Business Counterintelligence:
sustainable Practice or Passing Fad?

Christopher James Shear

Thesis presented in fulfilment of the requirements for the degree
Master of Arts
(Socio-Informatics)

STELLENBOSCH UNIVERSITY

Supervisor: Dr MS van der Walt

March 2009

Declaration

By submitting this thesis electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the owner of the copyright thereof (unless to the extent explicitly or otherwise stated) and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

Date: 23 February 2009

Summary

Traditional information protection mechanisms are no longer adequately placed to effectively deal with the adversarial threats that have arisen as a result of the rise in importance of knowledge for today's organisations. Business counterintelligence appears to be a protective entity, which in principle can effectively engage with and mitigate many of these newly manifested threats. Yet, business counterintelligence is also an entity that is accompanied by a great deal of haze and confusion as to its use, implementation and integration within different organisations. This is evident from the literature where there currently exist multiple fragmented definitions of what business counterintelligence is. Organisations may as a result adopt a particular business counterintelligence definition that may not be effective for their context. This can result in the ineffective protection of critical information assets and the misappropriation of organisational resources; something which is not sustainable.

This thesis proposes that in order to allay the confusion caused by these differing fragmented definitions, one needs to be able to arrive at a consolidated definition of what constitutes business counterintelligence; this thesis's primary objective. This has been examined by firstly contextualising business counterintelligence in order to better understand the topic; the information society was used as a backdrop for this purpose. Secondly, an examination of the prevailing views of business counterintelligence and its role within organisations is offered in order to build clarity. Thirdly, a consolidated definition of business counterintelligence is proposed and its implications for different organisations examined. Finally, the implications of this consolidated definition for the sustainability of business counterintelligence are discussed and conclusions based on the evidence presented within the thesis drawn. Based on the arguments presented, this thesis postulates that a consolidated definition of business counterintelligence is more effective and is thus more sustainable.

Opsomming

Tradisionele inligtingvrywaringsmechanismes is nie langer voldoende geplaas vir die effektiewe handeling van teenstaande dreigings, wat ontstaan het as gevolg van die toename in gewig van kennis aangaande hedendaagse organisasies nie. Besigheidsteeninligting blyk 'n beskermende entiteit te wees wat in beginsel effektief kan verbind met vele van hierdie nuutgeopenbare dreigings. Tog is besigheidsteeninligting ook 'n entitiet wat gepaartgaan met 'n groot hoeveelheid wasigheid en verwarring aangaande die gebruike, implimentasie en integrasie daarvan benni-in verskillende organisasies. Dit is duidelik uit die literatuur waar daar huidiglik veelvoudige fragmentele definisies bestaan van wat besigheidsteeninligting is. Organisasies mag as 'n gevolg 'n sekere besigheidsteeninligting definisie aanneem wat nie effektief vir die konteks daarvan mag wees nie. Dit kan voortspruit in 'n oneffektiewe beskerming van kritiese inligting bates en die verkeerde aanwending van instellingsbronne; iets wat nie volhoubaar is nie.

Hierdie tesis stel voor dat ten einde die verwarring veroorsaak deur hierdie verskillende fragmentele definisies te verlig, 'n mens in staat moet wees om tot 'n gekonsolideerde definisie te kom van wat besigheidsteeninligting is; die primere doelstelling van hierdie tesis. Dit is ondersoek deur eerstens besigheidsteeninligting te kontekstualiseer ten einde die onderwerp beter te begryp, die inligtingsamelweing is gebruik as 'n agtergrond vir hierdie doel. Tweedens, is 'n ondersoek van die heersende sienings van besigheidsteeninligting en sy rol binne organisasies aangebied om duidelikheid te skep. Derdens, is 'n gekonsolideerde definisie van besigheidsteeninligting voorgestel en die implikasies vir verskillende organisasies ondersoek. Laastens word die implikasies van hierdie gekonsolideerde definisie vir die volhouding van besigheidsteeninligting bespreek en gevolgtekkings opgeteken gegrond op die bewyse aangebied in die tesis. Gegrond op die argumente aangebied dui hierdie tesis aan dat 'n gekonsolideerde definisie van besigheidsteeninligting meer effektief is en dus meer volhoubaar.

Dedication

I would like to dedicate this work to my mother Maureen Johanna Hofmeyr Shear for all she has done for me over the years, by providing an enriching environment that has enabled me to achieve my dreams through very challenging circumstances.

Acknowledgements

I would like to extend a heartfelt thanks to all those in the department of Information Science that have contributed in their various ways to the completion of this thesis by providing me with the academic ground work, support and direction to undertake such an investigation. Special thanks are due to Professor Johann Kinghorn (Department Chair), for the help that he has provided to me through some challenging times and who was essential in offering me the motivational support to undertake this topic through the early manifestation of its structural formulation. I also would like to thank my thesis supervisor Dr Martin Van der Walt for his critical analysis, expert guidance and feedback throughout the research process without which I would not have been able to complete this study. Thanks are also due to Dr Hans Müller for his guidance relating to those specialised areas of this investigation beyond my level of expertise and Mr Christiaan Maasdorp for fielding some essential queries relating to critical research material. I would also like to kindly thank those who have taken the time to examine this thesis and have provided critical feedback along the way.

A further special mention of thanks must be extended to Mr Steve Whitehead (Managing Executive – CBIA) for kindly providing me with essential research material and for his correspondence during the initial stages of this study in order to help orientate my research direction. I would also like to thank Dr Grace Monis (Boston University and Washington University) for her inspiration as a friend, many long discussions over the phone and advice concerning the less academic formalities of the research process. A mention of thanks must also be extended to Professor Hans Akkermans (Amsterdam University) for his initial guidance relating to the acquisition of information from alternative sources and Mr Rowan Dorin (Harvard University and Cambridge University) for his help in tracking down some very elusive articles and serving as a companion during many a late night of thesis writing while working on his own dissertation.

Finally, I would like to extend a special mention of thanks to those family and friends who have offered their support by lending an interested ear as to the proceedings of my research, particularly: Air Vice-Martial William Rae (CB RAF, retired), Mr Peter Burkhalter

(Switzerland), Mr Åke Ahrsjo (Sweden), Mr Ian Taylor (South Africa and Spain), Professor Tom De Jonge (Netherlands), Mrs Rosemary Hofmeyr Giralt, Mr Maurice Gerald Hofmeyr (deceased February 2008, who's intellectual brilliance has served as a beacon of inspiration), Ms Madeline Groenewald (University of Cape Town, for making me take the time to look at the stars once in a while), Mr Neil Smit (University of Cape Town), Mr Sipho Lafleni (Durban University of Technology) and last but not least my father Mr William Hardwick Shear for his critical advice, love and support.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Introduction

The value of today's organisations is no longer merely defined by the comparative collection of physical assets which they posses, but rather in addition, by their use and retention of multitudinous knowledge in order to generate sustainable competitive advantage[1]. Knowledge and information capitalism[2] – through the need for intellectual capital retention and growth – have thus redefined the context in which today's companies operate[3], moving them into new dimensions of substantiated complexity; often breaking with the traditional conceptualised forms of how trade and industry should operate.

> The growing intensity and dynamism of competition across product markets has had profound implications for the evolution of strategic management thought during the 1980s and 1990s. Increasing turbulence of the external business environment has focused attention upon *resources* and organisational *capabilities* as the principal source of sustainable competitive advantage and the foundation for strategy formulation. As the markets for recourses have become subject to the same dynamically-competitive conditions that have afflicted product markets, so *knowledge* has emerged as the most strategically-significant resource of the firm[4].

Given this associated shift in economic conception, increased global reach and a reduction in the conceptualisation of traditional organisational boundaries[5], the need to effectively protect one's knowledge assets from theft and the prying eyes of one's adversaries has thus become

---

1 Arenas, T. 2008. *Intellectual Capital: object or process* p 77-85. As Clarke, T. & Clegg, S. 2000. *Changing Paradigms: The Transformation of Management Knowledge for the 21st Century* p 340, state: "A knowledge company is different in many ways...not only are the assets of a knowledge company intangible, it's not clear who owns them or who is responsible for them."

2 Castells, M. 1996. *The Rise of the Network Society: The Information Age* p 18.

3 Melody, H. 1991. *Manufacturing in the Global Information Economy* p 2. As cited in Webster, F. (2006) in his book *Theories of the Information Society (3rd Edition)* during his elaboration on the post-industrial society and its many meanings p 53, states: "Information...is fundamental to almost all productive activity, in a modern economy. The changing role of information lies behind the restructuring of all industries and the creating of the global information economy."

4 Zack, M. 1999. *Knowledge and Strategy* p 134.

5 Child, J. & McGrath, G. 2001. *Organizations Unfettered: Organizational Form in an Information-Intensive Economy* p 1137.

of critical importance[6]. However, many of today's organisation's often find themselves on an unstable security footing – concerning the protection of their intellectual capital – with clarity, distinctiveness of threats, structure, organisational boundaries, roles and responsibilities not always being well defined.

Business counterintelligence appears to be dynamic protective entity, which in principle, can effectively engage with and mitigate many of these concerns. Yet it is also an entity that is accompanied by a great deal of haze and confusion as to its use and implementation; associated with varying degrees of understanding; expressed through the myriad of definitions that can be found concerning the topic within the literature. This disjunction therefore opens the way for one to critically analyse the role played by business counterintelligence – as a protective entity within contexts of variability – leading one to question the sustainability of business counterintelligence, its adaptability within environments of change and what it ultimately means in terms of the development of a coherently integrated business counterintelligence definition.

1.2 The Problem Context

Within the field of business counterintelligence there seems to be no standardised praxes of implementation or operation; particularly concerning its integration with differing organisational protection frameworks[7]. As Criscuoli[8] outlines, the origins of acquisition and protection measures – in the form of intelligence and counterintelligence – were until a few decades ago largely situated within the context of government, with only limited skill sets being applied and needed within the framework of business[9]. A difficult task when faced with the rapid pace of change of the knowledge context.

From this point of view, counterintelligence practices seem to have transitioned the gap between organisations' and the formalised environments of government/military intelligence and counter-espionage the world over[10]. In many instances protection professionals also seem

---

6 As Hansche, S., Berit, J & Hare, C. 2004. *Official Guide to the CISSP Exam.* p xi, state: "As the networked world continues to shape and impact every aspect of life; threats to the global network infrastructure have continued to rise in parallel."

7 Within the field of business counterintelligence there is currently a large amount of dissimilitude presented in those literary works relating to the topic, what it means and how it should be integrated and applied within a particular business or organisational context; ultimately leading towards the creation of a non standardised context of understanding.

8 Criscuoli, E. 1988. *The Time Has Come to Acknowledge Security as a Profession.* p 100.

9 Criscuoli, E. 1988. *The Time Has Come to Acknowledge Security as a Profession.* p 102.

10 Schweizer, P. 1996. *The Growth of Economic Espionage.* p 9.

to have selected elements from these formalised intelligence practices and implemented them within their particular business framework; in the hope that they will be beneficial in terms of protecting their knowledge assets[11] - often motivated by examples such as the following:

> A 1993 study by R. J. Heffeman and Associates noted that an average of about three incidents every month involve the theft of proprietary information from American companies by foreign entities. These estimates are probably conservative[12].
>
> According to the American Society for Industrial Security, economic and industrial espionage cost US businesses an estimated $59 billion in 2005[13].
>
> Indications are that economic espionage, including trade secret threats and competitive business information/intelligence gathering, will intensify and be more aggressively pursued in the new millennium[14].

Due to this largely informal process of development, within the many areas that make up the current information protection field, there exists a large amount of disparity, confusion and misunderstanding when differing solutions are put into contention with one another. This lack of clarity, in combination with a radical shift in global economic interactions and organisational boundaries, has resulted in multiple perspectives being developed, many of which have drawn on elements from interrelated disciplines. The consequence of this is that business counterintelligence measures have become blurred in relation to their original intent.

Today's organisations' rely on global strategies for success, often having to accept projects with low return on investments but that will offer them longer term competitive payoff[15]. The same could perhaps be said of the organisational interest and adoption of certain business counterintelligence practices, particularly given the hazy environment of competition and operation that often accompanies business activity, within the capitalist driven knowledge economy. Organisation's may as part of their intellectual capital retention strategy, seek to adopt business counterintelligence measures – even if not well defined – in the hope that such measures will offer them some level of abeyant security payoff over the longer term.

---

11 Whitehead, S. 2007. *E-mail to the author with reference to opinions concerning counterintelligence.*

12 Schweizer, P. 1996. *The Growth of Economic Espionage.* p 11.

13 Kitfield, J. 2007.*Espionage the Sequel* [Online]. These statistics presented for 2005; the last year of record keeping for such statistical information regarding espionage activity within business.

14 Kalitka, P. 2000. As cited in Whitehead, S. 2001. *The Counterintelligence Page: Part 1* p 32.

15 Hout, T., Porter, M. & Rudden, E. 1982. *How Global Companies Win Out* p 98.

In addition, organisations operating in the highly competitive globalised economy are by their nature entities that are constantly looking for innovative processes, practices, procedures and methodologies in order to render sustainable competitive advantage[16]; allowing them to outperform their competitors. Organisations are also by their nature entities that will latch onto new ideas and approaches – fads and fashions[17] – if they think that these will help them outperform their competitors.

Subsequently, the development and implementation of an effective business counterintelligence strategy or function within one's organisation can metamorphose into a vastly complex process. Synergistic cooperation both internally and externally between organisation's sharing a common concernment, in the form of a better understanding of the broader protection picture and the proximate application of relevant resources, may therefore lack effective application. The resulting consequence of this inability to act effectively can lead to the inefficient use of one's resources, the implementation of unnecessary protection measures, lagging response times when protection requirements are needed most and broader organisational monetary losses; in contrast to what one would consider to be the objectives of a well defined protection function.

As stated by Prescott, security functions like business counterintelligence should be value adding in their dispensation towards an organisation[18]. If there is confusion relating to protection roles, the amount of added value that could be gained by such activities may be reduced. Thus the need for the development of greater clarity, the creation of increased awareness and understanding regarding business counterintelligence perspectives becomes of vital importance.

1.2.1 Approach to the Problem Context

In order to effectively engage with the challenges of the problem context as outlined above, one will thus need to provide a more comprehensive understanding of what business counterintelligence is – by clearing away the haze that surrounds it – therefore providing a theoretical point of departure for those wishing to investigate it further with the possibility of

---

16 These conceptual ideas were presented in *The Competitive Advantage of Nations* by Michael Porter, where he attempts to define the routes of competitive advantage that particular business entities within those nations have extrapolated to their maximum degree, in order to reach the highest levels of competitive advantage within their particular area of focus.

17 Gibson, J. & Tesone, D. 2001. *Management Fads: Emergence, Evolution, and Implications for Managers* p 122-124.

18 Prescott, J. & Miller, S. 2001. *Proven Strategies in Competitive Intelligence* p 5.

implementing such a function, in a clearly defined manner, within their particular organisational context. If one does not have a clear level of understanding of what business counterintelligence is or how it may be structured on a theoretical level of defined integration, then its translation into practice through implementation, may be greatly compromised. This is implied by the many divergent definitions and processes relating to business counterintelligence presented within the literary sources covering the topic.

My objective is to therefore arrive at a consolidated perspective of business counterintelligence and to provide suggestions about implementing it from a consolidated theoretical perspective. It is hoped that such an understanding will be more beneficial from a management point of view as one will then be able to have a firmer grasp of what business counterintelligence is, the relevance that it holds for one's organisation and the steps that need to be taken in order to implement it in an effective manner. One will then be better placed to infer whether or not business counterintelligence has the propensity for long term sustainability or whether it is something that will be a short term management fad. This will be based on the level of meaning that a consolidated definition of business counterintelligence can convey for one's organisation in a theoretical sense.

1.3 Research Questions

In order to deal with the challenge of confusion – and therefore a lack of clearly conceived understanding as relating to the topic of business counterintelligence – the research approach will follow a logical sequence of analysis based on broader themed areas of investigation. This will be done under the assumption, that in order to truly understand business counterintelligence, one therefore needs to be able to identify what constitutes *effective* business counterintelligence – in this instance *effective* meaning *sustainable* – actualised by the value and meaning that it conveys for one's organisation. The overall intention of the research may subsequently be expressed through the following primary research objective:

> *To arrive at a consolidated definition of what constitutes business counterintelligence?*

The questions have been developed with the primary objective in mind:

Context Primary and Sub-Questions

> *Q1: How can one best contextualise business counterintelligence and understand its importance for today's organisations?*

Q1.1: Why was business counterintelligence not considered an issue for organisations some two to three decades ago?

Q1.2: What in the context of the business environment has changed and now made it an issue for organisations?

Q1.3: Why is business counterintelligence now an issue for organisations of today?

Main Body Primary and Sub-Questions

Q2: What are the prevailing views of business counterintelligence and its role within organisations?

Q2.1: From what perspectives is business counterintelligence defined and regarded?

Q2.2: What are the different definitions and approaches to business counterintelligence?

Q2.3: What are the differences between these definitions and what is in common?

Q3: What would constitute a consolidated definition of business counterintelligence?

Q4: What are the implications of this consolidated definition of business counterintelligence for different organisations?

Conclusion Primary Question

Q5: What are the implications of this consolidated definition for the sustainability of business counterintelligence?

1.4 Study Flow

I will now briefly discuss the core study flow of the thesis which has lead to the manifestation of the research questions that will be used to meet the broader objectives of this investigation. Taking such an approach will allow one to keep a close wrap on the topic under investigation, while still allowing for some degree of flexibility; within those broader sectional contexts explained in more detail to follow. This will allow one the ability to better contextualise the research questions from within the greater structural framework of the analysis as presented below. The derived thesis framework will then be fleshed out through deeper engagement

with each of the research objectives; in terms of their sectional value in the chapters to follow.

1.4.1 Section 1 – Context

As a point of departure one needs to place particular emphasis on the origins of business counterintelligence, especially given that business counterintelligence and its lexicon are not easily definable entities. As business counterintelligence is not an easily definable entity, one must assume therefore that one needs to view it within a broader context of development, in this instance the information society/economy; as due to its hazy fragmented nature one cannot understand the topic in and of itself. This is predominantly a methodological consideration, an assumption that one has to contextualise business counterintelligence and its transition into the economic context as something that came about due to the rise in importance of information. This is in combination with a number of other relevant elements of *transition* which have lead to business counterintelligence becoming of importance for today's organisations; as opposed to some two to three decades ago as will be discussed in chapter 3. Contextualising business counterintelligence begins with an analysis of the information society which is used as the basis for this discussion; which is itself a disparate topic. The economic perspective of the information society is presented amongst other definitions of the information society.

This was felt to be of relevance, as due to the transition or rise in importance of information/knowledge from an industrial based era of operation, this shift and its resulting impacts have contributed to the redefinition of traditional forms of intelligence gathering. This has resulted in a shift in focus away from purely military/government based targets to economic ones. Thus counterintelligence in today's context has become concerned with the protection of economic entities in the form of critical business information as well as traditional military/government based sources of information. It is therefore no longer situated in the same context as it once was some two to three decades ago. The objective of this part of the investigation will be to act as a foundational basis of analysis for the commencement of a more in-depth analysis of the key topical points.

Hence, before one can deal with the more challenging topical areas under investigation, concerning the primary research objective, one firstly needs to have an understanding of how business counterintelligence developed as an entity, through its origins, transition and subsequent adoption into the realm of business. This can be best thought of in terms of its

historical context of origination, manifested through the primary objective of clarity and understanding.

1.4.2 Section 2 – Main Body Argument

With this historical contextualisation as a base, one can then begin to flesh out the core framework by shifting focus on to what constitutes *effective* or *sustainable* business counterintelligence activity. From the point of view of this thesis, it is important that sustainability should be seen as the highest form of actualisation for the organisation when dealing with the protection of intellectual assets, and the socio-technical implications of competitive advantage[19]. Business counterintelligence does not only need to be understood from a contextual point of view, it also has to carry meaning for the organisation.

Consequently, one needs to have a way of identifying what sustainable business counterintelligence practices are from an organisational perspective, the first step of which will be the development and analysis of an integrative coherent definition of business counterintelligence from amongst the many disparate literary sources on the topic. This will be done as a precursor to the discussion of information security *vis-à-vis* business counterintelligence, with the ultimate aim of contributing to clarity. This will then lead to the manifestation of a consolidated process driven approach to business counterintelligence, derived from key sources from amongst the literary haze.

It is important to remember however that in order to do so in an effective manner one has to be aware that there are many challenges to take into account. One such factor that must be considered is that of the innate variation that exists between organisations as they seek out ways to deal with the turbulent environment of large scale information based competition. This variation represented in the way they are structured, in the way they operate and in the way in which they are viewed both internally and externally.

> Much has been written about the breathtaking changes that are redefining the environment which are forcing companies in almost every sector to re-examine their organisational designs. Both profit-seeking and not-for-profit organisations are reeling from discontinuities created by an interdependent global economy, heightened volatility, hyper competition, demographic changes, knowledge based

[19] Samiotis, K., Poulymenakou, A. & Doukidis, G. 2002. *Organisational Reflections on the Introduction of Knowledge Management Systems: Evidence from Supporting (E-) Banking Activities* p 1.

> competition and demassificaiton of some sectors accompanied by enormous growth in others[20].

In order to progress in a structured manner, one firstly needs to deal with such challenges by attempting classification, through understanding how business counterintelligence can best be applied to different types of organisations according to their relevant level of security required. It is postulated in this case that such categorisations will be made clear through the level of applicable protection filters needed, as the level of protection required for different organisations will vary.

Once this has been established, one will then be able to commence with the consolidation of business counterintelligence types. This will allow one to formulate a generic structure of *process driven implementation* in accordance with relevant organisational variation, defined and constructed from amongst the literary haze. One can then begin to identify what *sustainable* business counterintelligence is – from the perspective of a generic process driven form – based on the differing contextual situations of dissension, in which many security professionals often find themselves; thus contributing to a better integrated understanding of the topic at hand.

1.4.3 Section: 3 – Discussion and Conclusion

In this final section conclusions reached will be discussed. These will then be tied up with the issue of the *sustainability* of business counterintelligence as opposed to fad, based on whether business counterintelligence is something to be taken seriously or not, dependent upon the level of sustainable meaning that it conveys. This will take into account the meaning derived from the integrated process driven approach and the coherently expressed business counterintelligence definition and its analysis. By engaging with these areas of concern in an orderly manner, one will hopefully be able to deal with the confusion that surrounds business counterintelligence, in its current state, in a far more structured and thorough form, thereby leading to the manifestation of increased understanding through derived effectiveness.

1.5 Research Methodology and Design

The topic being researched is one that is conceptual in nature and is thus suited to the realm of qualitative investigation, in this instance lending itself in favour of a literature study rather than a quantitative form of analysis which is less appropriate for the purposes of this

[20] Daft; R. & Lewin, A. 1993. *Where Are the Theories for the "New" Organizational Forms? An Editorial Essay* p i.

investigation. The use of a literature based study for this purpose will allow one to interpret and classify those differing perspectives on the matter in a tangible sense of generic form. This will allow one to more accurately define what needs to be protected, and also how business counterintelligence can be applied in contexts of disparity in order to achieve this in an effective manner.

The use of a literature study will also allow for better investigation and amalgamation of those various broader themed areas of discussion concerning the field of business counterintelligence. This is important, as in the context of those various organisations that make use of business counterintelligence activity – particularly the larger ones – it is not a feasible undertaking to transform the way they handle their business counterintelligence activities. Simply to test whether these findings have substance; given the time and resources at one's disposal. Therefore, it becomes a much better proposition to be able to supply contextual information concerning the topic, clearing away some of the haze and thus allowing organisations to gain a better perspective of business counterintelligence against the broader state of their operations. This will hopefully have the added benefit of allowing them to compare their practices and understandings of the topic, in a quest to develop a level of greater sustainability in their undertaking of business counterintelligence activity; a goal of this research.

In order to achieve these objectives, the research undertaken will be constructed around a variable approach of analysis relating to business counterintelligence. This is important as the problem context is one which lacks clarity and is thus made up of various differing points of view often relating to similar issues when dealing with business counterintelligence, its roles, how it should be handled and ultimately defined. This is however not without its challenges.

Writing from within the South African university system, perhaps due to the level and nature of our universities and their organisational research focus, there was a lack of essential resource material concerning the topic of business counterintelligence in general. There are security and counterintelligence journals available globally, but within the South African university library system itself, the availability of such resources was very much limited. One therefore had to be persistent in the search for information on the topic, using a degree of ingenuity to obtain material while still ensuring that the level of material obtained was of a high quality. This was achieved in part through the use of online libraries and open sources of information offering high quality literary content.

Other avenues of information gathering included contacting universities in other parts of the world where written material on the topic was more abundant in the form of journal articles relating to business counterintelligence activity. Regions where assistance was gained included the United Kingdom, the Netherlands and the United States of America. A more local approach was also included where information was requested from contacts that had security or counterintelligence journal subscriptions or whom were part of international bodies on or related to the topic that provided assistance. It was hoped that by pursuing research information in this way, would lead to the fulfilment of the requirements of this research study, as well as develop a good broader level understanding of business counterintelligence activity from amongst the literary haze.

1.6 The Importance of the Study

The importance of this study lies in its ability to consolidate a vast number of the differing approaches taken when dealing with business counterintelligence strategies; which if taken on their own, may lead to confusion and the implementation of ill defined counterintelligence strategies. The consolidation of approaches will allow for suggestions about sustainable business counterintelligence implementation requirements for variable organisational types, thus offering a view on what will constitute sustainable business counterintelligence practice measures – within divergent business settings – from a generically based process driven approach; with factors needed dependent on size and structure.

The aim of this chapter was to act as an introductory knowledge source, allowing for more insight to be gained into the topical area at hand while acting as a viable structural framework for further examination of the related issues to follow. The chapters to supervene will deal with the primary research objective and its subsequent questions. Thus, I will commence with a discussion of relevant factors which have contributed to the creation of the current context, from the perspective of this thesis being the rise in importance of information, expressed through a discussion on the information society and economy. This will be done in order to construct the foundation needed in order to contextualise business counterintelligence and as a necessary precursor for the examination of business counterintelligence's rise in importance for today's organisations discussed in chapter 3.

Chapter 2 – Section 1

Contextualising Business Counterintelligence

2.1 Introduction

This chapter will begin with a brief overview of the use of the term business counterintelligence as opposed to the term corporate counterintelligence. I will then discuss the concept of the information society and its perspectives for the purpose of contextualising business counterintelligence. I will then highlight its relevant theories, including the economic perspective, as it is itself a fragmented topic. This is important as disparate aspects tend to be dependent upon one another in a collective sense. If one wishes to contextualise business counterintelligence in the best manner possible, one cannot place a particular definition of the information society effectively without understanding it in relation to other information society perspectives. By discussing theories of the information society, it will provide a framework for contextualising business counterintelligence and understanding the fundamental changes that have taken place as business counterintelligence has risen in importance for today's organisations. This will be discussed in chapter 3.

2.1.1 Corporate Counterintelligence vis-à-vis Business Counterintelligence

Before I continue further with my analysis, I would firstly like to clarify the use of the term *business counterintelligence* within the context of this inquest *vis-à-vis* the use of the popular term *corporate counterintelligence*. The reason for this is that I feel that the use of the prefixed word *corporate* is somewhat erroneous in its connotative meaning when dealing with counterintelligence. In order to better understand my reasons for the use of the term *business counterintelligence,* one firstly needs to have a firm grasp of what the term *corporate counterintelligence* means; in the light of its component word entity *corporate.*

The word *corporate* can in this instance be defined as "shared by members in a group or united in a group[21]". This denotes the meaning – for a business context in this case, as the term may also be applied to a government situation – of *corporation* which can be thought of as "a business organisation owned by a group of stockholders, each of whom enjoys limited liability[22]". By viewing the term and subsequent functions of the term *corporate counterintelligence* from this perspective, it therefore eludes to a specific type of organisational context, if its related meaning *corporation* is also taken into account. It therefore excludes those various other types and levels of business structures who may operate under different legal prerogatives. This makes the term *corporate counterintelligence* sound as though it only applies to a particular organisationally structured business entity; when in fact it should in my opinion be far more inclusive in its application.

A further connotative point that should be taken into account, when engaging with the term *corporate counterintelligence,* is that of a lack of implied interaction and reliance on other intelligence processes for success. Counterintelligence, within the context of business, should be seen as an element which is reliant upon and forms part of a broader intelligence initiative, whose aims not only include the protection of intelligence but also the acquisition and understanding of competitive intelligence.

> Counterintelligence is highly dependent upon a comprehensive understanding of your rival's capabilities and intentions, which requires you to have a sound business intelligence (BI) process in place. Our consulting experience has taught us that an accurate assessment of corporate attitudes towards business intelligence helps us anticipate the odds of developing a good counterintelligence program[23].

From a semantic point of view, the term *business counterintelligence* denotes a far more inclusive meaning. *Business* in this instance can be defined as "a person, partnership, or corporation engaged in commerce, manufacturing, or a service; profit-seeking enterprise or concern[24]" therefore including more levels of business in terms of the structure and legal manifesto that it implies. The use of the term *business* also better incorporates the denoted idea of the relationship between business counterintelligence and business intelligence within organisations.

---

21 Oxford University. 1994. *The Oxford English Mini Dictionary* p 109.

22 Houghton Mifflin Company. 2005. *The American Heritage New Dictionary of Cultural Literacy* [Online].

23 DeGenaro, B. 2005. *A Case for Business Counterintelligence* p 12.

24 Dictionary.com 2008. *Dictionary.com Unabridged (v1.1)* [Online].

Although semantic meaning may not be seen as the most critical element to take into consideration, for the most part it plays a vital role in demystifying the concept to some degree and perhaps also allows it to be more accurate in terms of its connotative meaning and use. This should allow for an increased level of awareness concerning business counterintelligences application, interaction and use.

2.2 Information Society as a backdrop to Business Counterintelligence

As a central theme to this argument, the information society will now be discussed as a contextual backdrop to the rise in importance of business counterintelligence activity. This will be build upon in the chapter to follow, where I will argue that the business context and environment of the last three decades has changed greatly. This is in addition to the information context alone, thus leading to an increased need for more effective information gathering, protection and retention; in order to remain economically competitive within this environment. I will therefore begin my analysis with a brief outline of the information society and highlight the most important theoretical aspects and discussions that accompany it.

2.2.1 Perspectives of the Information Society

It is important to note that although the term information/knowledge society is often taken for granted as a real concept – I say term as both the words *information* or *knowledge* in this context, may be used in an interchangeable manner[25] – opinion on the factual existence of an information society is somewhat varied and divided. This conceived of as something radically new or as an everlasting form of continuum.

> On the one hand, there are those who subscribe to the notion that in recent times we have seen emerge information societies which are marked by their differences from hitherto existing societies. Not all of these are altogether happy with the term 'information society', but in so far as they argue that the present era is special and different, making a turning point in social development, I think they can be described as its endorsers. On the other hand, there are scholars who, while happy to concede that information has taken on a special significance in the modern era, insist that the central feature of the present is its continuities with the past[26].

[25] De Beer, J. 2005. *Open Access scholarly communication in South Africa: current status, significance, and the role for National Information Policy in the National System of Innovation* p 15.

[26] Webster, F. 2006. *Theories of the Information Society* p 6.

No matter what the outcomes of such division may be however, it is generally accepted across all understandings that "information has achieved a special pertinence in the contemporary world. The writing available may be characteristically disputatious and marked by radically different premises and conclusions, but about the special salience of information there is no discord[27]". I will therefore accordingly assume that the resulting ramifications of the information society, these being viewed as the dynamic role and prominence of knowledge or information, are bona fide in terms of their impact on today's societal contexts. I will also assume that the concept of the information society, in light of both the macro and micro business environment, is correct in so much as today's business world is dominated by a need for the effective handling of knowledge within these contexts[28]. This viewed primarily from an intelligence based perspective.

The intricacies surrounding the debate over the existence of new or continuous forms of society are outside the scope of this thesis. What is needed however is the construction of a general level of understanding associated with the development of those varying points of view and by what key factors these points of view may be measured. This can be achieved by delving into those key advancing steps; emphasising relative points of progression which outlines shifting foci, in terms of defined perspectives, and those elements which they express.

One may engage with these varyingly defined points of view by examining them as entities reliant on the understanding of technological, economic, occupational, spatial and cultural[29] definitions. These when combined can be used as an indicative form of analysis when defining the informational forces from a thematic outlook on business. This is achieved through the combination and refining of existing perspectives into a new form of self imposed understanding. What is useful about this approach is that it allows one to formally

---

27 Webster, F. 2006. *Theories of the Information Society* p 2.

28 Choo, C. & Bontis, N. 2002. *The Strategic Management of Intellectual Capital and Organizational Knowledge* p 606. The point of the effective handling of knowledge as a process or form of strategy is a main theme of this work. The fact that Choo & Bontis highlight the importance of such processes, gives further support to this idea. Of specific interest with regards to the point highlighted above is Choo's Integrated View of Firm Knowledge whereby he highlights the determinants of firm knowledge in light of inter-firm knowledge across boundaries; thus emphasising the importance of both the internal aspect of knowledge handling as well as the implications for the greater business environment at large.

