integrative objective necessitates a concise, recapitulative assimilation of notional propositions regarding vulnerabilities that emerged during the course of research so far. With reference to an analogy employed previously, a state's vulnerabilities to espionage are essentially 'clinks' in its defensive counterintelligence armour and inefficiencies in the wielding of the counterespionage sword in the protection of informational assets. Informational assets, Chapter Three (Section 6.5) asserted, reside in systems and humans. Informational assets are susceptible to espionage since the systems and humans in which they reside, as well as the means through which they are transferred, are fallible (Figure Five, Chapter Three). Micro-theoretically, vulnerabilities to espionage are situations resultant from the right assets being protected but with deficiencies in protection measures; and/or though the measures are not necessarily deficient, not all the right assets are safeguarded with the appropriate degree of protection. These measures were discussed in Chapter Three (Section Six) and Chapter Five (Section Seven) as ranging from passive-defensive physical security to aggressive counterespionage operations.

Within all-source counterintelligence, these measures, by and large, have as a complement built-in mechanisms and procedures through which vulnerabilities to espionage are ‘flagged’ for remedial action. In respect of personnel security, for example, predetermined criteria contained in a re-vetting risk profile could result in an individual being subjected to a comprehensive security investigation. Comparable criteria are also contained in procedures applicable to national-security relevant institutions which prescribe the reporting of behavioural patterns and incidents that reflect negatively on an employee’s security competency. In the TECHINT field, system audits are designed to detect weaknesses in INSYSEC measures (Section 6.3, Chapter Three).

The postulation on the subprocess for the open-source identification of own state vulnerabilities is based on the premise that the ToR does not permit parallel CE scanning access to the information generated by the counterintelligence measures and mechanism described above. A further premise applicable to Phase Ten is the ToR’s requirement for a panoptic counterintelligence perspective on the macro-environment (Section Three, Chapter Six). In line with this direction, macro-environmental drivers and trends impacting on own state vulnerabilities need to be explored. To this end, drivers and trends ascertained during the environmental probing in Phase Three (Section 5.4, Chapter Six) - which have implications for the own state’s vulnerability to espionage - are scrutinised in considerably more depth.

Since it was discussed in Chapter Two (Sections Two, Three and Four), the macro-environmental driver of globalisation is used for illustration purposes. A thorough scrutiny of globalisation’s impact on the own state’s espionage vulnerabilities, requires a society-specific, multi-disciplinary approach drawing on several disciplines outside Political Science, such as Sociology and Psychology. It is in conducting such multi-disciplinary research that OSINT stands out, and that constitutes one of the CE environmental scanning’s signature roles.

While there are few, if any, nation states unaffected by globalisation, the counterespionage implications thereof are determined by the nature of the particular state. There are, for example, differences in the manifestation in, and implications for, relatively homogeneous and ‘closed societies’ (for example the PRC and North Korea), and liberal, open societies such as the US. Assuming the own state to resemble the US in cultural diversification and technical advancement, the project team would have noted exemplary studies recently conducted under the auspices of the (US) Department of Defense’s Personnel Security Research Center. Of these, research by Herbig & Wiskoff (US, 2002*b*), Herbig (in US, 2008*b*; US, 2008*c*) and Kramer & Heuer (2007) stand out. These, and other studies, concluded multiple macro-environmental and societal trends, rooted in globalisation and technological advances, as increasing the US's vulnerability to "insider espionage" (US, 2008*b*; US, 2008*c*; US, 2005*e*: US, 2002*b*; Kramer & Heuer, 2007: 50-64).[17] In the methodical execution of scrutiny, it is advisable to adhere to a format that purposely links trends with implications for the own state. This methodology can be elucidated by means of the following tabulated summary in which only one of globalisation's multiple effects is highlighted:

Figure 63: Trends contributing to the own state's vulnerability to espionage

DRIVER : GLOBALISATION		
TREND : DIVERSIFICATION OF THE WORKPLACE		
Manifestation and impact		**Counterintelligence and counterespionage relevance**
Comparable state: **United States**	Over three decades (1970 – 2000) the total foreign-born population of the US increased with 191% and in 2005 stood at 10% of the total US population (US, 2005*e*: 17). A growing number of insiders with a foreign background have access to classified information (Kramer & Heuer, 2007: 56). Between 1992 and 2002 security clearances issued to naturalised or derived citizens for access to protected information increased by 23 % (US, 2007*e*: 17).	"Various foreign entities rely on ethnic recruitment. Of the individuals arrested for espionage in the US between 1990 and 2007, 35% were foreign-born, 58% had foreign attachments (relatives or close long-term friends abroad) and 49% had foreign cultural ties." (US, 2008: 28). Together with financial duress and technological advances, ethno-historic links are of primary concern (US, 2009*e*; US, 2008*b*; US, 2008*d*; US, 2008*e*; US, 2007*h*; US, 2001).
Own state	Findings as determined through the open-source scrutiny of the own state.	Findings as determined through the open-source scrutiny of the own state.

[17] The term "insider espionage" denotes the involvement in hostile espionage of individuals who have privileged access to own state sensitive and classified information.

	Recommendations: As in the US, foreign ethnic diversity in the own state's workplace is rapidly rising. It was ascertained during preceding phases of CE environmental scanning that espionage adversaries such as the PRC rely on ethno-historic recruitment. The own state is therefore increasingly vulnerable to insider espionage resultant from ethno-historic espionage recruitment. Ethno-historic links should be assigned apposite ranking in the revising of potential vulnerability indicators utilised in security clearances, vetting and re-vetting.

The value of macro-environmental scrutiny in respect of vulnerabilities thus clearly extends beyond mere 'academic background'. The outcome of the figure above is used to align counterintelligence instruments with a changing reality. Without distracting from its benefits to all-source counterintelligence, the said scrutiny's outcome in certain respects lacks specificity. At this stage it is neither clear which informational assets or national-security relevant institutions/individuals are at risk, nor which security measures are deficient. In the quest for specificity, the project team could conceivably endeavour to detect certain vulnerability indicators employed in all-source counterintelligence by means of open sources. Within the confines of a parallel project, the selective application of only some vulnerability indicators would of course realistically be achievable. Personnel lists of national-security relevant institutions may, for example, inform the application of vulnerability indicators derived from ethno-historic links. Indicators of this nature, however, should be applied as a collective that comprises of various other "categories", each with "multiple subcategories" (US (2007*g*: 52). Selective application is unsound counterintelligence practice and the outcome thereof is dubious.

The prudent approach to the open-source identification of own state's vulnerabilities to espionage recognises OSINT's limitations and does not attempt emulating the all-source effort in this regard. Given these limitations, the quest for specificity should be retrospectively directed towards Phases Four and Nine of the CE environmental scanning process.

During Phase Four two sets of counterespionage-relevant bodies of information were demarcated, namely those valued by the own state and those at premium in the macro-environment (Section Six, Chapter Six). These sets of information were appraised by means of a comparative appraisal (Section 6.4, Chapter Six). From the comparative appraisal, clusters of incongruences arise which are foundational to pronouncing on possible vulnerabilities in the own state's counterintelligence protection of its informational assets. Building on this foundation, Phase Ten scrutinises postulations Chapter Six (Section 6.4) advanced in explanation of the discrepancies and conclusions are reached on the plausible vulnerabilities in the own state's counterintelligence protection of pertinent informational assets. Since the location of the custodians of these informational assets were earlier determined (Phase Four – Chapter Six, Subsection 6.1.3) institutional vulnerabilities of specific national-security relevant entities are inferable.

The detection of espionage indicators *per* Phase Nine serves to give pointers to the plausible existence of a situation whereby an adversary exploits own state vulnerabilities in procuring own state informational assets through espionage. Espionage thus has the exploitation of vulnerabilities as a defining element. Espionage, *per absurdum*, cannot manifest against a state with impenetrable counterintelligence barriers (that is 'no vulnerabilities'). Consequently, the detection of espionage indicators simultaneously points towards plausible own state's counterintelligence vulnerabilities. It will be recalled that espionage indicators were designed to detect activities conducted by specific adversaries in the procurement (through espionage) of specific informational assets. Therefore it logically follows that espionage indicators can be employed to deductively infer vulnerabilities in respect of specific (own state) informational assets.

This section centred on the open-source identification of own state vulnerabilities to espionage. While the outcome of a macro-environmental scrutiny was found as being pivotal to align certain counterintelligence instruments to a changing macro-environmental and societal reality, it lacks specificity. Specificity in the identification of own state vulnerabilities to espionage, the section showed, relies on preceding phases of the CE framework.

Given open-source limitations, a lack in specificity regarding some own state vulnerabilities is nearly inevitable. Instead of endeavouring to 'bridge' open-source limitations through unsubstantiated inferences, specificity 'gaps' regarding own state vulnerabilities are categorically stated for pursuance by the commissioning intelligence service's all-source counterintelligence structures. Such statements, and the conversion of the CE scanning's outcome for pursuance by all-source counterintelligence, are done as part of a dedicated phase explicated in the next section.

8. COUNTERESPIONAGE ASSESSMENT AND CONVERSION

Ascertaining vulnerabilities, the preceding section emphasised, is not performed as a compartmentalised phase. Similarly, a counterespionage assessment is not performed in a single phase. Although the CE environmental scanning's culmination phase, the counterespionage assessment is a synthesis of appraisals executed throughout the process. Since the notion of 'espionage risk assessment' is imbedded in most phases, this notion was purposely addressed in considerable detail (in Section Two, Chapter Four) prior to proceeding to the explication of the CE environmental scanning *per se*. An 'espionage risk assessment' is a central component, but not the sum, of a counterespionage risk assessment. From a counterespionage perspective, espionage risks are opportunities for aggressive-offensively engaging the espionage opposition. Therefore, a counterespionage assessment is the broader construct within which an 'espionage risk assessment' is located, and as part of which it is further appraised for opportunities.

Against this background, the following is proposed as a format for the compilation of the CE scanning process's outcome:

Figure 64: A counterespionage assessment – a proposal on a format for use in open-source environmental scanning

	EXECUTIVE OVERVIEW
1	OWN STATE INFORMATIONAL ASSETS AT ESPIONAGE RISK
2	ESPIONAGE ADVERSARIES AND THEIR ACTIVITIES DIRECTED AGAINST THE OWN STATE
3	COUNTERINTELLIGENCE VULNERABILITIES AND DEFICIENCIES IN THE PROTECTION OF INFORMATIONAL ASSETS
4	COUNTERESPIONAGE PROJECTIONS
5	PRIORITISATION OF ESPIONAGE RISKS AND COUNTERESPIONAGE OPPORTUNITIES
6	RECOMMENDATIONS
7	CONCLUSION

The conversion of the CE scanning's outcome into actionable offensive countermeasures involves secret, offensive countermeasures. Prior to initiating such countermeasures, the CE scanning's outcome will self-evidently first be gauged against all-source counterespionage assessments. A primary motivation for conducting parallel CE scanning was to moderate the degenerative spiral discussed in previous chapters as endemic to all-source counterespionage assessments. It is therefore of the utmost importance, Chapter Five argued, that the CE scanning's product should be presented at a point in the all-source counterintelligence and counterespionage processes where it would have the optimal impact in 'breaking' this spiral. Chapter Five therefore extensively examined the CE framework's positioning from both theoretical and practical perspectives. It was found that the CE scanning's outcome (product) would be most beneficial to the all-source processes, if submitted to coincide with the comprehensive assessments typically conducted by statutory intelligence services annually or bi-annually (Figures 28 and 29, Chapter Five). So doing, the CE scanning process's outcome would optimally augment the (all-source) counterespionage assessment's formulation of counterespionage requirements and the setting of priorities. Should these priorities include espionage risks identified through the application of the CE framework, a contribution would have been made toward moderating the degenerative spiral.

9. CONCLUSION

This chapter presented the CE environmental scanning process's intermediate and final phases. This was done in accordance with the 'theoretical-integrative' and 'pragmatic-utilitarian' orientation explained in Chapter Six (Section One). In the explication of the phases, examples pertaining to the hypothetical 'own state' and the PRC were used.

The design of a subprocess for establishing justifiable grounds for asserting role players as espionage actors adversarial to the own state was explored firstly. The subprocess was found to span five phases, namely the identification and profiling of plausible espionage principles (Phase Five); the identification and profiling of plausible espionage adversaries (Phase Six); determining adversarial espionage *modus operandi* (Phase Seven); the design of open-source detectable espionage indicators (Phase Eight); and the application of these indicators (Phase Nine). The nature of the relationship between the own state and other macro-environmental role players was ascertained as a primary variable in determining not only espionage opponents, but also the (own state) secrets they would plausibly seek to procure through espionage. As mentioned, this subprocess also involved the design and the application of open-source espionage indicators. A proposal on the methodology of designing open-source espionage indicators, was advanced and illustrated by means of examples. It was found that within open-source CE scanning indicators should be designed pursuant to, and applied in the context of, a sound knowledge of a particular espionage principal and espionage opponent(s).

