THE CONCEPTUAL STRUCTURING OF THE INTELLIGENCE AND COUNTERINTELLIGENCE PROCESSES: ENDURING HOLY GRAILS OR CRUMBLING AXIOMS — *QUO VADIS*?

Dr Beer (P C) Duvenage*
State Security Agency, Pretoria

and

Prof Mike Hough (Emeritus)
Department of Political Sciences
University of Pretoria

ABSTRACT

This article, as undoubtedly many others, on the eve of the tenth commemoration of 9/11, deals with the ramifications of these, and related events, on international and national security thinking. In the wake of 9/11, the previously neglected and self-isolated Intelligence Studies discipline was propelled to academic prominence. The unprecedented surge in literature reflects intensifying endeavours among scholars and practitioners to address Intelligence Studies' theoretical poverty. This article explores one area of this theoretical inquest, namely the conceptual structuring of the intelligence process. It critically appraises some existing models with a view to address the problem statement: Do existing postulations of the intelligence process

*Based on a D.Phil thesis (Political Science), completed in the Department of Political Sciences, University of Pretoria, under supervision of Prof M Hough (Emeritus) during 2010. Views expressed in the article are those of the authors and do not reflect official government views or interpretations.

accommodate the counterintelligence and counterespionage processes sufficiently and, if not, what alternatives can be proposed? With some exceptions, Intelligence Studies' theorisation on the intelligence process continues to be overlaid upon crumbling axioms. Alternatives, this article advances, are not purported to be radically new. Instead, and mirroring the incipient status of intelligence theorisation, they are, for a substantial part, the mapping out of existing knowledge in a manner conducive to further theory construction.

1. INTRODUCTION

Raising the topic of 'theory' is unlikely to evoke an enthusiastic, captivating debate amongst the majority of practitioners engaged in the trenches of 'actual' intelligence work. In counterespionage for one, the intricacies of double-agent recruitment and the outwitting of an espionage adversary are issues for exciting conversation. Yet, theory underpins intelligence practice, and practice informs theory. Perhaps eclipsed by 'practical' line-functional demands, theory is for a significant part regarded as an abstract notion dealt with by a selected few practitioners and scholars within statutory intelligence's academic twin, Intelligence Studies.

Tabling the matter of intelligence theory on the academic front is simultaneously disconcerting and encouraging. It is disconcerting because of Intelligence Studies' critically under-theorised status. This under-theorisation is as old as the academic discipline itself. Since Intelligence Studies' inception in the late 1940s, this discipline for the remainder of the Cold War evolved in a self-isolated manner that for the most part was ex-practitioner driven and largely disregarded by scholars within Political Sciences (Scott and Jackson 2004: 7-8; Johnson 2007*a*: 1, 3). Even developments like the fall of the Berlin Wall, the collapse of the Union of Soviet Socialist Republics (USSR) and the end of the Cold War in 1991 did not spark an invigoration of Intelligence Studies' theorisation or advance the discipline to the academic mainstream. In what was some theoretical 'smoldering' and 'smoke', the post-Cold War debate in Security and Strategic Studies on the 'widening' and 'deepening' of the concept national security reverberated within Intelligence Studies (Watts 2005: 2). In contrast to the substantive and substantial theorising within Strategic and Security Studies, however, the deliberations within Intelligence Studies

on the expansion of the national security agenda, were driven by the practical consideration of ensuring the continued centrality of governmental intelligence structures in the face of declining budget allocations and the downsizing of statuary intelligence structures (Berkowitz and Goodman 2000: 24).

Intelligence Studies thus entered the dawn of the 21st century still at the fringe of the academic mainstream. However, and herein lies the encouraging reason for optimism, "key events of the early 21st century" not only "defined intelligence as a new cornerstone of government" but also propelled Intelligence Studies to academic prominence (Goodman 2006: 1). Moreover, the past decade has seen an acute self-awareness of, and intensifying endeavours among scholars and practitioners to address, Intelligence Studies' theoretical poverty.

This article explores one area of this theory inquest, namely the conceptual structuring of the intelligence process with specific reference to counterintelligence (CI). The article's aim to contribute to an aspect of a theoretical discourse imposes two imperatives to its structural approach. Firstly, theoretical notions central to the article's scope are demarcated. These include 'intelligence', 'theory', 'intelligence theory' and 'counterintelligence'. Secondly, the discourse on the intelligence process is concisely contextualised as part of the broader intelligence theory debate. This is done with an emphasis on the requisites for progress in theoretical construction to which the article's contribution to the discourse should comply. Moving from this theoretical and contextual premise, some existing views on the intelligence processes — of which the traditional intelligence cycle is by far the most predominating — are critically appraised. While the veracity of these views in general is examined, the article is specifically focused on addressing the problem statement: Do existing postulations of the intelligence process sufficiently accommodate the counterintelligence and counterespionage processes and, if not, what alternatives can be proposed? These alternatives are not purported to be radically new. Instead, and mirroring the incipient status of intelligence theorisation, they are, for a substantial part, the mapping out of existing knowledge in a manner conducive to further theory construction.

2. DEMARCATION OF KEY CONCEPTS

The above cited, not uncommon perception amongst intelligence practitioners of theory as a rather abstract notion with no apparent bearing on the execution of their line-functional work, is not without reason. Some aspects of theory are indeed highly abstract and the direct relevance thereof to intelligence practice not immediately apparent. This generalisation, however, cannot be extended to theory in its entirety.

2.1 A conceptualisation of 'theory'

In its broad denotation, 'theory' refers to a "set of statements ... devised to explain a group of facts or phenomena" (*American Heritage Science Dictionary [online]* 2005). Explanation *per se* is not theory's sole purpose. Intelligence theory's purpose is aptly summarised by Gill (2006: 4 — original emphasis) in his distinction between "theories *of* intelligence" and "theories *for* intelligence". Theories of intelligence, Gill (2006: 4) contends, are developed to "help academics research intelligence, come to understand it, and better explain it." Theories for intelligence "relate immediately to the needs of practitioners ... In one sense there is no conflict between these two. A good theory *of* intelligence should, by definition, be useful *for* intelligence" (Gill 2006: 4 — original emphasis). Theory is therefore fundamentally relevant to practice. So fundamentally in fact, that Betts (2006: 27) asserts "intelligence failures" to be, for a significant part, the "result of bad theory".

From a positivistic premise, theory can also not exist independent of intelligence practice. Theory, after all, aims to describe the referent object, in this case statutory intelligence, as a phenomenon. Moreover, and practitioners will revel in the thought, the manner in which intelligence work is executed is often the concrete manifestation of theory at the praxis level and indispensible to the sound formulation of theory at higher levels of abstraction.

2.2 A tentative delineation of 'intelligence' and related concepts

The referent object of intelligence theory is decidedly more complex

to define than the notion theory. The offering of a definition of 'intelligence' is an attempt to describe and explain the phenomenon. Therefore, no universally accepted denotative definition of intelligence exists. Only competing versions are found of attempts to advance denotative definitions of 'intelligence'. An article of this nature, self-evidently, requires some clarity of intelligence and related concepts. Consequently, concepts pertinent to the article — such as 'intelligence', 'counterintelligence', 'intelligence process' and 'model' — are for the most part delineated in enumerative terms. While some concepts are re-examined in the course of this article, a tentative delineation is here required as a basis for further discussion.

With this qualification, statutory intelligence is provisionally deemed to be the national-security relevant information and related services provided to a government by institutions established for those purposes (Godson 2001: xxi, 1, 17). Intelligence thus denotes a specific type of "knowledge", "organization", "activity" and the combination of these three (Kent 1966: 3, 69, 151-158). In emphasising the activity facet of intelligence, Lowenthal (2003: 8) offers the following useful "working concept" for describing intelligence:

> 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.

Though many would contest Lowenthal's definition, his proposition is underpinned by a notion that enjoys axiomatic acceptance. This axiom holds intelligence to comprise of four "major elements" (also referred to as "functions" and "disciplines"), namely collection, analysis, covert action and counterintelligence (Codevilla 1992: 4; Godson 2001: xxvii, 1). Counterintelligence, in turn, is widely accepted as consisting of defensive measures (security) and offensive actions. Counterespionage is a distinctive category of offensive counterintelligence actions "designed to detect, destroy, neutralize, exploit or prevent espionage activities through [the] identification, penetration, manipulation, deception, and repression of individuals, groups, or organizations conducting or suspected of conducting espionage activities" (United States of America 1974: 90 as cited by Zuehlke 1980:17, 38). Similar to counterespionage, 'covert action' comprises of offens-

ive measures undertaken against role-players of national-security relevance. Covert action seeks to influence role-players, conditions and events without revealing the sponsor's identity. To this end, measures instituted "are to one degree or another secret (hidden) or covert (disguised)" (Godson 2001: 2-3).

In what can be confounding, covert action and counterintelligence are often juxtaposed with intelligence. In this juxtaposed use, which is more often than not implicit and not categorical, 'intelligence' is an abbreviated reference to the concept 'positive intelligence'. Whereas positive intelligence informs the policymaker on developments and role-players relevant to national security in general, offensive counterintelligence is more specific. It protects against, and targets, adversarial role-players' intelligence activities and capabilities. In its common usage, positive intelligence is deemed to exclude passive and active countermeasures instituted by and pursued by means of the state's intelligence institutions.

2.3 A demarcation of the notions 'intelligence process' and 'intelligence process models'

The national-security relevant information and services just described involve a range of activities that are collectively referred to as the intelligence process. The term 'intelligence process', thus explicitly or (as often in consulted Intelligence Studies literature) implicitly suggests the overarching process that coherently accommodates actions undertaken in relation to positive intelligence, counterintelligence, analysis, collection, covert action and so forth. These activities are typically clustered in "various steps or stages in intelligence" by means of which the work of intelligence is conducted (Lowenthal 2003: 41).

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 and Goodman 2000: 72). As an idealisation, a model is "an aimpoint, of what the process should look like if everything goes as planned" (Berkowitz and Goodman 2000: 72). A model of the intelligence process serves as both a notional concept for theorising on intelligence and as an "organization principle" for the work of intelligence (Lowenthal 2003: 51; Berkowitz and Goodman 2000: 72). Depending on the model, this

"organization" could extend to one or more of an intelligence community/service's organisational structuring, its systems, work flow and processes (Agrell 2006: 22). Attesting to the latter is the following observation in a United States (US) (2005: 583 — original emphasis) commission report: "The process of tasking, collecting, processing, analysing, and disseminating intelligence is called the intelligence cycle. The *intelligence cycle* drives the day-to-day activities of the [US] Intelligence Community". In the authors' experience this view also predominates in the intelligence communities of multiple other nation states.