29 Webster, F. 2006. *Theories of the Information Society* p 8-28. It is these factual elements that come to mind when I use the term transition or change, when discussing the information society, not Bells perceived "shift from a manufacturing to service society" as indicated by Webster p 62.

categorise differing points of view – when dealing with associated authors[30] – into particular contexts of thought. This helps to enlightening ones' understanding of the topic at hand while allowing one to identify those areas of focus with regards to informational metastasis and integration.

2.2.2 Further Associated Points of Change

Although I highlight those dominantly defined contexts of the information society and make reference to subsequent factorial interpretations as the basis for my framework, it is important to note that other authors have put forward their own differing ideas. These ideas while sharing many similarities with the key definitions as expressed, exist outside the scope of the contexts put forward above. This is in part due to the fait accompli that theories of the information society are diverse in their expressions, therefore, so too are the interpretations that have been put forward of those relevant transitions which have taken place over the past decades. This based on relevant factors of identification.

For example Tuomi[31] states that there are three identifiable waves of the knowledge or information society; with the first and second waves being predominantly infrastructure centric. The first wave is characterised by claims of an information communications technology (ICT) revolution, which occurred during the period 1970 – 1990, with an emphasis on network infrastructure and deregulation. The second wave, which had its origins in the United States, honed in on aspects such as "...competitiveness, economic growth, access, regulation, privacy, security and intellectual property rights". The third wave from this point of view is characterised by the supplemental development of technological and social policies, which together have complementary objectives. One should take note that no clearly identifiable reasons are given as the precursor to the development of these events, particularly from a non-technologically based perspective. This point of view however remains relevant none the less as it differs somewhat from the classical technologically based definition in its approach and understanding; as it does not view technology as the sole influencing and modifying factor of society alone but rather as a dominant complementary entity.

---

[30] Webster mentions a number of varied authors throughout his work, when dealing with different theories of the information society, such as: Daniel Bell; Alain Lipietz; Michel Aglietta; Robert Boyer; Manuel Castells; Herbert Schiller; Anthony Giddens; Jürgen Habermas; Friedrich Nietzsche and others. All of whom fit within differentiating defined categories of analysis, as defined by Webster.

[31] Tuomi, I. 2001. *From periphery to center: emerging research topics on knowledge society* p 8. As cited in De Beer, J. 2005. *Open Access scholarly communication in South Africa: current status, significance, and the role for National Information Policy in the National System of Innovation* p 17.

Masuda highlights the importance of what he calls *the system of societal technology*[32], whereby he views societal transitions in human history as coming about due to axial technological and economic forces. These axial technological forces can be seen as: transformations in innovative technology leading to more complex technological systems; the integration of this technology into societal contexts; the rapid expansion of this new type of technology into productivity and the impact of this new productivity leading to new types of societal forms. This understanding to, although also following certain aspects of classical information society technological/economic reasoning, differs in its interpretation as it views technological advancement as influencing productivity factors which in turn lead to adaption's in the societal sphere. Rather than having a direct interacting influence on society, technology is seen as an element which is mediated through other productivity factors.

In today's context, the impact of this from a sociological perspective can be felt in terms of what Masuda calls *the replacement of man's mental labour* and *the amplification of mans intellectual labour*[33] leading to new forms of socio-economic systems[34], globalisation, a new information based economic system[35] and finally the restructuring of society itself. Many similar ideas are expressed in other works – such as *The New Knowledge Economy of Taiwan* by Chen and Lee – whereby they discuss the importance of ICTs, the impact of globalisation, knowledge economics, global production systems, new societal structures and new business structures[36]. All of these elements are postulated as either dependant or resultant on the increased importance of knowledge and the ability to deal with that knowledge in an effective manner.

2.2.3 The Importance of a Consolidated Conceptualisation

Although there are many differing points of view associated with the development of the information society – some of which have been highlighted above – what does become clear is that although all different, each one in its own way makes a meaningful contribution to our understanding of the topic at hand; whether good or bad. As Webster outlines in the following extract below however, one should be apprehensive of taking these points of view and their contents for granted, particularly concerning the idea of an information society and the role played by technological forces alone therein.

---

32 Masuda, Y. 1981. *The Information Society as Post-industrial Society* p vii.

33 Masuda, Y. 1981. *The Information Society as Post-industrial Society* p 56.

34 Masuda, Y. 1981. *The Information Society as Post-industrial Society* p 66.

35 Masuda, Y. 1981. *The Information Society as Post-industrial Society* p 87-99.

36 Chen, T. & Lee, J. 2004. *The New Knowledge Economy of Taiwan* p 2-17.

> So much commentary on the 'information age' starts from a naive and taken-for-granted position: "There has been an "information revolution", this will have and is having profound social consequences, here are the sorts of impact one may anticipate and which may already have been evident. This sets out with such a self evidently firm sense of direction, and it follows such a neat linear logic – technological innovation results in social change – that it is almost a pity to announce that it is simply the wrong point of departure for those embarking on a journey to see where information trends, technological and other, are leading. At the least, recognition of the contribution of social theory moves one away from the technological determinism which tends to dominate a great deal of consideration of the issues[37].

With the above extract in mind, I feel that a conjugated point of view, in terms of defined characteristics, is perhaps best when engaging with those elements of influence expressed as change or continuity leading to a knowledge economy and society. The reason for this is that although other approaches highlight some critical elements such as the influence of new scientific research, the development of ICTs and the role played by technological advancement, one is still analysing change from a singular perspective. This is in contradiction, as technological advancement is seen as the prime social influence yet conceptually it exists externally to that context.

> It [technology] most certainly is this, but more important is that it relegates into an entirely separate division social, economic and political dimensions of technological innovation. These follow from, and are subordinate to, the premier force of technology that appears to be self-perpetuation, though it leaves its impress on all aspects of society. Technology in this imagination comes from outside society as an invasive element, without contact with the social in its development, yet it has enormous social consequences when it impacts on society[38].

Technology is something which is not aloof to the social realm, but rather an integral part of that social realm, as indicated by the many studies which have shown how technologies bear the impress of social values[39]. Thus, one should rather in my opinion view any form of change as reliant upon a combination of these defined entities, each acting as a catalyst dependant on other factors for their existence and influence at a particular point in time.

[37] Webster, F. 2006. *Theories of the Information Society* p 264.

[38] Webster, F. 2006. *Theories of the Information Society* p 12.

[39] Webster, F. 2006. *Theories of the Information Society* p 12.

Rather than focusing on any one perspective and its relevant contributions as a means for explaining those societal changes dealt with in the present; operating as an all inclusive entity.

For example, if there was no consolidation of the nation state in combination with industrial capitalism[40], one has to question whether there would have been a base for the development of a platform for ICT advancement and the subsequent adoption of global knowledge based economic strategies by many nations. Leading one to question whether advancements in techno-economic ideology would have struggled for existence without increased networking's spatial influence, travel and new forms of social existence; riding waves of extended scientific research influenced by externalising factors.

2.3 Key Defining Forces of the Knowledge Society

I will now proceed to elaborate further on those key elements of analysis – technological, economic, occupational, spatial and cultural definitions – whereby they will act as a framework for my analysis. These elements will be fleshed out further by taking into account other important points regarding each elements influence, in an attempt to offer a level of forethought, acting as a component of and precursor to those questions posed in the previous chapter and as a base for the following chapter to come. One should also be aware that although all of these points may be somewhat generally applicable, they do vary depending on their context. The reason for this is that different countries and the societies which they contain are not homogeneous, as are those countries abilities to effectively make use of information resources and to apply those information resources with their specific situational context. For example countries differ in terms of their population size and their ability to afford access to their populous.

It is also important to note that although I deal with these elements in a partitioned manner, that it by no means implies that I view these elements as disconnected from one another in any particular way. By engaging with each defined element of change in the way I do, it affords one a certain level of sagaciousness and allows one the opportunity to compare forces in a collective manner. One should take note that it is not my aim at this stage of the discussion to offer any firm resolutions to the question of relevance; such determinates will follow in chapter 3.

[40] Webster, F. 2006. *Theories of the Information Society* p 265.

2.3.1 Technological Forces

The technologically defined perspective, where technology is seen as the overarching influencing factor, acting on societal structures which in turn lead to the reconstitution of these structures, is perhaps one of the more popular information society explanations. This has largely stemmed out of the ideology of conflict innovation. This innovation having been directed to the largest degree during and since World War II and the Cold War nuclear capped technological race which followed[41], whereby extended forms of military and eventually business based economic scientific research, lead to increased advancements in technological innovation. The American context being a key example of this.

> A distinctive feature of American government since World War II has been the emergence of "science policy" as a focus of thought and action. Before the war, numerous obstacles, institutional and traditional, worked against a significant role for science and technology in public affairs...cases of science and technology as the centrepieces of government action or the motivating forces behind new programs or agencies were rare before World War II[42].

World War II, a period of increased expansion in military and industrial research[43], sparked fervent scientific interest in a vast number of areas. This form of innovative ideology carried on well into the Cold War period[44] reignited on a broader scale by the launch of Sputnik by the then Soviet Socialist Republics in 1957 setting off alarm in the United States over a *science gap* and prompting a surge in investment in science and technology[45]. This can be thought of in the form of amplified competency and protection abilities through many channels. One element of this was the need for robust communication networks and increased capabilities in information processing that would be able to survive a nuclear strike[46]. This resulted in the development of the Advanced Research Projects Agency Network (ARPANET), the basis for the Internet of today.

The prolific nature of technological development during this time fuelled many of today's technological conceptions, predominantly centring on the array of information technology

---

41 Leslie, S. 1994. *Course Notes: The Cold War and American Science: The Military-Industrial-Academic Complex at MIT and Stanford* p 1-5.

42 Smith, B. 1990. *American Science Policy Since World War II* p 1-2.

43 Saettler, P. 1968. *A History of Instructional Technology* p na.

44 Nye, J. & Owens, W. 1996. *America's Information Edge* p 21.

45 Abbate, J. 1999. *Inventing the Internet* p 8

46 Abbate, J. 1999. *Inventing the Internet* p 9

innovations that have appeared since the late 1970's; with particular emphasis given to the rapid advancements in micro chip technology and its increasing capabilities[47]. These technological advancements include the advent and adoption of cable and satellite television, computer-to-computer communications, personal computers, new office technologies such as online information services, word processors and cognate facilities[48]; all of which are meaningful entities in a knowledge centric economy.

> Business, banking, and commerce all depend on information flow and are facilitated by new communication technologies. The hardware of these technologies tends to be systemic and integrated – computer, television, cable, satellite, laser, fibre-optic, and microchip technologies combining to create a vast interactive communications and information network[49].

In more recent times – particularly during the 1990's – technological and communication advancement, from an informational point of view has continued to progress. Advanced progression has resulted in the merging of newly developed information technologies with communications technologies forming advanced computer information exchanges[50]. This has been compounded further through the increased capabilities that broad band internet technology has offered, various modulations and applications of the World Wide Web and the advent of wireless mobile internet technology; creating what commentators have referred to as *placeless connectivity*[51]. The proliferation of information communications technologies has had far reaching impacts on what is meant for the way the businesses of today conducted themselves. This is especially true from an intelligence perspective. Thereby further influencing the adoption of communicative information networking capabilities within many organisations.

2.3.2 Economic Forces

The economically defined perspective, where information if seen as the largest contributing factor towards the gross national product (GNP) within an economy whose value is measured in terms of primary (quantitative) and secondary (qualitative) economic factors[52]. If dominating, thus results in both an economic and perceptive shift away from traditional

47 Webster, F. 2006. *Theories of the Information Society* p 9.
48 Webster, F. 2006. *Theories of the Information Society* p 9.
49 Barber, B. 1992. *Jihad vs. McWorld* p 54.
50 Webster, F. 2006. *Theories of the Information Society* p 10.
51 Webster, F. 2006. *Theories of the Information Society* p 12.
52 Webster, F. 2006. *Theories of the Information Society* p 13.

conceptualisations to what may be called an information economy and therefore information society as well.

> As such it is an Information Society where the major arenas of economic activity are the information goods and service producers, and the public and private (secondary information sector) bureaucracies[53].

Reasons for progression towards an information economy and thus society are rather varied in their expressions. In many economies such furtherance largely can be seen to have taken place due to rapid advancements in information communications technology, particularly in terms of the industry's growth in manufacturing, local market saturation and globalisation drives which began in the early 1970's[54]. This was done in the search for new market opportunities[55]. The result of which was an increasing need for infrastructure improvements to take place in order to support the communication of information both internally within a certain business context as well as between disparate satellite organisations on an increasingly global scale.

Such furtherance, whether shift or continuum, has also been seen to have come about as the result of increased reliance on the application of influential technological forces. The result of these changes can be felt as increasing levels of information infrastructure, the opening up of previously closed industrial society industries to the public, the expansion of social consumption, the stabilised development of the economy through a move away from the traditional economic ideas of mass production and increased management combined with capital participation[56]. This in stark contrast to those industrial foundations of labour, intensive mass production and small scale agrarian simplicity that were its predecessors, therefore leading to modifications within perceived ideas of industrial structure.

Some have referred to this as the control economy, with revolutions in control having taken place in those areas of mass production and distribution, mass consumption, data processing and bureaucracy predominantly leading from the economic shift sparked by the industrial

---

53 Porat, M. 1978. *Communication Policy in an Information Society* p 32. As cited in Webster, F. 2006. *Theories of the Information Society* p 13.

54 I refer to this period of discussion surrounding the information economy, as being fundamental, as further investigation by Porat had been done at that stage allowing for a more advanced dispensation. It is no less important to note however that as early as 1962 Machlup had already begun to use the term knowledge economy in earnest as can be seen in Beniger, R. 1986. *The Control Revolution: Technological and Economic Origins of the Information Society* p 4.

55 Trauth, E. 2000. *The Culture of an Information Economy: Influences and Impacts in the Republic of Ireland* p32.

56 Masuda, Y 1981. *The Information Society as Post Industrial Society* p 96-99.

revolution[57]. Today such control is seen not only as a response mechanism but also as the driving force of the information society, in this case from the point of view of the continuum of industrial society principles, its inspirational origin in essence. In its most basic form this is seen as the influence and necessity of technological advancement along this continuum acting as a means of response to those earlier identified influences[58]. Thus, technology is seen to be the driving force in dealing with those more advanced stages of economic growth, where it is able to respond to the requirements of control within this particularly defined economic sphere.

This ultimately leads to increased levels of information processing and the feedback of such advancements into both the societal and economic spheres, in a quest to control increasing entropy levels of the system; leading to a reconstitution of that system itself. Therefore allowing for ever increasing levels of optimisation, efficiency and refinement through the use of informational tools to better increase and assert those abilities found lacking due to rapid advancements in production, technology and subsequent socio-economic shift.

> In an economy where the only certainty is uncertainty, the one sure source of lasting competitive advantage is knowledge. When markets shift, technologies proliferate, competitors multiply, and products become obsolete almost overnight, successful companies are those that consistently create new knowledge, disseminate it widely throughout the organisation, and quickly embody it in new technologies and products. These activities define the "knowledge-creating" company, whose sole business is continuous innovation[59].

In our current context such understandings have shifted the perceived notion of what constitutes today's economic value. That economic value residing in the intellectual capital variances of an organisation, its ability to innovate and the level of knowledge an organisation operating within this new economic dispensation is able to utilise and retain for adequate periods of time in order to remain competitive.

2.3.3 Occupational Forces

The occupationally defined perspective, where occupational structure is examined over time and patters of change are observed, suggests that an information society has been achieved

---

57 Beniger, J. 1986. *The Control Revolution: Technological and Economic Origins of the Information Society* p 426.

58 Beniger, J. 1986. *The Control Revolution: Technological and Economic Origins of the Information Society* p 9-10.

59 Neef, D., Siesfeld, G. & Cefola, J. 1998. *The Economic Impact of Knowledge* p 175.

when the predominance of occupations are found to be in informational work activities; with the raw material of such activities being information itself[60]. The evidence of such occupational shift juxtaposed to its industrial work based forbearers can be seen by the large percentage of information occupation activities in a number of developed (and developing[61]) economies.

> Evidence of this [exists] in Western Europe, Japan and North America where over 70% of the work force is now found in the service sector of the economy, and white-collar occupations are now a majority. On these grounds alone it would seem plausible to argue that we inhabit an information society, since the 'predominant group [of occupations] consists of information workers' (Bell, 1979, p. 183)[62].

Occupational transition is seen to have largely had its origins during the post World War II and Cold War periods, where new innovations in scientific research were seen as the key factor of such resurgence. This created a greater level of intellectual need. The move towards service based occupations, from this point of view, was seen as society's way of attempting self organising regulation, with the transformation of the occupational sphere acting as an "organising principle of post-war society"[63]. This lead to the displacement of a once dominant industrial workforce and industrially based societal structure as well.

> The impact of industrialisation on the occupational structure of modern society has long been one of the major focuses in sociology. To the sociologist, a change in the occupational structure reflects not only changes in the economic relations of employment and the labour force but often significant transformations in social structure and social relations because occupation is generally regarded as the most important indicator of a person's social status and life style. A changing occupational structure mirrors changes in social organisation and human relationships[64].

In combination with scientific furtherance – as expressed as a continuum in many of these facets – those challenges posed by the post-war innovative environment require increased

---

60 Webster, F. *Theories of the Information Society* p 14.

61 According to the Canadian International Development Agency, 2008. 65 percent of South Africa's economy is in the service sector, 20 percent is in manufacturing, and 6 percent is in mining [Online].

62 Webster, F. *Theories of the Information Society* p 14.

63 Perkin, H. 1989, *The Rise of Professional Society: Britain Since 1880 p 406. As cited in Webster, F. Theories of the Information Society* p 16.

64 Kuo, E. & Chen, H. 1987. *Toward an Information Society: Changing Occupational Structure in Singapore* p 355.

levels of intellectual workers, in relevant fields, as is expressed by statistics highlighting the "rapid growth in the development of mass higher education following the Second World War[65]". As without such increased intellectual investment, societies operating within this context would struggle to engage effectively within the intensive information orientated social and work structures.

Although not of large scale importance in industrial era occupational ideology, information workers are viewed as a necessity rather than a novel rarity in today's occupational context. This is expressed by the importance of intellectual capital assets for today's organisations in order to maintain competitive advantage[66]. From this point of view the social shift towards informational occupations can in itself be thought of as a self creating entity through which increasing informational activity and those periphery services which surround larger core elements, contributed towards the creating of a knowledge society. This can be seen in terms of the way in which we think about our occupational opportunities in our current context.

2.3.4 Spatial Forces

The spatially defined perspective, where spatial elements are defined from a geographical point of view, places a firm emphasis on the increased proliferation of digital networks and the information flows that take place within those networks. Variously disparate spatial entities are thus able to connect to one another and the networks that are created have come to be seen as a prominent feature of today's information driven social organisation[67]. This level of networking and information flow is seen as translating into what can be called an information society through the manipulation of time and spatial conception.

> In a 'network society' constraints of the clock and of distance have been radically relieved, the corporations, and even the individual being capable of managing their affairs effectively on a global scale. Academic researchers no longer need to travel from the university to consult the Library of Congress since they can interrogate it on the Internet; the business corporation no longer needs routinely to fly out its managers to find out what is happening in their Far East outlets because computer communications enable systematic surveillance from afar. The suggestion of many

---

65 Gibbons, M. 1994. *The New Production of Knowledge: The Dynamics of Science and Research in Contemporary Societies* p 70.

66 Nahapiet, J. & Ghoshal, S. 1998. *Social Capital, Intellectual Capital, and the Organizational Advantage* p 242-266.

67 Webster, F. 2006. *Theories of the Information Society* p 17.

> is that this heralds a major transformation of our social order (Mulgan, 1991), sufficient to mark even a revolutionary change[68].

The early origins of the superseding nature of such networks were largely grounded in those rapid advancements which took place in networking technology during the Cold War. This was centred specifically on the development of ARPANET and its eventual adoption and translation into the Internet of today; as previously highlighted. With increased globalisation drivers, in the search for new and improved economic opportunities[69], the spatial context and in fact the global perception of time within the business and social sphere has been greatly altered.

The networks combined with the information that they carry have risen to a level of critical importance, through the subsequent compression of time and the destruction of perceived spatial restrictions. Such advancements within the networked context have also found support and expression in transportation, the requirement for advanced intellectual skill sets to be held by the individual, the increasing dominance of accentuated intellectual capabilities and the greatly emphasised economic value of these assets. This is displayed by the heavily valued and often critical nature of the information travelling across these networks in support of the expansion of social change and organisation.

> While the networking form of social organisation has existed in other times and spaces, the new information technology paradigm provides the material basis for its pervasive expansion throughout the entire social structure...Presence or absence in the network and the dynamics of each network vis-à-vis others are critical sources of domination and change in our society: a society that, therefore, we may properly call the network society, characterised by the pre-eminence of social morphology over social action[70]

In addition to the support of social morphology, such networks are seen to be crucial for the effective functioning and integration of peoples operating around the globe, forming part of this new networked information society world. An example of this being the increased level of collaborative abilities afforded for the manifestation of a global civil society where the "power of flows takes precedence over the flows of power"[71]. This can be expressed through

---

68 Webster, F. 2006. *Theories of the Information Society* p18.

69 The use and development of information communications technologies used to support this.

70 Castelles, M. 2000. *The Rise of the Network society* p 500.

71 Castelles, M. 2000. *The Rise of the Network society* p 500.

the facilitative abilities of advancing information communications technologies[72]. One can think of this as a single expression of what others have referred to as the manifestation of *Cyber society*[73] itself, where the pervasiveness of computers and the communication networks that they offer become as mundane as using electricity. This perspective is by no means limited to the individual sphere alone.

Contact with networks and their resultant information flows may take many forms and vary quite considerably. Even if one is not responsible for their direct manifestation or connection, one may still engage or come across networks in many forms while performing one's daily activities[74]. Although general social interactions are perhaps more minimal in terms of their level of information flow and networking interaction, informational flows at the level of international banks, intergovernmental agencies and between corporate players[75], are far more frenetic in their nature and proliferation. An important element of consideration from an intelligence stand point.

2.3.5 Cultural Forces

The culturally defined perspective is based on the idea that within current social conception there has been an extraordinary increase of information within social circulation[76]. The impacts of this increase are predominantly seen and attributed to the increased pervasiveness and proliferation of various types and channels of media operating today on a mass globalised scale. This in turn helps to produce the fabric of everyday life[77]. Through the integration and often manipulation of such channels, society's interactions and perceptions of that social context itself are shaped by the signals presented, interpreted and reflected upon by the masses. Such manipulation is seen as being an accepted and reflective part of this communicative process, therefore creating a functional stage for today's contemporary culture.

> Contemporary culture is manifestly more heavily information-laden than its predecessors. We exist in a media-saturated environment which means that life is quintessentially about symbolisation, about exchanging and receiving – or trying

72 Harasim, L. 1993. *Global Networks: Computers and International Communication* p 285.

73 Shade, L. 1996. *Data Trash: The Theory of the Virtual Class* [Online].

74 Harasim, L. 1993. *Global Networks: Computers and International Communication* p 284.

75 Webster, F. 2006. *Theories of the Information Society* p 17.

76 Webser, F. 2006. *Theories of the Information Society* p 19.

77 Kellner, D. 1995. *Media Culture: Cultural studies, identity and politics between the modern and postmodern* p 1-2.

> to exchange and resisting reception – messages about ourselves and others. It is in acknowledgement of this explosion of signification that many writers conceive of our having entered an information society[78].

With rapid advancements in information communications technologies and their subsequent large scale adoption having taken place since the post war period, signification has multiplied largely through its adoption and projection within multitudinous technologically based channels of communication. These channels being radio, television, film and the Internet as well as more traditional non-information technology based forms of print media such as newspapers, magazines and books[79]. These print media sources have themselves proliferated further due to their interaction with the cultural media networks of today.

An example of increased levels of signified projection, from this point of view, is evident when one examines the large increases in the number of television channels available today. This is a dominant form and example of such social media cultural projection[80]. Where the television channels of our present time seem to be endless in their proliferation[81], as opposed to those earlier times in televisions existence where they were limited to just a handful. Thereby, indicating the increased demand for informational services and the rapid growth of such services within our current context of signified cultural projection.

The interpretation and power of such signified projection, within the social context, has perhaps lost much of the meaning it once carried, therefore leading social entities to question their "knowledge of the real"[82]. This has lead to a loss of interest in previously once meaningful cultural perceptions of identity.

> One thing that is modern, Marx and Baudelaire both recognised in their own ways, is a new sense of time, a new velocity of experience, a new vertigo. When TS Eliot wrote, "we had the experience but we missed the meaning," he was speaking partly of the loss of traditional concepts of time and, conjointly, the mass availability of synthetic meanings. The synthetic time tables and images of the modern world suffuse and throw into question our knowledge of the real. The mass media

78 Webster, F. 2006. *Theories of the Information Society* p 20.

79 Webster, F. 2006. *Theories of the Information Society* p 20.

80 Williams, R. 1990. *Television: Technology and Cultural Form* p vi.

81 Wenner, L. 1998. *MediaSport* p 73.

82 Gitlin, T. 2003. *The Whole World is Watching: Mass Media in the Making & Unmaking of the New Left* p 233.

> *routinize* this "missing" and then not only propound meaning for experience but actually help constitute it[83].

Such changes also have specific impacts for the organisation and its intelligence functions which are also a construction of social culture and cultural perceptiveness. This perceptiveness is manifested through an organisation's employees and those channels by which the organisation must interact with the public. This contributes to a need for additional dimensions of protection and information sanitisation, as channels of distribution are subsequently greatly increased from what once they were. This when operating in a multitudinous sphere of communication, distribution and mass media enlightenment.

2.4 Conclusion in Brief

Given the multifaceted nature of business counterintelligence, it is essential that one should firstly construct a contextual framework in order to better understand its importance for today's organisations; this has partly been achieved. Firstly, through the clarification of the semantic variances that accompanies business counterintelligence as presented within the literature. Secondly, by outlining the disparate perspectives of the information society and highlighting the importance of a consolidated approach in this regard. This in order to act as a backdrop to the changes that have occurred, which have in turn lead to the manifestation of today's business context. For this purpose, the information society was outlined and briefly discussed in terms of its main perspectives, expressed as broader concepts of categorisation. This was done for the purpose of setting a contextual base for the discussion to follow.

By allowing for such categorisation, one will be able to better engage with those elements of change that have occurred within our current context leading to the rise in importance of business counterintelligence for today's organisations. Engagement with theories of the information society thus provides the impetus for the analysis of such change in terms of the rise in importance of business counterintelligence, its level of adoption and changes that have occurred within the business environment of today. These issues will be elaborated upon further in chapter 3.

---

[83] Gitlin, T. 2003. *The Whole World is Watching: Mass Media in the Making & Unmaking of the New Left* p 233.

Chapter 3

The Rise in Importance of Business Counterintelligence

3.1 Introduction

The aim of this chapter will be to demonstrate that business counterintelligence is a by product of the aforementioned shift to a society – and economy – where knowledge has achieved a special pertinence, and as such needs to be effectively protected. This will be done in the light of the content presented in the previous chapter, whereby the structural basis for this chapter was formed through an analysis of the information society. The sub-questions posed in chapter 1, under the heading *Context*, will be dealt with by examining business counterintelligence's role prior to such informational economic shift and looking at what elements in the context of this environment have changed. Finally, an analysis will be given as to what therefore has lead to business counterintelligence becoming an issue for today's organisations.

Engagement with the topic during this section of analysis will take the form of a multitudinous approach, as the juxtaposing of ideas in this instance will be accepted as a self explanatory form of understanding. By placing emphasis on the intricacies of the questions, it will allow for increased understanding, concerning both the mainstream and subtle points covered. This will be done in order to express a more comprehensively detailed approach. I will therefore begin this section of analysis by examining those issues concerning business counterintelligence and its level of importance for organisations some two to three decades ago.

3.2 Business Counterintelligence and the Industrial Landscape

Although espionage and its countermeasures have been around since the dawn of the economic system itself[84], advanced countermeasures as expressed in addition to multifaceted layers of physical protection from a physical security stand point[85] have only really begun to infiltrate the business arena in earnest since the early 1990's. This coincides with the ending of the Cold War[86]. There has been a progressive movement towards the increased protection of knowledge assets that has gradually grown in momentum over the last two to three decades.

Prior to this period, counters to information gathering attempts were not viewed of great importance within the business sector itself. Or at the very least were not viewed with the same level of intensity and protectionism as they are today. Rather countermeasures and investigations concerning the protection of information secrets, in an economic sense, remained largely within the limited domain of global intelligence agencies[87]. These agencies primary concern, with regards to the stealing of economic secrets, was often motivated and analysed in the light of those political and military forces at play during the Cold War.

The same can be said for much of the motivation behind the stealing of economic secrets during the Cold War industrial period – where-as in today's information driven societal context similar parallels can be found – rapid advancements in scientific and technological production in Western countries were seen at the time as key motivating factors behind such activities. These were concluded in order to gain economic, technological and primarily military advantage. The Komityet Gosudarstvennoy Bezopasnosti's (KGB's) intelligence gathering activities targeting the sphere of Western economic powers during the Cold War can be seen as an example of this.

---

84 Moule, G. 1996. *A Study of Security Countermeasures to Reduce Economic Espionage in the United States from 1975 to 1996* p 9-15 states that: "Counterintelligence has existed as long as the concept of espionage. Two thousand years ago, Sun Tzu stated in the Art of War that, "it is essential to seek out enemy agents who have come to conduct espionage against you" (Swartwood, 1993). A 1992 survey conducted by the Standing Committee for Safeguarding Proprietary Information of ASIS [American Society for Industrial Security] discovered that out of the 246 companies that responded, 76% of them had a formal Safeguarding Proprietary Information (SPI) program in place. This program however, is only updated annually by 33% of those companies (Heffernan, Swartwood, 1993)."

85 Lowry, J. 2001. *Observations on the Effects of Defence In-Depth on Adversary Behaviour in Cyber Warfare* p 187.

86 Hutchinson, W. (eds). 2002. *Business Intelligence Gathering* p 10.

87 Moule, G. 1996. *A Study of Security Countermeasures to Reduce Economic Espionage in the United States from 1975 to 1996* p 10.

> [The] post [World War II] Soviet Union was deeply in need for technological development and could definitely not afford the lawful acquisition or development of that technology. The KGB therefore played a very important role in acquiring foreign technology to send it back home...[intelligence gathering activities] provided the Soviets with crucial documentation and sometimes parts concerning computer networking systems, missile guidance systems, laser weapons, detection systems for high-speed low-flying targets, infra-red night-vision equipment for tanks, helicopters and other uses[88].

In addition to the scientific and technological targeted threats faced by predominantly Western based organisations during the time of the Cold War, much of the security thinking presented within these organisations, prior to the rapid growth and increased dependence on information, was naturally dominated by industrial security ideology. Such thinking was grounded within the realms of policy and practice where effective industrial security elements were often viewed as the implementation of physical security measures and barriers to prevent the stealing of physical material[89] and employee screening[90]. These security elements were seen as substantial enough to protect against the perceived security threats facing one's business and critical scientific information of the time.

As was highlighted in the previous chapter, during this period the knowledge society and its features were only beginning to emerge as a dominant form of understanding, bring with them many aspects of influence indicative of such shift. This can be thought of in terms of technological, economic, occupational, spatial and culturally defined forces as experienced in the present social, knowledge based business context. It was through a combination of these factors that such a shift from more traditional industrialised perceptions to those of a knowledge based economic context began to transcend with greater rapidity. This was evident in the light of increased social factorial dialogue; particularly when viewed from the perspective of the growing income gap[91] that began to appear within the United States at around the same time.

---

88 Mellon, J. 2001. *Assessment of KGB's Intelligence-Gathering Successfulness in the West During the Period of 1954 to 1991* p 6.

89 Trim, P. 2002. *Corporate Intelligence and Transformational Marketing in the Age of the Internet* p 262.

90 Stallings, W. 2006. *Cryptography and Network Security: Principles and Practice 4th ed* p 7-8.

91 As Nasar, S. 1999. *Book Review: The New Dollars and Dreams: American Incomes and Economic Change* [Online] outlines: "The chief culprit, argues Levy, isn't one of the popular suspects – the shift to service jobs, globalization or the Reagan tax cuts – but the Computer Age itself. For two decades, the demand (and hence, pay) for less skilled, less educated workers has grown much more slowly than for the highly skilled and educated. The trend is remarkably pervasive and stretches across industries, occupations and countries.