The chapter proceeded to examine the open-source identification of the own state's vulnerabilities to espionage. The outcome of a macro-environmental scrutiny emerged as useful in aligning certain all-source counterintelligence instruments to a changing reality. It was further found that preceding phases of the CE framework enable the identification of more specific own state vulnerabilities to espionage.

Lastly, a proposition was made on the CE environmental scanning process's final phase, namely an open-source counterespionage risk assessment. The critical importance of the CE scanning outcome's positioning in moderating the degenerative spiral endemic to all-source counterespionage assessments was emphasised. In accordance with Chapter Five's findings, a proposal was advanced on the CE framework's optimal location within all-source processes.

CHAPTER EIGHT

EVALUATION

Subsequent to the presentation of the process of, and framework for, open-source CE environmental scanning in Chapters Six and Seven, this chapter summarises the research conducted in these and other chapters. The chapter proceeds with evaluating the main assumptions which underpinned the research. It concludes with some observations and recommendations on areas for further research within Intelligence Studies on aspects related to this study.

1. SUMMARY AND OVERVIEW OF CHAPTERS

Chapter One advanced the study's objectives, research problems and questions, assumptions as well as a selective review of relevant literature. The research was posited as part of the quest by statutory intelligence services for theoretical constructs that can optimise the effective utilisation of the near overwhelming, and still exponentially increasing, body of open-source information. The literature overview provided in the chapter showed the need for theoretical frameworks of such a nature as being particularly acute within (statutory) counterespionage. At least in so far as Intelligence Studies is concerned, existing literature is practically silent on such frameworks within the counterespionage sphere. This void, it was argued, is partially ascribable to an over-reliance on secret information within the statutory counterespionage milieu. Counterespionage is, of course, directed towards adversaries that operate clandestinely and the subdiscipline is thus per definition inherently secretive. Nevertheless, an over-reliance on secret information has as near inevitable outcome a degenerative self-feeding spiral of prioritisation and collection. Moreover, such over-reliance deprives counter-espionage of the opportunity to identify and describe through open-source environmental scanning espionage risks not necessarily detected through secret collection methods.

The foregoing assertions on the near overwhelming challenge posed by the voluminous extent of open-source information and the need within counterespionage for theoretical constructs for the effective utilisation thereof, formed the basis for the study's two-pronged primary research question, namely:

- To what extent, and in which manner, will open-source environmental scanning benefit the statutory counterespionage function, specifically insofar as the identification, description and prioritisation of undetected espionage risks are concerned?

- What information should open-source counterespionage environmental scanning ideally 'look for' (collect) and how should the information be 'looked at' (identify and assess espionage risks)?

In addressing the research question, the study had the principal objective of designing, contextualising and elucidating a micro-theoretical framework for open-source environmental scanning within the civilian counterespionage milieu. In practical terms, and with the *caveat* that the research's aim is not the forwarding of a 'quick-and-simple recipe', the principal objective was explained as pertaining to the methodical structuring of open-source environmental scanning in clusters of activities ('steps'). It was emphasised that a micro-theoretical framework of this nature is a conceptual instrument employed within a broader process which also includes the framework's design and the planning of scanning activities. Consequently, the formulation of this broader counterespionage scanning process was advanced as a concomitant research objective. Counterespionage, in turn, is but one of counterintelligence's subdisciplines. Therefore, the examination of some existing views on the counterintelligence process, and if so required the construction of an alternative proposition accommodative of the CE framework were posed as sub-objectives. Lastly, the elucidation of the CE scanning framework and the process's theoretical design by means of examples were dealt with as a sub-objective.

Chapter Two presented the conceptual and theoretical foundation on which the research objectives and sub-objectives were pursued. This entailed, firstly, defining and demarcating concepts central to the research. The chapter commenced with an examination of 'national security' as the overarching concept in the theoretical approach to the study. The study ascertained that national security is a subjective notion that evades the assigning of even an enumerative, universally accepted definition. The chapter's finding on national security being the outcome of a subjective political choice - with its delineation varying from state to state - was centrally relevant to research further conducted. Certain variables that underpin a nation state's subjective national security perception, for example, were informative to the CE framework's design in later chapters. Other concepts defined and demarcated with a view to subsequent chapters, included 'intelligence', 'counterintelligence', 'counterespionage', 'risk' and 'threat'.

Secondly, and interlocked with the definitional conceptualisation, Chapter Two provided an overview of the theoretical discourses on respectively national security and intelligence (inclusive of counterintelligence and counterespionage). In contrast to Political Science's extensive *corpus* of literature on the debate on national security, Intelligence Studies emerged as a critically under-theorised academic field. Intelligence Studies' under-theorisation, the study contended, is in part ascribable to insufficient cognisance in academic studies of the different layers of theory, namely the meta-paradigmatic, paradigmatic, grand, meso, micro and the praxis levels. The research incorporated the different theory levels in a proposition on a *Matrix for the plotting of intelligence theories* (Figure Three).

In line with the study's assertion on the importance of purposely positioning theoretical contributions to Intelligence Studies, the micro-theoretical CE framework was superimposed on a positivistic meta-paradigmatic and a realist paradigmatic position. Given the infancy of Intelligence Studies' theoretical discourse, the superimposition of the CE framework on the grand and meso theory 'templates' was considerably more problematic. Instead of over-ambitiously endeavouring the postulation of a grand theory of intelligence, the research was limited to a contribution that at most constitutes a contour toward a grand theory of intelligence. The organism notion was proffered as an analogical construct for a broad theoretical configuration on the grand and meso-levels. The organismic notion was furthermore extended to include the concept of environmental scanning. The said theoretical configuration was concluded to be congruent with realist conceptualisations of intelligence and counterintelligence. Therefore, it presented a feasible higher order template for the CE framework's design.

Whereas Chapter Two explored theoretical imperatives**, Chapter Three** explicated the international security environment as the 'reality' according to which the CE framework's scanning focus needed to be aligned. While this chapter was predominantly devoted to examining the reality of international espionage and statutory counterintelligence, the research's micro-theoretical orientation necessitated propositions on the following conceptual constructs for systemising open-source environmental scanning of the expansive macro-environment:

- The structuring of the macro-environment in the following sectors: political, military, social, technological, economic, ecological (environmental), and informational.
- A distinction between external and internal environmental scanning.

- The calibration of the CE framework's focus on a continuum that moved from general scouting (for 'drivers' and 'strategic trends') to directed scrutiny (for 'espionage risks'). This varying resolution was concretised in distinguishing between the CE environmental scanning's 'contextual focus', 'focus areas' and 'focal points' (Figure Six).

In elucidating the CE environmental scanning's 'contextual focus', some open-source determined drivers, strategic trends as well the impact on contemporary espionage and counterintelligence were indicated.

Since the CE framework's primary aim is the open-source detection of adversarial espionage, the research proceeded with exploring 21st century espionage threats, risks and challenges confronting the nation state. This examination, in short, sought to respond the questions 'which are the nation state's most salient espionage adversaries?' and 'how do these espionage adversaries spy against the nation state?' The multitude of adversarial espionage actors concluded to be of particular relevance are listed in Section Two (Chapter Eight). Subsequently, the categories of information the actors collect, as well as the HUMINT and TECHINT collection methods they utilised, were discussed. In respect of TECHINT, a proposal was forwarded for the inclusion of CYBINT as a fourth main subdiscipline (alongside SIGINT, IMINT and MASINT). A key finding was that clandestine TECHINT collection methods, previously the prerogative of nation states, are increasingly at the disposal of other espionage adversaries.

Effective counterintelligence, the study emphasised, is a multi-disciplinary endeavour that requires the synergetic employment of countermeasures. Seeing that the CE framework is envisaged as a statutory counterespionage instrument to be used in conjunction with other counterintelligence methods and measures the nation state employs, these methods and measures were researched. The study found existing categorisations of countermeasures to be inadequate to provide for the 21st century's 'converged technological reality'. Therefore, INSYSEC was submitted as a subcategory of countermeasures.

Expanding on the theoretical and practical imperatives discussed in the preceding chapters, **Chapter Four** determined concrete requirements relating to the CE framework. The research was aimed at establishing not only requirements *posed to* the CE framework, but also the requirements *posed by* this framework's design. Requirements *posed by* the CE framework design, simply put, concerned the theoretical constituents ('building blocks') and conceptual approaches indispensible for its effective construction.

The open-source identification, description and assessment of espionage risks emerged as the primary and self-evident requirement which the CE framework should meet. Other salient requirements posed to the CE framework were the moderation of intelligence failures; the CE scanning process's synergetic integration with, and positioning, *vis-à-vis* all-source counterintelligence; a scanning outcome that should comprise of several types of intelligence; the moderation of intelligence failures and the optimal utilisation of open-source information. Should these requirements be met, the chapter argued, the open-source based CE framework could offer invaluable benefits to the all-source intelligence and counterintelligence effort.

In the course of the research, certain pre-conditions for attaining these benefits optimally transpired. It was found that the open-source CE scanning process would be best executed as a parallel ('red team') project. Furthermore, it emerged that the design of an effective CE framework required certain pivotal conceptual approaches and theoretical constituents. Propositions in Intelligence Studies on such approaches and constituents were found to be either lacking or directed towards positive intelligence and thus not apposite to statutory counterespionage. Proposals were thus submitted in respect of the following:

- A definitional categorisation providing for 'espionage risks', 'espionage threats' and 'corroborated adversarial espionage'.
- An overarching conceptual construct for the assessment and prioritisation of counterespionage concerns in general and counterespionage risks in particular.
- A typological schema of intelligence types with specific reference to counterespionage. This rather extensive schema was deemed essential since it provided clarity on the CE scanning process's outcome, enabled the aligning of the outcome with that of all-source counterintelligence and rendered insights valuable to the CE framework's design (such as the role of indicators in warning intelligence instruments).
- An alternative approach by means of which OSINT is synchronically aligned with all-source intelligence. Contrary to existing conceptualisations, the alternative approach posited OSINT not as a separate 'pillar' or 'foundation', but as a dimension of statutory intelligence as a whole. OSINT was depicted

as being amalgamated with the all-source effort, and as involving all collection subdisciplines. The contention of OSINT comprising of HUMINT and the different TECHINT collection subdisciplines was incorporated in the CE scanning process's design.

Albeit from different perspectives, Chapters Two to Four underscored the importance of presenting the micro-theoretical CE framework as part of a multilayered unison of the 'higher order' intelligence, counterintelligence and counterespionage processes. **Chapter Five** examined some existing postulations on these higher order processes with a view to ascertain their suitability for accommodating the CE framework. As subsequently explained in the testing of assumptions (Section Two, Chapter Eight), existing conceptualisations were found to be inadequate and alternative propositions on the counterintelligence and counterespionage process were advanced.

Based on a distinction between, on the one hand, the role of OSINT within the counterespionage process in general and, on the other hand, the specialised function fulfilled by the CE framework, the latter was subsequently aligned with the all-source counterespionage process. Given the CE framework's objective of moderating the earlier noted degenerative spiral endemic to all-source counterespionage, the positioning of the framework (within the all-source counterespionage process) was examined in depth.

Incorporating and expanding on constituent elements and other theoretical constructs submitted in preceding chapters**, Chapters Six and Seven** advanced the integrated process for open-source CE environmental scanning and risk assessment. Although structurally divided, Chapters Six and Seven formed a unit. The rest of the study overview therefore neither distinguishes between these chapters nor does it mirror the chronology in which the research's outcome was presented (within each of the respective chapters).

In expounding the process for open-source, CE environmental scanning and risk assessment, the study followed an approach that was concurrently theoretical-integrative, pragmatic-utilitarian and illustrative. Without compromising its micro-theoretical orientation, the research engaged 'real-life' challenges regarding the use of open-source information in statutory, counterespionage practice. On an illustrative level, as was noted in Chapter One, the process was elucidated through examples that employed a hypothetical own state that had the PRC as one of its primary espionage adversaries.

Given the earlier asserted need for the CE scanning process to be executed as a parallel *project*, Project Management literature on methodological project structuring was consulted. A hierarchical distinction between stages, phases and subphases was concluded to be suitable for the CE scanning process's structuring. Deviating from the conventional five-stage structuring, the research established a three-stage division as more apposite to the CE scanning process's needs. The three main stages proposed for the clustering of the various phases of the CE scanning process were the following: (a) conceptualisation, design and planning, (b) implementation, and (c) conversion. The stages, in turn, spanned a total of eleven phases. The phases and stages were furthermore linked to specific problem statements for guiding the CE scanning process (Figure 33).