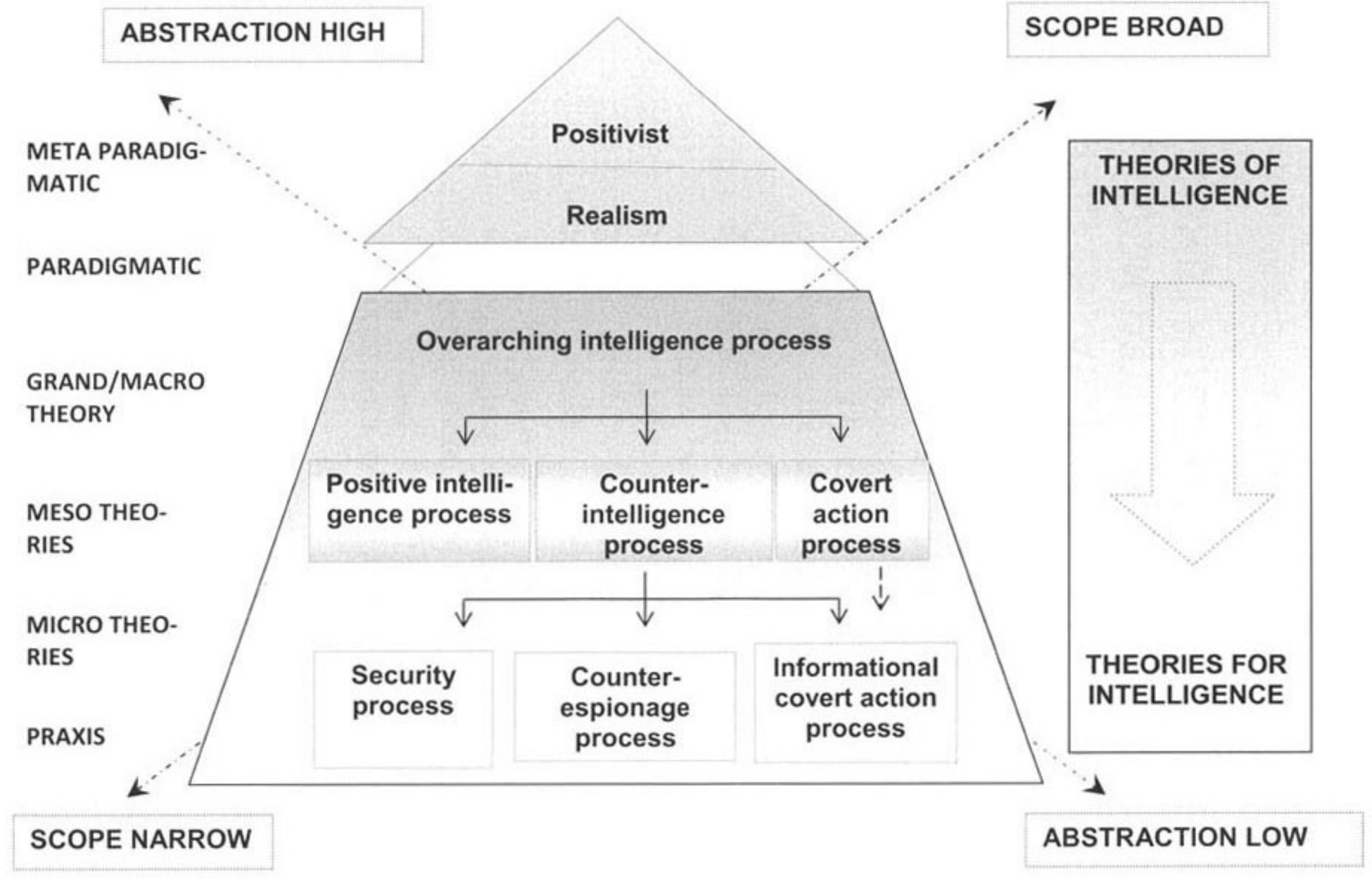
In its dimension as a construct for theorisation on intelligence, the concept 'process model' is not homogenous, but shares the stratification in abstraction and specificity that guide theory construction. There are, in other words, different types of process models at different levels of theory. The overarching intelligence process is located at, and at the core of, the grand- and macro-level theorisation. Johnson (2003*a*: 2), for example, asserts that "[a]ny theory of strategic intelligence must be built around the so-called intelligence cycle". Limited to process models pertinently focused on in this article, this stratification can diagrammatically be depicted as in *Figure 1*.

Apart from conceptual elucidation, the preceding notional demarcation of the 'intelligence process model' sets requisites against which such theoretical constructs can be gauged. A model should parsimoniously explain a process that encompasses diverse activities and elements. Furthermore, a model ought to be simultaneously congruent *with* reality and an idealised, simplified representation *of* reality.

3. THE STATUS OF, AND REQUISITES FOR PROGRESSION WITH, INTELLIGENCE THEORY CONSTRUCTION

Requisites for the modelling of the intelligence process extend beyond the above-noted enumerative definitional demands. Since it is but an aspect of a multi-facetted Intelligence Studies' theoretical discourse, the status of this debate and the requisites emerging for optimal progression in theorisation generally, are also pertinent to intelligence process modelling.

Figure 1: A selective theoretical taxonomy of intelligence process models



While the agenda is still crystallising, the unprecedented surge in literature in the last decade shows that theorisation is sure to impact profoundly on most of Intelligence Studies' areas of academic enquiry. These, to name but a few, include the "definitional project", ethics, comparative intelligence, history and historiography, intelligence disciplines and subdisciplines, management and oversight as well as — what is arguably the most arduous — the construction of competing grand theories of intelligence (Goodman 2006: 2; Johnson 2007*a:* 2-9; Treverton *et al* 2006: 9, 10, 12). In what is a fairly recent and promising trend, "all theories of intelligence or counterintelligence" are no longer "overlaid on the traditional realist approach to international affairs" (Taylor 2007: 5). Post-modernists and critical-realists also entered the arena. However prolific and enriching these contributions are, the legacy of Intelligence Studies' theoretical paucity clearly presents a daunting challenge. The road to a theoretical *corpus* comparable to that of Strategic and Security Studies will be long and the progress incremental. So incipient is this discourse that a considerable segment thereof revolves around the methodology and avenues that should be followed in the construction of this road.

Hence, the following circumspective qualification by the preeminent Intelligence Studies scholar L K Johnson (2003*a*: 1) in the introduction to his landmark contribution, still encapsulates the primary requisite for progression with intelligence theorisation in general: "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". It is imperative, this article contends, that the laying out of 'what we know' should not be constricted to the literature conventionally associated with Intelligence Studies. Theorisation in Intelligence Studies, in other words, should be enriched by 'what is known' in other related disciplines. It should likewise not be oblivious to perspectives that could be provided by intelligence practice — be it in statutory or other milieus. Equally important 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 enduring views and axioms in Intelligence Studies.

4. A CRITICAL APPRAISAL OF INTELLIGENCE PROCESS MODELS WITHIN INTELLIGENCE STUDIES WITH SPECIFIC REFERENCE TO COUNTERINTELLIGENCE

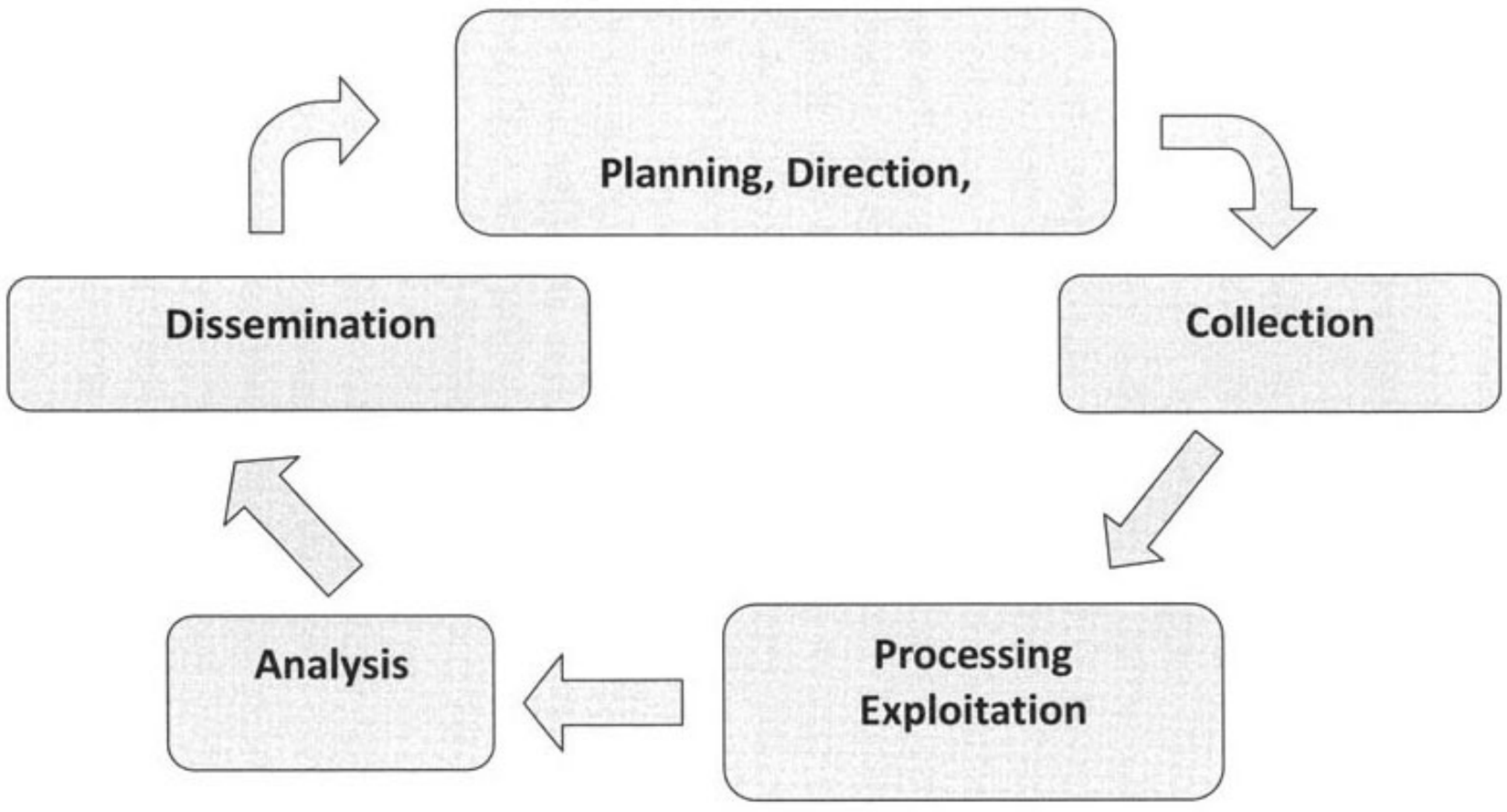
In line with these requisites, this section appraises some existing views on the conceptual structuring of the intelligence process. It commences with an examination of one of the most enduring notions in Intelligence Studies, namely the intelligence cycle.

4.1 The traditional view of the intelligence process

As it has done for more than six decades since its inception in the US and North Atlantic Treaty Organisation (NATO) military doctrine (Herman 1997: 283-286), the traditional view of a cyclic intelligence process continues to predominate thinking in the academic and statutory intelligence practice realms. "No concept", Hulnick (2007: 1, 19-20) observes, is "more deeply enshrined in the literature than that of the 'intelligence cycle'". In a similar vein, Berkowitz and Goodman (2000: 69) describe the concept of the intelligence cycle as pervading "thinking" about intelligence. While the intelligence cycle is well-known, academic neatness dictates an explication of this view. This model, in short, posits the following phases in a sequential, cyclic order: direction (the client expresses needs 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) that then leads to further needs expressed by the client and the repetition of the cycle (Berkowitz and Goodman 2000: 68-69). The degree to which the traditional view of the intelligence cycle has retained its core features over decades is reflected in the following graphical depiction (*Figure* 2) contained in recent, earlier cited, US government commission report.