What has become clear is that with the emergence of such shifts, the modern industrial age remained a phase in history where informational changes were only beginning to emerge in any kind of dominant form. This could be seen where industrial principles and understandings governing the social construction of the business environment and the economy, although beginning to falter, were still dominant factors at play within the industrial mind-set[92]. As such, although the use of information as a critical component of economic activity was on the rise, it had not yet obtained its special place in society and the economic context[93]. This is in contrast to today's economic and social order particularly in light of increased innovation[94]. Rather the knowledge economy could be seen to be in the early phase of its development, in a time of transition and resurgence, setting the foundational basis for the emergence and dominance of information activity in years to follow. In order to do this it had to operate through a very different set of perceptions about how economic success should be generated and sustained.

3.2.1 Globalisation and the Industrial Business Context

Another key factor to take into consideration is that of the perceived notion of globalisation. Global influence viewed from a service based economic perspective and its subsequent influence on organisational policy and decision making. This can be understood in terms of changing comprehensions from a national to international[95] economically expanded point of view.

There has always been some level of understanding regarding the global economic conceptualisation of world trade and other flow factors attributed to global influence,

---

"People with no more than high school education are frequently viewed as downscale in both commercial and social terms," writes Levy, and "many of today's older workers have not seen significant income gains over their careers" ".

92 This is indicated in the following extract taken from Carnoy, M. 2000. *Sustaining the New Economy: Work, Family, and Community in the Information Age* p ix, where he eludes to the impacts of the knowledge society through factorial transformation within Silicon Valley; as it was in the mid 1970's: "For the past thirty years, I have lived and worked in Silicon Valley's new economy. I have watched it transformed from the innovative edge of American industry to an engine of global growth. Around 1975, I began interviewing chief executive officers of technology-based firms and the workers building the chips and electronic devices that were the Valley's mainstay. In those days, we were still in the modern industrial age – Silicon Valley firms were focusing on hardware and manufacturing. Yet the essence of high-tech work was not very different than it is today. People changed jobs often and looked for start-ups where they could get a piece of the company. The eighty-hour work culture was in place, but it was not as ubiquitous as it is now. Fortunes were made, but not nearly as rapidly as they are today. The new gold rush was just beginning, and each decade has brought success on an even greater scale."

93 Webster, F. 2006. *Theories of the Information Society* p 2.

94 Jaffe, A. et al. 2002. *Patents, Citations, and Innovations: A Window on the Knowledge Economy* p 90.

95 Aharoni, Y. 1993. *Coalitions and Competition: The Globalization of Professional Business Services* p 2.

globalisation as a definitive concept is one that has only really begun to emerge in earnest, in very recent history[96]. An indication of such emergence can be seen by the increased proliferation of published materials making use of the term, particularly within academic circles, since the turn of the *new millennium*.

> Overall, the number of publications which used the word 'global' in their titles has now probably reached five figures but the processual term 'globalisation' was still relatively rare at the beginning of the 1990s. In February 1994 the catalogue of the Library of Congress contained only 34 publications with the term or one of its derivatives in the title. By February 2000 this number had risen to 284. None of these were published before 1987[97].

In more recent times, particularly if one views the rise of globalisation as a process of sustained continuity concerning the phases of early industrial development[98], the conceptual understanding and application of globalisation, in light of its social and economic impact, was by no means as broadly accepted as it is within today's business environment. Organisations operating within the business contexts of the past were faced with far less challenging levels of competitiveness, reliance on informational abilities and encroachment from multiple business regions. Foreign competition, within this context, was predominantly leveraged from forces limited to a vastly simplified international and multinational[99] business environment centred around core regions of trade and industry. This is in firm contrast to the present globalised era which carries with it far more multiplicity and uncertainty from an economic standpoint.

> The present "global" era...is a world economy of multiple centres, each with a distinct capacity for innovation and development. As a consequence, in contrast to its predecessors, this era lacks a dominant style. It is distinctively diverse and uncertain. It is not just that the terms of corporate competition have been altered. Rather, a multiplicity of corporate and national strategies competes to capture advantage in volatile markets. Speed, product differentiation, networking, and an

---

96 As Waters, M. 2001. *Globalisation* p 2, states: "Although the word 'global' is over 400 years old (OED 1989, s.v. global) the common usage of such words as 'globalisation', 'globalise' and 'globalising' did not begin until about 1960. *The Economist* (04/4/59) reported 'Italy's "globalised quota" for imports of cars has increased' and in 1961 *Webster* became the first major dictionary to offer definitions of globalism and globalisation. In 1962 the Spectator (5/10/62) recognised that: 'Globalisation is, indeed, a staggering concept'(OED 1989, s.v. globalism, globalisation, globalise, globalised)".

97 Waters, M. 2001. *Globalisation* p 2.

98 Waters, M. 2001. *Globalisation* p 26-28.

99 Borrus, M. & Zysman, J. 1997. *Globalization with Borders: The Rise of Wintelism as the Future of Industrial Competition* p 29.

> emphasis on intellectual property all join the necessities of price and quality to mark the new phase of competition...The global economy is, as a consequence, a complex and often contradictory story of global markets, national development strategies, regional dynamics and competing corporate strategies[100].

The concept of globalisation during the industrial period was as such largely limited in terms of the protection requirements deemed necessary to effectively deal with such challenges. The requirements for protection were simply not as great. What this means is that, when viewed from a business counterintelligence point of view, organisations operating within the non-aggrandised, partly global setting were not faced with the challenging elements of dynamic competitiveness that they are today.

What is indicative of the industrial competitive sphere – when discussed in the light of those changes that have occurred in today's social and economic contexts with reference to the information society – is that organisations operating within the industrial business environment were far less reliant on informational business activity for their survival[101]. Even if the core elements of mass production still remain a part of the today's economy, products developed during the industrial era were not embedded and constructed with the same level of knowledge[102]. Rather, organisations and the economies in which they operated although perhaps in the very early stages of certain types of knowledge activity remindful of our time[103], were still predominantly reliant on traditional industrial production methods. These were based on the use of natural resources, physical inputs[104] and mass production; factors seen as the dominant form of wealth creation and thus centrally important to the industrial context.

Although there are many factors to take into consideration when analysing the business context of the industrial society era, perhaps the one overriding consistency that is central to all of these factors is that they all in some way highlight the absence of critically perceived knowledge. The recognition of knowledge, as an economic entity of value within the industrial business context, was not seen as a commodity of central importance to the economic foundations of business operations. This therefore must carry with it a special

---

[100] Borrus, M. & Zysman, J. 1997. *Globalization with Borders: The Rise of Wintelism as the Future of Industrial Competition* p 29.

[101] Powell, W. & Snellman, K. 2004. *The Knowledge Economy* p 204.

[102] Powell, W. & Snellman, K. 2004. *The Knowledge Economy* p 201.

[103] Carnoy, M. 2000. *Sustaining the New Economy: Work, Family, and Community in the Information Age* p ix.

[104] Powell, W. & Snellman, K. 2004. *The Knowledge Economy* p 215.

relevance for business counterintelligence which itself can be conceived of as a form of knowledge[105] and therefore should be thought of as critical in this regard. Operating in today's context as an active element of the knowledge economy expressed within the business sphere. One may therefore question why this was not the case within the industrial economic context.

Firstly, if knowledge was not seen as a commodity of industrial era production, then there would be little need to take business counter-*intelligence* into consideration when dealing with industrial business activities. What this means is that without knowledge forming part of the dominant vocabulary of the industrial organisation, processes such as the information gathering intelligence cycle[106] – information gathering in the form of competitive intelligence being a commonly performed activity within the knowledge based business setting[107] – would not have constituted part of the vocabularies of organisations operation within the industrial business context.

Secondly, one can acknowledge that physical security was a requirement of industrial society business and therefore as such there was a certain level of industrial espionage to contend with[108]. However, the fact remains that knowledge and subsequently business counterintelligence, would have been non-entities within the industrial business environment. Industrial organisations were not operating in an environment where globalised business activity was anywhere near the level of complexity, turbulence and rapid progression that it is

---

[105] As stated by Kinghorn, J. 2007. *Personal communication,* information can be thought of as knowledge in transit and a synonym of information, as stated by *The American Heritage Dictionary, Roget's II: The New Thesaurus. 3rd ed. 2003* [Online], is intelligence. One could therefore in essence replace the word counter-*intelligence* with counter-*information*; in this instance knowledge in a different form thus containing the same connotative meaning. As outlined by Cortada, J & Woods, J. (eds) 1999. *The Knowledge Management Yearbook 1999-2000: 1999-2000* p 53, it is important however that when using such a comparison, that there is always some level of contextualisation accompanying: "The story I most frequently use to distinguish between knowledge and information is to use the metaphor of a map and a human guide. A map is a set of data organised into a coherent and reusable form – it is information. The guide, on the other hand, is knowledgeable. She does not need to consult a map, takes into account recent experience, and has the ability to relate my ability to her knowledge of the terrain. The guide is the fastest way to achieve my objective, provided that I trust her. If I do not have that trust, and am not prepared to take the risk of experimentation, then I will fall back on information – the map. It should also be noted that someone with knowledge of the territory has created the map. If I share the same culture and background as the map maker then I am able to use the information. A different background may mean that the map is just data – useless stuff without context."

[106] As stated by the Central Intelligence Agency. 2007. *The Intelligence Cycle* [Online], the intelligence cycle is made up of 5 phases, namely: Planning and Direction; Collection; Processing; Analysis and Production; Dissemination.

[107] Prescott, J. & Miller, S. (eds) 2001. *Proven Strategies in Competitive Intelligence: Lessons from the Trenches* p 1.

[108] Krages, B. 2007. *Legal Handbook for Photographers: The Rights and Liabilities of Making Images* p 45.

today[109]. This can clearly be seen when analysing relevant information society forces, as discussed in chapter 2, where organisations operating within the knowledge economy compete on many different fronts. Competition exists not only in the spatial sense but also within the digital world – in the form of the cyber front governed by the effective use of electronic business models (e-business models) – through increasingly proliferated global networks supported by the greater application of information driven technologies and processes. The extract given below highlights this from the point of view that the existence of such e-business models based on previously identifiable standards – traditional business models – do not stand up to today's level of complexity:

> The traditional organisational business model, driven by pre-specified plans and goals, aimed to ensure optimisation and efficiencies based primarily on building consensus, convergence and compliance. Organisational information systems – as well as related performance and control systems - were modelled on the same paradigm to enable convergence by ensuring adherence to organisational routines built into formal and informal information systems. Such routinization of organisational goals for realising increased efficiencies was suitable for the era marked by a relatively stable and predictable business environment. However, this model is increasingly inadequate in the e-business era that is often characterised by an increasing pace of radical and unforeseen change in the business environment (Arthur, 1996; Barabba, 1998; Malhotra, 1998b; Kalakota and Robinson, 199; Nadler et al., 1995)[110].

As industrial era organisations were not operating within such an unstable context, in the light of globalisation, it seems there would have been very little need for them to implement intelligence gathering initiatives in order to cope with increased complexity as is the case today. This is especially true when one considers that their relevant competitors would have been operating from within the same security paradigm. Any business counterintelligence activity should it have occurred, from an industrial business perspective, would have been very limited in its nature. This limitation would have existed as the reliance on identifiable organisational knowledge elements and advanced level security practices within the industrial business environment would have been few and far between. This when compared to today's knowledge intensive context.

---

[109] Borrus, M. & Zysman, J. 1997. *Globalization with Borders: The Rise of Wintelism as the Future of Industrial Competition* p29.

[110] Malhotra, Y. 2000. *Knowledge Management and Virtual Organisations* p 2.

3.3 Changes in the Industrial Business Context

To recapitulate, there would have been very little need for the implementation of advanced business counterintelligence activities for the industrial based organisation. Traditional security elements such as physical security barriers and the like would have been seen as sufficient to quell any dangers or threats posed by those targeting the organisation in industrial times. This coincides with a strong emphasis on the protection of physical assets[111], rather than information assets; particularly in a digital sense. Given the rapid shifts that have occurred since then however, physical security measures alone are no longer adequately placed within the competitive knowledge sphere[112] to effectively deal with those threats directed towards today's organisations. One therefore has to question why this is so and what changes have lead to such an occurrence taking place; regarding the significance of counterintelligence in the present business context.

Firstly however, one has to bear in mind that in order to engage with this question in an effective manner, one should hold clear the combined relevant occurrences that have evolved over time with reference to technological, economic, occupational, spatial and culturally[113] defined forces. Such shifts are valid areas of concern particularly when viewed not only as factors of the information society, but also as factors that have themselves acted as elements of reconstitution, who's impacts have been far reaching both within the social and economic contexts. Thus, creating a very different business environment in which present day organisations must operate within. This when opposed to the industrial based business environment of the past.

---

111 Kovacich, G. & Halibozek, E. 2003. *The Manager's Handbook for Corporate Security: Establishing and Managing a Successful Assets Protection Program* p xv.

112 As Kovacich, G. & Halibozek, E. 2003. *The Manager's Handbook for Corporate Security: Establishing and Managing a Successful Assets Protection Program* p xv states: "A global and technologically connected marketplace presents a different paradigm for the corporate security professional from that encountered just a decade ago. The traditional corporate security programs were concerned with the protection of facilities, equipment, and people by physical security means. From fences to guards and badges, standard security tools were used to ensure that physical assets were protected and kept on company property. Theft of product, property, and tools was the major concern of corporate security managers. Today, however, safeguarding corporate assets requires a state-of-the art asset protection program focused on the information systems that have become critical corporate infrastructure. Such a program must be flexible and adaptable to evolving corporate needs. It also must be cost-effective. A failure to develop potent and efficient security processes can materially weaken corporate competitiveness." Corporate security professionals have never been faced with so complex a task."

113 Webster, F. 2006. *Theories of the Information Society* p 8-28. It is these elements that come to mind when I use the term transition or change, when discussing the information society, not Bells perceived "shift from a manufacturing to service society" as indicated by Webster on p 62.

3.3.1 Complexity, Turbulence and Boundaries

In today's information intensive business environment, organisational boundaries have subsequently become less well defined[114]. In addition to this the dimensions of informational security threats faced have greatly increased. This is a fundamental shift away from traditional industrial security threats and practices, where the boundaries of the industrial organisation were far less complex in nature, faced less sophisticated forms of attack and could be defined in terms of the physical security perimeters that encapsulated the organisation. In today's context, this is not so easily done. Organisations and the people who they employ are more mobile and increasingly diffuse in their day to day business interactions[115]. They communicate and operate on multiple fronts, with multiple actors making use of different forms of communication and exchanging information across diverse regional boundaries[116]. Such exchanges take place on both a national and international scale, thus substantially increasing the risks posed towards today's information intensive organisations.

The increased dominance of knowledge over the past three decades has subsequently contributed to the creation of a far more multifaceted business environment, with the informational business context itself experiencing greater complexity and turbulence[117]. Security practices of the present have therefore had to adapt greatly in order to meet the challenges posed by this new knowledge intensive environment; adaption's and transitions in information security practices can be seen as an example of this[118]. In addition to spatial complexity the global balance of power, particularly in the economic sense, has seen considerable change since the end of the Cold War era[119] with the downfall of the Soviet Union and the emergence of new potential super economies such as those of India and China. Changes in the global balance of power in combination with the increased reliance on knowledge assets have thus had immense impacts on intelligence gathering activity. This has resulted in many countries and organisations around the world – desperate to catch up with their more advanced counterparts – willing to do almost anything necessary in order to

[114] Child, J. & McGrath, G. 2001. *Organizations Unfettered: Organizational Form in an Information-Intensive Economy* p 1137.

[115] Winkler, I. 1996. *Case Study of Industrial Espionage through Social Engineering* p 4.

[116] Winkler, I. 1996. *Case Study of Industrial Espionage through Social Engineering* p 4.

[117] Drucker, P. 1980. *Managing in Turbulent Times* p 151.

[118] Stallings, W. 2006. *Cryptography and Network Security: Principles and Practice 4th ed* p 7-8.

[119] Nasheri, H. 2004. *Economic Espionage and Industrial Spying* p 53.

achieve this goal; including both developed and developing nations[120]. This at a time when knowledge can be seen to have grown tremendously in terms of its economic and occupational value as outlined in chapter 2.

As such this has had profound consequences for business counterintelligence activity, both in terms of need and application, due to increased levels of corporate spying[121]. The need for greater counterintelligence protection has thus been fuelled by the proliferation of intelligence agents[122] – particularly those of the former KGB[123] and other intelligence agencies – who have made their way into the business environment, since the end of the Cold War[124]. This has taken place as a result of the dismantlement of their previously defined intelligence structures[125] and governments. Intelligence gathering activities are therefore conducted – by a number of nations and entities[126] – in an attempt to gain greater competitive advantage, who has adjusted their intelligence gathering focus away from military targets alone to include economic information gathering strategies[127]. This has been done in order to compete more effectively within the globalised knowledge intensive economy.

---

120 Nasheri, H. 2004. *Economic Espionage and Industrial Spying* p 13-14.

121 Nasheri, H. 2004. *Economic Espionage and Industrial Spying* p 17-20.

122 One should be aware that this is a somewhat debatable point as displayed in the following extract taken from: Whitney, M. & James, G. 1999. *Why Spy? An Inquiry into the Rationale for Economic Espionage* p 103-104: "It is often argued that the end of the Cold War has contributed to an increase in economic espionage by releasing intelligence resources. In addition, the perceived need for Western nations to cooperate against a common threat has eased, turning military allies into more vigorous economic competitors. The counter-argument is that the apparent growth of economic espionage may be an overstatement by national intelligence agencies as a ploy to protect their budget allocations. While it is difficult to determine either the extent or growth of economic espionage, there is no doubt that such activity does occur."

123 Nasheri, H. 2004. *Economic Espionage and Industrial Spying* p 14.

124 Hutchinson, W. (eds). 2002. *Business Intelligence Gathering* p 9.

125 As Nasheri, H. 2004. *Economic Espionage and Industrial Spying* p 13-14 states: "In the world of economic espionage, there are no true friendly relations, largely due to the fact that countries that engage in the activity are vying for a rung on the global market ladder. As former French intelligence chief Pierre Marion pointed out, "it is an elementary blunder to think we're allies. When it comes to business it's war." Second, developing nations are heavily involved in the trade, due to recent political developments, especially the decline of communism. Formerly communist states [and others] strive to quickly catch up with the West, and economic espionage often provides an avenue to do just that. Without communism, intelligence agents from Eastern bloc countries are unemployed and available in the open market. The involvement of Eastern bloc agents is threatening because their intelligence activities are not restricted by traditional notions of international business ethics. Therefore, such agents may go to any lengths to acquire the information they seek."

126 Spheres of attack through those targeting the organisation have increased drastically. These can include but are not limited to criminals, organisations and individuals with malicious intent who can reside both internally within a particular firm as well as within the external business environment in addition to traditional competitors and targeting by foreign government intelligence agencies.

127 Nasheri, H. 2004. *Economic Espionage and Industrial Spying* p 14-17.

3.3.2 Intelligence Gathering and Strategic Implications

As has been established in chapter 2, our present time is one where information has reached a special pertinence in this modern era[128] and as such forms a key part of the fabric of our social interaction and structure. This where the "economic prosperity of this new system rests upon knowledge"[129]. Since knowledge is viewed as a largely intangible asset[130], who's existence is distributed and can be found in many forms[131], entities have realised that if they are able to obtain such knowledge about their competitors they will also be able to align their prospective competitive strategic processes more effectively. This has the benefit of offering them a greater level of dynamic flexibility[132]. This is something that can be very useful when operating within the highly volatile economic conditions that most organisations are faced with on a daily basis; as was most certainly not the case for the previously defined industrial sphere of competition.

An example of this can be seen in the alignment of certain countries'[133] intelligence gathering activities with their strategic policy, whereby information gathering is seen as part of the natural business processes of their organisations[134]. This intelligence gathering often supported further by their respective intelligence agencies[135]. This allows organisations operating within these countries a greater level of adaptability and the more effective use and application of the knowledge that they have obtained. For example in the semi-conductor industry – an instance of strategic use of information gathered– as outlined in the following extract:

---

128 Webster, F. 2006. *Theories of the Information Society* p 6.

129 Teece, D. 2003. Essays in Technology Management and Policy: Selected Papers of David Teece p 47.

130 Kaplan, R. & Norton, D. 2004. *Strategy Maps: Converting Intangible Assets into Tangible Outcomes* p 202-203.

131 According to Kaplan, R. & Norton, D. 2004. *Strategy Maps: Converting Intangible Assets into Tangible Outcomes* p 203:"Intangible assets encompass patents, copyrights, workforce knowledge, leadership, information systems and work processes" which can be supported by effective strategies with a focus on competencies, information, culture, leadership, alignment and teamwork.

132 Rouach, D. & Santi, P. 2001. *Competitive Intelligence Adds Value: Five Intelligence Attitudes* p 552.

133 Japan and France are examples of countries who conduct such activities.

134 Hutchinson, W. (eds). 2002. *Business Intelligence Gathering* p 10.

135 It should also be noted that as Fraumann, E. 1997. *Economic Espionage: Security Missions Redefined* p 305 states: "To this day Japan does not have an intelligence agency to conduct economic espionage, but relies instead on its trade ministries to collect economic information through mostly nonintrusive means [and some intrusive methods as well]...Much of Japan's economic success is attributed to the coordination of its economic espionage through the Japan External trade organisation (JETRO), with offices in 59 countries, and the Ministry of International Trade and Industry (MITI)...the Japanese have people gathering data and sending it back to a central clearing operation run by MITI and JETRO (Schweizer, 1993, 80-84)".

> Through private communication channels, a development engineer often can learn about the technical problems encountered by a competitor. This information can be used by the engineer's company to alter the allocation of resources and to update expectations for future revenue streams. Depending on the progress of their competitors, technology managers may need to revise their projections for licensing revenues or cross-licensing opportunities. Product managers may need to release products earlier than initially planned which may compress future product planning cycles. As companies expand their product portfolios, they benefit from learning about organisational systems, as well as technical feats[136].

It is also interesting to note that due to the present nature of the globalised economic system and competition – as is the case within today's knowledge economy[137] – the feeling of urgency for entities to take part in such activities, when opposed to that of their industrial counterparts, is greatly increased[138]. This holds true, particularly concerning the acquisition and analysis of sensitive information, through whatever means may be deemed necessary, in order to achieve critical business objectives as defined by a particular organisation. An example of this is the increased reliance on competitive intelligence processes within organisations. A further contributing factor to this motivation, in addition to the technological and competitive advantages gained from such an approach, may also lie in the acquisition of critical financial knowledge. The acquisition of such knowledge perhaps as part of information warfare directed economic or financial attack[139], which may be used for the purposes of manipulation, particularly concerning the global market place and its industries. This would have primarily targeted the economic outcomes of the entity itself or an adversary, largely from the network perspective – contained within the spatial forces paradigm – of the information society.

> The issue here is the possibility of using digital information networks to do harm in more direct ways—be it to the Internet infrastructure itself, to other infrastructures increasingly dependent on it (e.g., electricity, transport, and financial systems), or to other applications...In the past, a person had to be physically present at a key point to perform sabotage, as a trespasser, an insider, or

[136] Choo, C. Bontis, N. 2002. *The Strategic Management of Intellectual Capital and Organisational Knowledge* p 548.

[137] Du Toit, A. 2003. *Competitive Intelligence in the Knowledge Economy: What is in it for South African Manufacturing Enterprises?* p 111-120. *Precise page numbers could not be given as only the HTML version of the journal article was available; the original PDF document link was not functioning correctly.

[138] Tuomi, I. 2002. *The Future of Knowledge Management* p 72.

[139] Eriksson, E. 1999. *Information Warfare: Hype or Reality?* p 59-61.

> a combination of the two (legitimately passing perimeter defences but trespassing through dedicated inner defences). In [the] Network Society, these categories are translated to the logical (i.e., computer code) domain...The tendency toward technological monocultures is another enabler of cyber attack. The network economy tends to encourage "winner takes all" situations in markets with high IT content[140].

The motivations behind such activity may possibly extend even further to include political mandates, the targeting and manipulation of business deals for the benefit – dominantly in monetary terms – of certain entities who take advantage of increasingly networked globalised economic structures. This approach is particularly interesting to note from the network point of view, in addition to the vulnerabilities of the physical network itself, in combination with the technological paradigm of the information society – in terms of attack capabilities[141] – as this is a substantial shift away from those means of infiltration that would have been available – and thus would need to be protected against – for industrial society based attackers.

3.3.3 The New Knowledge Complexity

As has been outlined in the previous chapter, the social and economic contexts in the form of a shift to an information dominated world from an industrial based one where the "economic prosperity of this new system rests upon knowledge"[142] – although sharing many similarities and continuums with the past – have become far more interconnected and complex in nature. The advent of an information dominated society, has brought with it a vast array of elements which seek to make one's business more effective, faster acting and global in disposition[143].

---

140 Eriksson, E. 1999. *Information Warfare: Hype or Reality?* p 61.

141 Eriksson, E. 1999. *Information Warfare: Hype or Reality?* p 61.

142 Teece, D. 2003. Essays in Technology Management and Policy: Selected Papers of David Teece p 47.

143 This is achieved through the use of an array of technologies, business examples of which are: the adoption of cable and satellite television, computer-to-computer communications, personal computers, new office technologies such as online information services, word processors and cognate facilities allowing for a seemingly placeless connectivity. This allows one's business to be better integrated in the spatial sense by the use of advanced communication networks operating under the backdrop of an information dominated economy combined with an information orientated workforce, which is itself further proliferated and shaped through a mass media driven cultural experience of existence; as expressed in chapter 2's 5 information society forces. In the business context – operating in the knowledge economy – such topics are further actualised through what Davis, S. & Botkin, J 1994. *The Coming of Knowledge-Based Business* p 167-169, call the "six elements of a knowledge based business" in other words its characteristics, centred on the concept of exchanged learning through business practice, namely: 1. The more you use knowledge-based offerings, the smarter *they* get; 2. The more you use knowledge-based offerings, the smarter *you* get; 3. Knowledge-based products and services adjust to changing circumstances; 4. Knowledge-based businesses can customise their offerings; 5. Knowledge-based products and services have relatively short life cycles; 6. Knowledge-based businesses enable customers to act in real time.

This has been achieved through the productive use of information[144] to better meet those challenges posed by the knowledge economy, but carries with it the adverse side effect of increased vulnerability as well.

The frenetic nature of today's business environment[145] has therefore been shaped by numerous information society influences operating on an aggrandised scale. Apart from the dominant social influences and interactions as perceived by each force, the combination of all five – when applied to the economic context – makes for a business environment that is governed by a level of complexity through interaction, operation and the vastness of information flows that dominate its fundamental activities. This was not the case in industrial era interactions when taking perceived commodities of value into account. Knowledge driven complexity as a precursor to increased vulnerability in this instance, has therefore been enabled through the multitudinous array of channels that one's business operates in. This is defined by information flows, from cyber interactions to personal face to face communications both internally and externally; on a daily basis as outlined by the technological, economic, occupational, spatial and cultural forces of the information society.

For example, with the information society acting as a backdrop, the knowledge driven business of today has a heavy reliance on the intellectual abilities of its work force and their ability to communicate effectively within information driven contexts[146] making up part of the organisation's intellectual capital assets[147]. Such businesses need to operate in many different settings and markets around the world; interacting with one another and their relative customers and suppliers all in real time[148]. For businesses operating within the knowledge economy, intellectual capital is of the utmost importance as is the effective management of knowledge based assets in order to help leverage their competitive advantage[149]; assets which would have been of little relevance to industrial society based organisations.

---

144 Davis, S. & Botkin, J. 1994. *The Coming of Knowledge-Based Business* p 168.

145 Shapiro, C. & Varian, H. 1999 *Information Rules: A strategic Guide to the Network Economy* p1.

146 Bennett, J. 1986. Executive Priorities for Effective Communication in an Information Society p 13-22.

147 Brooking, A. 1996. Intellectual Capital: Core Assets for the Third Millennium p12-13.

148 Interaction in this instance is maintained through the use of robust information communication technologies and global information networks which support this form of advanced information exchange; taking place in a multitudinous spatially disparate business sphere.

149 It is important to remember that as Boisot, M. 1998. *Knowledge Assets: Securing Competitive Advantage in the Information Economy* p 70, outlines, there is a paradox of value which needs to be understood when it comes to effectively gaining competitive advantage from knowledge assets "EMI in the late 1970's nearly bankrupted itself trying to commercialise its CT scanner, one of the biggest advances in radiography since

Access to further knowledge in this instance has become available through an array of media sources in addition to business information processes. This has been projected through media, media technologies and cultural entities supported by the huge advancements that have taken place in the micro chip's processing capabilities[150] over the years. The underlying economic goals of such business are largely driven by their information work, where knowledge is transposed into tangible competitive advantage through continuous innovation cycles[151]. This in combination with the information society forces as touched upon in the previous chapter.

For the knowledge based organisation of today, operation within our current hyper competitive business environment has become a vastly more complex process than that of its predecessors some two to three decades ago[152]. From an information society perspective this becomes evident when considering the volume of information that today's knowledge economy based businesses must handle in their day to day operations. In this instance knowledge can be viewed as the most strategically-significant resource of the modern day firm[153], which in turn contributes greatly to organisational strategic decision making processes[154]; a significant shift away from industrial society thinking.

As has been discussed – when highlighting the importance of the relevant spatial forces as one of the defining factors of the information society in chapter 2, information flows within and between organisations have now reached a critical level of importance. With effective knowledge retention and management – amongst other aspects supported by the use of knowledge management systems[155] – in this instance seen as key in enabling the organisation to remain competitive within today's business environment. This is something that was most certainly not the case within industrial society management and its strategic processes.

---

the discovery of X-rays. It ended up ceding the market for scanners to General Electric and then quitting the business altogether. Clearly, competitive advantage does not flow automatically from the possession of Knowledge assets. A firm has to know how to extract value from them."

150 Webster, F. 2006. *Theories of the Information Society* p 9.

151 Nonaka, I. & Takeuchi, H. 1995. *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation* p 3.

152 Volberda, H. 1996. *Toward the Flexible Form: How to Remain Vital in Hypercompetitive Environments* p 359.

153 Grant, R. 1996. *Prospering in Dynamically-competitive Environments: Organisational Capability as Knowledge Integration* p 375.

154 Kim, W. & Mauborgne, R. 1998. *Procedural Justice, Strategic Decision Making, and the Knowledge Economy* p 323.

155 Maier, R. & Lehner, F. 2000. *Perspectives on Knowledge Management Systems – Theoretical Framework and Design of an Empirical Study* p 4.

> The present period of history has been characterised as the Information Age. In order to realise the maximum competitive advantage from information and knowledge, organisations need to have in place effective information and knowledge management systems. Such systems are necessary because the volume of information and knowledge available which must be processed by organisations has increased phenomenally. According to Chaleff (1995), information distribution and storage are growing out of control, becoming more disorderly and increasingly complex. Employees are being overwhelmed with information and knowledge to such an extent that it has become a burden[156].

In addition to the increased volume of information within the business context and the implementation of those processes and systems needed to handle it in a more effective manner, the organisation of today is one that is operating in an environment of greater dynamic competition[157], constant shift and large scale turbulence[158]. Thus adaption and timeliness of response – through the remodelling of knowledge resources leading to the generation of new ideas[159], in combination with adaptations in previously defined industrial management structures as a result of societal information shift[160] – have emerged as critical elements of competitive success within today's knowledge economy.

3.3.4 Knowledge Flow and the Implications for Organisational Vulnerability

Knowledge flows in combination with the general wide scale shift in traditional conceptualised approaches of value creation and the value of particular commodities – such as the effective application of knowledge in this instance – have resulted in organisations extending themselves in many new directions in order to cope with requirements. This is true particularly from a knowledge based perspective[161]. Vulnerability in this instance is therefore increased as organisations are dealing with a commodity – knowledge – that is easily transferable, highly valuable and is spread across many forms and dimensions of the

---

156 Soliman, F. & Youssef, M. 2003. *The Role of Critical Information in Enterprise Knowledge Management* p 485.

157 Grant, R. 1996. *Prospering in Dynamically-competitive Environments: Organisational Capability as Knowledge Integration* p 376.

158 Audretsch, D. & Thurik, R. 1999 *Entrepreneurship and Unemployment in theKnowledge Economy* p6 [Online].

159 *Davenport*, T. & Prusak, L. 2000. Working Knowledge: How organisations manage what they know p17.

160 *Drucker*, P. 1980. *Managing in Turbulent Times* p 225-228. As Drucker outlines, in addition to these, such requirements for management shift should be viewed particularly in light of economic, monetary and socio political influences in combination with the spatial economic restructuring of the global economy; viewed from within a period of early, yet increasingly prevalent shifts towards a definable knowledge economy.

161 *Grant*, R. 1996. *Toward a Knowledge-Based theory of the Firm* p 110.

organisation in its day to day operational activities taking into account aggregation, appropriateness and acquisition[162]. The number of parties who come into contact with such knowledge through its flows is thus substantially increased from that of industrial society business interactions where the level of complexity and reliance on knowledge was far less.