The conceptualisation, design and planning stage was postulated to consist of three phases, namely the establishment of the ToR *(Phase One*); the derivation of the primary scanning requirements from the ToR (*Phase Two*); and the design and configuration of the execution of environmental scanning *(Phase Three)*. Phase Three had as a central subphase the design of a methodological schema (the CE framework) for the execution of the scanning. The study advised that, prior to proceeding to the execution stage, the practical feasibility of notional constructs – such as the CE framework – should be tested by means of a probing report.

With a view to the CE framework's design, the research evaluated and found the following as deficient in respect of counterespionage in general and open-source CE environmental scanning in particular:

- The use of quantitative-*cum*-numeric formulae for espionage risk identification and assessment. It was contended that such formulae convey illusory certainty over aspects that defy quantitative-*cum*-numeric 'weighing'. Therefore, the CE framework should be qualitative in its design.
- An indicators-at-the-start-and-centre approach to open-source environmental scanning. While the invaluable role of indicators in open-source CE scanning was recognised, reservations were raised about the practice of positioning indicators as the predominating nucleus of the design and execution of open-source environmental scanning. Reliable espionage indicators should be designed as part of, and not prior to, the execution of the CE scanning process. These indicators should furthermore be employed at a relatively advanced juncture of the scanning process.

- The ‘adversary-centric default starting point’, frequently and erroneously resorted to in all-source counterespionage. Instead, the execution stage should commence with the identification of espionage and counterespionage’s referent objects (‘secrets’).

In line with the last-mentioned finding, the determination of ‘secrets’ was posed as the CE environmental scanning execution’s launching phase *(Phase Four*). Of all the phases of the CE environmental scanning process, this phase was by far the one that was the most extensively discussed. The comprehensiveness of its discussion was asserted to be proportionate to both its importance and the actual effort allocated to it in practically performing open-source CE environmental scanning. Several subphases were proposed for demarcating two ‘sets’ of counterespionage-relevant bodies of information, namely ‘own state secrets’ and ‘premium informational areas’. Propositions were further made for the methodological structuring of subphases by means of specific steps and the employment of conceptual matrixes. Juxtaposed, and refined in accordance with the mandate of the civilian intelligence service, the convergence of own state secrets and premium informational areas offered qualitative premise for the identification and prioritisation of macro-environmental role players that may pose espionage risks to the own state.

Phase Five aimed to establish credible grounds for plausible assertions on which of the prioritised role players could be deemed to be the own state’s espionage adversaries. Credible grounds, it was argued, rest on the preconditions of ‘substantive motive’ and ‘sufficient espionage capacity’. The open-source determination of espionage motive proved to be particularly challenging. Endeavouring to meet this challenge, a three-tiered model for appraising espionage motive – reflected on in Section Two (Chapter Eight) – was proposed.

While useful, assertions emanating from the three-tiered model’s application would mostly be circumstantial-estimative and lacking in the specificity required for the tactical identification and assessment of espionage risks. Subsequent CE environmental scanning phases proposed to enable specific-conclusive assertions on adversarial espionage intent, opponents and activities were as follow: the profiling of espionage opponents (*Phase Six*); ascertaining adversarial espionage *modus operandi* (*Phase Seven*); designing of open-source detectable espionage indicators (*Phase Eight*); and applying open-source espionage indicators (*Phase Nine*). The research found that these phases’ cumulative outcome enabled credible pronouncements on the plausible existence of situations whereby adversaries are exploiting, or intend to exploit, own state vulnerabilities in procuring own state informational assets through espionage.

The open-source detection of espionage indicators, by way of inference, could also serve as pointers towards the identification of own state vulnerabilities. Own 'vulnerabilities', the study contended from a micro-theoretical perspective, is *sine qua non* to postulations of espionage risks. Therefore the CE scanning process could not suffice with indirect inferences. *Phase Ten* of the open-source scanning process was therefore centred on the purposeful identification and assessment of own state vulnerabilities on a strategic as well as a tactical level.

Lastly, a proposition was submitted on the CE environmental scanning process's final phase, namely an open-source counterespionage risk assessment (*Phase Eleven*). This included a proposed format for the product submitted to the intelligence service that commissioned the scanning.

On the basis of the foregoing summary and overview, it can be concluded that the study succeeded in addressing the research problem and that the research objectives were attained.

2. TESTING OF ASSUMPTIONS

The research, summarised and overviewed in the preceding section, was based on the following central assumption:

The environmental scanning and the contextual analysis of overt information enable the identification, description and prioritisation of espionage risks that would not necessarily have emerged through statutory counterespionage processes that rely on classified information. While complementary to the latter, the environmental scanning framework was presumed to offer a theoretical foundation to surmount an over-reliance on classified information and to enrich the counterespionage process on a tactical as well as strategic level.

Academic convention usually compels a case study in the validation of an assumption of this nature. It was, however, emphasised that a case study in support of the research theme would have required extensive resources – inclusive of a seasoned counterintelligence project team and relatively high-cost information services/databases. An academic justifiable case study would also have required secret information which statutory intelligence services would self-evidently not avail for an academic study. Substantiating the assumption's assertion on the enrichment of the all-source counterespionage effort by means of case study would, for example, entail a comparative appraisal of classified intelligence products. Understandably, neither the said resources, nor secret information was at the study's disposal.

Nevertheless, the research fully validated the primary assumption in two respects. Firstly, the open-source CE scanning process presents a micro-theoretical foundation for refining the praxis for the identification, description and prioritisation of espionage risks not necessarily detected through statutory counterespionage processes reliant on classified information. Secondly, the elucidation of the CE scanning process and framework by means of examples – which employed a hypothetical own state with the PRC as one of its primary espionage adversaries – supports the assumption.

2.1 ASSUMPTION ONE

A methodically demarcated referent premise enables the focusing and structuring of the counterespionage environmental scanning process amid the exponential proliferation of overt information.

In explicating the assumption, Chapter One postulated the referent premise as compromising of two sub-assumptions. Firstly, the convergence between a sponsor government's objectives and the legislative counterespionage mandate of a particular intelligence service would demarcate and prioritise the spectrum ('terrain') of overt information to be scanned and assessed. Secondly, the aim of the environmental scanning (namely the identification, assessment and prioritisation of espionage risks) would constitute the specific focal points of scanning within the demarcated 'terrain'.

The study found a referent premise that incorporates the convergence between a sponsor government's objectives and the legislative counterespionage mandate of a particular intelligence service as pivotal in directing and structuring the open-source CE environmental scanning process. Chapter Six (Sections Four to Six) showed the said convergence as underpinning the identification of the own state's critical informational assets in Phase Four of the CE environmental scanning process. Implicitly, the ToR are project-specific documentation of the convergence of the sponsor government's objectives and the intelligence service's mandate (Section Three, Chapter Six). In this sense, the convergence is foundational also to the CE scanning's conceptualisation, design and planning stage (Phases One to Three). The convergence can thus be concluded as indispensible to Phase

One to Four during which the CE scanning process referent premise is formulated. In the course of the research, however, it emerged that the referent premise requires a third 'pillar' namely, informational areas at premium in the macro-environment (Figure 37, Chapter Six).

In accordance with the assumption set out above, the research found CE environmental scanning's aim (of identifying, assessing and prioritising espionage risks) as the key determinant of specific, scanning focal points. This assumption was validated theoretically in Chapter Three (Figure Six) and practically illustrated in Chapters Six and Seven.

While most dimensions of the assumption were supported by the study, an addition to the CE scanning process's referent premise was necessitated. On the whole, the assumption was thus partially verified by the research conducted.

2.2 ASSUMPTION TWO

Effective environmental scanning of overt information for counterespionage necessitates a distinctive definition of 'risk' and 'threat', as these are interlinked yet different concepts. It is therefore asserted that current notions on 'threat' and 'risk' are inadequate for feasible employment within an overt counterespionage environmental scanning framework.

In explicating the assumption, an espionage risk was defined as 'a plausibility statement of a situation, resulting from the activities of an opposing intelligence entity, which exists or may develop in a manner impeding a sponsor government optimally in pursuing its strategy and realising its objectives.' An espionage threat was posed as 'a probabilistic statement (with a high degree of certainty) regarding such a situation.' A 'risk' was therefore expected to be distinguishable from a 'threat' primarily on the basis of an inherent quality of uncertainty.

Literature reviewed in the course of the research is silent on distinctive definitions of the concepts 'espionage risk' and 'espionage threat' (Taylor, 2007; Godson, 2001; Wettering, 2000; deGraffenreid, 1989; Johnson & Wirtz, 2004; Shulsky & Schmitt, 2002; Scott & Jackson, 2004). As was noted earlier, the limited propositions within Intelligence Studies relevant to such definitional distinction were found to be geared towards positive intelligence. Definitional distinctions and factors forwarded in propositions by Bernhardt (2003: 142-144; 2004: 63-64), the ASIO (as described by Wing, 1999: 86-94) and Quiggin (2007: 23-43, 199-202, 227-238) were evaluated for application in the formulation of the concepts ‘espionage risk’ and ‘espionage threat’. This evaluation ascertained existing postulations as not germane to the counterespionage sphere (Section 2.1, Chapter Four). Instead, a specific variant of ‘certainty’, namely the ‘degree of verification’, emerged as the key criterion to distinguish between ‘corroborated adversarial espionage’, ‘espionage threats’ and ‘espionage risks’. The distinction was central in the definitions of these concepts thus forwarded in Chapter Four (Section 2.3). While more refined, the definitions forwarded are in essence congruent with the definitional delineations of an espionage risk and espionage threat set out in the assumption. Consequently, the assumption was verified in full by the research.

2.3 ASSUMPTION THREE

A framework for overt counterespionage environmental scanning has as its primary requirement the ability to identify diverse risks, descriptively and predicatively, on a strategic as well as a tactical level.

Through an overview of the 21st security ‘reality’, as well as the design and elucidation of the CE environmental scanning process, the research demonstrated the identification and description of diverse risks as this instrument’s primary requirement. This diversity pertains to the multitude of actors and was ascertained to include opposing nation states; entities within private enterprise; NGOs; entities within the mass media; terrorist and extremist groupings; and unaffiliated individuals/groups. These role players were found to constitute the contemporary espionage ‘reality’ confronting the nation state (Treverton, 2005: 1-11; Burgess, 2008: 1-11; Kabay, 2008: 1-16; Kitfield, 2007: 1-7; Germany, 2005: 264-285; Wettering, 2000: 269-294; US, 2007*d*: 1-11). The CE framework was designed accordingly and configured to identify espionage risks posed by various categories of role players (Chapter Six: Section 6.3, Figures 46 and 47).

Secondly, the diversity of espionage risks relates to the various macro-environmental sectors and subsectors from which espionage risks emanate. Chapters Three, Six and Seven showed espionage to be prevalent in the political, social, economic, military, ecological, technological and informational sectors. By means of examples, Chapter Six and Seven moreover demonstrated the diversity of espionage risks within specifically the technological sector and its multiple subsectors. Hence, the CE framework’s design was aligned to detect the sectoral and subsectoral diversity of espionage risks (Figures 42 and 45, Chapter Six).

In outlining the CE framework’s outcome as an aggregate of intelligence types, Chapter Four (Section Three) validated theoretically the requirement for the open-source CE environmental scanning to function at a strategic-predicative level. Chapters Six and Seven reflected this requirement more practically in various aspects of the CE framework’s design and application. The strategic-predictive identification of own state informational interests and assets, for example, was illustrated through the employment of pro-active scenario building (Subsection 6.1.4, Chapter Six).

On the basis of the findings above, all aspects of the assumption can be deemed as verified by the study.

2.4 ASSUMPTION FOUR

The degree of adversity in the relationship between a government and an adversary constitutes the principal indicator and determinant of an espionage risk.

The stratification of the adversity in three tiers (cooperation, competition and conflict) was presumed to offer a ‘barometer’ for the presence of espionage risks and to inform the description and categorisation of such risks. It was further assumed that cooperation between a government and an opponent on a specific issue would denote a limited espionage risk, with the opposite applying should there be intense conflict. A consequential assumption was that in instances of intense conflict an opponent would resort almost exclusively to target-specific clandestine espionage activities, while cooperation would be accompanied by low-risk overt information gathering. The employment of this stratification was expected to ‘uncover’ espionage risks through the assessment of overt information and to be central in to the categorisation and prioritisation of risks.

The conducted research supported the assumption of the usefulness of a three-tiered relationship stratification as indicative of, and informative to, the description and categorisation (prioritisation) of espionage risks. The stratification was shown to be decisive in the open-source ascertainment of espionage principals as well as inferences on *inter alia* adversarial espionage motive, intent and collection mode (Figures 50 to 52, Chapter Seven). As was mentioned, the study forwarded an ideal-type model based on the three-tiered relationship stratification. The addition of ‘espionage value’ as correlation determinant enabled the refinement of the ideal-type model into matrixes and other conceptual tools for aiding the open-source CE scanning process (Figures 52 to 57, Chapter Seven).