In so far as the academic sphere is concerned, the five-volume anthology entitled *Strategic Intelligence* (Johnson, 2007 *c-g*) which represents a "landmark in the study of intelligence" (Johnson 2007*b*: i) bears testimony to the intelligence cycle's robustness in Intelligence Studies' thinking. More particularly the title of, and various

Figure 2: The intelligence cycle



Source: US 2005: 583 (adapted)

chapters in, Volume Two (*Strategic Intelligence — The Intelligence Cycle: The Flow of Secret Information from Overseas to the Highest Councils of Government*) reflect rife subscription to the intelligence cycle as a theoretical construct.[i)]

In stating the obvious, of the four commonly accepted intelligence disciplines, collection and analysis feature prominently in graphic depictions of the intelligence cycle. Counterintelligence and covert action are conspicuously absent. One therefore has to turn to narrative descriptions for clarity on where and how counterintelligence fits in with the intelligence process and for explanations on what the counterintelligence process looks like. Frequently, narrative descriptions are more confusing than useful. *Figure 2*, for example, is drawn from an appendix aimed at providing a "primer" on the functioning of statutory intelligence. The appendix, with the heading "An intelligence community primer", devotes a subsection to a discussion of the intelligence cycle. Neither counterintelligence nor covert action is mentioned as part of the discussion of the intelligence cycle. Instead the directly following subsection, entitled "Other intelligence activities: counterintelligence and covert action", explains the two disciplines without any reference to the intelligence cycle (US 2005: 584-585). Confusingly, counterintelligence and covert action are projected as integral parts of intelligence, yet then typified as "other intelligence activities" that are not part of the process by means of which intelligence is conducted. This implicit contradiction is left unexplained. Also in this instance, the example from the US mirrors the status of the thinking in the statutory intelligence communities of (probably most) other nation states.

More explicit views on counterintelligence's positioning *vis-à-vis* the intelligence cycle vary. Prompted on this matter some practitioners, notably those involved in counterespionage, nebulously posit offensive counterintelligence as 'fitting in somewhere' in the exploitation phase. There are also two further views which are not necessarily mutually exclusive. The first, and quite prevalent view, poses counterintelligence as protecting and being performed throughout the intelligence cycle (Codevilla 1992: 4, 26, 325-326). Counterintelligence is thus an integral part of, and executed within, all the sequential phases of the intelligence cycle. According to the second contention, the counterintelligence process itself mirrors the intelligence cycle in form. The counterintelligence process, in other words,

looks like, and is a midi-version of, the intelligence cycle. The Canadian Security Intelligence Service, by way of illustration, depicts the "security intelligence cycle" as comprising of a circular process with the phases "government direction", "planning", "collection", "analysis" and "dissemination" (Canada 2006). In synthesising the two views, Codevilla (1992: 325) asserts: "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".

4.2 Deficiencies of the intelligence cycle: from fissures to cracks

Uniting all traditionalist views on the intelligence cycle's accommodation of counterintelligence, just described, is the orthodox precept that this model is fundamentally sound — it just requires explanation and qualification. While the predominance of this view remains, the number of Intelligence Study scholars voicing critique over this model's congruency with reality has steadily been increasing in the post-Cold War era. In 1996, Johnson (1996: 670) remarked as follows on fissures between theory and practice: "In the textbooks, the intelligence cycle is depicted as cleanly sweeping curve, from tasking to dissemination. In reality, it can be like a back country road, replete with potholes, detours, and even bridges out". In the same year Herman (1997: 39, 43, 103, 283-296, 383)[ii] states that, while the intelligence cycle is a "useful cybernetic metaphor" for certain aspects of intelligence (such as managing intelligence production), it "mismatch[es]" the intelligence process within a civilian intelligence milieu. At the end of the millennium, more scholars sounded the alarm bells — fissures have widened to cracks. In 2000, for example, Berkowitz and Goodman (2000: 72-73) summarised the growing, yet still limited, recognition of the deficiencies of the intelligence cycle's theoretical construct as follows:

> 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.

Subsequently various practitioners and scholars articulated similar concerns. O'Connell (2004: 190) categorises the intelligence cycle as an "increasingly old-fashioned way of [depicting] how intelligence is conducted". In starker terms, Hulnick (2007: 20) concludes the intelligence cycle to be a "flawed vision, and thus poor theory. One need only ask those who have toiled in the fields of intelligence".

Deficiencies of the intelligence cycle cited in substantiation of critiques fluctuate from scholar to scholar. For purposes of this article, only some of the most prominent deficiencies mentioned are concisely highlighted and clustered into four areas for reasons of brevity. Firstly, the activities conventionally assigned to the intelligence cycle'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. "Intelligence managers" are thus the "real drivers" of the "intelligence collection process" (Hulnick 2007: 3). 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 dynamo 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, 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 once-off action, but generated and refined during various stages of the intelligence process. This refinement in-

volves analysis and management — that 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 dynamics demanded by contemporary intelligence practice. Deficiencies of this category cited in literature include the omission of "feedback" and "consumption" stages; failure to capture the "dynamic nature" of the interaction between the intelligence process and the "external environment" as well as the absence of a scanning or "scouting" phase (Gill and Phythian 2006: 3; Treverton *et al* 2006: 25; Lowenthal 2003: 41, 51-52; Bernhardt 2003: 27).

Fourthly, not so frequently mentioned in consulted literature and later elaborated on, is the intelligence cycle's dismal failure to accurately explain and truly accommodate counterintelligence and therefore counterespionage. 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. Own efforts in this regard were unsuccessful. Elaborate presentations and lectures by others received over a number of years were all conceptual quagmires endeavouring to artificially hammer a triangular peg (counterintelligence) into a round/cyclic hole (intelligence cycle). Reassuring then was to note seemingly similar experiences by authoritative and seasoned scholars. Hulnick (2007: 10) asserts that counter-intelligence "is not part of the traditional intelligence cycle — although some writers have tried to adapt the cycle into a counterintelligence model".

Omissions, tacit assumptions, vague references and elaborate explanations of counterintelligence fitting in 'somewhere in the exploitation' phase, being performed throughout the intelligence cycle and/or mirroring the intelligence cycle should be seen for what they are. They are all symptomatic fruits of 'actually we do not know how to conceptually integrate the fiddly counterintelligence discipline with the intelligence process'. Also the intelligence cycle *per se* should be seen for what it is. It is a model attempting to explain the positive intelligence process. By the look of the deficiencies listed above, it is

not particularly successful in this either.

4.3 The quest within intelligence studies for alternative intelligence process models

Given its predominance, regardless of patent deficiencies, the traditional view of the intelligence cycle can only be concluded as having almost acquired the elevated status of a 'Holy Grail' within statutory intelligence practice and Intelligence Studies. For now, most 'Knights of the Intelligence Order' are intrepid in their orthodox guarding of the grail. They are likely to continue doing so in the near future.[iii)] As implied in the preceding section, there is, however, dissent in the ranks, and the erstwhile unity around this theoretical construct is being eroded. Positions crystallising in this regard range from a neo-traditionalist defence of the traditional intelligence cycle to the categorical rejection of the notion that a viable overarching intelligence process model exists.

4.3.1 Neo-traditionalist views on the intelligence process

In contrast to orthodox proponents, neo-traditionalists acknowledge and identify further deficiencies of the intelligence cycle. In this respect, contributions by this school of thought are constructive to the academic discourse. The degree of propositions' constructiveness varies in step with the nature of the response to the intelligence cycle's deficiencies. At the one end of the spectrum, conventional neo-traditionalists admit that the intelligence cycle is flawed and acknowledge the possibility that more viable alternatives may emerge. As yet, it is further argued, viable alternatives have not been forthcoming and the traditional cycle "remains a useful way of understanding" how intelligence works (Quiggin 2007: 52-53). At the other end of the spectrum, reformist neo-traditionalists are advancing alternative postulations. This entails additions to, and is in some instances the remoulding of, the phases and activities described in the traditional cycle. Bernhardt (2003: 27), for example, adds a "scouting" phase and positions "analysis" (which is subdivided into various activities) at the centre of the intelligence process. Gill and Phythian (2006: 3-6) endeavour to compute for the impact of the internal and external environment on the process and, to this end, affix "external

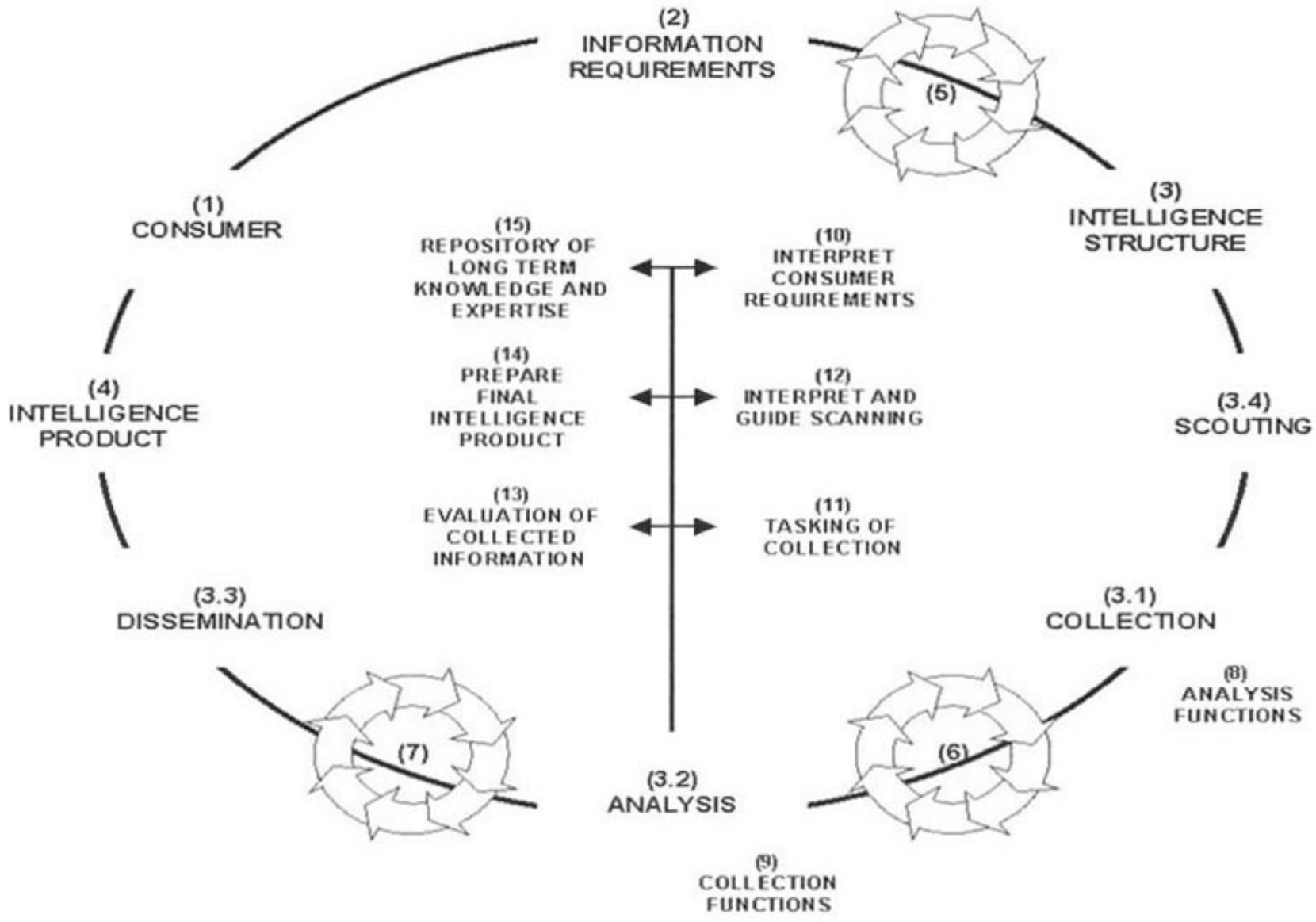
environment" and the "[i]ntelligence/policy environment" to the intelligence flow. Neo-traditionalist moderations, it must be emphasised, are done within the parameters of both the circular nature and the essential features of the traditional view of the intelligence process. On closer scrutiny they still ascribe to the intelligence cycle's core precepts and are essentially contemporised versions thereof. This is reflected in both the title and content of the graphic depiction of Bernhardt's proposition (see *Figure 3*).