In today's knowledge economy, organisations use their gained and self generated knowledge to attain competitive advantage through knowledge flow[163] and innovation. This is due to compressed product and service life cycles[164], where organisations are increasingly reliant upon the intellectual abilities of their work force with a focus on intellectual capital[165]. These are elements which are of great value to information seeking competitors. The volume of information that needs to be dealt with by organisations in their day to day activities has thus increased significantly[166]. This has forced organisations to employ new processes and technologies to handle the growing demand[167], thus further increasing the possibility of information exposure through newly defined channels of flow and communication. Examples in this instance being the infiltration of information communication networks and the communicative activities of employees outside the boundaries of the firm; or once those employees have left the firm altogether[168]. In addition to these channels of knowledge flow, organisations also access and project information through a variety of public media based forms, technologies and culturally defined constructions. An expression of media projection and information acquisition can be seen in the targeting of competitor websites by organisational competitive intelligence professionals, making use of advanced search and categorisation technologies.

> Traditionally, Competitive Intelligence (CI) relied upon published company reports and other kinds of printed information. In recent years, [the] Internet has rapidly become an extremely good source of information about the competitive environment of companies and has been reported by a Futures Group survey in 1997 to be one of the top five sources for CI professionals...CI Spider [an Internet

---

[162] *Grant*, R. 1996. *Toward a Knowledge-Based theory of the Firm* p 111-112.

[163] *Borghoff*, U. & Pareschi, R. 1997. *Information Technology for Knowledge Management* p 836.

[164] *Kandampully*, J. & Duddy, R. 1999. *Competitive Advantage through Anticipation, Innovation and Relationships* p 51.

[165] *Cortada*, J & Woods, J. (eds) 1999. *The Knowledge Management Yearbook 1999-2000: 1999-2000* p 126.

[166] *Edmunds*, A. & Morris, A. 2000. *The Problem of Information Overload in Business Organisations a Review of the Literature* p 18.

[167] *Edmunds*, A. & Morris, A. 2000. *The Problem of Information Overload in Business Organisations a Review of the Literature* p 20-21.

[168] *Borghoff*, U. & Pareschi, R. 1997. *Information Technology for Knowledge Management* p 835-838.

> search spider developed for such purposes] accepts as input the URLs the user specifies, and follows the embedded Web links to search for user-specified keywords. After collecting on the fly a certain number (user-definable) of Web pages, CI Spider performs further text analysis to extract noun phrases from these pages. These noun phrases represent a list of key topics covered on the Web sites of interest[169].

As has been established, in the knowledge driven economy, the economic dependence of one's organisation – and therefore that of one's competitors as well – rests substantially upon knowledge's effective use and application. This has been extrapolated through newly defined management structures and processes; knowledge management and knowledge management systems being examples of this. Through daily interaction with such knowledge – as part of the operational processes of the current business system – it is fair to say that the potential vulnerability posed towards one's knowledge assets therefore also substantially increases. This can be seen in the difficulties of securing a largely intangible asset, knowledge, and preventing it from being passed on to one's competitors through varying channels of flow. This is true particularly from a human nature and interaction perspective as is expressed in the following extract.

> Knowledge is also difficult to protect because *it is difficult to detect its expropriation, or illegal imitation*. For one, unlike most tangible assets, knowledge is inherently mobile... Similarly, knowledge about a manufacturing technology or a new product in development is accessible to the workers and managers involved, while final products can be observed by any buyer. In addition, knowledge is a public good (Arrow, 1962); one item of knowledge can be used by many individuals or organizations at the same time, without diminishing its productivity for any one user. Thus, illegal use of knowledge can be very difficult and costly to detect...In this case, if one member of a knowledge production team can obtain and absorb the knowledge of other team members, she has an incentive to expropriate that knowledge for her own use or to 'leak' it to competitors, eliminating the monopoly on that knowledge that the team might otherwise possess. In other instances, knowledge will require 'complementary' assets to be commercialized, such as manufacturing equipment or marketing expertise (Teece, 1986). Here, the owner of the proprietary knowledge must typically exchange it with the owner of the complementary assets for commercialization to proceed. For example, a scientist must reveal some of his research findings to a venture capitalist to obtain

[169] Chen, H. & Chau, M. et al. 2002. CI Spider: A tool for competitive intelligence on the web p 1-2.

> funding for development research. Again, there is an opportunity for the owner of the complementary asset to expropriate the knowledge for her own use and benefit[170].

What should be clear is that in order for the organisation to remain competitive and operate effectively within today's unstable knowledge driven context, such an organisation needs to have in place sustainable knowledge processes. These processes need to be enabled through the adequate retention and protection of highly critical knowledge and the sanitisation of publically available projected knowledge. Business counterintelligence can in this instance act as an enabling factor – in order to fulfil these objectives – and must be linked firmly with the strategic business processes of the organisation. This should be done in order to help ensure that critically available knowledge can be dealt with and utilised in a timely and effective manner while at the same time is not lost to the prying eyes of those who wish to possess it for their own advantage.

3.4 The Rise in Importance of Business Counterintelligence

In conclusion, with the above elements in mind, I will now engage with the final part of this analysis by examining why business counterintelligence should be considered of importance for today's organisations. This will once again be undertaken through engagement with those peripheral yet fundamental elements as dealt with throughout this examination. Analysis through contra-indication of the main elements can once again be taken as a given form of scrutiny in this instance, one which I will refrain from elaborating on in extended detail. I will therefore begin this final part of the analysis by examining those dimensions of occurrence that should be considered of importance, for the increased prominence of business counterintelligence within today's organisations.

Given the points which have been discussed thus far, perhaps the most obvious occurrence of shift in this context – that has lead the economic and social systems into a new complex dynamism of knowledge flow[171] – is the interest in and adoption of knowledge assets[172] and the interchange and feedback of this knowledge[173]. This is expressed through differing informational channels across diverse spatial backgrounds. The impacts of such shift, in terms of the restructuring of the social and economic conception, have meant that the

[170] *Liebeskind*, J. 1996. *Knowledge, Strategy, and the Theory of the Firm* p 96-97.
[171] *Boisot*, M. 1998. *Knowledge Assets: Securing Competitive Advantage in the Information Economy* p 20.
[172] *Boisot*, M. 1998. *Knowledge Assets: Securing Competitive Advantage in the Information Economy* p 70.
[173] *Boisot*, M. 1998. *Knowledge Assets: Securing Competitive Advantage in the Information Economy* p 20.

fundamental basis upon which industrial era security acceptance and practice has been based up until now no longer applies. This is evidential, particularly when viewed from an information security perspective and the complexity that has been added as a result of the increased proliferation of the digital information processing and networked business environment that challenges today's organisations.

> The requirements of information security within the organisation have undergone two major changes in the last several decades. Before the widespread use of data processing equipment, the security of information felt to be valuable to an organisation was provided primarily by physical and administrative means. An example of the former is the use of rugged filing cabinets with a combination lock for storing sensitive documents. An example of the latter is personnel screening procedures used during the hiring process...With the introduction of the computer, the need for automated tools for protecting files and other information stored on the computer became evident. This is especially the case for a shared system, such as a time-sharing system, and the need is even more acute for systems that can be accessed over a public telephone network, data network, or the Internet...The second major change that affected security is the introduction of distributed systems and the use of networks and communications facilities for carrying data between terminal user and computer and between computer and computer[174].

As we have seen, up until a few years ago counterintelligence activity was largely limited to operations conducted within the spheres of government and military intelligence with particular attention given to the protection of government and military based knowledge goals[175]. Little attention was therefore given to intelligence and counterintelligence activities targeting the economic arena or by those organisations operating within this economic arena themselves. An example of this is Cold War military targeting conducted by the KGB[176]. Since then however much has changed, with shifts taking place in both the perceived economic emphasis of governments and their organisations particularly from an intelligence gathering point of view. This is expressed in the following extract concerning the Post-Cold War Russian intelligence gathering focus of today:

> I believe that it is necessary to adjust the structure and goals of the intelligence services directing their efforts to back Russia's economic interests in the first

[174] *Stallings,* W. 2006. *Cryptography and Network Security: Principles and Practice 4th ed* p 7-8.

[175] *Cornel* C. 2007. *The Military Security System – Present and Perspective* p79-80.

[176] *Mellon,* J. 2001. *Assessment of KGB's Intelligence-Gathering Successfulness in the West During the Period of 1954 to 1991* p 6.

> place. I will demand that more effort be applied immediately in the following specific fields: to ensure an uninterrupted monitoring of the situation on the world markets of armaments, aviation and space equipment and to search for information on existing or developing technologies in the design of new armaments; to search for new designs in commercial technologies, both by state-run and private enterprises; to search for critical information on the plans and activities of the leading international financial institutions, major transnational corporations, banks and investment companies of all countries of the world; to organize information campaigns in foreign countries to attract more investment in the Russian economy. I believe it is necessary to allow the intelligence services to cooperate with major domestic production and financial enterprises of any form of property. The experience of France, Germany, Japan and China has proved the efficiency of cooperation for raising the competitiveness and technological potential of the domestic economy. These are the issues that I want to handle within the Security Council through coordinating the resources that already exist in the key financial and economic structures of the state[177].

What becomes clear is that the defined intelligence gathering parameters of the business context were largely based on a very different set of principles and security mechanisms. As has been established, the industrial based business environment was one that was also far less turbulent[178] in terms of the levels of connections that organisations had with others, the pace at which things were done and those levels of competition and innovation. For organisations this occurred both internally and externally within a global economic setting.

The acquisition of business secrets in this instance largely took place on an industrial espionage level conducted perhaps by a competitor, member of one's own organisation or criminal who sought such secrets for their own personal or national gain[179] , the impact of which in most cases would have been fairly limited. The lack of input was perhaps due to a lack of globalisation, less integration of advanced media and communication technologies and far less reliance on intellectual capital assets. Form this point of view it is fair to say that the idea that other countries or disparate competitors would target one's organisation within the industrial context, in the advanced manner that such activities are conducted today[180],

---

177 *Joyal,* P. 1996. *Industrial Espionage Today and Information Wars of Tomorrow* P 8.

178 *Borrus,* M. & Zysman, J. 1997. *Globalization with Borders: The Rise of Wintelism as the Future of Industrial Competition* p29.

179 *Samli,* A. & Jacobs, L. 2003. *Counteracting Global Industrial Espionage: A Damage Control Strategy* p 96.

180 *Podbregar,* I. 2006. *Some Patterns of Industrial Espionage* p 326-323.

would in most cases not have been part of the referential framework of the majority of industrial business security professionals.

Many of the advanced intelligence gathering techniques were in the industrial economic modus still situated within the realms of Cold War intelligence services; particularly those of the KGB. After the breakdown of the Union of the Soviet Socialist Republics (USSR) and the dismantlement of the KGB, many Soviet agents had to find a new field to apply their trade in, that field being the private security industry primarily servicing the business sector[181]. Such economic intelligence activity was not however merely limited to the services of former Soviet Union agents or Russia's new intelligence service alone. There are a varying number of global intelligence services[182], realigning their intelligence focus in support of newly emerging economic objectives that have since arisen as part of today's informational shift.

In the knowledge society such shifts in the focus of intelligence services have meant that security threats faced by the organisation of today are far more sophisticated than they once were. Businesses operating within the current context of global economic competition have thus become targets of advanced intelligence acquisition, whose biggest risks come from those competitors operating within this globalised business environment. These competitors are often supported by their broader national intelligence agencies, who have developed a keen interest in the economic success of their national business operations.

Organisations competing within the business environment of today thus need to have in place effective strategies and tools in order to help protect against the advanced intelligence gathering activities of their counterparts. However, even with this context in mind, there still remain those organisations that are absorbed with industrial era methodologies of security practice, which rely on these as the basis of their security operations[183]. This can be an arduous approach to follow, especially when trying to retain competitive advantage reliant upon intangible knowledge assets. The relevance of an intelligence function for today's organisations can therefore be seen as important, particularly from an intelligence gathering perspective with business counterintelligence forming an essential part of such operations. This can be thought of in terms of the informational feedback which it provides, with the reliance on gathered and processed information seen as an essential part of the decision

[181] *Podbregar,* I. 2006. *Some Patterns of Industrial Espionage* p 324.

[182] Joyal, P. 1996. *Industrial Espionage Today and Information Wars of Tomorrow* p 3-12.

[183] *Whitehead,* S. 2001. *The Counterintelligence Page: Part 1* p 32.

making process. The value of which has been recognised within the military sphere for many years.

> The military has extensive experience in collecting and analysing information and making decisions based upon the intelligence produced...The organisation needs a business intelligence gathering capacity in order to recognise that it is a target of intelligence gathering, know how to react, and be able to analyse who the intelligence gatherer is. It may be a competitor, a government agency, or an attacker with criminal intent. The intelligence operation may be undesired but legal and as a target in a business intelligence operation one should be able to respond with a planned strategy[184].

What this means for the organisation of today – besides potentially devastating monetary losses[185], is that targeted exogenous intelligence gathering, if left unchecked, may lead to the severe degradation of an organisations competitive knowledge driven capacity. Business counterintelligence and those relevant protection and mitigation aspects that accompany it should therefore be considered important tools for the organisation when attempting to deal with security threats of an intelligence orientated nature. Varied competitive entities may choose to orchestrate intelligence gathering activities across multitude channels of attack at any given time, in the attempted acquisition of one's critical knowledge in order to achieve their relative business and economic intelligence gathering objectives. Thus, in order to mitigate such risk, one needs to have in place effective tools that will allow one's organisation to remain competitive within the globalised business environment in combination with a firm level of understanding of the issues at hand.

In the light of this context, traditional security approaches of the past are therefore no longer adequately positioned to cope with such sophisticated forms of attack. In order to defend one's sensitive knowledge assets, one therefore needs to have in place concrete, up to date security practices that will allow one to effectively deal with the challenges posed by intelligence gathering and espionage activity within the knowledge economy. This does not simply mean implementing an isolated information or physical security function alone, or expecting that the implementation of some form of encryption software is going to be enough to deal with advanced intelligence gathering techniques. Rather, in order to safeguard one's organisational knowledge more effectively, a consolidated deployment of countermeasures,

---

[184] *Hutchinson*, W. (eds). 2002. *Business Intelligence Gathering* p 10.

[185] *Kitfield*, J. 2007.*Espionage the Sequel* [Online].

all interacting and providing feedback to one another are needed so as to better able to deal with threats directed towards one's organisation[186]. This deployment encapsulated under the umbrella of consolidated business counterintelligence operations.

The organisation of today therefore has to realise that if value is placed upon its sustainable business processes, then considering a more comprehensive knowledge protection approach, through the use and implementation of a business counterintelligence strategy, is of importance. Just as physical security and screening mechanisms have been used in the past industrial society based context[187], so to should the organisation of today consider business counterintelligence of importance. This should be thought of as part of the natural progression of security practices in order to help quell the many challenges posed by the complex and rapidly evolving business environment of today.

[186] This is not to say that the combined implementation of security measures will allow for the complete protection of one's critical knowledge, particularly if facing an attack from an advanced intelligence gathering source such as that of a government intelligence agency. But what it will do is allow one's organisation to mitigate a large percentage of the risk involved by making one aware that such intelligence gathering activities are being undertaken and therefore allowing one to deploy targeted strategies to quell or manipulate such intelligence gathering efforts; through the use of counterintelligence techniques such as appropriately directed misinformation.

[187] *Stallings*, W. 2006. *Cryptography and Network Security: Principles and Practice 4th ed* p 7-8.

Chapter 4 – Section 2

A Proposed Broader Definition of Business Counterintelligence

4.1 Introduction

The primary objective of this chapter will be to investigate how multitudinous business counterintelligence practices and methodologies can best be applied and understood from the perspective of variable organisational contexts. The purpose of this will be to render greater meaning for the organisation through effectively integrated protection practices. This will be done by examining the most applicable forms of business counterintelligence, filtered through appropriately selected risk management process structures. This will be discussed in conjunction with the operational security/counterintelligence process, acting as a structural framework of process driven implementation.

Before one can commence with the main objective of this chapter however, one firstly needs to construct a consolidated definition of what business counterintelligence is, derived from the literature. Secondly, one also needs to clarify the structural relationship that exists between information security and business counterintelligence, as there often exists a great deal of associated confusion in this regard, particularly when protection practices are viewed from a singularly based information security point of view. I will therefore begin this section of analysis by offering a consolidated definition of business counterintelligence and by briefly examining information security in relation to business counterintelligence. The latter will be examined from a structurally comparative point of view and the significance that this holds for the organisation in terms of its defined protection capabilities.

4.2 Defining Business Counterintelligence

In order to further solidify one's understanding of the concept business counterintelligence, I will now develop a definition of what business counterintelligence should mean, from a business perspective, within the context of this thesis. This will be accomplished by

examining a few carefully selected workable definitions that are currently explicit within the literature; as variations are abundant. These definitions can be seen as follows:

> (1) Counterintelligence, properly understood, aims to engage and neutralise a competitor's collection efforts through a variety of imaginative, flexible and active measures[188].
>
> (2) Counterintelligence...[deals] with intrusions that are neither illegal nor unethical. Whilst it can use barriers to prevent an exodus of information, they must be placed in company procedures and in the minds of staff, not across the entry points to sites[189].
>
> (3) Counterintelligence is the protective multi-layered *shield* that hides your weaknesses from those who, by knowing them, can benefit at your expense. It is also used to limit the exposure of your strengths to those who ought to know them. It is the ongoing defensive process by which an organisation "looks inward through the lenses of the adversary" to block its exposure to economic, cyber and industrial espionage, talent defections, fraud, terrorism, hacking, negligence, over-disclosure, illicit acquisition of proprietary information and other security risks[190].
>
> (4) As Competitive Intelligence is more widely integrated into corporate research and planning, so too is the practise of counter-intelligence - that is, safeguarding your company's data from intelligence efforts by other firms, either legally or illegally[191].
>
> (5) Counterintelligence...is actions taken to counter enemy intelligence, espionage or sabotage[192].
>
> (6) Counterintelligence deals with offensive and defensive activities to neutralise the effectiveness of foreign/hostile intelligence operation; to protect sensitive information; and to counter subversion, sabotage and terrorism directed against personnel, strategic installations and material[193].

---

188 Nolan, J. 2001. *Confusing counterintelligence with security can wreck your afternoon* p 53.

189 West, C. 2001. *Competitive Intelligence* p 184.

190 Martin, A. 2002. *Harnessing the Power of Intelligence, Counterintelligence and Surprise Events* p 79.

191 Miller, H. 2001. *Competitive Intelligence - An Overview* p 12.

192 Fleisher, C. & Blenkhorn, D. (eds) 2001. *Managing Frontiers in Competitive Intelligence* p 251.

193 South Africa. 1995. *Government White Paper on Intelligence* [Online].

(7) Counterintelligence's mission is to protect the entire entity – whether government or corporate – from outside or inside harm[194].

As one can see from the above definitions there is some diversity in expression concerning the relevant scope of counterintelligence, fragmentation and the role that it should play as a business entity. From a standpoint of dissimilarity, definition (2) promptly states that counterintelligence "[deals] with intrusions that are neither illegal nor unethical". However, definitions (4-6) contradict this statement. Firstly, in the case of definition (4) by stating that counterintelligence is concerned with both legal and illegal methods of intelligence gathering. Secondly, in the case of definition (5) that counterintelligence is concerned with espionage and sabotage. Thirdly, in the case of definition (6) that counterintelligence is concerned with the neutralisation of foreign/hostile intelligence operations, countering subversion, sabotage and terrorism; bearing in mind that this last form of the definition concerning intelligence gathering and counterintelligence is taken from a government orientated viewpoint.

Furthermore, definition (1) states that counterintelligence aims to "neutralise a competitor's collection efforts through...active measures". This is in contradiction to definition (3), whereby it is stated that counterintelligence should be conceived of as an "ongoing defensive process". From a standpoint of similarity, definitions 1, 3, 5, 6 and 7 all place a level of emphasis on the actions of an adversary in attempting to gain intelligence about one's organisation; in whatever form that organisation may take.

Finally, definition (1), although useful in the sense of highlighting the need for the use of active measures, is limited in that it does not include the use of passive measures in this regard. Definition (2), although highlighting the importance of the integration of business counterintelligence, is flawed in that it views counterintelligence as only concerned with legal intelligence gathering; which in today's globalised context is simply not the case. Definition (3), while highlighting some very important aspects of counterintelligence – the examination of one's organisation through the lens of an adversary being an example of this – is still not complete as it does not take into account active counterintelligence measures. Definition (4), while alluding to the importance of the relationship that exists between competitive intelligence and counterintelligence, is still limited in its conceptualisation as it views one's adversaries as existing only on a purely inter-organisational level. Definition (5) is slightly limited in that it does not specify what kind of enemy intelligence activity it is referring to.

[194] Sulc, L. 1997. *Law Enforcement Counterintelligence*. As cited in Whitehead, S. 2001. *The Counterintelligence Page: Part 1* p 32.

Definition (6) is rather comprehensive in its inclusion of counterintelligence activity; however the terminology it makes use of in this regards is not completely applicable to the business environment. Finally, definition (7), although summing up the core structural role of counterintelligence nicely is a little vague in its completeness, in so much as it does not make any firm statement as to how one may go about achieving this.

Granted, some of these definitions are intended for use in the military/government intelligence spheres and may therefore be somewhat different in their intention. However I feel that these definitions are still applicable and useful to the business context as DeGenaro states "the business of intelligence has been the purview of governments and a necessary part of statecraft for centuries – that's where the knowledge resides[195]". Thus, based on this analysis, one may offer a consolidated definition of business counterintelligence as follows:

> Something which supports the business intelligence process of the organisation, through the protection, retention, contribution and use of business knowledge, by following internalised offensive and defensive ethical procedures, to adequately engage with and neutralise harmful or potentially harmful activities, whether conducted against the business internally or externally, by legal or illegal means or by foreign or local hostile entities; with the concernment of one's knowledge.

Now that business counterintelligence has been defined in a consolidated form, one can now continue further with an examination of how business counterintelligence relates to information security. One can then proceed to discuss the role of business counterintelligence within organisations and the implications of a consolidated definition of business counterintelligence for different organisations.

4.3 Information Security vis-à-vis Business Counterintelligence

Security practices and the protection mechanisms that accompany them are often surrounded by a great deal of confusion, particularly due to user created expectations and the psychological barriers that these expectations manifest[196]. Apart from the self created user based conceptualisation of security solutions alone[197], further confusion can arise when it comes to the level of protection that a particular security strategy or entity may supply and

---

[195] DeGenaro, B. 2005. *A Case for Business Counterintelligence* p 14.

[196] Dourish, P. & Grinter, R. et al. 2004. *Security in the wild: user strategies for managing security as an everyday, practical problem* p 394-395. In this instance viewed from within a technologically dominant networked orientation space.

[197] Dourish, P. & Grinter, R. et al. 2004. *Security in the wild: user strategies for managing security as an everyday, practical problem* p 395.

how far each strategy should go in order to protect one's organisational knowledge assets[198]. This is often the case where *online/offline* security interaction is involved, thus potentially leading to a reduction in the effectiveness of security elements framed through a user based problem contextualisation[199]. Aside from this, there are many other areas of security practice where confusion can arise, due to an incomplete understanding of the larger strategic significance of the implemented security approaches chosen[200]. Structurally based functional confusion for example, is particularly relevant concerning the interaction, implementation and perceived relationship that exist between information security and its practices[201] and that of the role, responsibility and dominance[202] of business counterintelligence.

This limited understanding may therefore compromise the effectiveness of an organisations protection strategy, due to the variably ranging levels of applied security elements that may be adopted by differing organisational entities. The realm of computer security[203] application is an example of this, which in turn creates potential deficiencies in organisational wide implementations of broader security measures[204]. Such analysis will therefore aim to better clarify the role and applicability of information security within the larger integrative business counterintelligence context[205], thus helping to ensure a more securely defined and understood business protection environment.

---

198 As was outlined in a discussion with Meijer, H. & Meijer, F. 2007. *Personal Communication*, who are corporate information security professionals working in the Netherlands and South Africa; with 29 years experience between them.

199 As Dourish, P. & Grinter, R. et al. 2004. *Security in the wild: user strategies for managing security as an everyday, practical problem* p 395, states: "In other words, what we see from our observations is that, for everyday users, security is not purely an online matter; it extends into the physical world. The information which is to be protected, the resources to be managed, and the work to be carried out all exist in a physical setting too. Security practices may draw on the arrangement of technical resources and, again, providing people with technical solutions that cannot be understood or integrated into what people see as the "whole problem" will reduce their effectiveness".

200 Anderson, J. 2003. *Why we need a new definition of information security* p 313.

201 As Hansche, S., Berti, J. & Hare, C. 2004. *Official Guide to the CISSP Exam* p v-ix, list: information security deals with areas of Management; Access and Control; Applications and Systems Development; Operations Security; Cryptography; Physical Security; Telecommunications, Network, and Internet Security; Business Continuity Planning; Law, Investigations, and Ethics.

202 As was outlined in a discussion with Meijer, H. & Meijer, F. 2007. *Personal Communication*.

203 Often used as a synonym for information/information systems security.

204 Pfleeger, C. & pfleeger, S. 2003. *Security in Computing* p 3.

205 As Raval, V & Fichadia, A. 2007. *Risks, Controls and Security* p 25-56, note: as with the relationship between information security and internal control, although such concepts can be discussed in a separate manner in a theoretical sense, in practice these and other areas of security, measures and understandings are invariably linked in their application within the organisational context.

4.3.1 Defining Roles and Responsibilities

As is stated above, business counterintelligence can be defined as: something which supports the intelligence process of the organisation, through the protection, retention, contribution and use of business knowledge, by following internalised offensive and defensive ethical procedures, to adequately engage with and neutralise harmful or potentially harmful activities, whether conducted against the business internally or externally, by legal or illegal means or by foreign or local hostile entities; with the concernment of one's knowledge. The emphasis in this instance therefore rests within the broader intelligence scope, governed by strategic means, whereby the focus of such activity firmly depends upon the intelligence gathering intentions of one's adversaries and the intelligence functioning of one's own organisation.

Information security on the other hand is primarily concerned with those aspects relating to effectively implemented information architectures, focused around components such as policy, training, compliance, baselines, risk assessment and organisational infrastructure[206]. Each of these components can then be broken down further into particularly focused sub-areas of concern. Such sub-areas, relating to attack include: corporate and government insiders; foreign and domestic business competitors; intelligence agents and hackers with a goal of carrying out malicious activities such as corrupting or deleting data, gaining access to sensitive data and selling information[207]. Thus in this instance focus is given to policy and procedure with an emphasis placed on the identification of vulnerabilities and the mitigation of these vulnerabilities where data and informational flows may be targeted. Usually communicated over and stored on, but not limited to[208], Internet orientated information communications technologies and databases. Protection elements implemented in this instance are done for the security of such systems, in order to ensure the achievement of the commonly themed information security management objectives[209] of confidentiality, integrity and availability.

---

[206] Killmeyer, J. 2006. *Information Security Architecture: An integrated Approach to Security in the Organisation* p xxi.

[207] Killmeyer, J. 2006. *Information Security Architecture: An integrated Approach to Security in the Organisation* p xvii.

[208] Peltier, T. 2002. *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management* p 177.

[209] As Killmeyer, J. 2006. *Information Security Architecture: An integrated Approach to Security in the Organisation* p 1, states: "Security management seeks to establish controls and measures to minimize the risk of loss of information and systems resources, corruption of data, disruption of access to data, and unauthorised disclosure of information. Security management is achieved through effective policies,

With these points of view forming a contextual basis, information security, although sharing many similarities in terms of its information protection objectives[210] with that of business counterintelligence[211], is ultimately entrusted with the passive preservation and assurance of an organisation's information flows and storage[212]. Security mechanisms in this instance are enabled through the implementation and evaluation of predominantly physical and logical security measures[213]. These help to reduce vulnerability and thus opportunity for threat based infiltration. Such activities are largely conducted in line with an organisations business orientated objectives and goals[214], with the aim of preventing unsolicited access to the information flowing and stored within the organisation and its information systems.

---

standards, and procedures that will ensure the confidentiality, integrity, and availability of corporate information, applications, systems, and networks for authorized users only". A similar mention of these concepts can also be found in Hansche, S., Berti, J. & Hare, C. 2004. *Official Guide to the CISSP Exam* p 3-4, whereby they state: "Information Security Managers must establish and maintain a security program that ensures that three requirements: the availability, integrity, and confidentiality of the organization's information resources. These are the three basic requirements of security management programs." As the authors go on to state, such requirements are met largely through the implementation of physical controls, technical controls and administrative controls. It should also be noted however that as Anderson, J. 2003. *Why we need a new definition of information security* p 308, states: "What is information security? Is it, as one would have to conclude from a broad survey of published material, all about Confidentiality, Integrity and Availability (CIA)? There may be no one who says, "information SECURITY (INFOSEC) =CIA." Certainly, INFOSEC=CIA cannot be true in the canonical sense. To measure INFOSEC, one must measure the elements of CIA; measurements that are elusive. The bottom line is that we do not have generally accepted measurements of confidentiality, integrity and availability, other than the raw count of damaging incidents along with tenuous estimates of the damage. When the number of damaging incidents drops due to an effective INFOSEC program, the measurement problem increases."

210 As Peltier, T. 2002. *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management* p 1, states: "The purpose of information protection is to protect the valuable resources of an organisation, such as information, hardware, and software. Through the selection and applications of appropriate safeguards, security helps the organisation to meet its business objectives or mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets. We examine the elements of computer security, employee roles and responsibilities, and common threats [to these]. We also examine the need for management controls, policies and procedures, and risk analysis. Finally, we present a comprehensive list of tasks, responsibilities, and objectives that make up a typical information protection program."

211 An example being the implementation of physical barriers from an information security perspective to prevent direct access to a firms information system while also, from a counterintelligence perspective, ensuring the prevention of access to the firm, its technology, knowledge, information and people; an information system being one component of this.

212 Peltier, T. 2002. *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management* p 178.

213 Raval, V. & Fichadia, A. 2007. *Risks, Controls and Security* p 55.

214 Peltier, T. 2002. *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management* p 1-3. In addition as Raval, V. & Fichadia, A. 2007. *Risks, Controls and Security* p 14, also state: "The business structure shapes the information system it relies on for producing relevant information, and the business processes are mirrored in the information systems of the firm. How a business generates and uses information depicts how the business is run and how it is controlled."

Information security can therefore be thought of as "a well-informed sense of assurance that information risks and controls are in balance"[215]. This understanding limits confusion and those flaws associated with other information security definitions[216]. Business Counterintelligence, due to its greater strategic alignment, can thus be categorised as a protection entity that is largely concerned with the strategic security focus of the organisation as a whole. In this instance linked to its intelligence processes, whereby it acts as the meta-security element in this regard[217] with the aim of identifying and engaging competitive threats.

---

[215] As Anderson, J. 2003. *Why we need a new definition of information security* p 309-310, states: "We have definitions of 'computer security' or 'information security' suggesting that security is a process, or that it attempts to do things, or that it rests on important concepts, or that important things rest on it, or that it is concerned with certain things. I believe these don't really precisely define anything. Yet we need a definition for this important concept...The result of this confusion: when you are in charge of – or your organization is paying millions to get – something that is not very well defined, you may have a problem...I propose the following definition of enterprise information security: *A well-informed sense of assurance that information risks and controls are in balance.* This definition solves many important problems inherent in other definitions. It does not conflict with any of them or define away important aspects of security. It is not an unattainable absolute or ideal. Significantly, this definition brings out the important concept of assurance. The dimension of assurance is already a blind spot in many [information security] programs and needs more attention by CISOs [Chief Information Security Officers]. But most importantly for our profession, a discussion around an objective definition of 'information security' cannot help but further the general state of information security inside our large organizations."

[216] Further definitions of information security and their flaws as mentioned and discussed by Anderson, J. 2003. *Why we need a new definition of information security* p 309-310, are as follows: "Matt Bishop in his new text, states, "computer security rests on confidentiality, integrity and availability." While we might agree that computer security 'rests' on CIA, a lot of other things could also rest on CIA. This is the closest Bishop comes to defining the subject of the title of his prodigious book. Tom Peltier, another well known author and teacher in INFOSEC, states that, "Information security encompasses the use of physical and logical data access controls to ensure the proper use of data and to prohibit unauthorized or accidental modification, destruction, disclosure, loss or access to automated or manual records and files as well as loss, damage or misuse of information assets". Again, we do not quite get a definition. Rather, here is a description of what computer security does. But if it's done, do you have, at that point, security? Are you more or less secure? Another authoritative text offers another near definition: "Computer security attempts to ensure the confidentiality, integrity, and availability of computing systems' components." Here, it is the attempt that matters. There is no intrinsic concept of completeness or precision in this definition. Of course, there are many activities performed inside traditional IT departments, such as testing protocols that contribute significantly to integrity, which are covered by this definition yet would not be included by most observers in the group of functions known as 'information security' These near-definitions of information security all share at least one problem: they are so broad as to inadvertently encompass activities that almost everyone would agree do not belong as part of 'computer security' or 'information security'. This breadth problem mirrors what many INFOSEC managers struggle with every day inside their own organizations: lack of definition of the clear 'turf' of information security. We need a definition that helps as much to identify what information security is not as well as what it is. In his cornerstone book *Computer-Related Risks*, Peter Neumann, computer scientist, author and long-time moderator of the well-known ACM Risks Forum, writes that the term computer security "implies freedom from danger, or, more specifically, freedom from undesirable events such as malicious and accidental misuse. Security is also a measure of how well a system resists penetrations by outsiders and misuse by insiders." Later, Neumann admits that, "there is never an absolute sense in which a system is secure or reliable"."