The degree of adversity between a government and an adversary therefore constitutes a principal, but is not the sole indicator and determinant of an espionage risk. Since the addition of 'espionage value' as a co-variable ('correlation determinant') was required, the assumption was only partially verified by the research.

2.5 ASSUMPTION FIVE

The logical accommodation of a framework for overt counterespionage environmental scanning necessitates a distinctive counterintelligence cycle, as existing conceptualisations of the intelligence cycle are inadequate.

The research's appraisal of several conceptualisations within Intelligence Studies (including those of Gill & Phythian, 2006: 3-6; Lowenthal, 2003: 51-52; Bernhardt, 2003: 27; Codevilla, 1992: 4, 26, 35, 325-326) as well as official views on the intelligence process (US, 2005*b*: 583-585; Canada, 2004: 1), showed these to be apposite neither to counterintelligence and counterespionage in general, nor to the CE framework in particular. In what arguably remains the predominating conceptualisation, a cyclic counterintelligence process is seen as replicating the traditional (all-discipline) intelligence cycle in sequence and activities. As to the linking of counterintelligence with other intelligence subdisciplines, nebulous reference is made to counterintelligence being "performed throughout" the traditional intelligence cycle (Codevilla, 1992: 35).

Although Business Intelligence thinking cannot be summarily applied to Intelligence Studies and statutory intelligence practice, some propositions on comparable processes were reviewed. These included works by Nolan (1997: 53-61), Fleischer & Bensoussan (2003: 6) and Brouard (2004: 2-3, 5, 8-9). Business Intelligence transpired to be more developed in the conceptual structuring of the counterintelligence process and the integration of the latter with positive intelligence.

The construction of an overarching all-discipline intelligence process was deemed as intricately linked with a grand theory of intelligence and its formulation not realistically achievable within the bounds of an exploratory, micro-theoretical study. The study therefore sufficed with advancing a reductive conceptual nexus toward an all-discipline intelligence process (Figure 26, Chapter Five). This conceptual nexus advocated a clear distinction between 'intelligence 'subdisciplines', 'functional areas' and 'practicalities'. In contradiction of one of

Intelligence Studies' axioms, statutory intelligence was argued to consist of three principal subdisciplines, namely, 'positive intelligence', 'counterintelligence' and 'covert action'. 'Analysis' and 'collection' were posed as functional areas of activity that are performed within all three subdisciplines.

A proposition on the all-source, statutory counterintelligence process was also advanced. The proposition provided for clusters of distinctive offensive and defensive counterintelligence activities. These activities, it was contended, are interlinked through a multi-directional flow (Figure 27, Chapter Five). Within the parameters of the counterintelligence model, the study presented a proposal on the all-source counterespionage process (Figure 28, Chapter Five). As suggested in Section One (Chapter Eight), the research examined in considerable depth, the positioning of the open-source CE scanning process *vis-à-vis* the counterintelligence and counterespionage processes. The study's propositions on the latter were found to be accommodative of the CE framework. The earlier noted appraisal of some existing conceptualisation of the intelligence and counterintelligence processes, coupled with the subsequent construction of alternatives germane to the CE framework, thus fully validated the assumption.

This section, to summarise, showed the core of the assumptions, posited at the study's outset, to have been largely supported by the research conducted. In some measure, three assumptions nevertheless transpired to have certain shortcomings and amendments were necessary in the course of the research. The CE framework's referent premise (Assumption One) emerged to be lacking in its omission of a third 'pillar' (informational areas at premium in the macro-environment), while the addition of 'espionage value' to the three-tiered relationship (Assumption Three) was required for concretising this stratification into conceptual, environmental scanning aids. Lastly, the micro-theoretical study had as prerequisite alternative postulations not only in respect of counterintelligence and counterespionage (Assumption Five), but also all-discipline intelligence.

3. CONCLUSION

At the onset of the study, the challenges posed by research into the use of open sources in the secretive counterespionage sphere were anticipated. This challenge prompted the study and underpinned the research problem, the research questions as well as the research objectives. The compounding factor of forwarding an unclassified thesis – based solely on open-source information –

centring on this subdiscipline was also expected. Likewise, cognisance was taken of the implications for an academic study of 21st century counterintelligence's, and therefore counterespionage's, complexity.

The aftermath of 9/11 – especially from 2005 onwards – transpired to have been a watershed for theoretical thinking within Intelligence Studies. Consequently, the research needed to account for the discourse's crystallising agenda which, as was mentioned before, centres on the laying out of 'what we know'; the identification of 'what we do not know'; and the construction of theories *of* and *for* intelligence. In the wake of the discourse, some theoretical axioms that enjoyed relatively broad-based consensus for more than five decades are crumbling. A recurring reverberation throughout the study was that these axioms are simply no longer congruent with the way in which intelligence, counterintelligence and counterespionage function. Yet, the progression toward viable alternatives is still in its infancy. The sobering implications this held for a study aimed at advancing a micro-theoretical construction, are clear from the following (re-quoted) caution by the pre-imminent Intelligence Studies scholar L.K. Johnson (in Gill, 2006: 5): "The objective is less to impart new knowledge than to lay out what we know in such a manner as to suggest next steps in theory construction".

An attempt to circumvent this predicament through fleeting reference to 'what we know' and/or the qualified use of anachronistic intelligence theory, would have infringed on the study's academic integrity. The study's consequential attempt to contribute to laying out 'what we know' about counterespionage and its endeavour to offer exploratory propositions on those higher-order theories indispensible to the CE framework's design, profoundly impacted on the research. It is against this background, that the thesis should be viewed. Therefore, foundational chapters (Chapters Two to Five) are specifically relevant to micro-theoretical, counterespionage propositions and thus eventually to counterespionage praxis. A perusal of the study through this prism would show that the various chapters did not address salient aspects of counterintelligence and counterespionage (such as the range of offensive and defensive counterintelligence measures) in a repetitive manner. Each chapter examined such aspects with distinctive perspectives and different aims. Ostensive overlaps are in fact context essential for maintaining argumentative-logical coherence in theoretical deliberations on the most complex intelligence subdiscipline.

These reflections, coupled with the open-source CE environmental scanning framework and process's design, illustrated the opportunities afforded by what can possibly be best described as a revolution in Intelligence Studies thinking. On a grand theory level, the pressing need for an integrative construct providing for positive intelligence, covert action and counterintelligence, can hardly be overemphasised. Systems theory, rooted in the realist paradigm, was noted as one such promising option. It was also noted that, regardless of what route(s) pursued in the development of a theory of intelligence, it will probably be an incremental process benefiting from postulations on the praxis, micro- and meso-levels. Phrased differently, theories for intelligence will aid in postulating theories of intelligence (and *vice versa*).

Within the confines of this study only a few dimensions of open-source utilisation in counterespionage could be addressed micro-theoretically. The uses of open sources in counterintelligence, wider than a parallel CE environmental scanning project, remain largely unexplored – micro- as well as meso-theoretically. The research conducted into open-source espionage indicators was therefore not comprehensive. Micro-theoretical and praxis studies would undoubtedly find and refine many more.

Clearly then, the thesis affirms Johnson's (2007: 4) earlier quoted remark: "Overall, the studies on intelligence theory find that the discipline remains in its infancy, holding great promise for scholars interested in blazing new trails."

SUMMARY

Title: Open source environmental scanning and risk assessment in the statutory counterespionage milieu
By: P. C. Duvenage
Study leader: Prof. M. Hough
Degree: Doctor Philosophiae (Political Science)
Department: Political Sciences, University of Pretoria

The research focuses on the utilisation of open-source information in augmentation of the all-source counterespionage endeavour. The study has the principal objective of designing, contextualising and elucidating a micro-theoretical framework for open source environmental scanning within the civilian, statutory counterespionage sphere.

The research is underpinned by the central assumption that the environmental scanning and the contextual analysis of overt information will enable the identification, description and prioritisation of espionage risks that would not necessarily have emerged through the statutory counterespionage process in which secretly collected information predominates. The environmental scanning framework is further assumed to offer a theoretical foundation to surmount a degenerative counterespionage spiral driven by an over-reliance on classified information. Flowing from the central assumption, further assumptions formulated and tested in the research are the following:

- A methodically demarcated referent premise enables the focusing and structuring of the counterespionage environmental scanning process amid the exponential proliferation of overt information.
- Effective environmental scanning of overt information for counterespionage necessitates a distinctive definition of ‘risk’ and ‘threat’, as these are interlinked yet different concepts. It is therefore asserted that current notions of ‘threat’ and ‘risk’ are inadequate for feasible employment within an overt counterespionage environmental scanning framework.
- A framework for overt counterespionage environmental scanning has as its primary requirement the ability to identify diverse risks, descriptively and predicatively, on a strategic as well as a tactical level.

- The degree of adversity in the relationship between a government and an adversary constitutes the principal indicator and determinant of an espionage risk.
- The logical accommodation of a framework for overt counterespionage environmental scanning necessitates a distinctive counterintelligence cycle, as existing conceptualisations of the intelligence cycle are inadequate.

The study's objective and the testing of assumptions are pursued on both the theoretical and pragmatic-utilitarian levels. The framework for counterespionage, open-source environmental scanning and risk assessment is presented as part of a multilayered unison of alternative theoretical propositions on the all-source intelligence, counterintelligence and counterespionage processes. It is furthermore advanced from the premise of an alternative proposition on an integrated approach to open-source intelligence. On a pragmatic-utilitarian level, the framework's design is informed and its application elucidated through an examination of the 21st century espionage reality confronting the nation state, contemporary statutory counterintelligence measures and the 'real-life' difficulties of open-source intelligence confronting practitioners.

Although with certain qualifications, the assumptions are in the main validated by the research. The research furthermore affirms this as an exploratory thesis in a largely unexplored field.

KEY TERMS

BUSINESS INTELLIGENCE

COMPETITIVE INTELLIGENCE

COMPETITOR INTELLIGENCE

COUNTERESPIONAGE

COUNTERINTELLIGENCE

COVERT ACTION

CYBER ESPIONAGE

CYBER INTELLIGENCE (CYBINT)

DEFENSIVE CORPORATE INTELLIGENCE

ENVIRONMENTAL SCANNING

ESPIONAGE

ESPIONAGE INDICATORS

GREY/GRAY SOURCES

INDICATORS

INTELLIGENCE

INTELLIGENCE FAILURE(S)

INTELLIGENCE PROCESS(ES)

INTELLIGENCE SERVICES

INTELLIGENCE STUDIES

INTELLIGENCE THEORY

KNOWLEDGE MANAGEMENT

NATIONAL SECURITY

MASS MEDIA

METHODOLOGY

NONGOVERNMENTAL ORGANISATION(S)

OPEN SOURCES

OPEN-SOURCE INTELLIGENCE (OSINT)

ORGANISED CRIME

PEOPLE’S REPUBLIC OF CHINA (PRC)

RISKS

RISK ASSESSMENT

SECURITY STUDIES

STATUTORY

STRATEGIC STUDIES

TECHNO-SCIENTIFIC

THREATS

UNITED STATES OF AMERICA (US/USA)

BIBLIOGRAPHY

1. PRIMARY SOURCES

1.1 INTERGOVERNMENTAL ORGANISATIONS

Bjore, M. 2002. "Open source – lessons learned." In North Atlantic Treaty Organisation. 2002. NATO open source intelligence reader. Available at www.au.af.mil/au/awc/awcgate/nato/osint-reader.pdf. As accessed on 2007/07/13.

European Commission. 2007. "Notions of security – shifting concepts and perspectives." Sixth Framework Programme. Transnational terrorism, security and the rule of law. Available at http://www.transnationalterrorism.eu. As accessed on 2008/04/14.

Friedman, R. S. 2002. "Review essay – open source intelligence." In North Atlantic Treaty Organisation. 2002. NATO open source intelligence reader. Available at www.au.af.mil/au/awc/awcgate/nato/osint-reader.pdf. As accessed on 2007/07/13.

Jardines, E. A. 2002. "Theory and history of OSINT – understanding open sources." In North Atlantic Treaty Organisation. NATO open source intelligence reader. Available at www.au.af.mil/au/awc/awcgate/nato/osint-reader.pdf. As accessed on 2007/07/13.

North Atlantic Treaty Organisation. 2001. NATO open source intelligence handbook. Available at www.au.af.mil/au/awc/awcgate/nato/osint-rhdbk.pdf. As accessed on 2007/05/23.

North Atlantic Treaty Organisation. 2002. NATO open source intelligence reader. Available at www.au,af.mil/au/awc/awcgate/nato/osint-reader.pdf. As access on 2007/07/13.