4.3.2 Revisionist views

Similar to neo-traditionalists, revisionists do not necessarily reject all constituents of the intelligence cycle, but fundamental moderations and additions are forwarded in respect of one or more of the following: the remoulding or omission of certain of the traditional cycle's phases; the addition of process constituents (phase, steps, and the like); the re-orientation of the intelligence process to an alternative pivotal focus (of which Clarke's [2004: 18] "target-centric intelligence process" — is an example) and the directional flow by means of which activities are executed.[iv)] In addition to Clarke's model, revisionist propositions include those by Herman (1997: 39-47), Treverton (2001: 106)[v)] and Lowenthal (2003: 52). Revisionists' propositions generally incorporate an intricate multi-directional intelligence flow that more closely resembles the reality of intelligence practice. Consequently, the use of the term 'intelligence process', in these circles, is gaining ground over the use of 'intelligence cycle' (compare Lowenthal 2003: 51-52; Berkowitz and Goodman 2000: 72-73; Clark 2004: 18; Herman 1997: 39-47). Serving as an example is Lowenthal's model which is based on the contention that the intelligence process is "in reality … linear, circular, and open-ended all at the same time". The graphical depiction (*Figure 4)* illustrates the intricacies of this multi-directional flow.

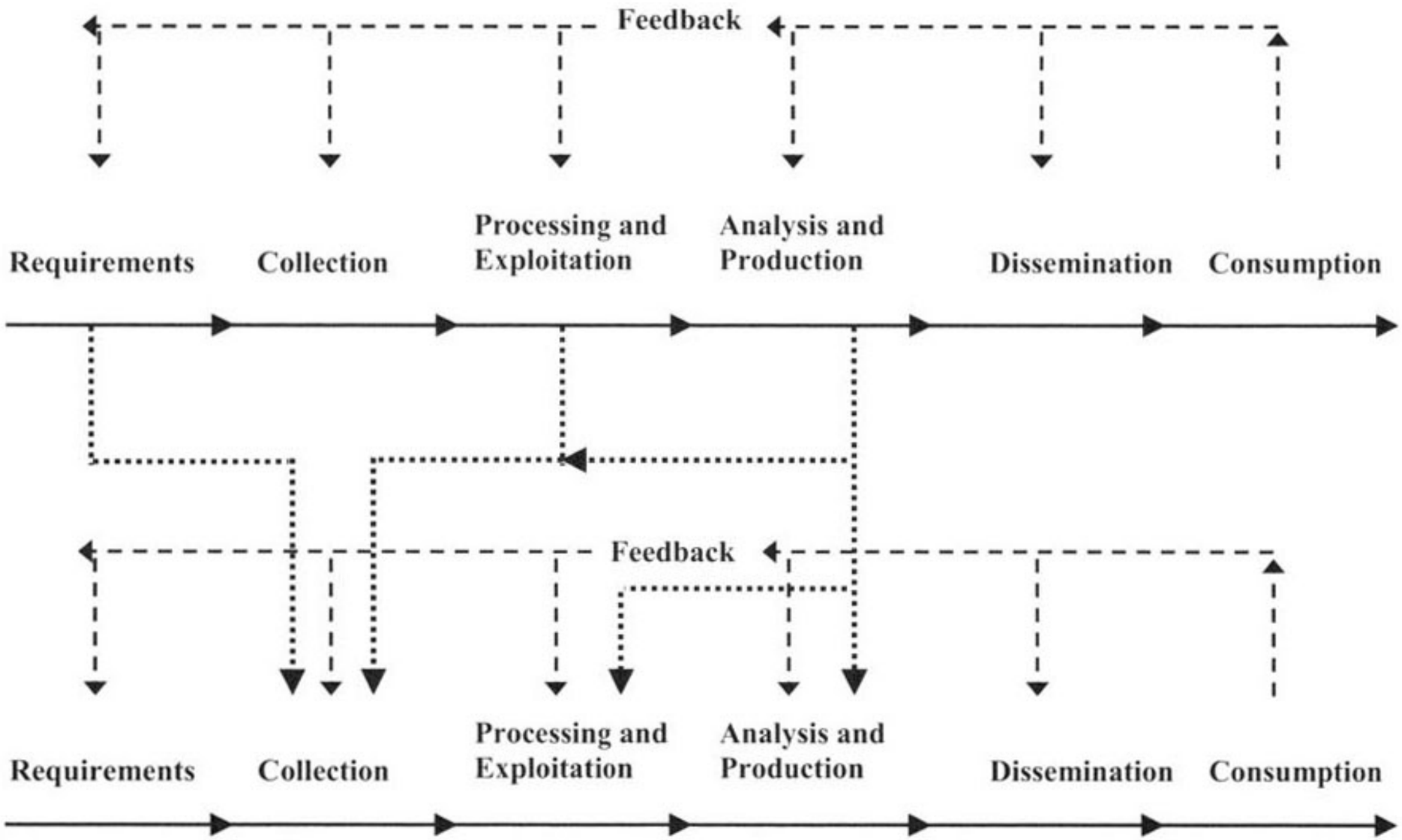
Regardless of the significant differences within and between the neo-traditionalist and revisionist positions, they *alas* share a common feature with the traditionalists — the neglect and more frequently the negation of counterintelligence. Counterintelligence is absent in graphic depictions, and references (to counterintelligence) in narrative explanations, if provided, are rather scant. Narrative explanations by Gill and Phythian, Bernhardt as well as Herman do not men-

Figure 3: The intelligence cycle (contemporary view)



Source: Bernhardt 2003: 27.

Figure 4: The multilayered intelligence process



Source: Lowenthal 2003: 52.

tion counterintelligence. Lowenthal is more forthright and explicit on counterintelligence. Counterintelligence is "not a separate step in the intelligence process but ... an important function performed throughout the process" (Lowenthal 2003: 113). He frankly qualifies this statement by stating "CI does not fit neatly" (Lowenthal 2003: 113). Similar to the traditional intelligence cycle, neo-traditionalist and revisionist views thus can be concluded as models geared toward positive intelligence. It needs to be reiterated that proponents of these models rarely qualify these as *positive intelligence* process models, but project their propositions as *intelligence* process models.

4.3.3 No intelligence process model — a Revolution in Intelligence Affairs?

Prompted *inter alia* by the negation of counterintelligence, an alternative position — which in Intelligence Studies terms is revolutionary — is emerging. It is revolutionary because it calls for overthrowing the notion that a justifiable overarching intelligence process model currently exists. While proponents of this position expressively reject the intelligence cycle, omissions of mentioning any other overarching intelligence process as well as the context of argumentation point to a rejection of such models in general (Agrell 2006: 21-22; Treverton *et al* 2006: 2; Hulnick 2007: 1-9). With the outstanding exception of Hulnick, the implications of this view for the conceptual structuring of the counterintelligence process have not been articulated. Hulnick (2007: 10, 14) is crystal clear and states as follows:

> 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: 14-7) proposes a "counterintelligence model" comprising a five-clustered "pattern", namely "identification", "penetration", "exploitation", "interdiction" and "claim success". Summarised, Hulnick's description of the phases of the counterintelligence model are as follows:

— The identification of espionage adversaries;

- the penetration of adversarial espionage intelligence structures;
- exploitation — as referring to the collection of information (on adversaries) and the institution of measures such as deception;
- interdiction that ensues when the "the case is turned over to law enforcement"; and
- public declarations by state authorities of successful counterintelligence actions.

Hulnick (2007: 10, 16) limits the counterintelligence model above to "active" counterintelligence. The latter includes, but is more encompassing than counterespionage. He 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" (Hulnick 2007: 10). 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).

Yet, the organisational functioning of hundreds of statutory intelligence structures globally attests to the existence of an overarching intelligence process. Likewise, counterintelligence in its offensive and defensive dimensions is executed as an integrated function or ought to be. Since the processes exist in reality, an idealised description thereof in a model or models is a theoretical possibility and a theoretical imperative. Confronted with a theoretical *corpus* of fragmented constructs, clarity on how this can be done is lacking. Admission of 'what we do not know' was mentioned as crucial to progress in theory construction. If the post-9/11 theoretical discourse within Intelligence Studies and statutory intelligence is in its infancy, the need for an agenda for the development of an overarching intelligence process is, figuratively and comparatively speaking, embryonic. In line with the requisites, earlier outlined, the setting of this agenda could benefit from advances made in other academic fields such as Business Intelligence and in particular Competitive Intelligence.

5. A CRITICAL APPRAISAL OF INTELLIGENCE PROCESS MODELS WITHIN BUSINESS INTELLIGENCE STUDIES WITH SPECIFIC REFERENCE TO COUNTERINTELLIGENCE

Unlike Business Intelligence which, since its establishment, drew extensively on Intelligence Studies' thinking, Intelligence Studies appears to be largely self-isolated and self-impoverished from enrichment by Business Intelligence. There are, naturally, various competing theories in this discipline and this article does not purport to be representative in its overview.

The pervasive influence of the intelligence-cycle concept is regrettably 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 sphere. 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 and Whitehead 2002: 4; Fleisher and Bensoussan 2003: 6; Brouard 2004: 4). These steps, and herein lies the difference, are increasingly qualified as an explanation of the "intelligence gathering process" (Nolan 1997: 56, 59). In the context of its use, "intelligence" is comparable to what in the statutory milieu would be categorised as positive intelligence.

Especially within (the Business Intelligence subdiscipline of) Competitive Intelligence, a clear distinction is drawn between the positive intelligence gathering process and the 'protection [competitive] intelligence process'. In the main, protective competitive intelligence is deemed to consist of two principal components, namely 'security measures' and 'counterintelligence'. Nolan advances the following concise differentiation: "Security seeks to *protect* a firm's assets, counterintelligence seeks to actively engage and *neutralize* a competitor's collection effort" (Nolan 1997: 55 — original emphasis). Security, explains Francq (2000: 71, 85), is of a passive nature and strives to reduce corporate vulnerabilities as well as to protect a firm's tangible and intangible assets (such as sensitive information) through a combination of policies, procedures and practices — on a lighter note re-

ferred to as "gates, guards, guns and dogs". Corporate counterintelligence, on the other hand, closely parallels statutory counterespionage. It is 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; Nolan 1997: 53). One of the "most proactive, aggressive, and effective" of these is "deception" — sometimes used interchangeably with "perception management" (Francq 2000: 75). Phrased in statutory intelligence lexicon, this means that counterespionage has facets of covert action in its countermeasures arsenal. Normative ideals and legality aside, those familiar with the starker side of the corporate world would agree that industrial counterespionage measures come in considerably more aggressive forms than deception and perception management.

With the *caveat* that there are variations, 'protective competitive intelligence' is widely accepted to consist of the following sequential steps: the formulation of protection requirements, an appraisal of the threat ("external danger") posed by competitors, an assessment of corporate vulnerabilities, the development and implementation of countermeasures, and lastly, the continual assessment and adaptation of the effectiveness of countermeasures in accordance with the changing environment (DeGenaro 2005: 14-15; Muller 2002: 4-5, 8; Francq 2000: 85). Statutory counterintelligence practitioners will recognise these steps as not radically new. They are an evolutionary, not revolutionary, adaptation of procedures that in the statutory counterintelligence milieu are phases described in Operational Security (OPSEC) manuals, namely the identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks (effectively adversarial intelligence capabilities measured against own state vulnerabilities) and the application of appropriate countermeasures (US 1996). What is new, is that Competitive Intelligence incorporates these steps in a model for explaining 'protective competitive intelligence'. A praxis theory for intelligence thus informed the design of (an aspect of) a theory of intelligence. What is furthermore new, is the emergence of models that endeavour to integrate 'protective competitive intelligence' with (positive) intelligence gathering conceptually.