[217] As Whitehead, S. 2007. *Personal Communication*, states: "information security, personnel security, document security, communications security, awareness briefings, security education, etc are all a subset of counterintelligence and intelligence (the other side of the counterintelligence coin). Information security is [thus] a part or subset of counterintelligence...In the modern world information security refers to the

> Counterintelligence is anticipatory and business-orientated. It aims to engage and neutralize a competitor's collection efforts through a variety of imaginative and active measures. Security, on the other hand, seeks to protect a firm's assets by a combination of policies, procedures, and practices. In summary, security is aimed at *reducing corporate vulnerability*, while counterintelligence and countermeasures are aimed at *reducing a competitive threat*[218].

This point of view is further supported by the military driven perspective of counterintelligence in relation to information security. From this perspective counterintelligence is viewed as an intelligence objective that assists in protecting friendly forces, through the use of active and passive measures intended to disaffirm one's enemy's valuable information about the friendly situation. This helps to deny intelligence to the enemy and plan appropriate security measures[219], controlling and mitigating an identified threat. Counterintelligence in this context plays an active role in the support of strategic security elements such as military security, operations security, information security and counter-reconnaissance[220] with the aim of serving the greater strategic intelligence objective. This is displayed in the following extract taken from the United States Marine Corp's handbook *Counterintelligence*, which outlines the responsibility of information security within the military and discusses counterintelligences supporting role in relation to military information security practices and objectives.

> The INFOSEC [information security] program – a responsibility of the unit's security manager – includes a proper security classification determination being made with applicable security regulations and the proper protection being afforded to the material throughout its life cycle. These measures include proper preparation, reproduction or manufacturing, storage, use, and destruction. Failure to comply with required INFOSEC measures exposes sensitive information to

---

information technology side of things...There are usually a number of policies and procedures dealing with these issues and they are normally standard and do not change a lot. Counterintelligence deals specifically with the actions of competitors or adversaries in the corporate environment and in the national security or government environment, with the actions of other governments and their specific intelligence actors. The counterintelligence focus in the corporate environment must be on information of critical importance to the firm's strategies and operations...that if compromised, would degrade organisational effectiveness [and] shorten the expected life of a critical business programme or alter the firm's direction."

[218] Fleisher, C & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 49. These broader *threats* and *vulnerabilities* should not be confused with the functional identification of threats and vulnerabilities that the two functions perform as part of their day to day activity. In this instance *threats* and *vulnerabilities* should be contextualised with reference to the broader strategic security operations of the two functions respectively.

[219] U.S. Marine Corps. 2007. *Counterintelligence* p 1.

[220] U.S. Marine Corps. 2007. *Counterintelligence* p 8-10.

> potential compromise. The rapid advancement of the microprocessor and the maturity of computer age technologies have presented a significant new area of exposure that leave us particularly vulnerable... Information system vulnerabilities include denial of service, information theft, information replacement or introduction of false data. Defensive measures to provide information assurance include the use of secure networks, firewalls, encryption, anti-virus scans to detect malicious code, and proper systems administration to include aggressive auditing. Information protection includes the authenticity, confidentiality, availability, integrity, and non-repudiation of information being handled by anyone involved with C2 [command and control]...The criticality for counterintelligence in this area is the ability to identify the adversary's potential capability to exploit, deny, degrade or destroy friendly C2 before an attack to counter the attempt. Reporting and tracking of attempted and successful attacks will, through trend analysis, assist in the development of countermeasures[221].

Interpreting counterintelligence from the organisational perspective, should be viewed as an entity that is concerned with the larger strategic intelligence objectives and protection mechanisms of the organisation. Theses should be specifically orientated towards the identification, analysis and mitigation of an *enemy* and its activity; the threat. In this instance, an orientation which will enable and support existing security practices such as information security, which is itself taken from within the military driven protection sphere[222]. Information security when applied to the organisational context is thus concerned with the protection of information – predominantly in the digital sense in today's knowledge driven economy – achieved through the mitigation of identified vulnerabilities; concerning the information life cycle within an organisation and its associated processes.

By viewing counterintelligence as the meta-security element in this regard, one should be aware that it by no means undermines the importance of those functions carried out by other security orientated practices; such as information security. Rather, business counterintelligence should encourage the organisation to closely examine the purposes and goals of its various security elements, with the aim of creating a more comprehensively secure protection environment devoid of unnecessary overlap, overreliance on inadequate protection measures[223] and confusion as to where protection measures should be applied.

---

[221] U.S. Marine Corps. 2007. *Counterintelligence* p 9.

[222] Raval, V. & Fichadia, A. 2007. *Risks, Controls and Security* p 62.

[223] Pfleeger, C. & Pfleeger, S. 2003. *Security in Computing* p 2-4.

4.4 Structural Integration, Business Counterintelligence and the Relevance of Risk Management

As a precursor to the primary objectives of this chapter, one firstly needs to elaborate further on a few critical areas of interest. I will therefore open this section of analysis with a discussion outlining the concerns as associated with my initial thoughts on a categorisation approach. I will then elaborate further why in the light of these concerns, the security risk management process – in combination with the operational security/counterintelligence process forms – was chosen as a more appropriate form of structural analysis for the purposes of this investigation. I will also highlight the benefits of an integrative conceptual approach concerning operational security and the business counterintelligence process in relation to risk management. This is opposed to one of isolation, in the light of the functional significance of competitive intelligence. The section will conclude with a brief discussion on the relevance of risk management and its structural form.

4.4.1 Initial Thoughts on Categorisation

In order to meet the objectives of this study, it was initially thought that grouped counterintelligence elements could be applied to correlating organisational contexts. This was done, as dependence on security requirements tends to differ from one organisational context to the next[224], through the use of correctly identified counterintelligence and organisational classifications[225]. This was to be undertaken with the aim in mind of creating a classification structure for business counterintelligence understandings similar in nature to that of the information society paradigms presented by Webster in *Theories of the Information Society*. The classification of organisational types was to be done in a congruous manner – with additional variable reliance on Morgan's *Images of Organisation* to be used as needed – whereby it was postulated that the level of security filters required by an organisation, would determine its overall security classification. This could then be subsequently translated into requirements for an applicable type of business counterintelligence as defined by the classification process.

However, upon further investigation, such an approach was found to be largely impractical for the purposes of this study, as it lacked any firm distinctiveness of clarity and return on

[224] Kinghorn, J. 2007. *Personal Communication*. For example, a bank may require far more stringent security control filters than a small family run estate agency.

[225] Categorising variable counterintelligence understandings into broader themed specifications identified and applied through organisational types of variance based on identified levels of security filters required.

research investment that could justify its undertaking. This was true particularly in terms of its ability to reduce confusion and add meaning in a sustainable form for the organisation. Additional investigation into this discrepancy resulted in the identification of a number of factors that were found to be of hindrance in its pursuit, raising the potential for divergence away from some of the original suppositions of this study.

Firstly, that using Morgan's *Images of Organisation* as a benchmark of variable reliance for organisational classification was found to be only partly applicable in the context of this analysis. The reason for this was that it allowed for further understandings of particular organisational contexts to be achieved in relation to their implication for security elements; through analysis and framing of situational dimensions from different *metaphorical* points of view[226]. It was thus not able to offer definitively applicable contextualisation's of organisational structural variability, particularly concerning relevant security elements, as needed for the purposes of this investigation.

Secondly, the defining of organisational types as a means for business counterintelligence identification, tends to leverage very little value in terms of the applicability of business counterintelligence as an organisational process, particularly without the integration of identified and validated broader environmental competitive threats. By doing so, such an undertaking would run the risk of not effectively identifying an adversary's intent and capability to collect information, due to the structural and contextual assumptions of categorical implementation. The implications of these assumptions would mean that organisations therefore run the risk of implementing unnecessary business counterintelligence processes, while having no firm grasp of who their competitors are; without first having analysed their cost in relation to their promised benefit. This could therefore lead to the ineffective use and application of security and organisational resources.

Thirdly, by analysing business counterintelligence in this manner, it was felt that it would run the danger of becoming yet another confusing point of view, adding to the ever growing proverbial pile of business counterintelligence implementation strategies and directives. This would be in contrast to the initial objective of this thesis, whereby greater understanding through the identification of effective business counterintelligence practice from an organisational perspective would not be achieved. This would lack tangibility and integration with already existing organisational procedural spheres.

[226] Morgan, G. 2006. *Images of Organisation* p 338.

Fourthly, as has been outlined in chapter 3, business counterintelligence is an entity which has grown in importance for the organisation in recent decades. This has been largely due to those wide scale changes that have taken place in the industrial landscape combined with increased levels of knowledge complexity, environmental turbulence and the dissipation of clearly defined organisational boundaries. Within this environment of complexity, as has also been established, the implementations of security measures are often accompanied by a great deal of confusion as to how they can and should be adequately applied in an effective manner. This offers a particular challenge as far as the application of identified fragmented counterintelligence measures in differing organisational contexts are concerned, as variation in the perceived understandings of business counterintelligence – combined with a lack of clearly defined security objectives – make for a rather hazy organisational setting to contend with. This problem is further exasperated when combined with ill conceived analytical categorisation processes.

In order to extirpate these concerns, it was therefore decided that one needs to have in place a mode of understanding and implementing business counterintelligence practices in a methodically driven way devoid of external categorisation; especially in contexts of variation and disparity. It was thus determined that a more beneficial result could be achieved through the integration of applicable risk management process forms, whereby these structural forms would act as identifying factors of procedural categorisation in combination with structural dimensions of the operational security/counterintelligence process. In this instance guided by military based intelligence management principles where counterintelligence is effectively implemented as a sustainable intelligence and supportive security orientated risk management tool.

> Security is a matter of vulnerability and threat assessment with effective risk management. CI [counterintelligence] helps identify the hostile intelligence threat, assists in determining friendly vulnerabilities to it, and aids with the development of friendly measures that can lessen or negate these. The commander weights the importance of intelligence and CI to be used as a tool in risk management[227].

This conclusion was reached with the objective in mind of defining what one needs to protect from a business counterintelligence perspective and examining how one can apply business counterintelligence within organisations to achieve this in a sustainable form. In this instance

[227] U.S. Marine Corps. 2007. *Counterintelligence* p 4.

best suited to match relevant organisational contexts of requirement, as a combined process driven approach affords one the advantage of self defined internalised quantification.

4.4.2 The Value of Integration: The Counterintelligence Process, Operational Security and Competitive Intelligence

Before one can commence further with an in-depth analysis – as to the structural integration of business counterintelligence in combination with selected risk management process forms – one firstly needs to establish the merits of undertaking such an approach. This has to be thought of in relation to those relevant existing points of view, as to how business counterintelligence can be implemented in an effective manner within one's organisation. This will be done by highlighting the benefits of an integrated approach as opposed to the existing partly isolated methodology of operational security/counterintelligence process implementation. This will be undertaken in the light of the close functional relationship[228] that exists between business counterintelligence and competitive intelligence.

The relevance of these procedural forms – particularly concerning operational security in the context of this discussion – hinges on their close structural relationship with that of the risk management process[229]. These include, the Business Counterintelligence Process consisting of: *Tasking*; *Defining Requirements*; *Assessing Competition*; *Estimating Vulnerabilities*; *Deploying/Employing Countermeasures* and *Analysis*[230] respectively. And the critical Operational Security (OPSEC) steps consisting of: *Identifying critical information*; *Indentifying potential threats*; *Indentifying areas of vulnerability*; *Conducting a risk assessment* and *Establishing appropriate countermeasures*[231]. Thus both of these approaches aim to increase the effectiveness of overall defensive intelligence[232] methodologies.

---

228 DeGenaro, B. 2005. *A Case for Business Counterintelligence* p 13.

229 For example as Mark, D. 1997. *Competitive Intelligence and the Corporate Jewels* p 67, states: "OPSEC [operational security] has a role in the risk avoidance approach but fits best within the risk management environment since it recognizes and deals with the fact that a company cannot protect all information."

230 Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 30-38.

231 Mark, D. 1997. *Competitive Intelligence and the Corporate Jewels* p 67.

232 DeGenaro, B. 2005. *A Case for Business Counterintelligence* p 13, outlines: "There are three major activities that are included in the overall title of defensive intelligence: 1. Security countermeasures are the traditional physical security activities of the firm and include gates, guards, access control, storage etc. All are very necessary but not sufficient; 2. Operational Security (OPSEC) deals not with the secret but evidence of a secret. The signals are emitted in the normal conduct of business. You might want to think of it as the opposite of indications and warnings intelligence. Warnings intelligence requires the establishing of indicators as the basis for collection tasks...OPSEC attempts to deny the adversary the ability to read indications created by your firm; 3. Counterintelligence is all about the discovery and neutralization of adversarial intelligence activities."

Some in the field recommend the implementation of such processes to be done in a form of distinctive procedural isolation – driven by competitive intelligence[233] and acting a tool of relevance[234] – from other forms of protective integration[235]. Certain aspects of this approach are valid in their request. The most important element of which is that business counterintelligence program elements should not be undermined in terms of their level of applicable relevance as standalone entities in conjunction with the broader organisational processes[236]. The reason being that they will by all accounts perform better when integrated with competitive intelligence; as such integration is predominantly critical for two primary reasons.

Firstly, it affords one the ability to recognise that one's competitors can collect information about one's own organisation in the same way that one might collect information about them[237]. It is therefore beneficial, when developing a business counterintelligence program, to understand how a competitor might look at one's own organisation and what kinds of information sources they may be targeting.

> Without a professional positive business intelligence process, an effective counterintelligence program is not possible. You must be able to assess the capabilities and intentions of a competitor before you can implement counterintelligence[238].

Secondly, business intelligence is seen as a critical element when it comes to the management of information, in that it allows one to understand how gathered intelligence may be managed as part of the daily operations of one's organisation[239]. This is an important step when developing a learning organisation and leveraging such intelligence with the aim of gaining and maintaining competitive advantage.

> The leaders of successful learning organizations realize that they are engaged in knowledge warfare and that the smarter organizations will win. Organizations with better learning capabilities recruit better, define markets better, and identify new opportunities and technologies better than their less well-informed rivals. The

233 Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 30.
234 DeGenaro, B. 2005. *A Case for Business Counterintelligence* p 12.
235 DeGenaro, B. 2005. *A Case for Business Counterintelligence* p 15.
236 Mark, D. 1997. *Competitive Intelligence and the Corporate Jewels* p 67.
237 Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 30.
238 DeGenaro, B. 2005. *A Case for Business Counterintelligence* p 13.
239 Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 30.

primary driver for innovation (a competitive necessity) is the rate of organizational learning[240].

However in spite of these merits, it should be noted that an overreliance on business intelligence could limit the success of one's business counterintelligence program, due to a lack of decision maker support concerning the value of intelligence. Integrative hindrance is thus most destructive for any business counterintelligence program, in that integrative disjunction can result in a general lack of understanding, appreciation and acceptance of such intelligence functions by an organisation. This is evident by the low number of world-class intelligence programs and managers in place[241], resulting in a lack of access to key decision makers and adoption by higher level management. Thus leading to the inevitable wasting of organisational assets[242] through engagement – should such intelligence functions be present – with irrelevant projects of analysis.

In contrast to isolated application, an integrative approach offers one the ability to retain many of the benefits of a smaller dynamic business counterintelligence function. Thus offering better structural integration, buy in and support by higher level management and the incorporation of further relevant risk management process elements; enhancing business counterintelligence's overall effectiveness. These benefits are presented and discussed as follows:

Increased support by management – as part of the fundamental requirement and integrative nature of enterprise risk management[243]. In addition, if threats to intellectual assets are seen as risks, knowledge risks that can be managed in a methodically driven way using business counterintelligence, such an understanding has the potential to bolster management's realisation of the importance of business counterintelligence. This is in conjunction to other operational risk management forms that may be present within the organisation. This emphasis is carried through further; especially when decision makers realise how little they may actually know about their competitors, how much competitors may already know about them, the value that their intellectual capital holds in determining innovation and competitive

[240] DeGenaro, B. 2005. *A Case for Business Counterintelligence* p 12-13.
[241] DeGenaro, B. 2005. *A Case for Business Counterintelligence* p 12.
[242] DeGenaro, B. 2005. *A Case for Business Counterintelligence* p 15.
[243] Lam, J. 2003. *Enterprise Risk Management* p 50-51.

advantage and the importance for the protection of such intellectual capital for the maintenance of that advantage.

Increased appreciation for the value of knowledge assets – through a combined integrative approach, as it will allow management to gain a better grasp of the value of intellectual assets to be protected and by implication the value lost by not protecting them effectively. This can be achieved through the help of an integrated risk management based cost benefit analysis[244]. This is in contrast to selecting and applying countermeasures from a purely core competency driven dynamic of selection[245]. Thus further bolstering management support for business counterintelligence by allowing for the effective application of potential protection measures, in terms of the cost of implementation relative to the value of the asset.

More effective quantification of knowledge assets – as an integrative approach by applying operational security and risk management methodology will allow one to analyse what knowledge assets are most important to the organisation and what therefore should be protected first. This means that protection resources – including funds – are applied only where they are needed most consequentially resulting in savings. This takes place as one is not attempting to protect knowledge assets that are of little concern to the organisation – or whose value is of a temporary nature – while those assets that should be of concern are left unprotected.

More effective communication between disparate functional units – within the organisation, through the integration of counterintelligence processes with risk management forms, scaled according to organisational functional requirements. This is in contrast to rather being reliant on singular functional communicative intelligence. Therefore potentially increasing the value of the information delivered and disseminated by the business counterintelligence function, as attacks targeting disparate areas of organisational concern can be recognised faster. This is more beneficial, particularly when combined with an effective knowledge management and competitive intelligence function, allowing one to leverage ones competitive advantage to a greater degree.

[244] Roper, C. 1999. *Risk Management for Security Professionals* p 85.

[245] Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 31.

4.4.3 The Relevance of the Risk Management Structural Form

Risk management is a well established concept, one that has been in existence in variable forms since the earliest times of recorded human history[246]. Throughout its life – identified as either a formal process or not – risk management has been applied and adapted to suite ever changing areas of concern, focused on topics ranging from broader decision making implications to the improvement of both individual and societal life[247]. With the large scale shifts that have taken place in recent decades, from an industrial based economic and social modus to that of a knowledge based one, risk management has in turn grown in importance and has been adapted in order to meet those challenges posed by the complex economic and social environment of today.

> There has been an increase in new risks fundamentally different in both character and in magnitude from those encountered in the past...In the past, risk management decisions were based primarily on common sense, ordinary knowledge, trial and error, or non-scientific knowledge and beliefs. In recent years risk management decisions have been increasingly based on highly technical quantitative risk analyses. Increased reliance on such analyses reflect a related trend – a growing societal preference for planning, forecasting, and early warning in contrast to *ad hoc* responses to crisis[248].

In the light of these changes, the need for better planning, forecasting and response to events holds a particular relevance for business operations and their managers as they seek increased stability in decision making[249]. An example of this being security decisions taken by management[250]. This has resulted in the application and adaptation of risk management and its elements to suite those functions and forms of varying organisational processes as

---

246 Covello, V. & Mumpower, J. 1985. *Risk Analysis and Risk Management: An Historical Perspective* p 103.

247 As Covello, V. & Mumpower, J. 1985. *Risk Analysis and Risk Management: An Historical Perspective* p 111-114, outline, examples include: natural disasters, disease, pollution, food contamination, fire and building codes, transport and occupational safety.

248 Covello, V. & Mumpower, J. 1985. *Risk Analysis and Risk Management: An Historical Perspective* p 116-117, go on to state when speaking about the increased use of risk management by the United States government in the 1980's, motivating factors included: "An accelerating rated of technological change, resulting in enormous increases in the physical and temporal scale and complexity of risks (for example, approximately 70, 000 chemicals are in current use, with perhaps 1000 new chemicals being introduced each year); An increase in the speed of scientific and technological developments, so that there are shorter and shorter time lags between scientific experimentation, technological development, and entrepreneurial production; The increasing role of government as a producer of risks through its sponsorship of scientific and technological research and development; The rising cost of technological risk control and damages – estimated by one research group to be 179-283 billion dollars a year." A risk management response to emerging information society shifts from the technologically driven paradigm.

249 Longenecker, J. & Broom, H. 1972. *Small Business Risk Management* p 463.

250 Vellani, K. 2007. *Strategic Security Management* p xviii.

necessary; often encapsulated in the business sense under enterprise risk management[251]. Broader environmental practices and business orientated processes – where risk management elements[252] have been adapted and applied to areas of concern – include:

> Financial Management – whereby risk management and its processes are applied to various elements of the financial system, including but not limited to: banking and electronic banking[253]; the internal financial system and transactions of an organisation[254]; general financial management and planning practices with a focus on market trading, investments, interest rates, foreign exchange, equity, commodities, accounting, credit and regulation[255]; entities which play an active role in the variable contexts of engagement and implementation within the financial management sector.
>
> Project Management – whereby risk analysis is applied to each stage of the project life cycle either in part or as an overall guiding influence of the initial progress of each stage in turn[256]. It is also important to note that risk in this instance is not merely

---

[251] Lam, J. 2003. *Enterprise Risk Management* p 51-52. In addition, it is important to note that the meaning derived for the purposes of this study is largely concerned with the implementation and adaption of risk management elements in the business context. This is not to say that such categorisations are in conflict with the broader categorical understandings that risk professionals often interpret. As is outlined by Lam, J. 2003. *Enterprise Risk Management* p 23, when discussing this broader categorisation: "Risks come in all shapes and sizes; risk professionals generally recognize three major types. Market risk is the risk that prices will move in a way that has negative consequences for a company; credit risk is the risk that a customer, counterparty, or supplier will fail to meet its obligations; and operational risk is the risk that people, processes, or systems will fail, or that an external event (e.g. earthquake, fire) will negatively impact that company...Other types of risk also have been suggested. Business risk is the risk that future operating results may not meet expectations; organisational risk is the risk that arises from a badly designed organisational structure or lack of sufficient human resources. In general, risk managers would consider market risk and credit risk as financial risk, and group all other risks as part of operational risk."

[252] Vellani, K. 2007. *Strategic Security Management* p 110 states: "Risk Management is truly a management process, where a risk assessment is simply a component of that continual management process. For many organisations, risk management involves much more than security functions and also includes insurance and legal issues." All of which can be classified as various elements of the broader organisational risk management initiative.

[253] As Kondabagil, J. 2007. *Risk Management in Electronic Banking* p 18 outlines that it is important to note that risk management in this instance is made up of multiple objectives of concern which include the broader risk management process itself, information security management, outsourcing management, business continuity management and legal and regulatory compliance.

[254] As Crouhy, M. Galai, D. & Mark, R. 2006. *The Essentials of Risk Management* p 93 outline, in this instance the oversight of such processes are the responsibility of the risk advisory director and include the review and analysis of internal controls to mitigate key market activities, financial statements, critical accounting principles, significant account judgements, material accounting estimates and off-balance-sheet financings, financial information and disclosures that are provided in support of securities filings, internal audit and external audit reports and associated management letters, intercompany pricing issues, transactions and auditing and stock exchange based requirements.

[255] Murphy, D. 2008. *Understanding Risk* p 3-76.

[256] As Chapman, C. & Ward, S. 2003. *Project Risk Management: Processes, Techniques and Insights* p 255-256, outline, the project management cycle consists of the stages of: conceive the product; design the

limited to those various challenges posed by each stage of the project life cycle, but can also manifest in elements[257] pertinent to the very nature of the project being undertaken.

Security Management – where in this instance the risk assessment process is followed, in one form or another, in order to help ensure the adequate prioritising of risks to effectively implement appropriate countermeasures aimed at the mitigation, at least in part, of security based vulnerabilities[258]. Risk assessment in this context is applied to security areas including data security, crime analysis, information communications technologies, physical security, personal management, premises security, forensic security and security consulting[259]. This has been done particularly in the light of the digital environment and the increased growth in complexity[260]. This includes the rise of information and the information communications technologies[261] – that have accompanied it.

Although risk management forms may be discussed in a theoretical sense of division from one another, it is essential in terms of practical application that the organisation wide risk management initiative be implemented and governed as a singular functional unit of shared responsibility[262]. Better integration of business counterintelligence within the organisation through this integrative structural application, should therefore allow for the manifestation of an environment of understanding and acceptance. This will help to reduce confusion, diversity in application of business counterintelligence implementations and the potential for redundancy created by not doing so.

> Risks are by their very nature dynamic, fluid, and highly interdependent. As such, they cannot be broken into separate components and managed independently. Enterprises operating in today's volatile environment require a much more integrated approach to managing their portfolio of risks...This has not always been recognised. Traditionally, companies managed risk in organisational "silos"...However, it has become increasingly apparent that such a fragmented

---

product strategically; plan the execution strategically; allocate resources tactically; execute production; deliver the product; review the process and support the product.

257 Edwards, P. & Bowen, P. 2005. *Risk Management in Project Organisations* p 40-50.

258 Vellani, K. 2007. *Strategic Security Management: A Risk Assessment Guide for Decision Makers* p 110.

259 Vellani, K. 2007. *Strategic Security Management: A Risk Assessment Guide for Decision Makers* p xviii-xxi.

260 Hanseth, O. & Ciborra, C. (eds). 2007. *Risk, Complexity and ICT* p 1-7.

261 Slay, J. & Koronios, A. 2006. *Information Technology Security and Risk Management* p ix.

262 Lam, J. 2003. *Enterprise Risk Management* p 43.

> approach simply doesn't work, because risks are highly interdependent and cannot be segmented and managed by entirely independent units...Attempting to manage them as if they are is likely to prove inefficient and potentially dangerous. Risks can "fall through the cracks," risk interdependencies and portfolio effects are not captured, and organisational gaps and redundancies result in suboptimal performance[263].

The risk management form thus allows one to effectively integrate collective points of view by acting as a structural catalyst for combined implementation; particularly concerning the operational security/counterintelligence process, knowledge risks and the structural diversities that accompany them. Risk management methodology therefore affords one the ability to apply and understand business counterintelligence in a firmer structurally based manner through better risk classification and integration. This offers support to other risk management processes active within a particular organisation, as well as being supported by them in return.

> Classifying risks enables us to consider them within a more coherent framework. Creating an acceptable taxonomy establishes a common basis for risk and risk management researches to proceed with their investigations and communicate their findings[264].

Through such an implementation, one can therefore better identify what one may need to protect from a business counterintelligence point of view[265]; in a more structurally driven manner, taking into account particular organisational dynamics. This is significant, as it will allow for the development of an organisational protection capability that is far less confusing and more structured in its conceptualisation and implementation. This in contrast to *ad hoc* process that may be applied in isolated forms of variance, differing in the fundamental principles of those applications.

> Risk management has been proclaimed to be the guiding philosophy of our modern security programs. Gail Howell, Chief of the Security Division in the Office for Security and Counterintelligence, Defence Intelligence Agency, has

[263] Lam, J. 2003. *Enterprise Risk Management* p 43.

[264] Edwards, P. & Bowen, P.2005. *Risk Management in Project Organisations* p 25.

[265] As often with a non-integrated approach there exists the danger of not effectively identifying all elements which need or justify protection.

referred to it as "our new way of doing business, and [it] will be with us for years to come[266].

4.5 Risk Management, Business Counterintelligence and the Integrative Structural Process

I will now move on to discuss business counterintelligence and its relevance as a business practice from an organisationally driven point of view, taking into account contextual variance, both in terms of the understanding of business counterintelligence and its applicability for differing organisational types. This will be analysed from appropriately selected risk management structural forms of integration in conjunction with the operational security/counterintelligence process. This shall be done in order to engage with those challenges as outlined in chapter 1. Firstly, types of organisations vary and operate on different levels of security and secondly that there are variations in what is identified as business counterintelligence from disparate points of view[267]. This will be done with the aim in mind of identifying a generically sustainable business counterintelligence form.

4.5.1 Choosing an Applicable Risk Management Process Form

The variable adaptation of the risk management process structure – due to the growing dynamic necessities of risk management elements within areas such as finance, project management and security – has resulted in the development of a number of generic process forms suited to meet these categorical challenges[268]. The requirement for such necessities has

---

266 Roper, C. 1999. *Risk Management for Security Professionals* p ix.

267 These points of view tend to lack conformity in their integrative interpretation of counterintelligence within the business context. This is partly due to those reasons expressed in the previous chapter, whereby there is a great variance in the way counterintelligence elements have been integrated into the business environment of today; made clear through the vast number of divergent literary perspectives, many of which do not hold a shared commonality.

268 Risk management standards and structures are accompanied by a great deal of variability depending on their relevant context of application. As Olson, D. & Wu, D. 2008. *Enterprise Risk Management* p 3, state "there are over 80 risk management frameworks reported worldwide" which invariably means a large number of different formulations of the risk management process, its entities and the methodologies that accompany it. There are however some approaches that are more commonly mentioned within the literature surrounding the topic, these are outlined as follows: Kondabagil, J. 2007 *Risk Management in Electronic Banking* p 57-60, highlights four international standards, COBIT 4.0, ISO 17799, OCTAVE and COSO-enterprise risk management, that are often used in practice. Calder, A. & Watkins, S. 2007. *Information Security Management for Iso27001/Iso17799* p 25-26, highlights the use of the ISO27001 methodology and those standards, namely: ISO17799; ISO13335-3; BS7799-3 that surround it. Vellani, K. *Strategic Security Risk Management: A Risk Assessment Guide for Decision Makers* p xvii, discusses the use of the TAG Risk Assessment Process as developed by the threat analysis group. Chapman, C. & Ward, S. 2003. *Project Risk Management: Processes, Techniques and Insights* p 55-62, outline the use of the generic risk management process framework for projects, known as the SHAMPU (Shape, Harness, And Manage Project Uncertainty) process.

meant that process forms – and often the standards and structures that accompany them – have been developed with the aim in mind of specific contextual implementations. This has been largely due to the lack of a formal industry based *one size fits all* risk management adaptability. An example of which is outlined concerning the application of risk management in the electronic banking sector.

> There is no formal industry standard or framework that has a one-size-fits-all type of adaptability, is specific to the banking sector, and offers comprehensive coverage of all issues relating to e-banking [electronic banking] risk management. An institution may need to use a combination of two or more available standards dependent on the nature, scope, complexity, and risk profile of the individual bank, and adapt them to meet the specific needs of the bank[269].

Since, as I have stated, organisations vary and operate on different levels of security – in combination with a broader variation in what is identified and in many cases applied as business counterintelligence from disparate points of view – the development of any generic risk management based process concerning business counterintelligence should be constructed on soundly applicable principles. It therefore makes sense to engage with business counterintelligence from the most appropriate generic model of implementation relevant to its needs, in order to ensure ease of application and understanding within the organisation.

One should be aware however that the development of such business counterintelligence risk management driven implementations should be viewed within an organisations broader strategic risk management direction, and in most cases, not seen as something that is separate or isolated from its other areas of concern. Such an attempted implementation, as is discussed in the following extract, runs the risk of creating further confusion rather than acting as a strategic mechanism for increased communication and understanding. This in the light of the maximisation of strategic risk management processes for the development of a more securely based level of shareholder value. This through increased competitive advantage[270] and operation within the knowledge based economy.

---

[269] Kondabagil, J. 2007. *Risk Management in Electronic Banking* p 56.

[270] As Clarke, C. & Varma, S. 1999. *Strategic Risk Management: the New Competitive Edge* p 417-423 outline: "Companies can attain significant competitive advantage from superior risk competencies...If a risk management program is instituted properly and with conviction, the resulting organisation will be stronger, financially more secure and the envy of its peers."

> Traditional risk management responsibilities and responses are typically fragmented as a result of their differing origins...There is a need for a holistic approach to understand enterprise-wide risk, rather than this piecemeal approach. In our experience, even in sophisticated companies, management becomes confused and fails to adequately manage risks for the company's advantage...A comprehensive understanding of the playing field is required, and an integrated risk management methodology must be used for identifying and evaluating risks. From this, a strategy can be developed to maximise shareholder value – but this requires effective risk management[271].