Steele, R.D 2002*b*. In "Open source intelligence: what is it? Why is it important to the military?" In North Atlantic Treaty Organisation. NATO open source intelligence reader. Available at www.au.af.mil/au/awc/awcgate/nato/osint-reader.pdf. As accessed on 2007/07/13.

Studeman, A. W. 2002. "Teaching the giant to dance: contradictions and opportunities in open source with the intelligence community." In North Atlantic Treaty Organisation. 2002. NATO open source intelligence reader. Available at www.au.af.mil/au/awc/awcgate/nato/osint-reader.pdf. As accessed on 2007/07/13.

Wing, I.W. 1999. "Optimising open source information sharing in Australia: report and policy prescription." In North Atlantic Treaty Organisation. 2002. NATO open source intelligence reader. Available at www.au,af.mil/au/awc/awcgate/nato/osint-reader.pdf. As accessed on 2007/07/13.

1.2 GOVERNMENTAL

Canada. 2008. Canadian Security Intelligence Service. "Methods used in economic espionage." Canadian Secret Intelligence Service (CSIS) – official website. Available at www.csis-scrs.gc.ca/prrts/spng/mthds-eng.asp. As accessed on 2008/12/14.

Canada. 2004. Canadian Security Intelligence Service. "The CSIS and the security intelligence cycle." Canadian Secret Intelligence Service (CSIS) – official website (archive). Available at http:// www.csis-scrs.gc.ca/nwsrm/bckgrndrs/ bckgrndr03-eng.asp. As accessed on 2008/12/13.

Canada. 2003. Canadian Security Intelligence Service. 13th Annual public report by the Canadian Security Intelligence Service (CSIS). Available at http://csis-scrs.gc.ca/en/publications/annualreport/2003/report.asp. As accessed on 2008/03/26.

Germany. 2008. Federal Ministry of the Interior. Annual report 2008 on the protection of the constitution. Berlin.

Germany. 2005. Federal Ministry of the Interior. Annual report 2005 on the protection of the constitution. Berlin.

United Kingdom. 2008. The national security strategy of the United Kingdom – security in an interdependent world. London. Cabinet Office.

United Kingdom. 2007. Ministry of Defence. The DCDC Global Strategic Trends Programme: 2007 – 2036. Third edition. Swindon. Development, Doctrine and Concepts Centre (DCDC).

United Kingdom. 2004. Report of a Committee of Privy Councillors to the House of Commons [under chairmanship of Lord Butler]: review of intelligence on weapons of mass destruction – 14th July 2004. London. The Stationary Office.

United Kingdom. 2003. Ministry of Defence. Joint Doctrine and Research Centre - Strategic trends: methodology, key findings and shocks. March. Swindon. Joint Doctrine and Research Centre (JDCC).

United States of America. 2009*a*. Central Intelligence Agency. CIA world fact book. Available at https://www.cia.gov/library/publications/the-world-factbook/. As accessed on 2010-04-30

United States of America. 2009*b*. National Counterintelligence Executive. Annual report to Congress on foreign economic collection and industrial espionage - FY 2008. July 23. Office of the National Counterintelligence Executive (ONCIX) .Available at www.ncix.gov/ publications/reports /fecie.../2008_FECIE_Blue.pdf. As accessed on 2009-10-30.

United States of America. 2009*c*. Federal Reserve Bank of San Francisco. “U.S. household deleveraging and future consumption growth.” Newsletter. No. 16. May 15. Available at www.frbsf.org/publications/economics/.../2009/el2009-16.html. As accessed on 2009-11-06.

United States of America. 2009*d*. Department of Defense. “Espionage and other compromises of national security – case summaries from 1975 to 2008.” August 11. Monterey (California). Defense Personnel Security Research Center (PERSEREC).

United States of America. 2009*e*. U.S.-China economic and security review commission. 2009 Report to Congress of the U.S.-China economic and security review commission. Washington (D.C.). US Government Printing Office. (Also available at http://uscc.gov)

United States of America. 2008*a*. Annual threat assessment – 2008. Statement to the House Permanent Select Committee by McConnell, M. (Director of National Intelligence) on February 7, 2008. Available at http://ww.dni. gov/testimonies/ testimonies.htm. As accessed on 2008/04/02.

United States of America. 2008*b*. Department of Defense. “Changes in espionage by Americans: 1947-2007.” Technical report 08-05. Herbig, K. L. Monterey (California). Defense Personnel Security Research Center (PERSEREC). Available at www.dhra.mil/perserec/reports.html. As accessed on 2009/06/1*.*

United States of America. 2008*c*. Department of Defense. “Allegiance in a time of globalization.” Technical report 08-10. Herbig, K. L. Monterey (California). Defense Personnel Security Research Center (PERSEREC). Available at www.dhra.mil/ perserec/reports.html. As accessed on 2009/06/01*.*

United States of America. 2008*d*. Department of Energy. Counterintelligence awareness guide.” National Training Centre. Available at http://ntc.doe.gov/ curriculumareas/ cita/ci_awareness_guide/home.htm. As accessed on 2009/11/10

United States of America. 2008*e*. Department of Energy. “Counterintelligence in our changing world – national security begins with you.” Counterintelligence awareness brochure. Available at http://.www.doe.gov/offices/OCI/Brochures/ index.html. As accessed on 2008/12/4.

United States of America. 2007*a*. National counterintelligence strategy (March 2007). Available at http://www.dni.gov/publications/ publications.htm. As accessed on 2007/04/28.

United States of America. 2007*b*. Annual threat assessment to the House Permanent Select Committee on Intelligence: Negroponte, J. D. (Director of National Intelligence). Published on January 18 on http://www.dni.gov/ testimonies/testimonies. htm. As accessed on 2007/03/22.

United States of America. 2007*c*. Congress. Report for Congress: Open source intelligence (OSINT): issues for Congress. December 5. Washington (D.C.). Congressional Research Service (CRS). Available at http://rand.org/pubs. testimonial/CT. As accessed on 2008/05/24.

United States of America. 2007*d.* National Intelligence Council. Nonstate actors: impact on international relations and the implications for the United States. (Discussion document qualified as not reporting US Government views).

United States of America. 2007*e.* Strategic counterintelligence: protecting America in the 21st century. Address by J.F Brenner (National Counterintelligence Executive) to the NRO/National Military Intelligence Association's counterintelligence symposium. October 24.

United States of America. 2007*f.* Counterintelligence in the 21st century: not just a government problem. Address by J.F Brenner (National Counterintelligence Executive) to the AFCEA counterintelligence conference. December 4. Sunnyville (California).

United States of America. 2007*g.* Department of Defense. Adjudicative desk reference - background for personnel security adjudicators, investigators and managers: counterintelligence module*.* Version 3.1. September. Monterey (California). Personnel Security Research Center (PERSEREC). Available at www.dhra.mil/ perserec/ADR/ ADR/.

United States of America. 2007*h.* Department of Defense. "Potential CI risk indicators*.*" Supporting file for use in conjunction with Adjudicative desk reference - background for personnel security adjudicators, investigators and managers: counterintelligence module*.* (US, 2007*g*). Monterey (California). Personnel Security Research Center (PERSEREC). Available at www.dhra.mil/perserec/ ADR/ ADR/*.*

United States of America. 2007*i.* Department of Defense. *"*One country's program to obtain U.S. S&T Secrets*."* Supporting file for use in conjunction with Adjudicative desk reference - background for personnel security adjudicators, investigators and managers: counterintelligence module. (US, 2007*g*). Monterey

(California). Personnel Security Research Center (PERSEREC).Available at www.dhra.mil/ perserec/ADR/ ADR/.

United States of America. 2007*j.* Director of Intelligence. PRC media guide. March. Open Source Center (of the Director of Intelligence). Available at www.fas.org/irp/dni/osc/prc-media.pdf. As accessed on 2010/09/07.

United States of America. 2006*a*. Annual report of the United States intelligence community. Published in February 2007 at http://www.dni.gov/publications/ publications.htm. As accessed on 2007/04/28.

United States of America. 2006*b*. Department of Defense. Open source intelligence: interim field manual. December. Washington (D.C.). Headquarters of the Army. Available at http://www.fas.org.irp.doddir/ army/fmi2-22.9.pdf. As accessed on 2008/05//29.

United States of America. 2006*c*. Department of Defense. Technology collection trends in the U.S. Defense Industry. Alexandria (Virginia). Defense Security Service. Available at http://www.dss. smil.mil. dhra.mil/perserec/reports.html. As accessed on 2008-12-12.

United States of America. 2006*d*. Department of Defense. Developing science & technology list - Section 17: Information security technologies. Available at http://www.dss.smil.mil. dhra.mil/perserec/reports.html. As accessed on 2008-12-18.

United States of America. 2005*a.* National intelligence strategy. Published on 25/10/2005 at http://www.dni.gov/publications.htm. As accessed on 2007/01/06.

United States of America. 2005*b.* The Commission on the intelligence capabilities of the United States regarding weapons of mass destruction. Report to the President of the United States on the intelligence capabilities of the United States regarding weapons of mass destruction - March 31. Washington (D.C.).

United States of America. 2005*c*. Intelligence challenges through to 2015. Remarks by Gannon, J. C. (Chairman: National Intelligence Council) to the Columbus Council on World Affairs.

United States of America. 2005*d*. Department of Defense. “Reporting of counterintelligence and security indicators by supervisors and co-workers.” Technical report 05-6. Wood, S. (*et al)*. Monterey (California).Defense Personnel Security Research Center (PERSEREC). Available at www.dhra.mil/ perserec/ reports.html. As accessed on 2007-08-07*.*

United States of America. 2005*e*. Department of Defense. “Technological, social, and economic trends that are increasing U.S. vulnerability to insider espionage.” Technical report 05-10. Kramer, L. A. (*et al)*. Monterey (California). Defense Personnel Security Research Center (PERSEREC). Available at www.dhra.mil/ perserec/reports.html*.* As accessed on 2007-08-06.

United States of America. 2004*a* Senate Select Committee on Intelligence. Report on the US intelligence community’s prewar intelligence assessments on Iraq. Washington (D.C.).

United States of America. 2004*b*. Federal Bureau of Investigation. Federal Bureau of Investigation (FBI): Strategic plan: 2004 – 2009. Available at http://www.fbi.gov/publications/strategicplan/ strategicplantext.htm. As accessed on 2008/01/02.

United States of America. 2003. National Imagery and Mapping Agency Understanding global change – National Imagery and Mapping Agency workshop to identify external factors shaping geospatial intelligence beyond 2020. Austin (Texas). Technology Futures Inc.

United States of America. 2002*a*. Congressional Research Service (CRS) – intelligence issues for Congress. January 8. Washington (D.C.). Congressional Research Service. The Library of the United States’ Congress. (Order code: IB10012).

United States of America. 2002*b*. Department of Defense. “Espionage against the United States by American citizens: 1947 – 2001.” Technical report 02-5. Herbig, K. L. & Wiskoff, M. F. Defense Personnel Security Research Center (PERSEREC). Monterey (California). Available at www.dhra.mil/perserec /reports.html. As accessed on 2007-08-06*.*

United States of America. 2001. Department of Energy. Counterintelligence in our changing world - national security begins with you. Brochure. August. Available at http://www.ch.doe.gov/offices/OCI/Brochures/BrochurePDF.pdf. As accessed on 2008-12-14

United States of America. 2000*a*. A national security strategy for a new century. (D.C.). Available at http://clinton6.nara.gov/2000/01/2000-01-05-national-security-strategy-for-new-century.htm. As accessed on 2008/04/02.

United States of America. 2000*b*. National Intelligence Council. Global trends 2015: a dialogue about the future with non governmental experts. Available at http://www. ocdi.gov/cia/reports/globaltrends2015/index.html. As accessed on 2008/03/28.

United States of America. 1999. House of Representatives' Select Committee on U.S. national security and military/commercial concerns with the People's Republic of China. Report of the Select Committee on U.S. national security and military/commercial concerns with the People's Republic of China - 1999. All-volume overview. Washington (D.C.). US Government Printing Office.

United States of America. 1998. Department of Defense. Counterintelligence – US Marine Corps working procedure 2-14. (D.C.). Department of the Navy. Available at www.tscm. com/ marineCI_mcwp2-14.pdf . As accessed on 2008/03/11.

United States of America. 1997*a*. National Security Council. National Security Council working document: a national security strategy for a new century. Washington (D.C.). Available at http://clinton2.nara. govWH/EOP/NSC/Strategy-Cached. As accessed on 2008/03/25.

United States of America. 1997*b*. Department of Defense. Suspicious indicators and security countermeasures for foreign collection activities directed against the U.S. Defense industry. Monterey (California). Defense Personnel Security Research Center (PERSEREC).