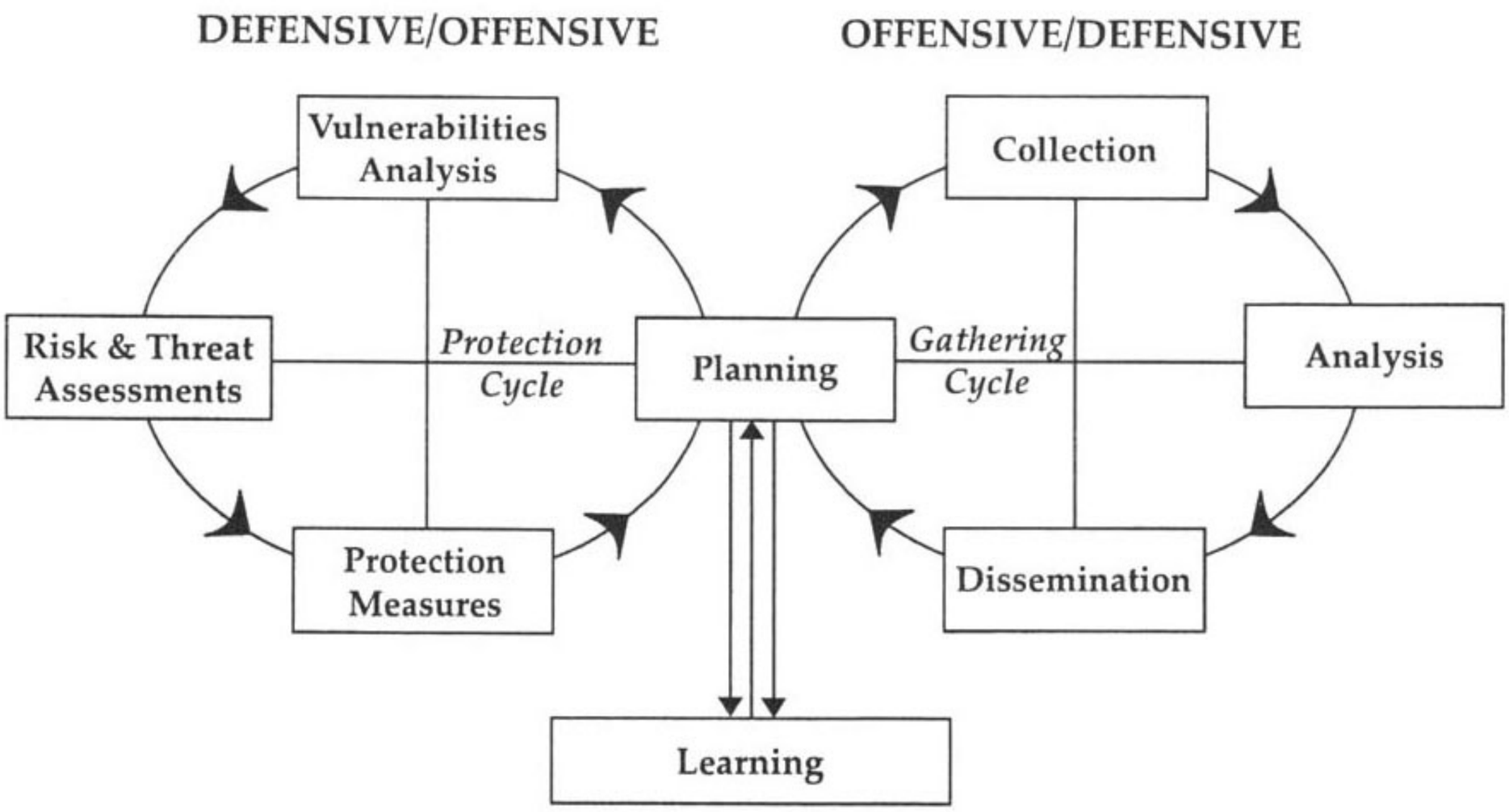
A seminal model forwarded in this regard by Nolan (1997) not only conceptually structures corporate counterintelligence, but also aims to integrate the latter with positive business intelligence. Nolan depicts positive business intelligence and corporate counterintelli-

gence, each as executed by means of repetitive circular process initiated by the "Strategist and Decision Maker" (Nolan 1997: 59). The diagrammatic depiction of the two overlapping circles resembles Brouard's model discussed below (*Figure 5*). The corporate counter-intelligence sequential cyclic is posited to comprise the following steps: "Define Protection Requirements", "Asses the Competition", "Estimate Vulnerabilities", "Develop Countermeasures", "Employ Countermeasures", "Analysis" and "Dissemination". Also sequentially executed, the intelligence gathering cycle has as steps the following: "Define Collection Requirements", "Tasking to Collectors", "Collection Activities", "Processing", "Analysis" and "Dissemination" (Nolan 1997: 59). The two cycles, as described, converge in the shared steps of "Analysis" and "Dissemination" resulting in "Actionable Products" to the "Strategist and Decision Maker" (Nolan 1997: 59).

Considering Competitive Intelligence terminology, Nolan's model is limited to linking positive intelligence with offensive counterintelligence. While exploratory in nature, some more recent works within Competitive Intelligence endeavour to integrate the whole of corporate defensive intelligence (that is, corporate offensive counterintelligence as well as security measures) with positive business intelligence. Serving as an example is a proposition by Brouard (2004: 2-3, 5, 8-9) on an "intelligence gathering and protection intelligence process". As suggested by the title of the model, and as depicted by *Figure 5*, Brouard's model consists of a "gathering process" (geared towards positive corporate intelligence) and a "protection" process (dealing with the defensive corporate intelligence process).

Statutory intelligence provided the theoretical and practice-directed cornerstones for the establishment of Competitive Intelligence. Paradoxically, Competitive Intelligence seems to have overtaken Intelligence Studies in endeavouring to structure the counterintelligence and counterespionage processes notionally. Competitive Intelligence thinking can of course not be summarily applied to Intelligence Studies and statutory intelligence practice. Neither are the Competitive Intelligence models discussed without inherent deficiencies. Nevertheless, the subsequent section will show this academic field's propositions on the counterintelligence process, and the integration thereof with the positive intelligence process, as informative to the theoretical progression within Intelligence Studies.

Figure 5: Intelligence gathering and protection intelligence process



Source: Brouard 2004: 5.

6. A CONTOUR TOWARD THE THEORETICAL STRUCTURING OF THE OVERARCHING INTELLIGENCE PROCESS

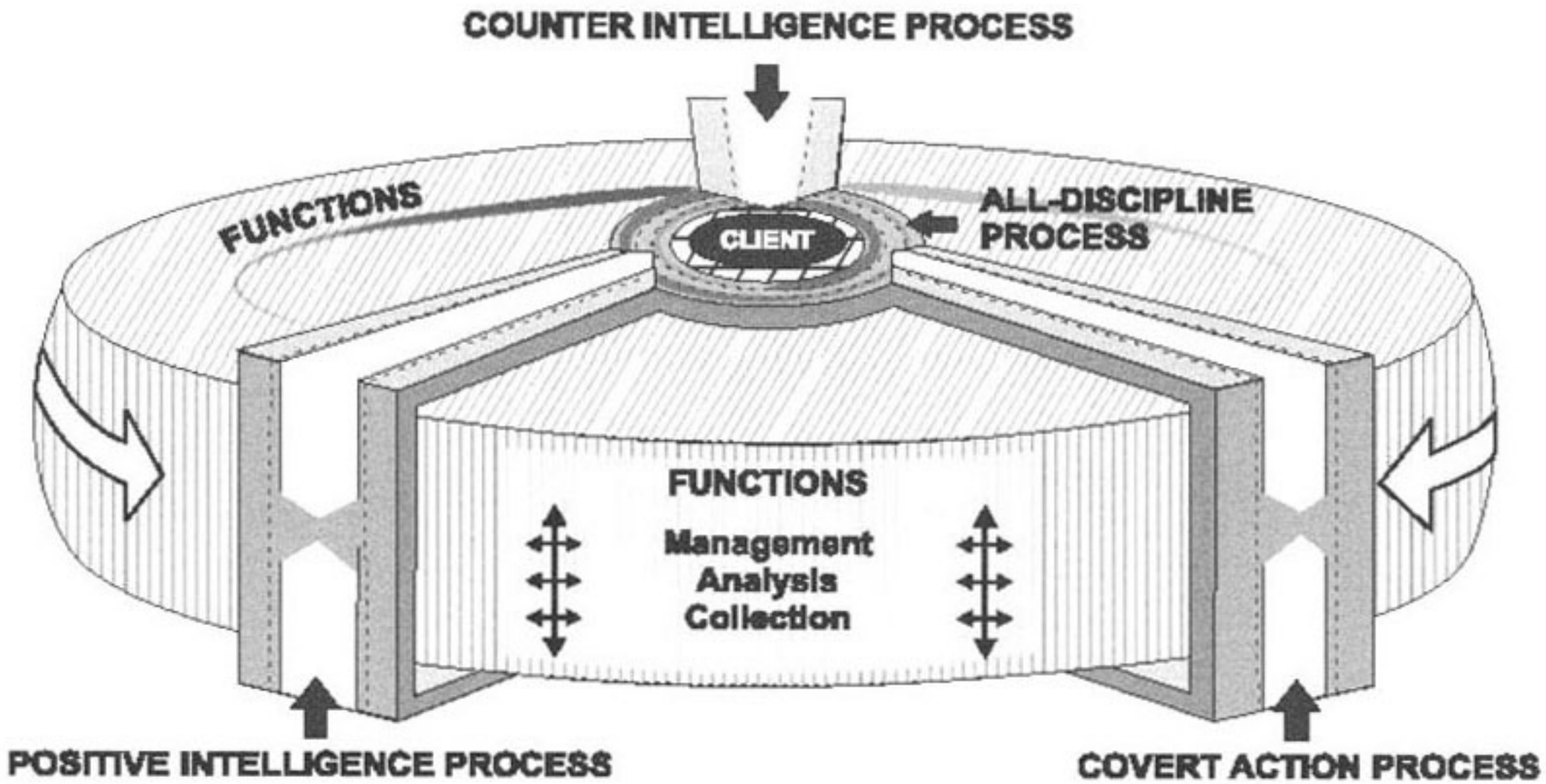
The aim of the critical appraisal of thinking on the intelligence process within Business Intelligence as well as Intelligence Studies, to re-iterate, is the laying out of existing knowledge in a manner that offers suggestions on the next steps in theory construction. These suggestions could conceivably be presented as a tentative proposition on an overarching intelligence process. This would require a eureka-type insight which the article does not purport to advance. Instead, it suffices with offering the following 'contour' that will hopefully be useful to the incremental progress towards an overarching process (see *Figure 6*).

The proposition above is reductive and reductionist. It is reductive in its simplification, and some would justifiably argue an oversimplification of a vastly more intricate process. Aspects and activities cited in Section 4.3 that ought to be incorporated in an overarching process are, for example, not computed. The proposal is reductionist in that it advances the intelligence process as a 'sum of parts'. The intelligence process is posited as a nexus which combines various processes and functions. These functions simultaneously traverse the subprocesses and the central (all-discipline) process itself. Since the combined aspects could be more than the 'sum of parts', this reductionism (as apposed to holism) is a simplification. Nonetheless, at this early juncture, simplifications of this sort are conducive to theory construction.

The nexus's reductive-reductionist attributes are reflected in the following key contentions on which it is based:

— The overarching statutory intelligence process is the sum of processes executed in three *principal disciplines*, namely, positive intelligence, counterintelligence and covert action. Each of these has a distinctive and, to a degree, a unique pattern of activities. This contention builds on the proposition by Hulnick and those within Competitive Intelligence. The axiom of intelligence consisting of the four principal disciplines is thus contested. It is unclear how the common acceptance of 'analysis', 'collection',

Figure 6: A reductive, conceptual nexus towards an all-discipline intelligence process



'counterintelligence' and 'covert action' as the principal intelligence subdisciplines originated or evolved. Future studies by Intelligence Studies' historians and historiographers might well find that it was influenced by the organisational structuring of some post-World War II, Western statutory intelligence services. Whatever the reason, this axiom is incongruent with reality.