In the light of these perspectives, with the broader counterintelligence process acting as a structural backdrop, it was therefore concluded that the most appropriate course of action would be to consider the implementation of a strategically based security orientated risk management approach. A number of risk management forms were reviewed for their contextual appropriateness, contained within the broader areas of operational risk, counterparty risk, market risk and even risk[272]. This was done for the purposes of reducing confusion through the adaption, implementation and structural applicability of business counterintelligence in a generic strategically based risk management form. This was done in order to effectively meet those challenges posed by divergent organisational and business counterintelligence integration requirements.

Although some points of view as found within the literature contextualise the implementation of business counterintelligence as part of general security management processes[273], most do not. Those points of view that do, maintain an ever present reliance on traditional elements of security management[274] combined in many cases with integrated information security

---

271 Clarke, C & Varma, S. 1999. *Strategic Risk Management: the New Competitive Edge* p 415-424.

272 Clarke, C & Varma, S. 1999. *Strategic Risk Management: the New Competitive Edge* p 421, identify four major areas of risk, these include – Operational Risk, consisting of: Operational Control Risk, Project Risk, Transaction Risk, Systems Risk; Event Risk, consisting of: Reputation Risk, Legal and Regulatory Risk, Disaster Risk, Political Risk; Market Risk, consisting of: Demands, Equity Price Risk, Interest Rate Risk, Foreign Exchange Risk, Liquidity Risk, Port Concentration Risk, Correlation Risk; Counter Party Risk, consisting of: Credit Risk, Continuity of Demand of Supply all of which form part of Enterprise Risk.

273 Authors expressing this point of view include Walsh, Sharma, McCrie and Robinson; but to name a few.

274 Walsh, J. 2003. *Asset Protection and Security Management Handbook* p 55-303, discusses topics largely focused on physical security mechanisms that include structural barriers (p 55), general locking concepts (p 79), alarms (p 111), various forms of access control (p 187), information systems security (p 279) and investigation and interrogation techniques (p 303) but to name a few. Sharma, R. 2004. *Industrial Security Management* p 10, discusses aspects relating to traditional safety and security management in a variety of contexts contained within an industrial centred understanding of economic interactions, as interpreted from an Indian economic point of view, where he states: "Lately, is has been noticed that the general awareness regarding the need for security has occupied a place for concern in the mind of the corporate world. However, "Industrial Security" is yet to be regarded as one of the main Management Functions. As per the

approaches[275], or an outright focus thereupon[276] in order to meet the security challenges posed by the information society. This is usually associated with risk assessment and driven by operations security support[277] in order to deal more effectively with advanced information based threats.

Upon completion of review, it was therefore found that the form of strategic security risk management – which may be viewed in this context as relevant to operational risk, driven

---

available definition in the Industrial Disputes Act, the "Industry" has been defined in a generic sense as: All manufacturing units; Agricultural farms; Commercial organizations (all); Miscellaneous units, i.e. colleges, schools, hospitals, etc." McCrie, R. 2006. *Security Operations Management* p 308, refers to the importance of physical and technological security mechanisms in security operations where he states: "Security Operations planners sometimes think first of physical security in their protection strategies. Several reasons support this tendency: physical security substantially requires a one-time cost only; physical measures are usually clearly visible and deter unlawful or unwanted acts; care and upkeep are limited; specific standards have been set in many cases to guide the security planner on decisions; and physical security measures are uncomplicated to purchase, install, and care for. However, the primary goal of security measures is to protect people, not physical or intellectual assets...Technology can be used as a powerful tool in well-conceived security programs. It can perform complex monitoring operations and control features that individual security personnel cannot control. As a result, contemporary high-tech implements permit a higher level of confidence in protective programs than in the past. Just as changes in communications, sensing, and computing have affected society at large, these developments also have re-shaped the means and quality by which security services are performed. Indeed, a security planner learning of a new technological development is likely to wonder how it can be applied to enhance operating security programs tomorrow, if not today." Robinson, R. 1999. *Issues in Security Management* p xi, broadly speaking, deals with issues as relating to crime prevention, security personnel, closed circuit television (CCTV), investigations and planning a security program and general security and protection techniques for a range of varying contexts compiled from a number of authoritative views from a slightly different approach. As he states: "There is a great deal more to effective security than increasingly sophisticated equipment. Protecting people and their assets is basically dependent upon how the planners and directors of security – and members of their staff – think about their tasks and the way in which they discharge their responsibilities. An awareness of this reality is what has guided the selection of material for this anthology...All sectors of the security industry share a common goal: the safety of society itself. In a word, providing security is a public service...This larger view – beyond the production of business profit – is not always evident in the behaviour of companies and individuals. We are sometimes in danger of becoming too narrowly focused on a single idea, a device, a system, a means of enhancing the bottom line. This is not conducive to growth, nor to real job satisfaction."

[275] Walsh, J. 2003. *Asset Protection and Security Management* p 247 states: "The varied applications of computers make them appear to be some mysterious mechanism – too complex to understand. As a result, many security directors are reluctant to get involved in protecting their organisations IS [information systems]. But, with an understanding of information processing technology, security directors can grasp the security implications of information processing and make an important contribution to the information systems program."

[276] Cazemier, J., Overbeek, P. & Peters, L. 1999. *Security Management* p 3, state: "Security Management is the process of managing a defined level of security on information and IT [information technology] services. Included is managing the reaction to security incidents. The importance of information security has increased dramatically because of the move of open internal networks to customers and business partners; the move towards electronic commerce, the increasing use of public networks like Internet and Intranets. The wide spread use of information and information processing as well as the increasing dependency of process results on information requires structural and organised protection of information...Security management is more than locking server rooms or insisting on password discipline. Integrity aspects of information processing like timeliness or correctness require careful consideration of information flows and safeguards against incorrect value."

[277] Fay, J. 2005. *Contemporary Security Management* p 291-303.

from a systemic approach[278] – would be best aligned to match the objectives of the operational security/counterintelligence process for such purposes. This as the structural basis and topics dealt with were substantially more consistent in nature with the objectives of business counterintelligence than other structural forms of risk management reviewed[279]. Given the variance present in the plethora of possible approaches at one's disposal, this was done with the objective in mind of allowing for better informed decisions to be made concerning the use and application of business counterintelligence resources within the organisational context[280]. This was done in the light of security risk management's close structural orientation to that of the operational security/counterintelligence process.

4.5.2 Choosing Applicable Strategic Security Risk Management Process/Assessment Forms

The strategically based security risk management process/assessment, is one that is – as with most topics of discussion in this field of analysis – largely variable in its approach and implementation[281]. For the purposes of this investigation – given the constraints imposed by such a format – I will therefore focus my attention on the constitution of a guiding framework derived – in the risk management sense – from two specifically selected security risk management process/assessment[282] forms. These forms are highlighted by Vellani in *Strategic Security Management* and Roper in *Risk Management for Security Professionals* respectively. These approaches are deemed to be relevant for such a categorical construction in the light of the structural significance and integrative qualities that they possess. In this

---

278 Roper, C. 1999. *Risk Management for Security Professionals* p 7-13, states: "Each profession or field of endeavour has its own unique terminology and definitions; risk management is no different. As I researched the subject matter, I found that different organizations (and sometimes, their sub elements) might "reverse" a given term to meet their own needs. Thus, in many places, the terms referred to the same thing, but were defined differently and thus were interpreted and used in a slightly different manner. Herein, the terms and their definitions are those used by risk managers and practitioners who have the ability to see beyond local organizational boundaries. The use of a set of terms that crosses organizational boundaries means that everyone is on the same wavelength when talking with another individual from a different organization, even in a different state or country, or business enterprise."

279 Project risk management and financial risk management implementations being examples of non fitting contexts, as these forms of risk management structure are driven by a largely different set of rudiments; as far as the flow and focus of their generic risk management processes are concerned.

280 Roper, C. 1999. *Risk Management for Security Professionals* p ix, states: "Risk management offers a rational and defensible method for making decisions about the expenditure of scarce resources and the selection of cost-effective countermeasures to protect valued assets."

281 Roper, C. 1999. *Risk Management for Security Professionals* p 13

282 As Hansche, S., Berit, J & Hare, C. 2004. *Official Guide to the CISSP Exam* p 12, state: "For consistency...the term "risk assessment" hereafter is used to characterize both the process and the result of analyzing and assessing risk."

instance concerning the combined integration of business counterintelligence and risk management elements as outlined in the paragraphs to follow.

Vellani outlines the strategic security risk assessment process in its simplest form – defined by the Threat Analysis Group (TAG) – as one consisting of *Asset Identification*, *Current Security Measures* (including the sub facets of policy and procedure, physical security and security personnel), *Threat Assessment* (including the sub-facet of crime analysis), *Vulnerability Assessment* and *Risk Assessment* (including the sub-facets of cost benefit analysis and reporting and recommendations)[283]. This form of structural analysis is of particular importance, when dealing with business counterintelligence, as it is largely concerned with analysing security management in a strategically based, globally assertive risk assessment sense[284]. In this case with a firm focus on business, rather than one predominantly centred around operational security elements alone.

Although this structural form is not specifically tailored towards the implementation of business counterintelligence in itself, it does allow for the formation of a strategically based security management foundation. This is important when integrating other forms of risk management structure, as it enables one to keep in mind the broader elements of process flow while creating awareness of increased levels of concern and diversity. The inclusion of this strategically based identification, evaluation and determination techniques relating to one's critical assets being an example of this. This is in relation to standard counterintelligence structures, when dealing with the operational/counterintelligence process sphere.

Roper views the security orientated risk management process as one based on five steps, in its most reduced form, namely: *Asset Assessment*; *Threat Assessment*; *Vulnerability Assessment*; *Risk Assessment* (providing feedback for the asset and vulnerability steps); *Determining Countermeasure Options* (supported by cost and benefit analysis); ultimately allowing for the informed making of *Risk Management Decisions*[285]. This structural form is of particular

---

[283] Vellani, K. 2007. *Strategic Security Risk Management: A Risk Assessment Guide for Decision Makers* p xviii.

[284] Vellani, K. 2007. *Strategic Security Risk Management: A Risk Assessment Guide for Decision Makers* p 2, states: "Today's business risk environments have become increasingly more sever, complex, and interdependent, both domestically and globally. The effective management of these environments is a fundamental requirement of business. Boards of Directors, shareholders, key stakeholders, and the public correctly expect organizations to identify and anticipate areas of risk and set in place a cohesive strategy across all functions to mitigate or reduce those risks. In addition, there is an expectation that management will respond in a highly effective manner to those events and incidents that threaten the assets of the organization. A proactive strategy for mitigation of the risk of loss ultimately provides a positive impact to profitability and is an organizational responsibility of senior management and governing boards."

[285] Roper, C. 1999. *Risk Management for Security Professionals* p 20.

importance as the risk management process – in this instance – is viewed as the main driving force for the cost-effective protection of assets. An example of this is the cost-benefit analysis and selection process. Thus it is therefore applied as the primary form of procedural concern within the organisation, from a singularly dominant perspective of protection based implementation.

> Risk management is important to each of us simply because it is the *best* method available that allows us to determine the protection required for varied assets[286] at the most reasonable cost. Thus it is an investment in the present and the future, an investment that benefits everyone concerned[287].

4.6 The Generic Integrative Structural Process

With these process-based foundations in mind, one can now proceed with the development of an integrated generic protection structure, acting as a guiding framework of procedural business counterintelligence implementation. This will be done by taking those topical aspects of structural process importance – as outlined in the preceding sections of this discussion, concerning strategic security risk management and the operational security/counterintelligence processes – and assessing them through an integrative structural matrix of comparison. This will be done in order to develop a sustainable generic form of business counterintelligence process flow. By applying these relevant process forms in this manner, it will allow one to better maximise the prospective associated benefits[288] of the integrated approach.

4.6.1 The Structural Integration Matrix and Combined Process Flow

The structural integration matrix as presented in Table 1 below consists of those associated forms of process flow as discussed in the preceding sections of this analysis. Starting from left to right columns A-D represent those broader structural steps associated with business counterintelligence and risk management process forms respectively. From a business counterintelligence point of view, column A represents the *critical operational security*

[286] Although these approaches are able to identify variable assets for protection, in the case of business counterintelligence one is predominantly concerned with the identification of knowledge based assets.

[287] Roper, C. 1999. *Risk Management for Security Professionals* p 4.

[288] Prospective benefits as discussed earlier under the heading "The Value of Integration: The Counterintelligence Process, Operational Security and Competitive Intelligence" include: Increased support by management; Increased appreciation for the value of knowledge assets; More effective quantification of knowledge assets; More effective communication between disparate functional units. This in addition to the broader objectives of this investigation in terms of defining what constitutes good or sustainable business counterintelligence from the organisational point of view, and increasing understanding relating to the topic of business counterintelligence.

steps[289] with column B representing the *counterintelligence process*[290] as has been elaborated upon earlier in this chapter. Column C the *TAG strategic risk assessment process*[291] and column D the *security risk management process*[292], are associated with the broader strategic security risk management process forms and although similar, are therefore juxtaposed to columns A and B. Column E the *combined business counterintelligence risk management process structure* is derived from the collective integration of columns A-D, selected from those steps deemed critical for the development of an effective, sustainable business counterintelligence process framework.

[289] As most notably expressed by DeGenaro, B. 2005. *A Case for Business Counterintelligence* p 15, Mark, D. 1997. *Competitive Intelligence and the Corporate Jewels* p 67 and Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 49, amongst others.

[290] As represented by Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 30-38.

[291] As outlined in Vellani, K. 2007. *Strategic Security Risk Management: A Risk Assessment Guide for Decision Makers* p xviii.

[292] Roper, C. 1999. *Risk Management for Security Professionals* p 20.

Table 1: The Operational Security, Counterintelligence and Risk Management Structural Process Integration Matrix

	A	B	C	D	E
	Business Counterintelligence Orientated Process Forms		**Risk Management Orientated Process Forms**		
	Critical Operational Security Steps	**Counterintelligence Process**	**TAG Strategic Risk Assessment Process**	**Security Risk Management Process**	**Combined Business Counterintelligence Risk Management Process Structure**
1.		Tasking			Engage with management and assign responsibility for the program.
2.	Identifying Critical Information	Defining Requirements	Asset Identification	Asset Assessment	Define and assess what knowledge resources need to be protected.
3.			Current Security Measures (including the sub facets of policy and procedure, physical security and security personnel)		
4.	Analysing Threats	Assessing Competition	Threat Assessment (including the sub facet of crime analysis)	Threat Assessment	Identify and assess threats targeting knowledge resources.
5.	Analysing Vulnerabilities	Estimating Vulnerabilities	Vulnerability Assessment	Vulnerability Assessment	Identify and assess vulnerabilities that may be exploited by identified threats.
6.	Assessing Risks		Risk Assessment (including the sub facets of cost benefit analysis	Risk Assessment (providing feedback for the	Evaluate and prioritise risks associated with identified

			and reporting and recommendations)	asset and vulnerability steps)	knowledge assets in terms of threat and vulnerability assessments.
7.	Applying Appropriate Countermeasures	Deploy/Employ Countermeasures		Determining Countermeasure Options (supported by cost benefit analysis)	Select appropriate countermeasures in relation to their cost/benefit trade-off.
8.				Make Risk Management Decisions	Make recommendations to appropriate decision makers & implement findings.
9.		Analysis			Conduct continued analysis.

The relevant logical weighting of columns A-D, in terms of their appropriateness for the collective column E, was done in the light of those critical areas of concern relating to the operational security and counterintelligence processes as presented in columns A and B. This was done in order to remain consistent with the essential business counterintelligence form. The risk management structure columns of C and D therefore carried a lesser logical weighting and were used primarily for the purpose of increased relevance and assessment concerning the business counterintelligence process elements presented in columns A and B.

Thus, cell B1 *Tasking* was found to be of greater critical importance for the effective development of the integrated business counterintelligence process – even though not mentioned in those other forms of structural process flow – largely to meet the concerns of implementation as relating to business counterintelligence within the organisation. This was included in terms of responsibility and to address the need of increased higher level management support[293]. Cell B9 *Analysis* was also found to be of importance for inclusion in the final integrated structural form as represented in column E, as it highlights the importance of continuous evaluation and analysis concerning business counterintelligence. It highlights the importance of not simply implementing business counterintelligence as a once off process

[293] Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 30.

within the organisation, and expecting that implementation to remain effective over the longer term[294]. Adversely to this, cell C3 *Current Security Measures* was found to be largely irrelevant for the effective implementation of business counterintelligence, thus relating more to traditional security approaches of analysis[295]. This as mechanisms for the evaluation of existing protection forms of business counterintelligence are conducted through – and therefore implicitly applied within – the *Vulnerability Identification/Assessment* and *Analysis* process stages. These elements were therefore deemed to be redundant for the purposes of integrative implementation relating to the business counterintelligence context.

The remaining consolidated categorisation of approaches, as represented in column E, were integrated by analysing both the operational security and counterintelligence processes in relation to the risk management structural process forms of security and strategy that were deemed to be value adding in their dispensation. It was thus felt that through such a form of selective logical weighting, a more effective, integrated business counterintelligence process could be developed. This while still remaining true to the original structural fundamentals of existing business counterintelligence process forms.

In terms of its integrated representation of flow, the business counterintelligence risk management process structure can thus be seen as displayed in Figure 1, where each step of the process, once completed, should in turn lead to and support the next. In order to gain a deeper level of understanding as relating to the broader specifications of each stage, I will now move on to discuss their basic fundamentals. I will also include additional insight where necessary[296], as represented within the core literary works used for the development of this generic form.

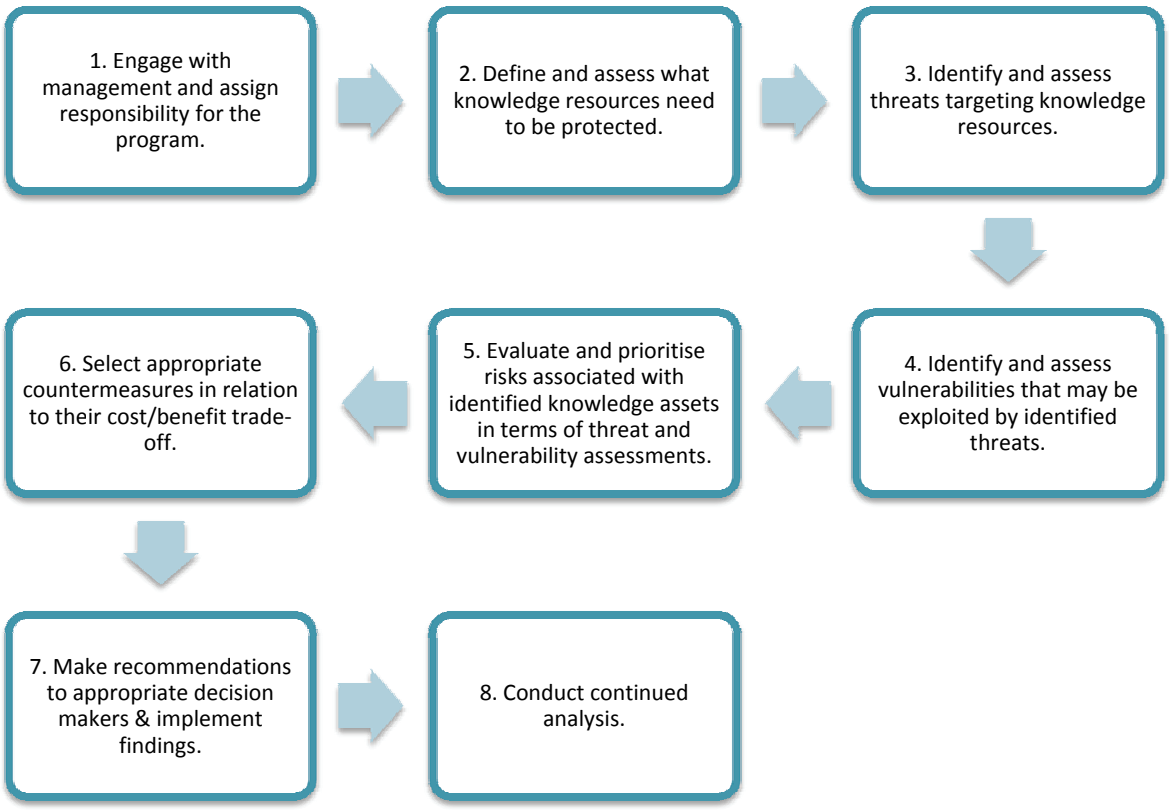
---

294 Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 30.

295 Vellani, K. 2007. *Strategic Security Risk Management: A Risk Assessment Guide for Decision Makers* p 20-21.

296 It is important to note that this analysis will be done in a simplified explanatory form due to the confines and restrictions imposed by the format of this study in terms of its objective outcomes. Should one require greater detail as to the procedural specifics of a particular task – represented within a selected stage of the process – it is suggested that one conduct further research on one's own by consulting those resources as mentioned in this investigation; supplying further elaborative detail.

Figure 1: The Combined Business Counterintelligence Risk Management Structural Process Flow



4.6.1.1 Stage 1 – Engage with management and assign responsibility for the program

Engaging with management and appropriately assigning responsibility for the business counterintelligence program is the first task of the process. Top level management support should be seen as essential[297] in this regard, as it will allow one to ensure that resources to support the initiative are obtained and that management backing is given to any recommendations that may arise as a result of the completed process. Once management has given the go ahead, options for assigning responsibility include recruiting a counterintelligence specialist, broadening the mandate of the head of security beyond physical security, assigning responsibility to an existing member of staff who is close to intelligence gathering operations or assigning responsibility to the staff member who is responsible for controlling the dissemination of information about the company[298]. The assignment of responsibility for business counterintelligence should in most cases go beyond the traditional security department of one's organisation, unless the department possesses a

[297] Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 30.

[298] West, C. 2001. *Competitive Intelligence* p 188.

deep understanding of one's business, objectives, strategy and plans[299]. Assignment should therefore be aligned with one's competitive intelligence function[300] and carried out by a few highly skilled individuals.

> Only a few (depending on the size of the company) highly skilled and trusted individuals reporting to the company's CEO should staff the counterintelligence section or unit. Counterintelligence personnel should understand your competitors and your business, and also have knowledge of basic security principles and measures[301].

Alignment with competitive should take place for two reasons. Firstly, the in-depth knowledge of a competitive intelligence team gives them a key understanding of how external interested parties may interpret the company's activities[302]. One must therefore be able to assess the capabilities and intentions of one's competitors before one can implement business counterintelligence in an effective manner[303]. Secondly, because of the large learning curve that one may have to overcome[304] – in relation to the interdependent nature of both offensive and defensive intelligence[305] – the integrative positioning of the two can thus help to decrease the challenge posed. This is viewed predominantly from an offensive intelligence standpoint.

As some state, from an operational security point of view, business counterintelligence should be implemented in a fragmented sense of separated identity[306]; which is essential in terms of its ability to retain key functionality and structural effectiveness. However, one needs to remain aware that through such an undertaking –in the integrated risk management sense of strategic implementation – if one is to view business counterintelligence as effective in this regard, than one should do so only if one is absolutely certain of the greater strategic ramifications of such an action[307]. Particularly in terms of consistency with an organisation's

---

299 Bernhardt, D. 2003. *Competitive Intelligence: Acquiring and using corporate intelligence and counter-intelligence* p 92.

300 Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 31.

301 Bernhardt, D. 2003. *Competitive Intelligence: Acquiring and using corporate intelligence and counter-intelligence* p 92.

302 Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 31.

303 DeGenaro, B. 2005. *A Case for Business Counterintelligence* p 13.

304 DeGenaro, B. 2005. *A Case for Business Counterintelligence* p 15.

305 DeGenaro, B. 2005. *A Case for Business Counterintelligence* p 15.

306 Mark, D. 1997. *Competitive Intelligence and the Corporate Jewels* p 67.

307 Clarke, C. & Varma, S. 1999. *Strategic Risk Management: the New Competitive Edge* p 415, state: "Risk management is a strategic business process. Management needs to assess whether the company's business

larger strategic objectives, as this can hold direct implications for success given an organisation's level of strategic advancement[308]. This is measured in terms of acceptance and development.

4.6.1.2 Define and assess what knowledge resources need to be protected

The second step of the process involves the identification of those core knowledge-driven competencies that are critical for the maintenance of one's competitive advantage[309]; recognising the fact that a company cannot protect all of its information to the same degree[310]. From a security risk management point of view this is assessed by determining those critical assets that require protection, identifying what undesirable events could happen to those assets, what the expected impacts of such undesirable events would mean for each asset and prioritising the various assets based upon the consequence of their loss[311]. These are usually researched as part of an integrated organisational interview process[312], expressed in qualitative terms.

> Up front, it is very important to recognize that the loss of people, information, and activities is difficult to quantify in terms of dollars. Therefore, it may be more appropriate to provide a qualitative statement expressing the consequence of that loss than it would be to quantify it in terms of dollars[313].

Knowledge competencies can include – but are not limited to – proprietary product technology, manufacturing processes, training techniques, internal operational systems, new product launches, mergers and acquisitions, research and development,

---

activities are consistent with its stated strategic objectives, and how risk management is linked to investment and growth decisions."

308 As Clarke, C. & Varma, S. 1999. *Strategic Risk Management: the New Competitive Edge* p 419, outline, companies typically range – and progress over time – in terms of risk management sophistication from: the identification of risks, having consistent measures across risks, linking risks and returns, employing capital allocation techniques, understanding dynamic capital allocation moving to a fully comprehensive value based strategy.

309 Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 31. As Bernhardt, D. 2003. *Competitive Intelligence: Acquiring and using corporate intelligence and counter-intelligence* p 88, also states: "The information companies need to protect includes technological as well as financial and commercial information that gives them a competitive edge over their competitors."

310 Mark, D. 1997. *Competitive Intelligence and the Corporate Jewels* p 67.

311 Roper, C. 1999. *Risk Management for Security Professionals* p 23.

312 Vellani, K. 2007. *Strategic Security Management: A Risk Assessment Guide for Decision Makers* p 17, states: "Asset information can come from various sources; however, critical asset information is best obtained from those who manage the day-to-day operations of the organisation. This may be the asset owners themselves or operations managers. Comprehensive interviews of these people should be conducted to obtain the information regarding each asset."

313 Roper, C. 1999. *Risk Management for Security Professionals* p 23.

financial details, or strategic plans[314] as well as information on the organisation's business competitive and counterintelligence functions. Understanding what needs to be protected is a very strategic consideration and should involve key stakeholders from diverse functional units within one's organisation. This should be done not only to identify critical information from an internal perspective, but from an adversary's point of view as well.

> This most important step should involve people well beyond the security circle. The involvement of functions such as research and development, strategic planning, human resources, intellectual property law, security, and business intelligence provide a necessary multidisciplinary approach to answering the question...You need to identify critical information not only from an internal view but also from a competitor's perspective. The process may even raise serious concerns about strategy but will undoubtedly contribute to the rich analysis of what makes the firm competitive[315].

Critical analysis from the competitor's perspective is essential as assets deemed to be of lesser importance within one's organisation may hold greater value for an adversary[316]. Asset assessments must therefore be based not only on their mission-critical level of importance, but also on the potential value that disparate assets may contain, in enabling an adversary to discover more critical forms of one's knowledge competency and organisational strategy.

Finally, it is important to note that the size of one's organisation is not necessarily related to its need for knowledge competency protection; i.e. assuming that larger organisations require greater levels of protection, while smaller organisation do not[317]. Rather than placing emphasis on the size of one's organisation, one should rather place a greater emphasis on identifying those areas of sensitive information found within one's organisation, through a process such as this one. One can then set about correctly evaluating these either internally or with the help of a trusted consultant[318], in terms of the degree of importance that such information may present for a potential adversary.

---

314 As Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 31, outline, this can be anything that might allow a competitor to out-manoeuvre ones organisation.

315 DeGenaro, B. 2005. *A Case for Business Counterintelligence* p 14.

316 Vellani, K. 2007. *Strategic Security Management: A Risk Assessment Guide for Decision Makers* p 17.

317 As Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 31.

318 Vellani, K. 2007. *Strategic Security Management: A Risk Assessment Guide for Decision Makers* p 17.

> Many companies mistakenly believe that they are too small to be thought of as having valuable information. A good example of how that assumption can lead to disaster is the story of a small, 20-person software engineering firm in Palo Alto, California, that was infiltrated by an agent of the French Government (Nolan, 1996b). Although the perpetrator was caught and charged, the firm had no idea that they might be a target of intelligence gathering until their proprietary information was "out there"[319].

4.6.1.3 Identify and assess threats targeting knowledge resources

Identifying and assessing threat entities that may be targeting one's knowledge resources is of critical importance for business counterintelligence. Understanding these potential threats requires an understanding of one's adversary, in terms of their intentions and motivations, as well as their capabilities to obtain and compromise one's critical knowledge assets[320]. From an integrated risk management perspective this is achieved by identifying adversaries, assessing the intent and motivation of those known or suspected adversaries, assessing the capabilities that these adversaries have, determining the frequency with which such incidents have taken place (derived from historical data) and estimating the degree of the threat posed relative to one's identified knowledge assets[321]. This is assessed in conjunction with the help of one's competitive intelligence function.

> Primarily, you want to understand your competitor's (or potential competition's) intelligence-collection capability and its underlying, governing philosophy (Nolan, 1997)...Assessing this threat is a classic CI [competitive intelligence] function, and you may already have most of the information you need from your regular CI processes...A thorough understanding of their CI capability can let you know exactly what you are up against, and perhaps provide the opportunity for you to control the information they get[322].

---

319 As Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 31.

320 As Roper, C. 1999. *Risk Management for Security Professionals* p 24, outlines, to identify and characterize the threat, one should prepare a list of potential threats and, once identified, determine if there is a specific group or individual; assess their intent, capability, and history (if known); and then make a judgement based on your assessment of the threat level as it relates to each specific asset or undesirable even that could occur. It is important to quantify the risks. For more operational risks such as safety or technology risks; quantification often requires making assumptions, this can be done qualitatively through the use of a critical, high, medium or low ratings structure in relation to a particular knowledge asset and the likelihood of any potentially undesirable events occurring.

321 Roper, C. 1999. *Risk Management for Security Professionals* p 20.

322 Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 31-32. In addition, as Mark, D. 1997. *Competitive Intelligence and the Corporate Jewels* p 68, states: "While a company is attempting to acquire information on a competitor's marketing plans it would task its human source

In its broadest sense, threats to knowledge assets can be posed by one's competitors or potential competitors (both foreign and domestic), foreign government's intelligence services (both hostile and friendly), criminals of all types, terrorists and activists[323]. These threat entities may deploy a variety of active measures[324] in order to achieve their knowledge acquisition goals; not always directed in a legal or ethical manner[325]. The most potentially devastating measure – from amongst the intelligence gathering plethora[326] predominantly in an espionage sense – is through the use of a penetration agent who may act alone or attempt to coerce other employees to act in conjunction with his objectives. This may be due to a particular psychological, ideological or materialistic motivational weakness.

---

collectors to also develop information that might indicate efforts by the competitor to collect its corporate information. Thus, while a company seeks to learn from suppliers information that might indicate that a competitor is gearing up for a new line of business, it would also seek to learn whether the suppliers are aware of any information that might indicate an intelligence interest by the competitor company in its operations."

323 Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 33.

324 Bernhardt, D. 2003. *Competitive Intelligence: Acquiring and using corporate intelligence and counter-intelligence* p 91, outlines that possible indicators of intelligence operations being directed against ones company, include occurrences such as: Competitors know about your new projects, confidential business, trade secrets and strategies; Various enquiries are made by strangers such as 'students, researchers and others' about your company's secrets and new projects; Repair technicians show up to do 'technical work' when no one has called them; The same competitors regularly beat you in tenders and business contracts; Electronic bugging or surveillance devices are discovered on your business premises; There are constant foreign requests for information or for permission to visit your company or facility; Competitors beat you to the market with new products looking very similar to your own designs; Confidential material, information and equipment such as laptops are stolen under suspicious circumstances; Key staff leave your company to go and work for a competitor.

325 Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 32-33, state: "It must be remembered that not everyone interested in what your organization does is ethical. The possibility that illegalities might be undertaken to harm your company must be seriously considered...These threats can come from a wide variety of organizations with a surprising variety of reasons for wanting to damage your business. They can take an assortment of forms, from simple break-and-enter to the more sophisticated hacking into computer systems or electronic eavesdropping...Recent events that are interesting examples of threats coming from non-competitive sources are groups that have been dubbed "hacktivists". These groups launch software attacks on companies involved in activities to which they are politically opposed, such as nuclear proliferation or pollution, and perform acts of sabotage as a form of protest. An electronics company manufacturing electrical components used in a nuclear power plant could suddenly find itself under attack and its business stability threatened by an enemy it didn't even know it had."