United States of America. 1996. Operations security intelligence threat handbook. Interagency operational security support staff. May. Available at www.fas.org/ irp/nsa/ioss/threat96/part03.htm. As accessed on 2007/08/11.

United States of America. 1993. Department of Defense. Assessment of position factors that increase vulnerability to espionage. Crawford, K. S. & Bosshardt, M. J. October. Monterey (California). Defense Personnel Security Research Center (PERSEREC). (Reference:Pers-tr-94001).

2. SECONDARY SOURCES

2.1 BOOKS

Berkowitz, B.D. & Goodman, A.E. 2000. Best truth: intelligence in the information age. New Haven. Yale University Press.

Betts, R.K. 2004. In “Analysis, war, and decision: why intelligence failures are inevitable.” In Johnson, L.K. & Wirtz, J.J. (eds.). Strategic intelligence: windows into a secret world (an anthology). Los Angeles. Roxbury Publishing Company.

Booth, K. (ed). 1991. New thinking about strategy and international security. London. Harpers Collins Academic.

Bozeman, A. D. 1992. Strategic intelligence and tradecraft. Washington (D.C.). Brassey’s Publishers.

Burstein, H. 2004. Introduction to security. Englewood Cliffs. Prentice Hall.

Buzan, B. 1991. People, states and fear: an agenda for international security studies in the post-cold war era. Harlow. Pearson Education Limited.

Buzan, B. & Hansen, L. 2007. “Editor’s introduction.” In Buzan, B. & Hansen, L. (eds.). International security. Vol.1. London. Sage Publishers Ltd.

Buzan, B. & Wæver, O. 2005. Regions and powers – the structure of international security. Third print. Cambridge. University Press.

Buzan, B, Weaver, O, & de Wilde, J. 1998. Security – a new framework for analysis. London. Lynne Rennier Publishers.

Carl, L. D. 1996. The CIA insider's dictionary of US and foreign intelligence, counterintelligence and tradecraft. Washington (D.C.). NIBC Press.

Chapman, B. 2004. Researching national security and intelligence policy. Washington (D.C). CQ Press

Choo, C. W. 1998. The knowing organization: how organizations use information to construct meaning, create knowledge, and make decisions. New York. Oxford University Press.

Choo, C. W. 2001. Information management for the intelligent organization: the art of scanning the environment. Third edition. Medford. Information Today Inc.

Codevilla, A. 1992. Informing statecraft – intelligence for a new century. New York. The Free Press.

Crampton, J. (*et al*). 2006. "Information security." In Gill, M. (ed.) The handbook of security. London. Palgrave Macmillan.

De Beer, A.S. 1998. "Mass communication in society – pervasive messages and images of our time." In De Beer, A. S. (ed.). Mass media - towards the millennium: the South African handbook of mass communication. Second edition. Pretoria. J.L. van Schaik Publishers.

deGraffenreid, K. 1989. "Counterintelligence." In Godson, R. (ed.). Intelligence requirements for the 1990's: collection, analysis, counterintelligence and covert action. Lexington. Lexington Books.

De Vos, A.S. 2006*a*. "Scientific theory on professional research." In De Vos, A.S. (*et al*) (eds.). Research at grass roots for the social science and human science professions. Third edition. Pretoria, Van Schaik Publishers.

De Vos, A.S. 2006*b*. "Building a scientific base for the helping profession." In De Vos, A.S. (*et al*) (eds.). Research at grass roots for the social science and human science professions. Third edition. Pretoria. Van Schaik Publishers.

Dilworth, G. 2003. "Are there linkages between theories of intelligence and the practice of competitive intelligence?" In Fleisher, G.S. & Blenkhorn, D. L. (eds.). Controversies in competitive intelligence - the enduring issues. Westport (Connecticut). Praeger Publishers.

Encarta World English Dictionary. 1999. London. Bloomsbury Publishing.

Fisher, R. J. & Green, G. 1998. Introduction to security. Sixth edition. Boston. Butterworth-Heinemann.

Fleisher, G.S. & Bensoussan, B. E. 2003. Strategic and competitive analysis. New Jersey. Prentice Hall.

Fleisher, G.S. & Blenkhorn, D. L. (eds.). 2003. Controversies in competitive intelligence - the enduring issues. Westport (Connecticut). Praeger Publishers.

Francq. A. 2000. "The use of counterintelligence, security, and countermeasures." In Fleisher, F. S. & Blenkhorn, D. L. (eds.). Managing frontiers in competitive intelligence. Westport . Quorum Books.

Garcia, M. L. 2006. "Risk Management." In Gill, M. (ed.). The handbook of security. London. Palgrave MacMillan.

Geer, J. 1989. "Counterintelligence." In Godson, R. (ed.). Intelligence requirements for the 1990's: collection, analysis, counterintelligence and covert action. Lexington. Lexington Books.

Gill, M. (ed.). 2006. The handbook of security. London. Palgrave MacMillan.

Gill, P. & Phythian, M. 2006. Intelligence in an insecure world. Cambridge. Polity Press.

Gilluffo, F.J, Marks, R.A, & Salmoiraghi, G.C. 2004. “The uses and limits of US intelligence.” In Johnson, L.K. & Wirtz, J.J. (eds.). Strategic intelligence: windows into a secret world (an anthology). Los Angeles. Roxbury Publishing Company.

Godson, R. 2001. Dirty tricks or trump cards - U.S. covert action and counterintelligence. New Brunswick. Transaction Publishers.

Godson, R. (ed.). 1989. Intelligence requirements for the 1990’s: collection, analysis, counterintelligence and covert action. Lexington. Lexington Books.

Godson, R (ed.). 1988. Comparing foreign intelligence – the U.S., the U.S.S.R., the U.K. and the Third World. McLean (Virginia). Pergamon-Brassey’s International Defense Publishers.

Godson, R. 1980. (ed). Intelligence requirements for the 1980’s: counterintelligence. Vol. 3. Washington (D.C.). National Strategic Information Center. Inc.

Goodman, A.E. 1996. “Intelligence in the post cold war era.” In Goodman, A. E., Treverton, G.F., and Zelikow, P (eds.). The report of the Twentieth Century Fund task force on the future of US intelligence. New York. The Twentieth Century Fund Press.

Goodman, A. E., Treverton, G.F., and Zelikow, P (eds.). 1996. The report of the Twentieth Century Fund task force on the future of US intelligence. New York. The Twentieth Century Fund Press.

Henderson, R. 2007. Brassey's International Intelligence Yearbook London Brassey's International.

Herman, M. 1996. Intelligence power in peace and war. Cambridge. Cambridge University Press.

Hess, K. & Wrobelski, H.1996. Introduction to private security. Fourth edition. Minneapolis. West Publishing.

Hulnick, A. S. 2007. “What’s wrong with the intelligence cycle.” In Johnson, L.K. (ed.). Strategic intelligence - the intelligence cycle: the flow of secret information from overseas to the highest councils of government. Vol. 2. Westport. Praeger Securities International.

Johnson, L.K. & Wirtz, J.J. 2004. (eds.). Strategic intelligence: windows into a secret world (an anthology). Los Angeles. Roxbury Publishing Company.

Johnson, L. K. 2007. “An introduction to the intelligence studies literature.” In Johnson, L.K. (ed.). Strategic intelligence - counterintelligence and counterterrorism: defending the nation against hostile forces. Vol. 4. Westport. Praeger Securities International.

Kalaris, G & McCoy, L. 1989. “Counterintelligence.” In Godson, R. (ed.). Intelligence requirements for the 1990’s: collection, analysis, counterintelligence and covert action. Lexington. Lexington Books.

Kent, S. 1949. Strategic intelligence for American foreign policy. Princeton. Princeton University Press.

Kent, S. 1966. Strategic intelligence for American world policy. Third edition. Princeton. Princeton University Press.

Kerzner, H. 1998. Project management – a systems approach to planning, scheduling and controlling. Sixth edition. Berea (Ohio). Van Nostrand Reinhold.

Laqueur, W. 1985. A world of secrets: the uses and limits of intelligence. New York. Basic Books.

Knip, V. 2003. “What is the relationship between competitive intelligence and knowledge management?” In Fleisher, G. S. & Blenkhorn, D. L. (eds.). Controversies in competitive intelligence – the enduring issues. Westport. Praeger.

Lapstra, S. A. & Knip, V. 2005. “Best applications of global competitive intelligence: macro-level scanning and cultural analysis.” In Blenkhorn, D. L. &

Fleisher, G. S. Competitive intelligence and global business. Westport (Connecticut). Praeger Publishers.

Leedy, P.D. & Ormrod, J.E. 2005. Practical research. New Jersey. Pearson Premice Hall.

Lowenthal, M.M. 2003. Intelligence: from secrets to policy. Second edition. Washington (D.C.). CQ Press.

Lynn-Jones, S. M. 1999. "Realism and security studies." In Snyder, G. A. (ed.). Contemporary security and strategy. London. MacMillan Press Ltd.

McCandless, B. 2003. "What key learning should CI specialists acquire from their military intelligence counterparts." In Fleisher, G.S. & Blenkhorn, D. L. (eds.). Controversies in competitive intelligence - the enduring issues. Westport (Connecticut). Praeger Publishers.

Marx, G.T. 2004. "Some concepts that may be useful in understanding the myriad forms and contexts of surveillance." In Scott, L.V. & Jackson, P. (eds). Understanding intelligence in the twenty-first-century - journeys in the shadows. London. Routledge.

McNeil, P.P. 2004. "The evolution of the US intelligence community – an historical overview." In Johnson, L.K. & Wirtz, J.J. (eds.). Strategic intelligence: windows into a secret world (an anthology). Los Angeles. Roxbury Publishing Company.

Mena, J. 2003. Investigative data mining for security and criminal detection. Burlington (Massachusetts). Butterworth Heinemann.

Meyer, H. E. 1987. Real world intelligence. New York. Weidenfeld & Nicolson.

Miler, N. S. 1980. "What is counterintelligence – discussants." In Godson, R. (ed). Intelligence requirements for the 1980's: counterintelligence. Washington (D.C.). National Strategic Information Center. Inc.

Moffat, L. & Fleisher, G. S. 2003. "How can an organization's culture be changed to better support competitive intelligence?" In Fleisher, G.S. & Blenkhorn, D. L.

(eds.). Controversies in competitive intelligence - the enduring issues. Westport (Connecticut). Praeger Publishers.

Mouton, J. 2005. How to succeed in your master's and doctoral studies – a South African guide and resource book. Ninth impression. Pretoria. Van Schaik Publishers.

Muller, M. & Whitehead, C. 2002. "What is competitive intelligence?" Competitive intelligence series. Vol. 1. Randburg. Knowledge Resources (Pty) Ltd.

Muller, M. 2002. "Creating intelligence." Competitive intelligence series. Vol. 4. Randburg. Knowledge Resources (Pty) Ltd.

Mununta, G. & Mununta, R. 2006. "Theorizing about security." In Gill, M. (ed.) The handbook of security. London. Palgrave MacMillan.

Mutimer, D. 1999. "Beyond strategy: critical thinking and the new security studies." In Snyder, G. A. (ed.). Contemporary security and strategy. London. MacMillan Press Ltd.

Nolan, J. A. & Quinn, J. F. 2000. "Intelligence and security." In Miller, J. (ed.) Millennium intelligence. Medford. Cyber Age Books.

Odom, W.E. 2003. Fixing intelligence for a more secure America. New Haven. Yale University Press.

Pollard, A. 1999. Competitor intelligence – strategy, tools and techniques for competitive advantages. London. Pitman Publishing.

Quiggin, T. 2007. Seeing the invisible – national security in an uncertain age. London. World Scientific Publishers.

Rogers, B.B. 2006. "Engineering principles for security managers." Gill, M. (ed.). The handbook of security. London. Palgrave MacMillan.

Scott, L.V. & Jackson, P. (eds). 2004. Understanding intelligence in the twenty-first-century - journeys in the shadows. London. Routledge.

Shulsky, A.N. 1993. Silent warfare – understanding the world of intelligence. London. Brassey's.

Shulsky, A. N. & Schmitt, G. S. 2002. Silent warfare - understanding the world of intelligence. Third edition. Dulles. Potomac Books.

Smith, N. L. 1980. "Counterintelligence organization." In Godson, R. (ed). Intelligence requirements for the 1980's: counterintelligence. Washington (D.C.). National Strategic Information Center. Inc.

Snow, D.M. 2004. National security for a new era – globalization and geopolitics. New York. Pearson Incorporated.

Snyder, G. A. (ed.). 1999. Contemporary security and strategy. London. MacMillan Press Ltd.

Steele, R.D. 2007. "Open source intelligence." In Johnson, L.J. (ed.). Strategic intelligence the intelligence cycle: the flow of secret information from overseas to the highest councils of government. Vol. 2. Westport. Praeger Securities International.