— Analysis and collection are *functional areas* of activity performed within all three principal disciplines and as part of the collective all-discipline process. Notwithstanding obvious similarities, there are simultaneously significant differences in emphasis and methodology in the manner in which these functions are executed within the respective primary disciplines. In comparison with positive intelligence, counterintelligence analysis for one is more diverse in its scope, methodology and techniques. Cognisance is taken of the fact that some practitioners may categorise collection and analysis as 'disciplines' or 'subdisciplines'. If so, then they are functional, not primary disciplines. Be that as it may, functional areas are not limited to analysis and collection. The identification of further functional areas would require dedicated research and this article suffices in proposing 'intelligence management' as an addition. The critical appraisal in the preceding section has shown intelligence management, in conjunction with analysis, to be the real interface with the client (decision-maker) in the actualities of intelligence practice.

— Drawing on Lowenthal's (2003: 52) proposition, the nexus assumes the intelligence process to be conducted by means of a *multi-directional activity flow*. The latter applies to the respective principal disciplines, the functions and the combination thereof in the all-discipline process.

The contour provided clearly requires considerable refinement and substantiating research. Notwithstanding its cursory nature, the nexus already holds out against the litmus test for conceptual clarification. The notional 'uncluttering' of the relationship between counterintelligence and transnational security concerns such as counterproliferation (of Weapons of Mass Destruction — WMD), organised crime and counterterrorism serves as an example. While some scholars consider counterterrorism as part of counterintelligence, others assert

counterterrorism to have "developed" into a "separate intelligence discipline" (Wettering 2000: 266; Codevilla 1992: 325; Hulnick 2007: 10). Counterterrorism is neither a separate intelligence discipline, nor is it part of counterintelligence. It is a security concern that involves facets of positive intelligence, covert action as well as counterintelligence.

The nexus furthermore suggests one possible route in the construction of an overarching intelligence process model. The design of the latter requires and should be preceded by conceptual clarity on the three disciplinary processes. A sound intelligence process, in other words, can only be constructed pursuant to the formulation of the respective disciplinary models. The subsequent section advances tentative suggestions on the theoretical structuring of the process of one of these disciplines, namely counterintelligence.

7. A CONCEPTUAL DELINEATION OF COUNTERINTELLIGENCE

As suggested by the section's heading, the theoretical structuring of the counterintelligence process is inseparably linked with a notional delineation of counterintelligence itself. The notional delineation — enumerative, ostensive or otherwise — mentioned in Section 2.2, is at the core of theorisation. The way in which counterintelligence is delineated, in other words, is central to the structural modelling of the counterintelligence process. Such a demarcation, moreover, positions counterintelligence *vis-à-vis* the other disciplines and consequently explicates counterintelligence's slotting in with the overarching intelligence process. While a satisfactory graphic model of this 'dovetailing' evades, a narrative description offers a start.

Attempting this 'start' is daunting. Counterintelligence is arguably the most complex and "least understood" of all disciplines (Godson 1980: 1). It defies easy description because of its multifaceted nature. In this regard, Miler (1980: 40) aptly 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 counterintelligence is a combination of so many aspects of the intelligence business

and other political, military, economic and societal factors ...

This article does not venture into the protracted deliberations accompanying a denotative definition as this would detract from the article's focus. Counterintelligence is demarcated through addressing three basic problem statements, namely 'What does counterintelligence protect?', 'Against what does counterintelligence protect?' and 'How does counterintelligence protect'? *Figure 7* is used as a conceptual aid in guiding the response to these questions.

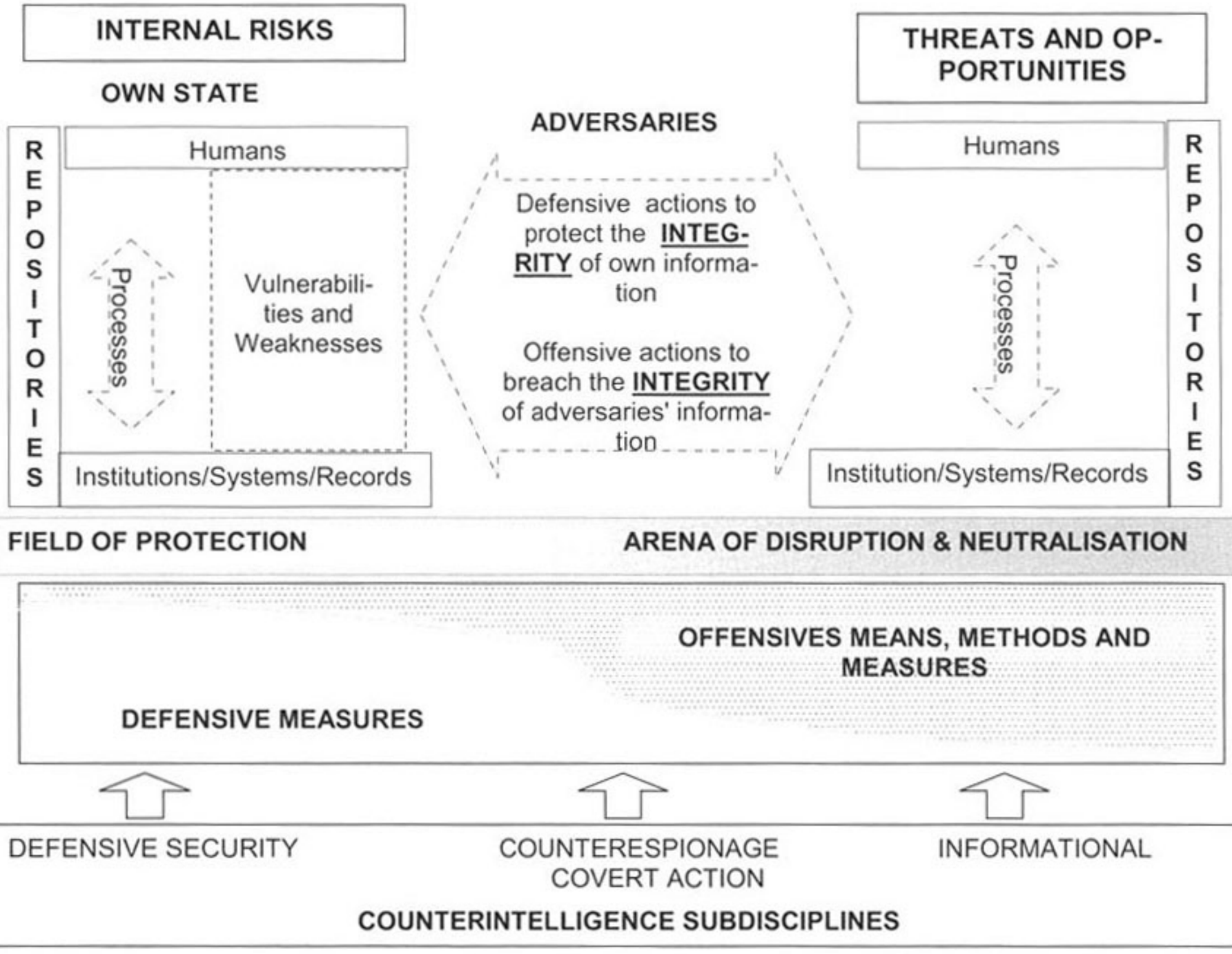
7.1 What does counterintelligence protect?

Counterintelligence protects the integrity of national-security relevant information. 'Integrity' in its use here refers to, on the one hand, the inherent integrity of the information's veracity/reliability and where applicable its confidentiality. Counterintelligence, simply put, guards against the malicious tampering of information, disinformation and from the unauthorised disclosure of information. On the other hand, 'integrity' refers to informational functionality and reliability. It thus pertains to the effective working of systems, repositories and processes pertaining to such information. Underpinning the latter, is the notion that national-security relevant information is not amorphously loose standing. Information resides in systems (including physical records and Information Technology [IT] systems), processes (such as communication) and humans (individuals and personnel). Institutions and individuals are custodians of information. Counterintelligence therefore safeguards the relevant institutions and ensures the integrity of humans with access to the information. An intelligence service is naturally one of these institutions, and the protective shield is employed in respect of the counterintelligence function itself, positive intelligence information and activities as well as covert action information and operations.

7.2 From and against what does counterintelligence protect?

Albeit implicit, the preceding paragraph already provided a partial response to this question. Counterintelligence protects against internal risks (weaknesses and vulnerabilities) and external threats. The com-

Figure 7: A notional structuring of counterintelligence



promising of information through human negligence or insecure systems is an example of an internal risk. External threats are posed by role-players that seek, or may attempt, to breech the integrity of national-security relevant information. These adversarial actions assume various forms and can broadly be clustered in espionage, aspects of covert action (disinformation) and the disruption or manipulation of information through, for example hostile cyber activities. Adversarial action is executed by the use of diverse instrumentalities. Espionage, to illustrate, exploits humans (HUMINT) and technical means (TECHINT). The latter, in turn, comprise of Signal Intelligence (SIGINT), Imagery Intelligence (IMINT), Measurement and Signature Intelligence (MASINT) and Cyber Intelligence (CYBINT). Equally diverse are adversarial role-players. They include opposing nation states, entities within private enterprise, non-governmental organisations (NGOs), entities within the mass media, terrorist and extremist groupings, and unaffiliated individuals/groups. In the contemporary espionage reality these role-players as well as the clusters of adversarial actions are interwoven in an intricate web.

7.3 How does counterintelligence protect?

Counterintelligence, as previously mentioned, protects national-security relevant information from internal vulnerabilities and against external threats defensively, offensively and the combination of these two. Offensive actions engage adversaries with the aim of exploiting, manipulating and neutralising their intelligence activities. The institution of defensive and offensive measures is informed by the collection and assessment of all-source information. Some of this information is collected and assessed by counterintelligence. Effective counterintelligence, however, also benefits in this regard from information provided by the other disciplines. Likewise, counterintelligence generates information of value to positive intelligence and covert action. For its part, and given its offensive dimension described above, offensive counterintelligence uses aspects of covert action to influence and mislead espionage adversaries. Within a civilian, statutory intelligence context, offensive counterintelligence and the informational aspects of covert action are in some instances nearly undistinguishable — and so it should be.[vi)] Dimensions of covert action are part of counterintelligence. This is fittingly encapsulated in the following ob-

servation by Codevilla (1992: 349): "Action against the enemy through the enemy's own intelligence is the very consummation of CI".

Mirroring counterintelligence's missions, specific measures range from non-aggressive passive measures to highly aggressive offensive methods. Possibly the most passive and defensive cluster of counter-intelligence 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). At the other end of the spectrum, are aggressive offensive measures that include expulsion, extra-ordinary rendition, prosecution and the execution of adversarial spies. Between these two, lies a wide array of other measures such as pre-employment personnel security, in-service personnel security, technical surveillance countermeasures (TSCM), encryption, surveillance (physical, static, mobile and electronic), multiple types of agent operations and continued monitoring. Care should be taken to not conceptually pigeon-hole these measures as within the domain of particular counterintelligence subdisciplines or as having only a defensive or an offensive purpose. In various instances they are useful to more than one (See *Figure 7*). Similarly their uses are not restricted to counterintelligence and they benefit the other primary intelligence disciplines.