326 As Pattakos, A. 1998. *Threat Analysis: Defining the Adversary* p 56-57, states: "Each of the collection disciplines employs several sources for collection – redundancy for confirmation and for full coverage is part of most collection plans...HUMIT [human intelligence], for example may use one or more agents – those deliberately recruited, co-optees, unwitting sources, defectors, refugees etc. HUMIT may also use technical penetrations (monitoring/eavesdropping), observation, garbage rummaging, or hand-held photography...SIGINT [signals intelligence] includes communications and non-communications electronic signals. Telemetry and instrumentation signals used during testing systems, and radar is used in the latter method. IMINT [imagery intelligence] includes photography, electro-optics and optical methods as well as radar and infrared images. MASINT (Measurement and Signature Intelligence) includes a wide variety of sources, including aspects of each of the foregoing as well as laser, radiation and nuclear and their measurements. The actual materials, knowledge of materials used in the research or in the development of a product, or an analysis of the debris discarded during the product research or developmental process is also important intelligence. DATAINT [data intelligence] may include outsiders (hackers/crackers), and insiders with access to computer systems, and technical exploitation."

> Probably the biggest threat is the 'penetration agent', a staff member working for the competitor. This allows the competitor access to records, files, documents, products, equipment, strategic plans, and customer and sales records to increase their competitive edge. This industrial spy will look for 'holes' to penetrate the business under attack. One such hole is of course the angry or dissatisfied employee [who may be motivated by] material, emotional and/or ideological reasons. This motivation to spy could be caused by a deep dissatisfaction about status, insecurity, being a member of a minority group, being overly ambitious or fanatical or could also be caused by some obsession. Alcohol, drugs, gambling and sex are just a few of the vices that can easily turn into an obsession[327].

In addition to illegal intelligence gathering – given the large proportion of information that can be obtained easily through available open sources of collection[328] – one should not underestimate the effectiveness of legal intelligence gathering initiatives targeting one's organisation directed through adversaries' competitive intelligence gathering functions. The gathering of such information by an adversary can pose a serious threat to one's organisation, should one not have in place adequate business counterintelligence protection practices.

> Given the current emphasis on the national and global information highways, the Internet, the proliferation of commercial databases, electronic news groups, and peoples' propensity to "chat" about what they do, the threat and thus wide-ranging capability for collection using open sources [of intelligence] (OSINT) is a

[327] Bernhardt, D. 2003. *Competitive Intelligence: Acquiring and using corporate intelligence and counter-intelligence* p 90-91. Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 33, state: "One common methodology is to exploit people already within the company. Candidates for this method could include such insiders as on-site nonemployee workers (contract personnel), regular employees who have something to hide (blackmail), disgruntled employees, thrill seekers, activists, ideologues, departing employees, or former employees (Winkler, 1997). In short, anyone against whom some leverage could be used...These people need not be exploited by an outside agency. Personal motivations could lead them, of their own volition, to commit the thefts and then look for buyers. Most commonly, insiders will remove, copy, photograph, download, or otherwise steal sensitive information from your organization. They might also simply overhear, electronically bug, or eaves-drop conversations (Tracy, 1998)." From personal experience I have been in a situation where I was conducting research work for a large organisation. The office was open plan and the head of the organisation could be heard talking away about key business moves and strategies to his associates primarily on the phone. If I had been of such a dispensation that I wished to use this against the organisation, it would have been very easy to do so by eaves-dropping or even employing further technical surveillance measures inside the office in order to record these valuable conversations. In addition Pattakos, A. 1998. *Threat Analysis: Defining the Adversary* p 57, states: "However, there are other insiders as well who may have indirect access and still provide bits and pieces of information of value to a collector. These indirect insider sources may include vendors, suppliers, subcontractors, and employment agencies, to name a few. Those with direct access [such as insiders] may or may not be employees. Among others, this group might include bankers, teaming/joint venture partners, board members, interns, auditors, and family members."

[328] National Counterintelligence Centre. 1997. *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage* p 6, states: "Open-source collection activities include, but are not limited to, review of trade journals or corporate annual reports, marketing surveys, and attending conferences and symposia."

> significant threat to corporate secrets. Some 80 to 90% of needed intelligence is available using no-risk open sources of information[329].

Finally, once possible adversaries and the potential collection methods that they may employ have been identified, it is then important to interpret both the intentions and capabilities of these adversaries to collect information. This should be done as the overall risk posed by an adversary may be reduced sharply when either one of these elements are missing[330]. This can be effectively achieved by conducting a threat analysis whereby different adversaries are assessed with the help of a qualitative threat matrix[331]. This in terms of their intent to collect knowledge; their capability to collect this knowledge; indications that they are attempting to collect knowledge; the probability that they will aim to collect knowledge and the methods that they are employing or will employ in order to do so[332]. All of which enable one to build a more comprehensive understanding of one's adversaries or potential adversaries and their capability and intention to collection critical information.

4.6.1.4 Identify and assess vulnerabilities that may be exploited by identified threats

Vulnerability in this instance refers to any weakness within one's organisation that will provide an adversary with the opportunity for exploitation[333]; in this case concerning one's identified critical knowledge assets[334]. From a risk management point of view, this is assessed by identifying the potential vulnerabilities related to specific assets, identifying those existing countermeasures in place, their level of effectiveness in reducing vulnerabilities[335] and estimating the degree of vulnerability relative to each asset and threat entity[336]. One can also seek to examine one's organisation for vulnerability from an adversary's perspective – through competitor emulation – as it provides one with a base for understanding the true,

---

329 Pattakos, A. 1998. *Threat Analysis: Defining the Adversary* p 57.

330 Roper, C. 1999. *Risk Management for Security Professionals* p 24.

331 Pattakos, A. 1998. *Threat Analysis: Defining the Adversary* p 58-60.

332 Pattakos, A. 1998. *Threat Analysis: Defining the Adversary* p 60.

333 Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 33.

334 The importance of which is outlined by Mark, D. 1997. *Competitive Intelligence and the Corporate Jewels* p 68, in the following extract: "It was proposed and accepted by management to determine the very few aspects of the technology that were truly unique for the company's competitive posture and to try and develop a protection program for them. This made the job of determining vulnerability and threat much easier as the company was able to take a realistic look at company operations and then devise legal and security countermeasures that had a chance of actually protecting the critical jewels. If the company had simply attempted to protect all information deemed sensitive, such a program would have been futile since there was no way to monitor losses or to evaluate its importance to the program."

335 Roper, C. 1999. *Risk Management for Security Professionals* p 26, explains that one must not assume that existing countermeasures in place are still adequate, as this is a commonly made assumption, one that can be detrimental to an organisation and its knowledge assets over the longer term.

336 Roper, C. 1999. *Risk Management for Security Professionals* p 21.

rather than purely hypothetical[337] nature of vulnerabilities faced. This is in some instances referred to as a Red Team test.

> More firms are showing an interest in learning just what leaks they have. This is especially true if the company has been stung or is convinced through reading about other cases that the threat is real...During this analysis, it is important to determine what kind of competitor they wish the Red Team to emulate. The team should include experienced intelligence people able to emulate the most aggressive competitors. The project should be closely held but involves security, legal, and senior management. Guidelines for situations (such as an employee being offered money for information) should be worked out in advance. A little preliminary work can go a long way towards insuring a successful project[338].

Threat based vulnerabilities concerning one's knowledge assets that may be discovered as the result of assessment and Red Team test, can be broadly categorised in terms of operational, physical, personal and technical vulnerabilities[339]. Undertaking such vulnerabilities involves a considerable amount of organisational self-examination in order to effectively identify as many weaknesses – relating to one's critical knowledge assets – as one can[340]. Elements contained within these broader areas of categorisation – as part of the business counterintelligence process outlined by Fleisher and Blenkhorn[341] – can be discussed and summarised as follows:

> Operational Vulnerabilities – refer to weaknesses in the way an organisation operates, in terms of giving out information, on a day to day basis, potentially revealing its

---

337 Roper, C. 1999. *Risk Management for Security Professionals* p 26.

338 DeGenaro, B. 2005. *A Case for Business Counterintelligence* p 14. As Bernhardt, D. 2003. *Competitive Intelligence: Acquiring and using corporate intelligence and counter-intelligence* p 95, outlines: "*Penetration testing* refers to the assessment of the vulnerabilities of sensitive facilities, areas and activities to outside attack. High-value commodities within the business environment are targeted on a daily basis by perpetrators attempting to penetrate facilities, systems or countermeasures to reach their aim. Where physical high-value commodities are involved the loss may be felt within a short time and be directly linked to a specific incident that took place. When incidents of penetration take place to copy documents or other information or to gather information by electronic eaves dropping the loss may only be discovered long after the penetration has been perpetrated...Most security systems cannot withstand an effective penetration effort by a professional espionage team. This is mainly due to a lack of properly conducted security and counterintelligence surveys and analysis of critical factors, systems designs not tested in practice, the human factor, a low level of security and information protection consciousness, the absence of regular auditing and the absence of penetration testing of implemented systems. Regular penetration testing will evaluate the effectiveness of the systems in place, improve overall security and limit opportunities for the industrial spy."

339 Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 33.

340 Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 33.

341 Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 33-35.

future strategic objectives[342]. Such information can be discovered by adversaries due to the large volumes of formal documents generated by an organisation (both private and public) including securities exchange filings, strategic plans, manufacturing and product specifications and financial reports[343]. Indirectly, clues including travel records indicating the occurrence of meetings and bills of lading that may reveal who is purchasing what from whom, can be significant in the context of other information an adversary may already have gathered. Perhaps the most significant operational vulnerability is the lack of general awareness among personnel as to what exactly constitutes sensitive information. Employees through legal methods of exploitation may adversely reveal sensitive information to a competitor[344] that they should not have.

Physical Vulnerabilities – are another area of significant exploitation. Many organisations do not have suitable access controls in place, combined with a lack of effectively trained physical security staff. In addition the biggest vulnerabilities are often created by not using what is readily available to one's organisation. This includes simple activities such as the locking of drawers and rooms that contain sensitive information. Computers may be left on or contain no password protection so that anyone gaining physical access could make use of the system. A messy desk is vulnerable, as documents that should be stored away are left in the open for any passerby to read. Such vulnerability may be compounded further by improper disposal procedures, resulting in the leaking of sensitive information to competitors through activities such as *dumpster diving*.

---

342 Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 33, provide a simple example of this: "the chief executive officer who was trying to show the Environmental Protection Agency that his company could not afford the large fined that it was being assessed. In attempting to do so, he brought his financial spreadsheets to the hearing. As part of the minutes from the hearing, they became part of the public record (Richard Combs Associates, 1998)" thus exposing them to the organisations rivals.

343 Martin, P. 2002. *Harnessing the Power of Intelligence, Counterintelligence and Surprise Events* p 81, in addition states: "Most companies secrets are obtained legally. Topping the sources is excessive disclosure to government (corporate filings), the staff (internal newsletters), the media (press releases, impromptu briefings), trade publishers, banks, credit agencies (Standard & Poor's, Dun & Bradstreet) and other third parties who disseminate these intelligence leaks."

344 Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 34, provide the following examples: "Many things can be learned because somebody phoned and asked for the information. Most of these information calls go unreported to those for whom the pattern of inquiry may make up a picture. People also take work with them to do in public places, such as the commuter train, where interested parties could simply read over their shoulder. Casual conversations in public places can be very revealing as well."

Personnel Vulnerabilities – focus on the way in which companies hire and manage their employees. Not conducting extensive personal background checks on prospective candidates and verifying claims made on their resumes can result in the acquisition of unsuitable individuals. These could be people with criminal intent or susceptibility to exploitation by an adversary. In addition, if it is not well disseminated that a particular individual's employment has been terminated, this person could still continue to gain access to the organisation's critical knowledge assets and inflict severe damage.

Technical Vulnerabilities – are essentially weaknesses that can allow for compromise of organisations' critical knowledge assets through their computer systems[345]. The risk associated with these insecure computer systems is why – when advertising to hire technical people – one should not list those systems on which one would like candidates to have had experience. The reason for this is that it essentially tells adversaries what they need to know, should they wish to compromise one's information systems. In addition to this, the use of poorly defined password protocols, not closing unused accounts, uncontrolled modem access and poor systems personnel training are other factors that create technical vulnerabilities. Existing employees can exploit these without using the Internet by having direct access to one's local area network (LAN), may copy poorly protected information or create holes for it to be removed externally, either alone or with co-conspirators.

4.6.1.5 Evaluate and prioritise risks associated with identified knowledge assets in terms of threat and vulnerability assessments

The evaluating and prioritising of risks associated with one's identified knowledge assets are primarily a form of risk assessment[346]. In this context as applied to business

[345] Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 34, state: "Each computer system on the market has known vulnerabilities that hackers try to exploit. Failure to secure known weakness in the systems with readily available patches is a very significant problem in many organizations."

[346] As Roper, C. 1999. *Risk Management for Security Professionals* p 73, outlines when discussing security risk management: "Risk assessment is the process of evaluating threats to and the vulnerabilities of an asset to give an expert opinion on the probability of loss or damage, and its impact, as a guide to taking action." From a strategic security point of view Vellani, K. 2007. *Strategic Security Management: A Risk Assessment Guide for Decision Makers* p 112, sums up risk assessments as follows: "Risk assessments are comprehensive and rational reviews that offer a logical and defensible method for security professionals to make decisions about security expenditures and to select cost-effective security measures that will protect critical assets and reduce risk to an acceptable level...Risk assessments are typically a staged process whereby critical assets are identified, current countermeasures are enumerated, threats are identified, vulnerabilities are defined, and prioritized recommendations are made to protect critical assets based on probabilities of attack."

counterintelligence, risk assessment is used in order to determine the likelihood of compromise based on the broader assessment of previously collected data[347]. This is achieved by estimating the degree of impact relative to each critical knowledge asset, the likelihood of an attack by a potential adversary, the likelihood that a specific vulnerability relating to an identified asset will be exploited, aggregating the degree of impact that a successful attack will have (threat x vulnerability) to determine the degree of associated risk and prioritise risks based on this integrated assessment[348]. From an operational security point of view – as applied to business counterintelligence – this is seen as key in determining how the approach may be implemented in the organisational context; in relation to the effective application of defined countermeasures.

> The final two steps (assessing risk and applying countermeasures) further determines how you implement operations security....At this point in the process, it is key to convince management that OPSEC [operational security] is an essential tool and won't consume the total organization. It can be implemented incrementally and will contribute value by providing immediate awareness[349].

The evaluation of risk, as outlined from a security driven risk assessment perspective[350] begins by conducting a baseline review of one's existing risk under current protection conditions; including any countermeasures already in place. This is done with the help of a *Risk Analysis Matrix* which identifies unacceptable risks and determines one's protection priorities in terms of the integrated evaluation of: potential undesirable events, the impact rating, the threat rating, the vulnerability rating, the overall rating and the combined risk acceptability rating. This allows one to prioritise risks from most important to least important. In the case of critical knowledge assets this is best evaluated qualitatively in terms of high, medium or low ratings[351]. This rating allows one to deduce if a risk is acceptable or not and

---

347 Roper, C. 1999. *Risk Management for Security Professionals* p 21.

348 Roper, C. 1999. *Risk Management for Security Professionals* p 21.

349 DeGenaro, B. 2005. *A Case for Business Counterintelligence* p 14.

350 Roper, C. 1999. *Risk Management for Security Professionals* p 27.

351 Vellani, K. 2007. *Strategic Security Management: A Risk Assessment Guide for Decision Makers* p 112, states: "Quantitative assessments are normally used when the assets in need of protection are of lower value or when data is not available. Qualitative risk assessments may also be used when insufficient historical information or metric data exists, precluding a quantitative approach. The results of qualitative assessments depend on the assessment skills of the people involved in the assessment. Risk levels are normally given in abstract values such as high, medium, or low or colour coded... Risk assessments can be both qualitative and quantitative, or a hybrid...Hybrid risk assessments utilize quantitative data where available and qualitative where metrics are not readily available or insufficient. While assessing risk is more art than science, the risk assessment methodology should be structured so that the results and recommendations can be replicable given a different assessment team. Risk assessments should generally be quantitative to the extent possible,

therefore helps one to determine the degree of protection that may be required – when selecting appropriate countermeasures in the process step to follow – relative to one's organisational knowledge asset risk ratings at that present moment in time.

4.6.1.6 Select appropriate countermeasures in relation to their cost/benefit trade-off

The objective of this stage is to identify countermeasures that are able to reduce or eliminate one or more identified vulnerabilities and then conduct a cost-benefit analysis[352] to determine which of these countermeasures are going to be the most cost-effective. From a security risk management perspective this means identifying potential countermeasures to reduce one's vulnerabilities, identifying each countermeasure's capability and its effectiveness, identifying the cost of countermeasures and conducting a countermeasures cost-benefit and trade-off analysis[353]. These elements thus aim to effectively protect one's knowledge assets from compromise in the most effective way possible.

The costs associated with countermeasures may be measured in monetary terms, inconvenience, time, or personnel[354]. In this instance consideration in terms of cost should not only be given to those tangible manifestations of the countermeasure, but also the on-going operational costs associated with the countermeasure and its implementation[355]. The evaluation of cost in relation to the potential benefit of a proposed countermeasure should be analysed by closely examining how the asset value will relate to the proposed cost of implementing each countermeasure and which potential option will therefore provide the best protection. This should be measured in terms of its effectiveness mitigating the associated

---

recommendations for additional security measures should be the result of a cost-benefit analysis, and measures should be benchmarked against industry standards."

[352] Roper, C. 1999. *Risk Management for Security Professionals* p 28-29, states: "Benefits are expressed in terms of the amount of risk reduction that is possible based on the overall effectiveness of the countermeasures...Countermeasures should relate directly to the vulnerabilities associated with an unacceptable risk." This can be examined by assessing countermeasure options in relation to high priority vulnerabilities in terms of: listing current undesirable events that may affect a particular asset, listing the existing risk level, the related vulnerabilities, those countermeasure options that can be implemented and the new level of associated risk that will be gained.

[353] Roper, C. 1999. *Risk Management for Security Professionals* p 21.

[354] Roper, C. 1999. *Risk Management for Security Professionals* p 82. In the context of this discussion the monetary aspect of cost will be focused upon, due to its relevance as a tangible form of measurement concerning the protection of one's knowledge assets.

[355] As Roper, C. 1999. *Risk Management for Security Professionals* p 82-83, states: "Written procedures are usually the least expensive type of security countermeasure. Hardware is generally more expensive than written procedures, and manpower costs are typically the most expensive form of countermeasures." One can thus determine the monetary cost of a countermeasure by examining cost elements such as the purchase price and the life-cycle maintenance costs, the countermeasures life expectancy and the salaries of staff and contractors needed to implement or maintain it.

risk of a particular asset to an acceptable level[356]; based in part upon one's previously evaluated risks.

One can then proceed to prioritise one's countermeasures by giving preference to those options that address more than one undesirable event or collectively lower the risk for all identified knowledge assets[357]. One may also take into account the period of protection required, as assets that have a shorter life span, may require a less costly or different form of protection. This is done in order to lower their level of associated risk, depending on the longevity of value that they contain.

> Thus, the protection requirements could be less stringent and less costly. This is a key factor in protecting any information: It should be protected using only those methods necessary, and only for the time period required, based on the value of that information over time[358].

Business counterintelligence countermeasures can be implemented in both an active and passive sense, with passive implementations being more commonly recommended within organisational contexts[359]. Passive counterintelligence measures are orientated defensively and aim to counter what an adversary may do. Such countermeasures include awareness briefings, technical surveillance countermeasures (TSCM) and penetration testing[360]. Active measures as opposed to passive measures are offensive in character – which when employed aggressively are also a collection process[361] – with the aim of conducting operations that will eliminate any ongoing or threatening activity directed towards one's organisation[362]. Business counterintelligence countermeasures can once again be categorised briefly into broader areas

---

356 As Roper, C. 1999. *Risk Management for Security Professionals* p 85.

357 As Roper, C. 1999. *Risk Management for Security Professionals* p 85, explains, one should bear in mind that "the costs of protective measures should not typically exceed a reasonable percentage of the total value of the assets requiring protection. However, there is no one "reasonable" percentage across the board for all assets, or even for all assets within a given group."

358 Kovacich, G. & Halibozek, E. 2003. *The Manager's Handbook for Corporate Security* p 82.

359 Bernhardt, D. 2003. *Competitive Intelligence: Acquiring and using corporate intelligence and counter-intelligence* p 89-94, states: "Passive counterintelligence aims to counter what a competitor may do and comprises mostly preventative measures. These measures are also recommended for most companies...It is better to prepare in advance against what a competitor can do than to deal with the information loss after it has occurred. This will minimize or prevent the success of potential actions by competitors...The measures are not expensive to implement and will enhance efforts to protect sensitive and confidential information."

360 Bernhardt, D. 2003. *Competitive Intelligence: Acquiring and using corporate intelligence and counter-intelligence* p 89; which in the context of this procedural outline can be thought of primarily as a form of vulnerability assessment, and therefore applicable to that section of analysis.

361 Bernhardt, D. 2003. *Competitive Intelligence: Acquiring and using corporate intelligence and counter-intelligence* p 89.

362 Bernhardt, D. 2003. *Competitive Intelligence: Acquiring and using corporate intelligence and counter-intelligence* p 89.

of discussion relating to operational, physical, personnel and technical based countermeasures as outlined by Fleisher and Blenkhorn[363]; discussed and summarised in addition to other key perspectives as follows:

> Operational Countermeasures – The primary operational countermeasure that one should consider is that of an awareness program. Such a program should educate employees about the critical relationship that they play concerning the organisation's knowledge assets in the light of its on-going operations relative to that of its adversaries[364]. The awareness program should be supportive and non-threatening, as threats can result in the manifestation of poor morale and may therefore potentially increase vulnerability. An awareness program should educate employees of the value of information to both the organisation and its adversaries, how adversaries may collect and assess it and the employees' role in the countermeasures to prevent it.
>
> To further support this higher level of awareness, an incidence-reporting protocol should also be established. Requests for information by unknown entities should be reported and dealt with on a call back basis only; the employee dealing with the call should capture the details of the caller, the information being asked for and the timeline for the request. The need for information both externally and internally should always be verified. In addition to these steps, sensitive information should be placed in controlled environments and reporting should be encouraged concerning attempted or unauthorised access. Furthermore, any document containing an employee name should be considered confidential. Proprietary information relating to specific projects should be restricted on a need to know basis and sensitive financial information should be restricted to those for whom it is relevant.
>
> Companies spend millions on computer firewalls, access control and other security barriers but few invest in awareness training for their staff. The best security systems will be useless if staff members are ignorant about the tactics and modus operandi employed to steal business secrets. Regular awareness training will

[363] Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 35-38.

[364] Bernhardt, D. 2003. *Competitive Intelligence: Acquiring and using corporate intelligence and counter-intelligence* p 94, states: "Counterintelligence education aims to heighten the awareness of personnel and alert them to the threats of business espionage and other dangers to information...The best security systems will be useless if staff members are ignorant about the tactics and modus operandi employed to steal business secrets. Regular awareness training will improve staff's knowledge of the legal, unethical and illegal information-gathering techniques."

> improve staff's knowledge of the legal, unethical and illegal information-gathering techniques[365].

Physical Countermeasures –include the training of security guards, restricting copier use, shutting down of computers, locking doors and drawers, making sure that desks and in-boxes are cleared of sensitive information, discarded papers are suitably shredded and that generally speaking unusual activity is questioned. One should also conduct training to ensure that business conducted away from the office is done so in a discreet manner. Documents that are to be published and speeches presented should be reviewed for any unsuitable content that they may contain. One can also establish non-disclosure agreements with suppliers to help ensure that they do not reveal crucial components or usage information to adversaries. One's website should be sanitised to only include general information devoid of any criticality. Regulatory documents and findings reports submitted to government agencies should only include the minimum necessary amount of detail to comply with their requirements.

Personnel Countermeasures – centre on the effective management and handling of employees and associated employee orientated protection elements; background checks and termination procedures being examples of this. In addition, information detailed within job advertisements posted by one's organisation can also be restricted to prevent revealing too much. One can also categorise employees as permanent, temporary and contract in order to impose appropriate restrictions on what these different types of employees have access to. Such an action can help to prevent those with a lesser interest in the company taking advantage of one's organisation for the purposes of intelligence gathering; all of which should be supported by one's human resources function. One can also make provision for non-disclosure and non-competitive agreements so as to deter one's employees from taking up employment with specified competitors within a stated future period of time. Programmes can also be developed to help identify and monitor employees deemed to be vulnerable to outside coercion.

> An employee assistance programme (EAP) can become an important counterintelligence tool...defensive measures should be able to help to identify those with the problems mentioned above and the EAP should be aimed at

[365] Bernhardt, D. 2003. *Competitive Intelligence: Acquiring and using corporate intelligence and counter-intelligence* p 94.

> improving the well-being of the troubled staff member. The EAP offers counselling and other support to help people find solutions to the problems that distract them[366].

Technical Countermeasures – deal with issues relating to technical vulnerability and include additional training and awareness elements as well. Systems administrators' knowledge about the importance of dealing effectively with system vulnerability is an example of this. Further education relating to the effective use and management of passwords by ones employees can also be done. This should include the development of protocols for assigning passwords in person, the use of strong passwords and change mechanisms for regularly expiring passwords. In addition one can develop policies related to where and how proprietary information is stored and handled within the system, as well as the implementation of access controls. Much of this can be supported by one's information systems security function, and may also include the implementation of cryptography measures[367] and telecommunications, network and internet security elements[368]. The implementation of other countermeasures will depend on one's budget and those system complexities faced. These can include antivirus software, intrusion alert software and mirrored logs. In addition to information system orientated countermeasures, one can also employ technical surveillance countermeasures, which aim to identify illegal devices planted within one's organisation for information collection purposes. Technical surveillance countermeasures should be considered as an additional measure of protection, particularly if one has already implemented a successful basic business counterintelligence programme.

> Technical surveillance countermeasures (TSCM) are a set of measures to identify hostile and illegal technical devices planted for information collection purposes. If all avenues to a company have been successfully cut off for the industrial spy he or she will turn to technology...Major decisions are often made orally long before they are committed to writing. The audio surveillance of important meeting places and boardrooms where decisions are made can give the industrial spy not only the information required but also the lead time to make good use of the information...It is important to note that professionals utilizing appropriate equipment and

[366] Bernhardt, D. 2003. *Competitive Intelligence: Acquiring and using corporate intelligence and counter-intelligence* p 94.

[367] Hansche, S., Berti, J. & Hare, C. 2004. *Official Guide to the CISSP Exam* p 377.

[368] Hansche, S., Berti, J. & Hare, C. 2004. *Official Guide to the CISSP Exam* p 515.

> techniques should conduct technical surveillance countermeasure surveys. Regular TSCM surveys have become a standard business practice. The sensitivity level of the area will dictate if more or fewer inspections are required[369].

Finally, another very effective but sometimes costly countermeasure tool[370] is the use of deception or perception management, with the aim of creating a false impression or confusing one's adversarial intelligence gathering mechanism[371]. The use of deception can relate, for example, to a rival organisation's competitive intelligence function. This is done so that their decision makers make incorrect assessments of one's own organisation or no longer trust the information they are receiving from their intelligence gathering mechanisms[372]. Perception management tactics are usually not employed as an organisational wide strategy, but rather as a form of specific deception relating to a sensitive project[373]. Such an undertaking should be carefully managed and applied in a refined yet effective way, so as not to adversely affect the image of one's organisation to its stakeholders.

> Great care must be taken – especially in a publicly traded company – when creating false impressions. For example, a recent case of fake website postings by a company's employee implying a coming merger caused the stock to skyrocket and led to a charge of securities fraud (Wyatt, 1999). That being said, misinformation that isn't illegal is not necessarily immoral. After all, you don't owe someone the information just because they asked for it[374].

4.6.1.7 Make recommendations to appropriate decision makers & implement findings

The penultimate stage of the process consists of making recommendations to appropriate decision makers and implementing approved findings, based on one's prioritised knowledge risks. The costing and risk information generated in the previous steps of the process should be used to help support management's decisions in this regard. Recommendations should be made in terms of a few key possibilities ranging from least expensive to most expensive, with variability's presented in-between. This should include the advantages and disadvantages of each option being expressed and a recommended approach chosen with its associated rationale clearly explained.

---

369 Bernhardt, D. 2003. *Competitive Intelligence: Acquiring and using corporate intelligence and counter-intelligence* p 94-95.

370 Hutchinson, B. 2002. *Proceedings of the European Conference on Information Warfare and Security* p 71.

371 Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 43-44

372 Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 43-44

373 Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 38

374 Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 38.

> The cost information will be used to help you decide which countermeasure option to recommend to the customer. One of the options you identify should represent a risk avoidance/elimination approach, providing maximum protection (most likely at the greatest cost), one should represent the least expensive approach, and the other option(s) should be between these two examples...One of the options should be recommended and the rationale clearly spelled out. The customer makes the final decision about countermeasures employed and assumes the risks present in that option[375].

Once decision makers have weighed up all the options presented to them and selected a relevant approach, the organisation can then proceed with its implementation. This should be done by the business counterintelligence function and associated stakeholders involved in those key areas of countermeasure application where deemed necessary. Policies and procedures should be drawn up in conjunction with any countermeasures to be implemented and all information and records relating to the process should be documented and secured effectively. It is important to remember that the process of implementing a business counterintelligence plan should be treated as confidential and should only involve those stakeholders that are necessary for its implementation. Decisions about cost allocation and funding for the various countermeasure projects to be implemented should be done in conjunction with key decision makers when selecting an appropriate approach. These should then be finalised when specific solutions relating to a selected outcome are chosen. Again all such information in this regard should also be appropriately secured.

4.6.1.8 Conduct continued analysis

Continued analysis is important if one wants to make a success of any such integrated business counterintelligence process form implemented within one's specific organisational context; particularly over the longer term. Such analysis should include a regular and rigorous review of the success in prevention of one's selected approaches and adversaries' successes in obtaining information[376]. This is important as intelligence gathering is a dynamic process and it is unlikely that adversaries will continue to use the same approaches if they find these approaches are no longer working. In addition technological change may offer up new avenues of vulnerability and therefore new avenues for an adversary to exploit[377].

[375] Roper, C. 1999. *Risk Management for Security Professionals* p 85-86.

[376] Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 38.

[377] U.S. Marine Corps. 2007. *Counterintelligence* p 9.

Organisations also change over time, venturing in new directions, changing their structures and capabilities and targeting new markets both locally and abroad; therefore facing new adversarial threats. If one seeks to implement an effective sustainable form of business counterintelligence and build an environment where knowledge risks are lower and intellectual capital is better protected, than continued analysis through the use of the consolidated business counterintelligence process and its elements are essential.

> The collection of information should be difficult enough that the true CI professional will not be able to form a full or clear picture of your intentions in a timely manner. The collection of information by those using less ethical means should be difficult enough that they will go elsewhere to seek easier prey. The self-analysis process must be continuous. Each activity must be thought of in terms of what it might tell someone else, and then, conversely, how it might be done so as not to be too revealing[378].

4.7 Conclusion in Brief

Given the large amount of disparity that surrounds the topic of business counterintelligence, this chapter has attempted to improve one's understanding and clarity. This has been undertaken by investigating how applicable business counterintelligence practices and methodologies – from amongst the literary haze – can best be applied and explained in an effective form of organisational implementation[379]. This has been achieved by examining the prevailing views of business counterintelligence and its role within organisations. This has in turn lead to the constitution of a consolidated definition of business counterintelligence and the implications that this consolidated definition has for organisations. In addition, this was done in order to overcome the limitations of excessive diversity.

By offering a consolidated perspective of business counterintelligence, it is hoped that one will have a firmer grasp of the topic. This firmer grasp manifested both in terms of the implementation of business counterintelligence in an effective manner, as well as in relation to the broader objective of this thesis. With this consolidated definition in mind, I will now proceed to engage with the final analysis as pertaining to the objectives of this investigation.

---

[378] Fleisher, C. & Blenkhorn, D. 2001. *Managing Frontiers in Competitive Intelligence* p 38.

[379] It should be noted that smaller organisations may find certain aspects of the business counterintelligence process difficult to implement and grasp; largely due to the learning curve involved, available resources and the need for effective competitive intelligence operations. However, in spite of these difficulties, smaller organisations can still set about implementing many of the procedural countermeasures mentioned in this discussion in simplified yet effective manner; for more complicated aspects, should resources be available, trusted consultants can be called upon for help.

This will be presented in the concluding chapter to follow where I will discuss the implications of this consolidated definition for the sustainability of business counterintelligence.

Chapter 5 – Section 3

The Sustainability of Business Counterintelligence

5.1 Introduction

The primary objective of this chapter will be to examine the implications of the consolidated definition for the sustainability of business counterintelligence. As has been outlined in chapter 1, a more consolidated definition of business counterintelligence has been proposed due to the fragmented nature of the definitions currently concerning business counterintelligence as presented within the literature. I will now analyse the sustainability of business counterintelligence based on the evidence presented in this thesis; predominantly centring on the discussion presented in chapter 4. This will be done by firstly examining what needs to be in place to make business counterintelligence effective and thus sustainable. Secondly, by examining what will not make it effective and thus not sustainable. Thereafter, I will proceed to discuss the limitations of this investigation, recommendations for further research and my final thoughts and conclusions in brief.