Steele, R.D. 2004. "The importance of open source intelligence to the military". In Johnson, L.K. & Wirtz, J.J. (eds.). Strategic intelligence: windows into a secret world (an anthology). Los Angeles. Roxbury Publishing Company.

Steele, R. D. 2002*a*. The new craft of intelligence. Oakton (Virginia). OSS International Press.

Steele, R. D. 2001. On intelligence – spies and secrecy in an open world. Oakton (Virginia). OSS International Press.

Sterling-Folker, J. (ed.). 2006. Making sense of international relations theory. Boulder (Colorado). Lynne Rienner Publishers.

Taylor, S.A. 2007. "Definitions and theories of counterintelligence." In Johnson, L.K. (ed.). Strategic intelligence - counterintelligence and counterterrorism:

defending the nation against hostile forces. Vol. 4. Westport. Praeger Securities International.

Timm, H. W. & Christian, K.E. 1991. Introduction to private security. Pacific Grove. Brook-Cole Publishing.

Todd, P. & Bloch, J. 2004. Global intelligence – the world's secret services today. Second impression. New York. Palgrave Macmillan.

Vibert, C. (Ed). 2004. An introduction to online competitive intelligence research. Ohio. Thomson Publishers.

Zuehlke, A. A. 1980: "What is counterintelligence?" In Godson, R, (ed), Intelligence Requirements for the 1980's: Counterintelligence. Vol. 3. Washington (D.C.). National Strategic Information Incorporated.

2.2 JOURNALS

Andrew, C. 2004. "Intelligence, international relations and 'under-theorization'." Intelligence and National Security. No. 19. Summer.

Bar-Joseph, U. & Scheaffer, Z. 1998. "Surprises and its causes in business administration and strategic studies." International Journal of Intelligence and Counterintelligence. Vol. 11, no. 3.

Bernhardt, W. 2004. "Bridging the uncertainty gap in intelligence analysis: a framework for systematic risk and threat assessment." Strategic Review for Southern Africa. Vol. 26, no. 2. November.

Betts, R.K. 1983. "Warning dilemmas: normal theory vs exceptional theory". Oribis No. 26. Winter.

Brouard, F. 2004. "Business intelligence for Canadian corporations after September 11." Journal of Competitive Intelligence and Management. Vol. 2, no. 1. Spring.

Clift. A.D. 2003. “Intelligence in the internet era – from semaphore to predator.” Studies in Intelligence. Vol. 47, no. 3. Available at https://www.cia. gov/library/ center-for-the-study-of-intelligence/csi. As accessed on 2008/03/03.

Daft, R. L. & Weick, K. E. 1984. “Toward a model of organizations as interpretation systems.” Academy of Management Review. Vol. 9, no. 2.

Daley, P. 2005. “Spy anxiety”. The Bulletin. Vol. 123, no. 26. June, 28. Australia.

Davies, P.H.J. 2002. “Ideas of intelligence: divergent national concepts and institutions,” Harvard International Review. Autumn.

DeGenaro, B. 2005. “A case for business counterintelligence.” Competitive Intelligence Magazine. Vol. 8, no. 5. September.

Dunne, T. 1999. “The spectre of globalization.” Indian Journal of Global Legal Studies. Vol. 7, nr. 17.

Du Plessis, A. 2001. “International relations theory and the discourse on terrorism: preliminary reflections on contexts and limits.” Strategic Review for Southern Africa. Vol. 22, no. 2. November.

Dupont, A. 2003. “Intelligence for the twenty-first century.” Intelligence and National Security. Vol. 18, no. 4. Winter.

Gendron, A. 2005. “Just war, just intelligence: an ethical framework for foreign espionage.” International Journal of Intelligence and Counterintelligence. Vol. 18, no. 3. Fall.

Gilluffo, F.J . (*et al.*) 2002. “The uses and limits of US intelligence.” The Washington Quarterly. Vol. 25, no. 1. Washington (D.C.). The Centre for Strategic and International Studies.

Goodman, M. S. 2006. “Studying and teaching about intelligence: the approach in the United Kingdom.” Studies in Intelligence. Vol. 50, No. 6. Available at http://www.au.af.mil/au/awac/wacgate/teaching-intel.htm. As accessed on 2008/01/05.

Handel, M.I. 1983. "The study of intelligence." Orbis . Nr 26. Winter.

Hansen, J. 2004. "U.S. intelligence confronts the future." International Journal of Intelligence and Counterintelligence. Vol. 17, no. 4.

Hastedt, G.P. 1991. "Toward the comparative study of intelligence." Conflict Quarterly. Summer.

Hough, M. 2006. "The concept of national security strategy: the case of the United States and South Africa."Strategic Review for Southern Africa, Vol. 38, no. 2. November.

Hough, M. 2004. "Warning intelligence and early warning with specific reference to the African context." Strategic Review for Southern Africa. Vol. 26, no. 2. November.

Hough, M. 2003. "National security and threat perception: when is an issue a national security threat?" Strategic Review for Southern Africa. Vol. 25, no. 2. November.

Hulnick, A.S. 2002. "Risky Business – private sector intelligence in the United States." Harvard International Review. Available at http//www.hir.harvard.edu/articles/1065/. As accessed on 2007/11/11.

Hulnick, A.S. 1986. "The intelligence producer-policy consumer linkage: a theoretical approach." Intelligence and National Security. Vol. 1. May.

Johnson, L. K. 2003. "Preface to a theory of strategic intelligence." International Journal of Intelligence and Counterintelligence. Vol. 16, no.4.

Johnson, L.K. 1996. "Analysis for a new age." Intelligence and National Security. Vol. 11, no. 4.

Kahn, D. 2001. "An historical theory of intelligence." Intelligence and National Security. Nr. 16. As featured on http://david-kahn. As accessed on 2008/01/13.

Kitfield, J. 2007. “Spies of all stripes have discovered that there is life after the Cold War – the espionage sequel.” Air Force . Vol. 90, nr. 3. (Journal of the US Air Force Association). Available at http://www.afa.org/magazine/march 2007/0307espionage. html. As accessed on 2008/04/25.

Kramer, L.A. & Heuer, R.J. 2007. “America’s increased vulnerability to insider espionage.” International Journal of Intelligence and Counterintelligence. Vol. 20, no1.

Mercado, S.C. 2005. “Re-examining the distinction between open information and secrets.” Studies in Intelligence. Vol. 49, no. 2. Available at https://www.cia. gov/library/center-for-the-study-of-intelligence/csi/publications/csi.../re-examining_ the_distinction_3.h. As accessed on 2008/05/26.

Nolan, J. A. 1997. “Confusing counterintelligence with security can wreck your afternoon.” Competitive Intelligence Review. Vol. 8, no. 3.

Northcott, C. 2007. “The role, organization and methods of MI5.” International Journal of Intelligence and Counterintelligence. Vol. 20, no. 3.

O’Connel, K. M. 2004. “Thinking about intelligence comparatively.” Brown Journal of World Affairs. Vol. 11, issue 1. Available at http://www.watson.institute. org.bjwa/ archive/11.1/espionage/oconnel.pdf. As accessed on 2008/03/04.

Pattakos, A. N. 1997. “Keeping company secrets secret.” Competitive Intelligence Review. Vol. 8, no. 3.

Smith, S. 1999. “The increasing insecurity of security studies: conceptualising security in the last twenty years.” Contemporary Security Policy. Vol. 20. No. 3.

Troup, M. 2003. “Moving targets: the US intelligence community and the changing world context.” Critique: Student Journal of Politics. Fall.

Upano, A. 2003. “Will a history of government using journalists repeat itself under the Department of Homeland Security.” The News, Media and the Law. Vol. 27, no. 1. Available at http://www.rcfp.org/news/mag/27-1/cov-willahis.html. As accessed on 2007/06/05.

Warner, M. 2002. “Wanted: a definition of ‘intelligence’ ” Studies in Intelligence. Vol. 46, no. 3. 2002. Available at http://www.cia.gov/csi/studies/vol46no3/ articale02. html. As accessed on 2007/11/13.

Wettering, F.L. 2000. “Counterintelligence: the broken triad.” International Journal of Intelligence and Counterintelligence. Vol. 13, no. 3. Fall.

2.3 *AD HOC* PUBLICATIONS, PAPERS, SEMINARS AND UNPUBLISHED DISSERTATIONS

Al-Rodhan, N.R.F. & Stoudman, G. 2006. Definitions of globalization: a comprehensive overview and a proposed definition. Geneva. Geneva Centre for Security Policy. Available at www.gcsp.ch/e/.../Publications/Pillars/definitions-of-globalization.pdf. As accessed on 2008/02/19.

Beer, S. 2006. Intelligence Institutions and state relations in the twentieth century: a central European perspective. Second Plenary Session of Cliohres. Available at www.cliohres.plenary/reykjavik/conferencematerials.pdf. As accessed on 2008/02/12.

Bernhardt, W. A. 2003. A qualitative conceptual framework for conducting risk- and threat assessment in the South African domestic intelligence environment. Unpublished PhD thesis. Pretoria. University of Pretoria.

Betts, R.K. 2006. “How can intelligence be measured.” In Treverton, G.F. (*et al*). Toward a theory of intelligence – workshop report. RAND Cooperation. Available at http://www.rand.org/pubi/larf/proceedings/2006 Rand – CF219.pdt. As accessed on 2008/02/14.

Brauch, H. G. 2005. Reconceptualising security in the 21st century. Seminar: Facing the challenges of global environmental change and globalisation. Bonn.

Bruneau, T.C & Dombroski, K. 2004. Reforming intelligence: the challenge of control in new democracies. Monterey (California). Naval Post Graduate School. Proceedings from an international roundtable on intelligence and democracy. August. Available at http://www.ccmr.org/public/library_file_proxy.cfm/lid/5258. As accessed on 2008/03/16.

Burke, C. 2007. "Freeing knowledge, telling secrets: open source intelligence and development." Research Papers: Bond University's Centre for East-West Cultural and Economic Studies (CEWCES). Queensland (Australia). Available at http://epublications.bond.edu.au/cewces.papers/11. As accessed on 2008/04/16.

Crane, A. 2003. In the company of spies: the ethics of industrial espionage. Research paper series. Nottingham. International Centre for Corporate Social Responsibility (ICCSR).

Der Derian, J. 2005. Global security manifesto. Watson Institute. Global security Program. Available at http://www.watsoninstitute.org/gs/beyondterror/global securitymanifesto.htm. As accessed on 2008/02/18.

Ecklund, M. V. 2005. "Strategic communications: how to make it work." IO Sphere. Publication of the US Joint Operations and Information Centre. Available at www.au.af.mil/info-ops/iosphere/iosphere/fall05_ecklund.pdf. As accessed on 2008/02/23

Edwards, C. 2006. The case for national security. Demos Report (February). Available at http://www.demos.co.uk/projects/networkedsecurity. As accessed on 2007/06/11.

Gill, P. 2006. "'What is intelligence theory?' In Treverton, G.F. (*et al*). Toward a theory of intelligence – workshop report. RAND Cooperation. Available at http://www. rand. org/pubi/larf/ proceedings/2006 Rand – CF219.pdt. As accessed on 2008/02/14.

Heide, R. L. (*et al*). 2004. Peacekeeping intelligence: new players, extended boundaries. Conference Report. Center for Security and Defence Studies. Carleton University. Ottawa.

Johnson, L.K. 2006. "Is there an American theory of intelligence?" In Treverton, G.F. (*et al*). Toward a theory of intelligence – workshop report. RAND Cooperation. Available at http://www.rand.org/pubi/larf/proceedings/2006 Rand – CF219.pdt. As accessed on 2008/02/14.

Kabay, M. E. 2008. Industrial espionage. Northfield (Vermont). Norwich University.

Karoly, L. A. & Panis, C.W.A. 2004. The future at work – trends and implications. (Research brief - summary). Santa Monica. RAND Cooperation. Available at http:// www.rand/org/publications/RB/RB5070. As accessed on 2008/02/02.

Kearns, I. & Gude, K. 2008. The new frontline: security in a changing world. London. Institute for Policy Research (IPPR).

Kostoff, R. N. (*et al)*. 2006. The structure and infrastructure of Chinese science and technology. United States' Office of Naval Research. Available at http://www.fas. org/irp/world/china /documents. As accessed on 2009-06-02.

Lewis, B.C. 1998. Information Warfare. Federation of American Scientists' Intelligence Resource Program. Available at http://www.fas.org/ rp/eprint/snyder/ info warfare/htlm. As accessed on 2008/04/15.

Molander, R.C; Riddile, A. S. & Wilson, P. A. 1996. Strategic information warfare – a new face of war. St. Monica (US). RAND Cooperation.

Parks, R. C. & Duggan, D. P. 2001. Principles of cyber-warfare. Workshop on information assurance and security (June 5 – 6). West Point. United States Military Academy.