7.4 The counterintelligence trident

Although counterintelligence measures have multiple uses, notionally there are three distinctive patterns regarding the respective aims and manners in which they are structured, combined and deployed. Hulnick, will be recalled, posits 'counterespionage' ("active" counter-intelligence) as a specialisation field with a characterising "path" and 'protective security' is widely regarded as another. To this 'informational covert action' can be added. This addition is done from a civilian intelligence perspective and pertains to informational covert action directed against espionage adversaries. While synergy with the covert action discipline is imperative, informational covert action in the counterintelligence sphere is not only highly compartmentalised but also has a distinguishing configuration of execution. Informational

covert action, protective security and counterespionage, constitute the three subdisciplines of a counterintelligence trident that is yielded offensively and/or defensively with their distinctive patterns apparent throughout the whole of the counterintelligence process. The next section is devoted to the conceptual structuring of this process.

8. THE CONCEPTUAL STRUCTURING OF THE COUNTERINTELLIGENCE PROCESS

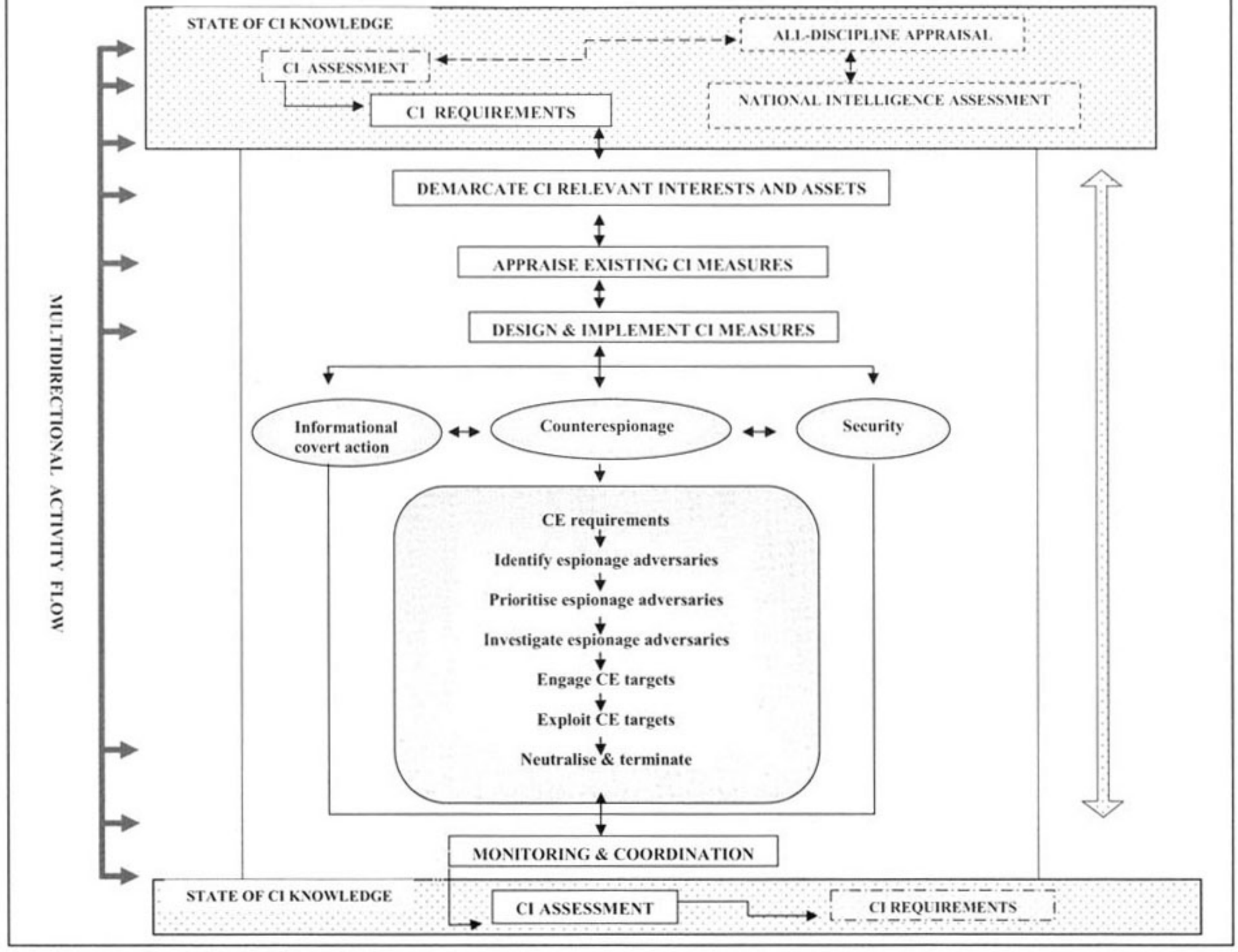
This being an exploratory article, only brief reference can be made to the distinctive pattern of one of the subdisciplines, namely counter-espionage. For the same reason, the discussion of the model on counterintelligence *per se* is but a cursory outline. Graphically, the model can be depicted as in *Figure 8*.

8.1 The formulation of counterintelligence requirements

A model of the counterintelligence process, to recapitulate, represents a simplified idealisation of "what the process should look like if everything goes as planned" (Berkowitz and Goodman 2000: 72). Ideally, the counterintelligence process would commence with the client expressing requirements. In a broad sense counterintelligence requirements refer to that 'intelligence' (information) and those 'services' (actions) the client expects from its counterintelligence apparatus in order to pursue its vital interests and objectives optimally. Given its extensive mission, counterintelligence "needs guidance from policy makers. Counterintelligence cannot protect everything. Policy makers need to determine what to defend, what to neutralize, and what to manipulate" (Godson 2001: 4). "Given the finite nature of its CI resources", affirms deGraffenreid (1989:151), clarity is required on, "those values, secrets and institution" that warrant counterintelligence protection.

Even if a utopian relationship would have existed between a statutory counterintelligence structure and its client, no reasonable practitioner would expect a neatly packaged 'wish list' with clear-cut, all-encompassing requirements and priorities. What is required from the policymaker is clarity on national security objectives, policies,

Figure 8: The counterintelligence process



priorities and strategy. Herein, to paraphrase Johnson (2003*b*: 639, 641) "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". A counterintelligence model should be congruent with and compute this reality — idealisation should not regress into over-idealisation. Failure to do so is, after all, is a deficiency several existing intelligence process models share.

Hence, the model depicts counterintelligence requirements *as derived and not received*. It is derived from a comprehensive all-disciplinary effort involving all functions (see *Figures 6* and *8*). This typically culminates in a National Intelligence Assessment (NIA) that intelligence services produce annually.[vii)] An NIA is preceded by comprehensive continual assessments within an intelligence service's fields of responsibility. Within counterintelligence, this assessment ought to embody the existing 'state of counterintelligence knowledge'. The 'state of knowledge', not only entails clarity on what the counterintelligence structure 'knows', but also on 'what it does not sufficiently know' and 'what it needs to know'. The last two aspects are in effect counterintelligence requirements often self-generated and inferred by the intelligence service. In the linear facet of the multidirectional activity flow, the counterintelligence assessment is therefore simultaneously at the 'start', performed throughout, as well as at the 'end' of the counterintelligence process. Illustrating the overlapping nature of phases is that, based on the principal counterintelligence requirements contained in the national counterintelligence assessment, more specific requirements are generated throughout the counterintelligence process. This phase, as all the others, is therefore not rigidly sequential. Phases are linked with an activity flow that is — as suggested by Lowenthal (2003:52) — at the same time linear, circular, open-ended and in continuous interaction.

8.2 The demarcation of informational interests and assets of counterintelligence relevance

Without detracting from the multi-directional reality, theory construc-

tion's aim to simplify in some instances necessitates the posing of hypothetical problem statements. Should the counterintelligence process have been conducted *ad novo* and guidance from the policy-maker fragmented, what would the first step have been of the process that culminated in the counterintelligence assessment described above?

Using the term 'counterintelligence protection' in its offensive and defensive connotations, deGraffenreid (1989:150 — emphasis added) 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 a lot of them". With the same connotations, Godson (2001: 188 — emphasis added) endorses this standpoint and advises as follows: "Ascertaining what really needs protection is the right place to *begin*".

This is an exhaustive process which entails inferring the national-security relevant information noted in Section Seven. It involves the identification of the state's informational interests through an appraisal of national-security interests in the political, social, technological, economic, military, ecological (environmental) and informational sectors. 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. This encompasses the whole body of information available to the nation state and which is necessary for its survival, prosperity as well as the expansion of its national interests. 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 counter-intelligence measures or undermining the informational integrity of an adversary).

8.3 The evaluation of existing counterintelligence measures

Following, and in various respects overlapping with the preceding phase, the counterintelligence process progresses from assessing the vulnerabilities of the state's informational interests to identifying and assessing risks and threats. Concurrently, the effectiveness and

pertinence ('appropriateness') of existing counterintelligence measures are evaluated. This is done with consideration of the relative value of informational interests and assets, internal risks (inclusive of vulnerabilities) and external threats. From a defensive and offensive perspective, it is ascertained which interests and assets are unnecessarily protected, overprotected and underprotected. While the distinctive patterns of the three counterintelligence subdisciplines are visible in all phases, they are particularly apparent in this, and even more so, during the following phase.

8.4 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', areas for directing the analysis and collection effort are also 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?' Decisions taken in this regard are formulated 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 subsequently conducted within the respective counterintelligence subdisciplines of which only counterespionage is explicated in Section 9.

8.5 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 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 within the cyber sphere could, for example, be left apparently weak to entice suspected hostile espionage.

8.6 Counterintelligence assessment

Although the drafting of assessments is a continual activity, an intelligence service will — as noted above — additionally schedule comprehensive appraisals of the effectiveness of counterintelligence measures typically on an annual basis. Such an appraisal is indispensable to a revision of the comprehensive counterintelligence assessment which — in the linear dimension of the activity flow — was conducted at the 'start' of the counterintelligence process. Also, the counterintelligence assessment at the 'end' of the process is informed by the integrated all-discipline appraisal from which a national intelligence assessment is derived.

This section, in summary, advanced a conceptual structuring of the counterintelligence process. Even simplified as a model, this process is multi-facetted and diverse. It is patently clear that existing propositions that purport counterintelligence to somehow mirror or fit processes actually designed to explain positive intelligence, do simply not withstand the reality test. The counterintelligence process was shown to comprise a trident of three subdisciplines. These subdiscip-

lines are notionally distinguishable, but are not separable — whether in practice or in conceptual models. It is within the context of symbiotic relationship between the subdisciplines that the explication of the counterespionage process in the next section should be viewed.

9. A CONCEPTUAL STRUCTURING OF THE COUNTERESPIONAGE PROCESS

It was earlier noted that counterespionage, as the other two subdisciplines, follows a distinctive pattern of activities throughout the whole of the counterintelligence process. The explanation here is limited to a phase of the counterintelligence process during which this pattern is particularly apparent (See *Figure 8*). With this qualification, counterespionage can be presented as the six-phased process discussed below.

9.1 Identification of espionage adversaries

From a counterespionage perspective, the prior phases of the counterintelligence process 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- or unprotected, and thus rendered vulnerable to hostile espionage endeavours; and

— deficiencies in the intelligence picture regarding adversarial espionage directed against critical information interests.

The identification and prioritisation of espionage adversaries (discussed below) should not be equated with an adversary-centric 'default starting point', frequently and erroneously resorted to in counterespionage. An adversary-centric 'default starting point' 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 of this is where classified information on the activities of foreign intelligence service

X exists and the service is identified as a priority for counterespionage collection. In most instances, the collection produces more information on service X, leading to the continued or higher prioritisation of this service. This self-feeding cycle results in the continual direction of resources to know espionage adversaries, with the concomitant risk of other role-players potentially posing threats to national security, exceeding those of service X, going undetected. The identification of espionage adversaries therefore should ideally be based on the state's informational interests and assets determined in preceding steps of the counterintelligence process (See Section 8.1 and 8.2) and be enriched by parallel open-source environmental scanning.[viii)]

9.2 Prioritisation of espionage adversaries

Intelligence services, as was previously remarked, 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. Espionage adversaries are consequently prioritised for further scrutiny according to the threats they pose.