Rennstich, J.K. 2003. War in the digital age: informational power, geopolitics and the fifth dimension. Paper delivered at the annual meeting of the International Studies Association: February, 26 – March 1. Portland (Oregon).

Smith, S.2002. "The contested concept of security." The concept of security before and after September 11. Singapore. Institute of Defence and Strategic Studies of Singapore.

Szalacha,J. 2007. Non-state actors as the main factor of power shift in global intelligence issues. European Consortium for Political Research. (Proceedings of 4th Conference – 6-8 September). Pisa. Available at http://www.essex.

ac.uk/ecpr/events /generalconference/pisa/papers/PP1731.pdf . As accessed on 2008/02/18.

The Task Force on the future of American innovation. 2005. The knowledge economy: Is the United States losing its competitive edge? Available at http://www.shrm.org/foreign/cn/Documents/Benchmarks.pdf. As accessed on 2009-12-08. (Remark: The said Task Force, launched in 2004, is an alliance of US companies, research universities and several scientific societies.)

Treverton, G.F. 2005. Emerging threats to national security. Testimony presented to the House Representative Permanent Select Committee on Intelligence on February 2. RAND Cooperation. Available at http://www.rand.org/pubi/ larf/proceedings/2005 Rand. As accessed on 2008/01/29.

Treverton, G.F. (*et al*). 2006. Toward a theory of intelligence – workshop report. RAND Cooperation. Available at http://www.rand.org/pubi/larf/proceedings/2006 Rand – CF219.pdt. As accessed on 2008/02/14.

Van Cleave, M. K. 2007. Counterintelligence and national strategy. School for national security executive education. April. Washington (D.C.). National Defense University Press.

Watts, W.L. 2005. Intelligence reform in Europe's emerging democracies – conflicting paradigms, dissimilar contexts. Available at ww.cia.com/csi/intelligence 20% in20Europe. As accessed on 2008/04/12.

Williams, P. 1997. "Transnational criminal organisations and international security." In Arquilla, J. & Ronfeldt, D. (eds.) In Athena's camp - preparing for conflict in the information age. St Monica. Rand Cooperation.

Zaccor, A. 2005. Security cooperation and non-state threats: a call for an integrated strategy. Washington (D.C.). The Atlantic Council of the United States.

3. MEDIA

3.1 NEWSPAPERS

Bell, S. 2006."Foreign espionage alive and well in Canada." National Post. July 19. Available at http://www.nationalpost.com/story-printer.html?id04a73096-b758-4f-83ae-c3c821. As accessed on 2008/03/23.

Bowermaster, D. 2005. "Boeing probe intensifies over secret Lockheed papers". The Seattle Times. January 9. Available at http://seattletimes.nwsource.com/cgi-bindocument_id=2002146025&zs. As accessed on 2008/04/25.

Chivers, C. J. 2006. "Kremlin puts foreign NGOs on notice". The New York Times. October 20. Available at http://www.nytimes.com/2006/10/20/world/ europe/20 russia.html. As accessed on 2008/01/21.

Deutsche Welle. 2007/12/15. "Germany expelled Iranian diplomat over fuel enrichment." Available at http://www.dw-world.de/03006385,00.html. As accessed on 2008/01/11.

Eringer, R. E. 2008. "And now the Manchurian chip." The Investigator. October, 18. Available at http://cryptome.info/0001/manchu-chip.htm. As accessed on 2008-12-27.

European Tribune. 2006/10/03. "Subversive espionage ring busted." Available at http://www.eurotrib.com/story/2006/10/02/24437/8678. As accessed on 2007/12/03.

The Guardian. 2006. "Special report: how the balance of power and influence is changing: new diplomatic priorities." March 04.

Jung-a, S. 2007. "Seoul raises defences against industrial spies." The Financial Times. June, 28. Available at http://www.ft.com/cms/s/946244a4-2513-11dc-bf47-000b5df10621.html. As accessed on 2008-08-30.

Kramer, A. E. 2007. "Russia expels 4 British diplomats." July, 19. International Herald Tribune. Available at http://www.int.com/bin/print.php?id=673748. As accessed on 2008-07-09.

Penketh, A. 2007. "German journalists face prosecution over rendition documents." The Independent (August 9). Available at http://www.independent. co.uk.news/ europe/. As accessed on 2008/01/21.

Warren, P. 2006. "Chinese hackers attack UK Houses of Parliament." The Register. January 20. Available at http://www.futureintelligence.co.uk/index2.php. As accessed on 2008/05/14.

Warren, P. 2005. "Terrorists launch cyber attacks on US defence companies." The Register. April 18. Available at http://www.futureintelligence.co.uk/ index2.php. As accessed on 2008/05/14.

The Washington Times. 2007/05/12. "Chinese hackers get the drop from fashion houses." Available at http://www.washingtontimes.com/news/2007/12/20070512-1.As accessed on 2008/05/14.

York, G. and Avery, S. 2006. "China's got RedBerry." Globe and Mail (Canada). April 11. Available at www.theglobeandmail.com/eceRedirect?articleId=819974. As accessed on 2007-11-03.

3.2 MAGAZINES

Borden, A. 1999. "What is information warfare?" Air & Space Power . Available at http//www.airpower.maxwell.af.mil/airchronicles/apje.html. As accessed on 2007/11/23

Cooper, S. 2006. "How China steals U.S. military secrets." Popular mechanics . August. Available at http://www.popularmechanics.com/technology/military_ law/3319656.html. As accessed on 2009/10/12.

Grant, I. 2008. "Hacking US military systems was child's play, says Gary McKinnon." Computer Weekly. July 13. Available at http://computerweekly. com/Articles/ 2008/06/13/231057. As accessed on 2008/07/03.

Hesseldahl, A. 2006. "BlackBerry vs. Redberry in China." Business week. April, 13. Available at www.businessweek.com/technology/.../tc20060413_266291. As accessed on 2007/11/03.

Novoye Vremya, 2005. “China is still trying to steal military secrets from Russia.” No. 35. September, 06. (Translated from the original Russian).

4. INTERNET

Barlow, J P. 2002. ‘Why spy?- if the spooks can’t analyze their own data, why call it intelligence.” Forbes.com (online). July, 10. Available at http://www.forbes. com/asap/ 2002/1007/042_print.html. As accessed on 2008/08/02.

BBC News. 2007/02/14. “EU endorses damning report on CIA.” Available at http://www.bbc.co.uk/go/pr/fr/_/2/hi/Europe/6360817.52519.stm. As accessed on 2008/06/02.

BBC News. 2007/03/15. “Russian spies ‘at Cold War level’.” Available at http://www.bbc. co.uk/go/pr/fr/_/2/hi/uk_news/6452519.stm. As accessed 2008/05/31.

Britannica Online Encyclopaedia: 2008/09/09. “Ideal type”. Search: http//www.britannica.com/EBchecked/topic/281796/ideal-type.

Burgess, C. 2008. “Nation states’ espionage and counterespionage - an overview of the 2007 global economic espionage landscape”. CI Centre. As published on http://cicentre.com/articles/cb_nation_states_esionage_esionage.html on April 21. As accessed on 2005/05/25.

Christenson, J. 1999. “Bracing for guerrilla warfare in cyberspace”. Available at http://www.cnn.com/TECH/specials/hackers/cyberterror/. As accessed on 2007/02/02.

CI Centre. 2008. “Col. Alexander Litvinenko”. Home web page: The Centre for Counterintelligence and Security Studies. Available at http://www.cicentre.com /documents/litvinenko2.html. As accessed on 2008/05/31.

Collins Essential English Dictionary. 2006. Accessed through The Farlex Free Dictionary – online at http//:www.the freedictionary.com. As accessed on 2008/07/28.

Elroy, B. 2006. "Inside the Chinese intelligence agencies." BBC Monitoring International Reports. February, 08. Available at http://www.military photos.net/forums/archive/index.php/t-72090.html. As accessed on 2008/10/19.

EUR News Service. 2000/11/20. "Russian Federation: environmental activist Grigory Pasko faces new imprisonment." All index EUR 46/045/2000. News service, nr. 219.

Eurasian Secret Services Daily Review. 2007/11/12. Available at http:www. axisglobe.com/article.asp?article=1427. As accessed on 2008/03/11.

Global Secure Systems. 2006. "Gary McKinnon: inside the head of a super hacker." July 13. Available at http//www.gss.co.uk/news/article/3007/. As accessed on 2008/05/28.

Henwood, D.1988. Spooks in blue. Available at www.cia-on-campus.org/yale.edu /henwood.html. As accessed on 2008/03/011.

Hoffman, S. 2007. "McAfee report projects wave of international cyber crime." Channel Web. Available at http://www.crn.com.security/204301389. As accessed on 2008/03/07.

Houghton, K. 1997. "Subverting journalism: reporters and the CIA." Attacks on the press in 1996. Committee to Protect Journalists. Available at http://www. cpj.org/attcaks96/sreports/cia.html. As accessed on 2007/06/06.

India-Defense: online. 2009. "South Africa: Defense equipment copied by China." January 08. Available at http://www.india-Defense.com.reperts/4125. As accessed on 2010-01-02.

Industrial Espionage News. 2008. Available at http://www.tscmvideo.com/ news/industrial-esionage-news.html. As accessed on 2008/06/25.

Jackson, P. 2006. "From fake rocks to dummy NGOs." BBC News. February 2. Available at http://news.bbc.co.uk.go/pr/fr/-/2/hi/europe /4672126.stm. As accessed on 2008/04/06.

Lunev, S. 1997. China's Intelligence machine. Available at http://www.findarticles.com/p/ articles/mi_m1571/is.../ai_19986874/.

Mailonline. 2008/06/13." Bungling spy who left secret files on train faces the sack." Available at http://mailonsunday.co.uk/news/article-1025810/. As accessed on 2008/06/13.

Merriam-Webster Online Dictionary: 2008/06/23. Search: http://www.merriam-webster.com/dictionary/matrix.

Merriam-Webster Online Dictionary: 2008/06/16. Search: http//www.merriam-webster.com/ model+rule+of+thumb.

Messagelabs Intelligence. 2010. "The nature of cyberespionage: most malicious file types identified and encrypted spam from Rustock." Monthly report. March. Available at www.messagelabs.com/mlireport/MLI_2010_03_Mar_FINAL-EN.pdf. As accessed on 2010-05-11.

Ostroff, S. 2000. Systems theories: towards a meta-perspective. Available at www.acsa.net.au/atricles/Systems-theoreis-metaperspective.pdf. As accessed on 2008/01/15.

Peng, X. F. 2010. "China's Xinhua Expands With Mobile TV Search Venture. " Available at www.internetevolution.com/author. asp?section_ id=789&doc. As accessed on 2010/09/04

Richter, J. 2007. "Czech intelligence: half of Russia's diplomats in the Czech Republic are spies." Radio Prague. Available at www.radio.cz/print/en/97844. As accessed on 2008/01/11.

Schlesinger, R. 2004. "The private contractor-GOP gravy train." Salon. Available at http://dir.salon.com/story/news/feature/2004/05/11/private/index.html. As accessed on 2008/03/21.

Spiegelonline. 2008/05/26. "Did DeutscheTelekom spy on journalists and board members?" Available at http://www.spiegel.de/international/business/555363,00.html. As accessed on 2008/06/04.

The Earth Times. 2008/03/20. “Russia’s FSB detains 2 US citizens on charges of industrial spying.” Available at http//www,earthtimes.org.articles/show/193730. As accessed on 2008/05/01.

The Farlex Dictionary. 2008. “Globalization.” Available at http://encyclopedia. thefreedictionary.com/globalization. As accessed on 2008/03/26.

thefreedictionary.com: 2008/10/17. Search: http://www.thefreedictionary.com/p/ motive.

The Oxford Medievalist. 2007. “In defence of pre-technology intelligence.” Available at http://oxfordmedievalist.blogspot.com/2007/02/in-defense-of-pre-technology.html. As accessed on 2008/01/18

Vlahos, K.B. 2005. “Non-secret intelligence gets the cold shoulder”. Fox News. July 28. Available at www.foxnews.com/story/0,2933,163889,00.html. As accessed on 2008/05/30.

WorldNetDaily.com. 2003. “America's China syndrome.” August 19. Available at http://www.wnd.com/?pageId=20358. As accessed on 2008/07/07.

Wright, S. & Williams, D. 2007. “Revealed: poisoned ex-Russian spy Litvinenko was paid-up MI6 agent.” MailOnline. October 27. Available at http://www.dailymail. co.uk/newsarticle-490007/. As accessed on 2008/06/04.

YourDictionary.com: 2008/11/17. Search: http://www. yourdictionary.com/intent.

DISTRIBUTION AND COPYRIGHT