9.3 Investigation of espionage adversaries

The further 'scrutiny' of espionage adversaries can, for 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 on prioritised espionage adversaries by means of overt and secret methods. Secret methods of collection vary in risk and resource implications. High risk and cost measures would typically only be employed if so justified by a preliminary investigation.

The aim of the preliminary investigation, in short, is 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 it warrants the employment of counterespionage measures carrying a high risk and with sizeable resource implications. 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.

9.4 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 use of 'engagement' in this article instead of 'penetration' to describe 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.

9.5 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, decep-

tion, 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 cited in Section 7.2. In their practical execution, the respective measures are dimensions of a converged and multifaceted entirety.

9.6 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 well-known Ames and Hanssen cases 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.

10. CONCLUSION

Phrased in more detail, the article's title poses two questions. Firstly, whether certain axioms in Intelligence Studies offer sufficient theoretical explanations of, or could provide constituents foundational to the construction of models of the intelligence and counterintelligence processes. It is clear that these axioms are crumbling in the wake of the post-9/11 theoretical discourse in Intelligence Studies. Superficial modifications of these axioms are nothing more than (unsuccessful) symptomatic repairs to anachronistic disintegrating 'Holy Grails'. Alternatives need to be found.

The title, secondly, raises the question of the way forward in so far as theorisation on these processes is concerned. In line with the requisites for progression on this road, existing postulations on the intelligence and counterintelligence processes were critically appraised. This informed the restructuring of what is, for the most part, existing knowledge. Furthermore, this was done in a manner that aimed to aid further theorisation.

The article advanced, as one of the requisites of progression in theory, forthrightness in stating 'what we do not know'. If nothing else, the propositions on the intelligence, counterintelligence and counterespionage processes demonstrated an abundance of fragmented knowledge of 'what we know'. What counterintelligence practitioners and scholars 'do not know' is how to structure these multi-facetted processes in a manner that satisfactorily meets models construction's demand of reflecting this reality in a simplified notional construct with real explanatory power. This article should be viewed as part of the gradual progression towards such viable intelligence process models.

ENDNOTES

i. See in particular the remark by Hulnick, (2007:1): "The intelligence cycle is so nicely described in other chapters that there seems no need to go over it here".

ii. The second print of Herman's(1997) work was used in the research for the article. The work was first published in 1996.

iii. See the following remark by Hulnick, A S, *op cit*, pp 19-20: "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".

iv. As cited by Duvenage, M A, 2010: 13.

v. As cited by Duvenage, M A, 2010: 9.

vi Conventionally, the type of adversary is employed as distinguishing criterion. Counterintelligence targets opponents with intelligence capacities, while covert action is more generally focused on other adversarial role-players.

vii Depending on the intelligence service's practice, a National Intelligence Assessment (NIA) is a comprehensive appraisal from which the National Intelligence Estimate (NIE) is derived.

viii A conceptual framework for such parallel, environmental scanning is described in Duvenage, P C, *Open Source Environmental Scanning and Risk Assessment in the Statutory Counterespionage Milieu*, Unpublished DPhil thesis, University of Pretoria, Pretoria, 2011.

BIBLIOGRAPHY

Agrell, W. 2006. "Which Assumptions should be Overturned?", in Treverton, G F *et al*, *Toward a Theory of Intelligence — Workshop Report*. RAND Corporation. Available at: http://www.rand.org/pubi/larf/proceedings/2006Rand–CF219.pdf. Accessed 14 February 2008.

American Heritage Science Dictionary (online). 2005. Boston: Houghton Mifflin Company. Available at: http://www.thefreedictionary.com/theory. Accessed 21 November 2010.

Berkowitz, B D and A E Goodman. 2000. *Best Truth: Intelligence in the Information Age*. New Haven: Yale University Press.

Bernhardt, W A. 2003. *A Qualitative Conceptual Framework for Conducting Risk- and Threat Assessment in the South African Domestic Intelligence Environment*, unpublished DPhil 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 Corporation. Available at: http://www.rand.org/pubi/larf/proceedings/2006Rand–CF219.pdf. Accessed 14 February 2008.

Brouard, F. 2004. "Business Intelligence for Canadian Corporations after September 11". *Journal of Competitive Intelligence and Management*, Vol 2, No 1.

Canada. 2006. "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. Accessed 13 December 2008.

Clark, R M. 2004. *Intelligence Analysis: A Target-Centric Approach*. Washington (DC): CQ Press as cited by Duvenage, M A. 2010. *Analysis in the Knowledge Age — An Analysis of the Challenges Facing the Practice of Intelligence Analysis*, unpublished MPhil dissertation. Stellenbosch: University of Stellenbosch.

Codevilla, A. 1992. *Informing Statecraft — Intelligence for a New Century*. New York: The Free Press.

DeGenaro, B. 2005. "A Case for Business Counterintelligence". *Competitive Intelligence Magazine*, Vol 8, No 5, September.

DeGraffenreid, K. 1989. "Counterintelligence" in Godson, R (ed). *Intelligence Requirements for the 1990's: Collection, Analysis, Counterintelligence and Covert Action*. Lexington: Lexington Books.

Duvenage, M A. 2010. *Analysis in the Knowledge Age — An Analysis of the Challenges Facing the Practice of Intelligence Analysis*, unpublished MPhil dissertation. Stellenbosch: University of Stellenbosch.

Duvenage, P C. 2010. *Open-source Environmental Scanning and Risk Assessment in the Statutory Counterespionage Milieu*, unpublished DPhil thesis. Pretoria: University of Pretoria.

Fleisher, G S and B E Bensoussan. 2003. *Strategic and Competitive Analysis*. New Jersey: Prentice Hall.

Francq, A. 2000. "The Use of Counterintelligence, Security, and Countermeasures", in Fleisher, F S, and D L Blenkhorn (eds). *Managing Frontiers in Competitive Intelligence*. Westport: Quorum Books.

Gill, P. 2006. "What is Intelligence Theory?", in Treverton, G F *et al*. *Toward a Theory of Intelligence — Workshop Report*. RAND Corporation. Available at: http://www.rand.org/pubi/larf/proceedings/2006Rand–CF219.pdf. Accessed 14 February 2008.

Gill, P and M Phythian. 2006. *Intelligence in an Insecure World*. Cambridge: Polity Press.

Godson, R. 2001. *Dirty Tricks or Trump Cards — U.S. Covert Action and Counterintelligence*. New Brunswick: Transaction Publishers.

Godson, R. 1980. "Counterintelligence: An Introduction", in Godson, R (ed). *Intelligence Requirements for the 1980s: Counterintelligence*, Vol 3. Washington (DC): National Strategic Information Center Incorporated.

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. Accessed 5 January 2008.

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. 2007*a*. "An Introduction to Intelligence Studies Literature", in Johnson, L K (ed). *Strategic Intelligence — Understanding the Hidden Side of Government*, Vol 1. Westport: Praeger Securities International.

Johnson, L K (ed). 2007*b*. "Preface", in *Strategic Intelligence — Understanding the Hidden Side of Government*, Vol 1. Westport: Praeger Securities International.

Johnson, L K (ed). 2007*c*. *Strategic Intelligence — Understanding the Hidden Side of Government*, Vol 1. Westport: Praeger Securities International.

Johnson, L K (ed), 2007*d*. *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 (ed), 2007*e*. *Strategic intelligence — Covert Action: Behind the Veils of Secret Foreign Policy*, Vol 3. Westport: Praeger Securities International.

Johnson, L K (ed), 2007*f*. *Strategic Intelligence — Counterintelligence and Counterterrorism: Defending the Nation against Hostile Forces*, Vol 4. Westport: Praeger Securities International.

Johnson, L K (ed), 2007*g*. *Strategic intelligence — Intelligence and Accountability: Safeguards Against the Abuse of Secret Power*, Vol 5. Westport: Praeger Securities International.

Johnson, L K. 2003*a*. "Bricks and Mortar for a Theory of Intelligence". *Comparative Strategy*, Vol 22, No 1, January.

Johnson, L K, 2003*b*. "Preface to a Theory of Strategic Intelligence". *Interna-*

tional Journal of Intelligence and Counterintelligence, Vol 16, No 4.

Johnson, L K. 1996, "Analysis for a New Age". *Intelligence and National Security*, Vol 1, No 4, October.

Herman, M. 1997. *Intelligence Power in Peace and War*, (1st reprint). Cambridge: Royal Institute of International Affairs, Press Syndicate of the University of Cambridge.

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.

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.

Kent, S. 1966. *Strategic Intelligence for American World Policy*, (3rd edition). Princeton: Princeton University Press,

Lowenthal, M M. 2003. *Intelligence: From Secrets to Policy*, (2nd edition). Washington (DC): CQ Press.

Nolan, J A. 1997. "Confusing Counterintelligence with Security Can Wreck Your Afternoon". *Competitive Intelligence Review*, Vol 8, No 3.

O'Connell, 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/oconnell.pdf. Accessed 4 March 2008.

Miler, N S. 1980. "What is Counterintelligence — Discussants", in Godson, R (ed). *Intelligence Requirements for the 1980s: Counterintelligence*, Vol 3. Washington (DC): National Strategic Information Center Incorporated.

Muller, M. 2002. *Creating Intelligence — Competitive Intelligence Series*, Vol 4. Randburg: Knowledge Resources (Pty) Ltd.

Muller, M, and C Whitehead. 2002. *What is Competitive Intelligence? — Competitive Intelligence Series*, Vol 1. Randburg: Knowledge Resources (Pty) Ltd.

Quiggin, T. 2007. *Seeing the Invisible — National Security in an Uncertain Age*. London: World Scientific Publishers.

Scott, L V. and P Jackson. 2004. "Journeys in Shadows", in Scott, L V and P Jackson (eds). *Understanding Intelligence in the Twenty First Century — Journeys in the Shadows*. London: Routledge.

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.

Treverton, G F. 2001. *Reshaping National Intelligence in an Age of Information. Cambridge:* Cambridge University Press as cited by Duvenage, M A. 2010. *Analysis in the Knowledge Age — An Analysis of the Challenges Facing the Practice of Intelligence Analysis*, unpublished MPhil dissertation. Stellenbosch: University of Stellenbosch.

United States of America. 2005. *Report to the President of the United States on the Intelligence Capabilities of the United States regarding Weapons of Mass Destruction*. Washington (DC): Commission on the Intelligence Capabilities of the United States regarding Weapons of Mass Destruction.

United States of America. 1996. *Operations Security Intelligence Threat Handbook*. Interagency Operational Security Support Staff. Available at: http:www.fas.org/*irp/nsa/ioss/threat96/part03.htm*. *Accessed 11 August 2007.*

United States of America. 1974. *Dictionary of Military and Associated Terms*. Washington (DC): Department of Defense as cited by Zuehlke, A A. 1980. "What is Counterintelligence?", in Godson, R (ed). *Intelligence Requirements for the 1980s: Counterintelligence*, Vol 3. Washington (DC): National Strategic Information Center Incorporated.

Watts, W L. 2005. *Intelligence Reform in Europe's Emerging Democracies — Conflicting Paradigms, Dissimilar Contexts.* Available at: http:// www.cia.com/csi/intelligence 20%in20Europe. Accessed 12 April 2008.

Wettering, F L. 2000. "Counterintelligence: The Broken Triad". *International Journal of Intelligence and Counterintelligence*, Vol 13, No 3.

Zuehlke, A A. 1980. "What is Counterintelligence?", in Godson, R (ed). *Intelligence Requirements for the 1980s: Counterintelligence*, Vol 3. Washington (DC): National Strategic Information Center Incorporated.