5.2 Evidence in Support of Sustainability

The shift of today's social and economic contexts due to the rise in importance of information as part of the shift from an industrial based economic modus to that of a knowledge based one, has resulted in a number of influencing forces coming to the fore. These can be encapsulated within the technological, economic, occupational, spatial and culturally defined perspectives of the information society. From an organisational point of view, these forces have resulted in the rapid merging of information communications technologies forming advanced information exchanges[380], greater emphasis on intellectual capital and innovation[381], a rise in the perceived importance of information occupations[382], an increase in

[380] Webster, F. 2006. *Theories of the Information Society* p 10.

[381] Neef, D., Siesfeld, G. & Cefola, J. 1998. *The Economic Impact of Knowledge* p 175.

the proliferation of digital networks and information flows[383] and the increased proliferation of information in the social sphere[384] enabled through mass media influence[385]. Such influencing factors therefore highlight the importance of knowledge as a critical asset of value for organisations operating within today's complex environments of integrated competition.

In addition other factors of influence have also arisen, developed in either an isolated sense of parallelism or as associated forms of influence in conjunction with these forces mentioned above; as has been discussed in chapter 3. These elements can be regarded under the auspices of *change* and *importance* and broadly include: increased levels of globalisation and competitiveness[386]; growth in the economic and strategic significance of knowledge[387]; increased levels of vulnerability actualised by the need for effective management of knowledge, participation in complex knowledge environments[388] and shifts in the global balance of power and intelligence gathering focus[389] respectively.

The transition towards a new perception of the importance of information and the ramifications that such a transition hold – in terms of the collective forces of influence relating to the protection of one's knowledge assets – have thus had profound consequences for the role of intelligence gathering, and thus business counterintelligence. This where the emphasis of adversarial focus has broadened away from traditional conceptualisations of

---

382 Nahapiet, J. & Ghoshal, S. 1998. *Social Capital, Intellectual Capital, and the Organizational Advantage* p 242-266.

383 Webster, F. 2006. *Theories of the Information Society* p 17.

384 Webser, F. 2006. *Theories of the Information Society* p 19.

385 Gitlin, T. 2003. *The Whole World is Watching: Mass Media in the Making & Unmaking of the New Left* p 233.

386 The increased prominence of globalisation and the manifestation of global competitiveness where organisations are extending themselves in new directions in order to cope with such requirements and where global interaction dictates the systemic targeting of knowledge; through environments of complexity and turbulence where organisational boundaries have become blurred.

387 Economic prosperity rests largely with knowledge and is viewed as a strategically significant resource of the modern day firm, contributing to decision making and the creation of competitive advantage through the use of self processed knowledge and intellectual capital; organisations have adopted knowledge assets.

388 Vulnerability is increased through the sheer volume of knowledge that organisations have to contend with, though multiple channels of communication, the intangibility and distributed nature of knowledge interactions all through those tools, techniques and technologies used in order to manage it more effectively. The adversarial intelligence gathering parameters of the past were very different than they are today leading to more advanced forms of intelligence gathering taking place, whereby adversaries may choose to orchestrate exogenous intelligence gathering activities across multiple channels of attack.

389 Due to shifts that have taken place in the global balance of power, many nations and their organisations have chosen to target their intelligence gathering initiatives within the economic sphere in order to gain and/or maintain a greater level of global competitive advantage; as outlined by *Joyal*, P. 1996. *Industrial Espionage Today and Information Wars of Tomorrow* P 8, there has been a move away from targeting isolated military targets to focusing more intensely on economic targets as well.

value[390], leaving one's knowledge assets in a position of particular vulnerability. The broadening of the adversarial threat thus, carries with it important implications for the level of sustainability rendered by a consolidated definition of business counterintelligence in terms of the effectiveness that it conveys for one's organisation.

Firstly, as has been outlined in chapter 4, a consolidated perspective of business counterintelligence is able to deal more effectively with these altered states of adversarial focus than fragmented perspectives. This has been achieved by allowing one to effectively expand one's protection capabilities far beyond the existing definitions of business counterintelligence currently available. Sustainability is also rendered, through its ability to not only meet the challenges of diversified protection, but to also effectively integrate itself within variable organisational contexts, existing mechanisms of protection and the strategic focus of different types of organisations in an effective manner. This has the result of raising levels of associated understanding without dramatically increasing its burden upon management[391]. Integrative implementation thereby allows for the creation of effectiveness not only in a self contained sense of value, but also for broader organisational objectives as well.

Secondly, sustainability is rendered by consolidated business counterintelligence's ability to identify and engage with threats posed to one's organisation in a structured, integrated manner. This is opposed to ad hoc forms of fragmented investigation that may be dependent upon one's naturalistic decision making capability, common in environments of complexity[392]; which one can postulate is less effective. This is valuable as it ensures the validity of recommended protection measures, which are in turn supported by the contextual analysis[393] of one's particular risk situation. This is also of value as it counters the probability that *shock factor* analytics will be used by those proposing recommendations for protection measures. This is important as decisions made based on ill conceived research analysis and

---

390 Bernhardt, D. 2003. *Competitive Intelligence: Acquiring and using corporate intelligence and counter-intelligence* p 92.

391 DeGenaro, B. 2005. *A Case for Business Counterintelligence* p 15.

392 As Olsen, R. 2002. *Professional Investors as Naturalistic Decision Makers: Evidence and Market Implications* p 161, outlines when discussing decision making in complex, ill-structured situations – with security decisions in today's environment being an example of this – in this case referring to investment decision making: "Naturalistic decision procedures tend to be used by experts making decisions in complex, ill-structured, and indeterminate situations. Survey results indicate that investment professionals, like other naturalistic decision-makers, rely heavily on mental imagery, reasoning by analogy, and decision procedures that become more intuitive as complexity increases. Also, they are "satisficers," not optimizers. In other words, their primary aim is to make an acceptable choice; finding the best choice is not necessary."

393 Contextual analysis including cost to benefit trade-off.

information sources can result in less effective decision making. This is discussed below from an information security perspective.

> Survey data on information security trends and concerns are used to justify increased expenditures on security tools and technologies...The numbers, however, are anecdotal, are not generalizable to the business level, and are reported in cumulative form...While these problems are not unexpected, there is a larger problem that the data is being taken from the popular press and used by policy and decision makers to guide resource allocations...Managers need to be able to justify expenditures, through showing an avoidance of costly jeopardy, return on investment, or other managerial tools used to make rational decisions regarding enterprise resource allocations. These calculations must be driven by data that provides such things as the probability distributions of events and expected loss from certain problems[394].

By applying business counterintelligence in a consolidated form, it thereby creates additional sustainability for one's organisation by allowing one to effectively protect one's critical knowledge assets in a structurally based manner[395]. This helps to ensure that one's organisational resources are applied as effectively as possible. This therefore, helps one to better secure one's competitive advantage by ensuring the retention of one's critical knowledge assets for adequate periods of time[396] and in turn allows one the ability to better predict adversarial intelligence gathering strategies.

Thirdly, there are also subtle differences that exist between traditional conceptualisations of fad in relation to the characteristics of a consolidated definition of business counterintelligence. One can postulate that the sustainability of a consolidated definition of business counterintelligence is implied when one examines the characteristic focus of

---

394 Ryan, J. & Jefferson, T. 2003. *The Use, Misuse, and Abuse of Statistics in Information Security Research* p 1.

395 Although conceptually simple, this is not to say that the generic protection driven process of business counterintelligence is a *paint-by-numbers* solution; particularly in so far as adaptation is concerned. As stated in chapter 4, it will ultimately involve a large degree of critical self evaluation by key stakeholders within one's organisation in order to ensure its subsequent success. As Hilmer, F. & Donaldson, L. 1998. *Management Redeemed: The Case Against Fads that Harm Management* p 16, state: "Even where the need for analysis in management is conceded, it can be subtly denigrated by the simple adoption of a canned technique. Just open the can and add water for instant coffee management. Or just paint by the numbers and put a blob of paint in each box. The idea is that one need only follow a preset technique. No real thought is required. Again anyone can do it, so there is no need for managers or for according respect to those who manage. In point of fact, few aspects of management can be reduced to a simple technique. This is true, in part, because the complexities of managing real organizations tend to make infeasible the reduction of problem solving to universal prescriptions that hold for all situations."

396 Kovacich, G. & Halibozek, E. 2003. *The Manager's Handbook for Corporate Security* p 82.

perceived management fads – such as that of Total Quality Management or Business Process Reengineering[397]. Generally speaking, both Total Quality Management and Business Process Reengineering tend to allay their focus on the complete dominance of their proposed objectives through every aspect of an organisation's structure[398]. This is turn can lead to a form of structural reconstitution of the organisation.

However, unlike these fads, rather than seeking to fundamentally alter an organisation's structural aspects or management approach, a consolidated definition of business counterintelligence seeks to adapt to them. This has the result of minimising the impact of its implementation on organisational resources as far as possible; which one can postulate is more effective. Subsequently, one is able to infer to a limited degree[399] that by not correlating with this general characteristic of a management fad – in so far as the organisational context is concerned – that a consolidated definition of business counterintelligence does therefore not inherently follow the commonalities of a management fad. This in itself implies that a consolidated definition of business counterintelligence must have a disposition towards some degree of sustainability; when opposed to traditional management fads.

5.3 Evidence of a Lack of Sustainability

Before one can make any final assumptions, as to the sustainability of business counterintelligence, one firstly needs to assess its implied limitations as evidence of a lack of sustainability[400]. These limitations predominantly centre on areas of concern identified in the light of the discussion as presented in this thesis.

Firstly, a lack of sustainability is implied due to the conceptualisation of *innovation* and *competitiveness* as relating to a consolidated perspective of business counterintelligence,

---

397 Ponzi, L. & Koenig, M. 2002. *Knowledge Management: another management fad?* p 145.

398 As Dahlgaard, J., Kristensen, K. & Khanji, G. 2005. *Fundamentals of Total Quality Management* p 8, outline: "Total Quality Management involves the understanding and implementation of quality management principles and concepts in every aspect of business activities. Total Quality Management demands that the principles of quality management must be applied at every level, every stage and in every department of the organization." And as Grover, V. & Kettinger, W. 1995. *Business process Change* p 5-6, outline: "[Business Process] Reengineering espouses radical, order-of-magnitude change; its advocates urge taking a "clean sheet of paper" approach to work design...process innovation initiatives start with a relatively clean slate, rather than from the existing process. The fundamental business objectives for the process may be determined, but the means of accomplishing them is not. Designers of the new process must ask themselves, "Regardless of how we have accomplished this objective in the past, what is the best possible way to do it now?" (Davenport, 1993, p. 11)."

399 It is important that one should remain aware as to the limitations of these latter forms of reasoning, as they could be interpreted to be verging on logical fallacy if taken out of their context of implied meaning.

400 The term *lack of sustainably* was chosen as preferable in this regard, as a non-sustainable entity may be attributed to aspects other than elements of fad alone.

from a conceptual definition of a management fad. Conceptually a fad can be defined as a "person's particular like or dislike; [a] craze[401]". Such an understanding relating to *innovation* and *competitiveness* – in the management sense – therefore revolves largely around its perceived benefits, in terms of the level of innovation and competitive advantage created by its adoption. In this instance when its promised benefits do not materialise and it is quickly abandoned in favour of something else.

> A management fad can be considered an innovative concept or technique that is promoted as the forefront of management progress and then diffuses very rapidly among early adopters eager to gain a competitive advantage. After organizational leaders come to the realization that the concept has fallen short of its expected benefits, the concept is quickly discontinued or drops back to very modest usage[402].

Given the nature of business counterintelligence, whether fragmented or consolidated, if viewed in this sense where innovation and competitiveness – the focus of management fads – fall short in practice, it may run the danger of being conceived of as an entity that is of faddish orientation[403]. Such an understanding may therefore diminish its perceived sustainability, particularly if the concept is applied in an ill-conceived manner, where its tangible benefits are not immediately realised and it is abandoned after a short period of time in favour of another form of protection.

The second point of limitation, implying an absence of sustainability, is that of the low level of primary counterintelligence literature proliferation[404]. This when compared to other concepts of protection such as information security, as encountered while conducting this investigation. This has been affirmed in principle through the use of a rudimentary bibliographic analysis[405]. Such an interpretation could be indicative of a number of possible scenarios.

---

401 Oxford University. 1994. *The Oxford English Mini Dictionary* p 180.

402 Ponzi, L. & Koenig, M. 2002. *Knowledge Management: another management fad?* p 145.

403 One should note however that such a conception is rather limited in its ability to provide concrete evidence in this regard, as business counterintelligence may not readily correlate with other associated aspects of management fad. One would thus need to conduct further field research to affirm or disaffirm this supposition.

404 Measured in terms of counterintelligence's appearance in the title of literary works.

405 As a rudimentary form of analysis relating to the proliferation of business counterintelligence literature as opposed to that of information security (acting as a benchmark in this regard), the terms *counterintelligence* and *information security* were searched for broadly within the titles fields of a number of randomly selected databases, across all fields of literary media contain therein. The term *counterintelligence* was used so as to avoid the pitfalls of naming conventions as discussed in chapter 2. One should also be aware that by using

Firstly, that business counterintelligence could be on the verge of wide scale growth and acceptance[406]. Secondly, that the level of maturity development of the process is not far advanced enough for its wide scale application. Thirdly, that there is a general lack of management awareness and understanding. In this instance largely due to the level of associated development relating to business counterintelligence's maturity and therefore its adoption by organisations. One can postulate that both the second and third points seem to indicate a lack of clear understanding of business counterintelligence, especially if viewed in its current literary state as a series of fragmented definitions; rather than as broader consolidated definition.

In support of this postulation, unlike other entities of fad or sustainability – on the surface – business counterintelligence does not seem to meet the principle characteristics of these objectives[407]. This is evident in so much as there seems to be a constant low level surge of literature relating to the topic as presented for the better part of the last ten years[408] rather than a shorter time frame of early article proliferation followed by decline.

---

the terms *counterintelligence* and *information security* in this manner, that all aspects of occurrence are included; rather than limited to a business contextualisation's alone. The elementary findings were as follows: EBSCO Host: Counterintelligence 231 / Information Security 2384; JSTOR: Counterintelligence 10 / Information Security 58; ProQuest: Counterintelligence 65 / Information Security 1120; Science Direct: Counterintelligence 3 / Information Security 461; Springer Link: Counterintelligence 3 / Information Security 368; Wiley Inter Science: Counterintelligence 5 / Information Security 24, indicating in a limited sense of expression that *counterintelligence* literature, when compared to other protection aspects currently in circulation, could be of a lower level of representation. However one can by no means rely on these findings as fact as there are a number of other dynamic elements that come into play. Should one wish to conduct further research in this regard, it is suggested that one make use of a more systematic approach as outlined by Ponzi, L. & Koenig, M. 2002. *Knowledge Management: another management fad?* p 145, where they explain that a comprehensive form of bibliographic analysis – in order to establish fad or sustainability – focuses on the use of article counts in order to capture time-series data relevant to the inclusion of key terms in either the title or abstract of targeted works. Through such analysis, one is able to better grasp the concept of fad or sustainability through graphic representation, and infiltration of a particular topics interdisciplinary breath as it progresses over time.

406 This could be conceived of as either the start of a fad as outlined by Ponzi, L. & Koenig, M. 2002. *Knowledge Management: another management fad?* p 145, the emergence of a sustainable process as explained by Gibson, J. & Tesone, D. 2001. *Management Fads: Emergence, Evolution, and Implications for Managers* p 12-124, when discussing the stages of fad: "In Stage 1, the discovery stage, the fad is just beginning to come to the public's attention. Very early articles are appearing in the literature. It is during Stage 2, however, the wild-acceptance stage, that the fad becomes very popular. During Stage 3, digestion, critics begin to suggest that the fad is not the panacea it might once have seemed to be. In Stage 4, disillusionment, there is more widespread recognition that problems exist with the fad, and in Stage 5, hard core, only the staunch supporters remain loyal to the fad."

407 Relating to the rapid growth of a fad or rapid growth, decline and then resurgence of a mature entity as outlined by Ponzi, L. & Koenig, M. 2002. *Knowledge Management: another management fad?* p 145.

408 As Gibson, J. & Tesone, D. 2001. *Management Fads: Emergence, Evolution, and Implications for Managers* p 12-124, state: "In Stage 1, the discovery stage, the fad is just beginning to come to the public's attention. Very early articles are appearing in the literature." Ponzi, L. & Koenig, M. 2002. *Knowledge Management: another management fad?* p 145, go on to explain that such proliferation from inception to decline in relation to management fads usually takes place over a average period of 5 years. Given that works such as

In the light of this evidence, it appears to be more likely that business counterintelligence has experienced a lower level of adoption due to other circumstantial factors, including: its level of development, its maturity as a concept and the level of awareness and understanding that it carries within organisational circles. This point of view can be substantiated to some degree from the research presented in this study, in so much as there exists a great deal of associated confusion relating to the topic. When interpreted in this manner, such confusion indicates that business counterintelligence has not been able to reach a level of form that has been widely applicable to organisations, due to the complexities that have resulted as a consequence of its variability of application.

Further support in this regard – indicated in the research presented in chapters 3 and 4 – is that of a general lack of awareness within organisations as to the importance of such activity. This seems to be in part due to outdated conceptualisations of business counterintelligence and competition and therefore the protection mechanisms needed in order to secure one's knowledge assets. As this is a theoretical investigation, one cannot determine for sure whether a consolidated definition of business counterintelligence, in practice, may not also face similar problems of awareness, which would in turn diminish its chances of sustainability. With these points of concern in mind one can now proceed with a final assessment as to the sustainable or faddish driven nature of business counterintelligence.

5.4 Sustainable Entity or Passing Fad?

In today's knowledge context, organisations should at the very least be willing to investigate business counterintelligence and its implications for their organisations. However, from the analysis of the literature as it currently stands, it becomes clear that there is little consolidation between the definitions of business counterintelligence presented. Thus, organisations wishing to implement business counterintelligence may as a result choose business counterintelligence definitions that are not as effective – and thus sustainable – as they could be. This lack of clarity can lead organisations down a path of greater security risk and the wasting of essential resources without much in return. This can result in them jumping from one definition of business counterintelligence to the next; which is not sustainable.

---

that by Kristen, M. titled *Business Counterintelligence and the role of the U.S. intelligence community* can be found relating to the use of topic *business counterintelligence* as early as 1994, and works used in this investigation as that by DeGenaro, B. titled *Business Counterintelligence* published 2005, this is clearly not the case with business counterintelligence.

My goal has thus been to create a consolidated definition of business counterintelligence that will help to defined what a sustainable form of business counterintelligence might look like. It is hoped that such an analysis will help organisations to have a better grasp of what they are dealing with when engaging with business counterintelligence. This will hopefully allow organisations to also avoid many of the pitfalls of a management fad; that they may be faced with if business counterintelligence remains a fragmented entity. Based on the evidence presented, one can thereby conclude that there appears to be a strong case in favour of business counterintelligence as an entity that is sustainable; when presented in a consolidated form.

However, such an assessment cannot be without some level of reservation. Simply because business counterintelligence has met the requirements of sustainability, it would be potentially flawed for one to subsequently transpose such sustainability over to the greater business environment. Although this investigation supports the theoretical potential for business counterintelligence to carry this sustainability through to a level of practical implementation, such an assumption cannot be definitively made until further practical research has been conducted. This should include the intricacies that relate to management awareness and acceptance as a further determination of the effectiveness of a consolidated view of business counterintelligence. Nevertheless, such reservation should not be viewed as an attempt to disregard business counterintelligence. Based on the evidence presented in this thesis one would be foolish to do so. Rather such reservation is used to make one aware of the potential pitfalls that can arise due to an ill-conceived, hastily rendered implementation; this where all avenues of analysis have not yet fully been explored.

5.5 Limitations and Recommendations for Further Research

This thesis has examined business counterintelligence from a prevalent theoretical sense of application, but not from a practical sense of investigation. Although briefly touched upon, it also excludes additional quantifiable analysis of the literature relating to the sustainability and fad of business counterintelligence. Both of these limitations are thus areas that require further investigation. In addition, recommendations for areas of further practical research include:

> An investigation into those factors limiting the adoption of business counterintelligence within the organisational setting relating to management awareness of business counterintelligence and the transition of its sustainability as

determining factors of success. Although touched upon in this investigation, more substantial field work in this area would be beneficial.

In the light of the proposed investigation mentioned above – and the generic nature in which business counterintelligence is dealt with for the purposes of this study – more research could be beneficial as to the current state of business counterintelligence within organisations. Such an undertaking could also include elements relating to the use of business counterintelligence – and its perceived necessity – within both developed and developing economies.

Finally, due to the intricacies of literature variability and proliferation rates concerning business counterintelligence, more research is needed relating to the quantitative analysis of the literature. This could be conducted in support of a further review relating to the sustainability of business counterintelligence from an externalised set of values. One could then build upon the clarity and understanding leveraged within this investigation – particularly concerning the consolidated definition of business counterintelligence and the implications that this holds for the organisation as outlined in chapter 4. This would be done in order to better establish the commonalities of sustainability in this regard.

5.6 Final Thoughts and Conclusion in Brief

The objective of this chapter has been two-fold. Firstly, to act as a consolidated form of analysis relating to those broader themed areas of discussion as have been presented in this thesis. Secondly, to examine the implications of the consolidated definition for the sustainability of business counterintelligence. It has been argued that due to the shift in intelligence gathering that has occurred in recent decades that counterintelligence has in turn arisen to a level of importance whereby organisations should now pay attention to it. The sustainability of a consolidated definition of business counterintelligence has been argued in theory, through its increased effectiveness as opposed to fragmented definitions of business counterintelligence. By defining business counterintelligence from a broader perspective, it has been shown that it can be conceptualised in a way that is easily understood and carries with it applicability for different organisational contexts and structures. Thus, this thesis has attempted to meet those areas of concern relating to the topic of business counterintelligence, by manifesting a broader level of clarity and insight. This thereby helps to alleviate some of the haze and confusion that surrounds the topic within the current literary context.

Bibliography

Abbate, J. 1999. *Inventing the Internet*. Cambridge: MIT Press.

Aharoni, Y. 1993. *Coalitions and Competition: The Globalization of Professional Business Services*. New York: Routledge.

Anderson, J. 2003. Why we need a new definition of information security. *Computers and Security*, 22(4): 308-313.

Arenas, T. 2008. Intellectual Capital: object or process. *Journal of Intellectual Capital*, 9(1): 77-85, January.

Audretsch, D. & Thurik, R. 1999. *Entrepreneurship and Unemployment in the Knowledge Economy*. [Online]. Available: http://www.sbaer.uca.edu/research/icsb/1999/53.pdf [20 May 2008].

Barber, B. 1992. Jihad vs. McWorld. *The Atlantic Monthly: 54*, March.

Beniger, R. 1986. *The Control Revolution: Technological and Economic Origins of the Information Society*. Cambridge: Harvard University Press.

Bennett, J. 1986. Executive Priorities for Effective Communication in an Information Society. *Journal of Business Communication*, 23(2): 13-22.

Bernhardt, D. 2003. *Competitive Intelligence: Acquiring and using corporate intelligence and counter-intelligence*. Harlow: FT Prentice Hall.

Bernhardt, D. 2003. *Competitive Intelligence: Acquiring and using corporate intelligence and counterintelligence*. London: FT Prentice Hall.

Boisot, M. 1998. *Knowledge Assets: Securing Competitive Advantage in the Information Economy*. Oxford: Oxford University Press.

Borghoff, U. & Pareschi, R. 1997. Information Technology for Knowledge Management. *Jounral of Universal Computer Science*, 3(8): 835-842.

Borrus, M. & Zysman, J. 1997. Globalization with Borders: The Rise of Wintelism as the Future of Industrial Competition. *Industry and Innovation*, 4(2): 29, December.

Brooking, A. 1996. *Intellectual Capital: Core Assets for the Third Millennium*. London: Thompson Business Press.

Calder, A. & Watkins, S. 2007. *Information Security Management for Iso27001/Iso17799*. Cambridgeshire: IT Governance Ltd.

Canadian International Development Agency, 2008. *Ubuntu Working Together for a Bright Future*. [Online]. Available: http://www.acdi-cida.gc.ca/CIDAWEB/acdicida.nsf/En/JUD-222121812-NAY [08 May 2008].

Carnoy, M. 2000. *Sustaining the New Economy: Work, Family, and Community in the Information Age*. Cambridge: Harvard University Press.

Castells, M. 1996. *The Rise of the Network Society: The Information Age.* Malden: Blackwell Publishers.

Castells, M. 2000. *The Rise of the Network Society.* Malden: Blackwell Publishers.

Cazemier, J., Overbeek, P. & Peters, L. 1999. *Security Management*. London: The Stationary Office.

Central Intelligence Agency. 2007. *The Intelligence Cycle.* [Online]. Available: https://www.cia.gov/kids-page/6-12th-grade/who-we-are-what-we-do/the-intelligence-cycle.html [28 May 2008].

Chapman, C. & Ward, S. 2003. *Project Risk Management: Processes, Techniques and Insights*. Chichester: John Wiley & Sons.

Chen, H. & Chau, M. et al. 2002. CI Spider: A tool for competitive intelligence on the web. *Decision Support Systems*, 34: 1-17.

Chen, T. & Lee, J. 2004. *The New Knowledge Economy of Taiwan*. Cheltenham: Edward Elgar Publishing.

Child, J. & McGrath, G. 2001. Organizations Unfettered: Organizational Form in an Information-Intensive Economy. *The Academy of Management Journal*, 44(6): 1135-1148, December.

Choo, C. & Bontis, N. 2002. *The Strategic Management of Intellectual Capital and Organizational Knowledge.* New York: Oxford University Press US.

Clarke, C. & Varma, S. 1999. Strategic Risk Management: the New Competitive Edge. *Long Range Planning*, 32(4): 414-424.

Clarke, T. & Clegg, S. 2000. *Changing Paradigms: The Transformation of Management Knowledge for the 21st Century*. London: HarperCollins Business.

Copland, T. 2000. *The Information Revolution and National Security.* Carlisle: Strategic Studies Institute

Cornel C. 2007. The Military Security System – Present and Perspective. *Strategic Impact*, 1(22): 79-85.

Cortada, J & Woods, J. (eds) 1999. *The Knowledge Management Yearbook 1999-2000: 1999-2000*. Boston: Butterworth-Heinemann.

Covello, V. & Mumpower, J. 1985. Risk Analysis and Risk Management: An Historical Perspective. *Risk Analysis*, 5(2): 103-120.

Criscuoli, E. 1988. The Time Has Come to Acknowledge Security as a Profession. *Annuals of the American Academy of Political and Social Science*, 498: 98-107, July.

Crouhy, M. Galai, D. & Mark, R. 2006. *The Essentials of Risk Management*. New York: McGraw-Hill Professional.

Daft; R. & Lewin, A. 1993. Where Are the Theories for the "New" Organizational Forms? An Editorial Essay. *Organization Science*,4(4): i, November.

Dahlgaar, J., Kirsten, K & Khanji, G. 2005. *Fundamentals of Total Quality Management.* London: Routledge

Davenport, T. & Prusak, L. 2000. *Working Knowledge: How organisations manage what they know*. Cambridge: Harvard Business Press.

Davis, S. & Botkin, J 1994. The Coming of Knowledge-Based Business. *Harvard Business Review*, 165-170, September-October.

De Beer, J. 2005. *Open Access scholarly communication in South Africa: current status, significance, and the role for National Information Policy in the National System of Innovation.* Stellenbosch: University of Stellenbosch. (MA Thesis.)

DeGenaro, B. 2005. A Case for Business Counterintelligence. *Competitive Intelligence Magazine,* 8(5): 12-16, September-October.

Dictionary.com Unabridged (v1.1). 2008. Random House Inc. [Online]. Available: http://dictionary.reference.com/browse/busines [26 March 2008]

Dourish, P. & Grinter, R. et al. 2004. Security in the wild: user strategies for managing security as an everyday, practical problem. *Pers Ubquit Comput,* 8: 391-401.

Drucker, P. 1980. *Managing in Turbulent Times*. New York: Harper & Row.

Du Toit, A. 2003. Competitive Intelligence in the Knowledge Economy: What is in it for South African Manufacturing Enterprises?. *International Journal of Information Management,* 23(2): 111-120, April.

Edmunds, A. & Morris, A. 2000. The Problem of Information Overload in Business Organisations a Review of the Literature. *International Journal of Information Management,* 20: 17-28.

Edwards, P. & Bowen, P. 2005. *Risk Management in Project Organisations*. Oxford: Elsevier Butterworth Heinemann.

Eriksson, E. 1999. Information Warfare: Hype or Reality?. *The Non-proliferation Review,* 59-61, Spring Summer.

Fay, J. 2005. *Contemporary Security Management*. Woburn: Butterworth-Heinemann.

Fleisher, C. & Blenkhorn, D. (eds) 2001. *Managing Frontiers in Competitive Intelligence*. Westport: Greenwood Publishing.

Fraumann, E. 1997. Economic Espionage: Security Missions Redefined. *Public Administration Review,* 57(4):303, July-August.

Gibbons, M. 1994. *The New Production of Knowledge: The Dynamics of Science and Research in Contemporary Societies*. London: Sage.

Gibson, J. & Tesone, D. 2001. Management Fads: Emergence, Evolution, and Implications for Managers. *The Academy of Management Executive,* 15(4): 122-133, November.

Gitlin, T. 2003. *The Whole World is Watching: Mass Media in the Making & Unmaking of the New Left. Berkeley*: University of California Press.

Grant, R. 1996. Prospering in Dynamically-competitive Environments: Organisational Capability as Knowledge Integration. *Organisational Science*, 7(4): 375-387, July August.

Grant, R. 1996. Toward a Knowledge-Based theory of the Firm. *Strategic Management Journal*, 17(Special Issue): 109-122, Winter.

Grover, V. & Kettinger, W. 1995. *Business Process Change*. Hershey: IGI Global

Hansche, S., Berti, J & Hare, C. 2004. *Official Guide to the CISSP Exam.* Boca Raton: Auerbach.

Hanseth, O. & Ciborra, C. (eds) 2007. *Risk, Complexity and ICT*. Cheltenham: Edward Elgar.

Harasim, L. 1993. *Global Networks: Computers and International Communication. Cambridge*: MIT Press.

Hilmer, F. & Donaldson, L. 1998. Management Redeemed: The Case Against Fads that Harm Management. *Organisational Dynamics*, 7-20, Spring.

Hout, T., Porter, M. & Rudden, E. 1982. How Global Companies Win Out: *Harvard Business Review Special Collection*, 60(5):98, September-October.

Hutchinson, W. (eds). 2002. Business Intelligence Gathering. *Proceedings of the European Conference on Information Warfare and Security*, Uxbridge, 8-9 July 2002, 10. Reading :Academic Conferences International.

Jaffe, A. et al. 2002. *Patents, Citations, and Innovations: A Window on the Knowledge Economy*. Cambridge: The MIT Press.

Joyal, P. 1996. Industrial Espionage Today and Information Wars of Tomorrow. *Proceedings of the 19th National Information Systems Security Conference*, Baltimore, 22-25 October. Washington: Integer Security Inc. Information and Analytic Services.

Kalitika, P. 2000. *Periscope*, March.

Kandampully, J. & Duddy, R. 1999. Competitive Advantage through Anticipation, Innovation and Relationships. *Management Decision*, 37(1): 51-56.

Kaplan, R. & Norton, D. 2004. *Strategy Maps: Converting Intangible Assets into Tangible Outcomes*. Cambridge: Harvard Business Press.

Kellner, D. 1995. *Media Culture: Cultural studies, identity and politics between the modern and postmodern*. London: Routledge.

Killmeyer, J. 2006. I*nformation Security Architecture: An integrated Approach to Security in the Organisation*. New York: Auerbach.

Kim, W. & Mauborgne, R. 1998. Procedural Justice, Strategic Decision Making, and the Knowledge Economy. *Strategic Management Journal*, 19: 323-338.

Kinghorn, J. 2007. [Personal communication]. October 18.

Kitfield, J. 2007. Espionage, the Sequel. *Airforce Magazine.* 90, 3, Mar. [Online]. Available: http://www.afa.org/magazine/march2007/0307espionage.asp [8 January 2007]

Kondabagil, J. 2007. *Risk Management in Electronic Banking*. London: John Wiley & Sons.

Kovacich, G. & Halibozek, E. 2003. *The Manager's Handbook for Corporate Security: Establishing and Managing a Successful Assets Protection Program*. Boston: Butterworth-Heinemann.

Krages, B. 2007. *Legal Handbook for Photographers: The Rights and Liabilities of Making Images*. Buffalo: Amherst Media.

Kuo, E. & Chen H. 1987. Toward an Information Society: Changing Occupational Structure in Singapore. *Asian Survey*, 27(3): 355, March.

Lam, J. 2003. *Enterprise Risk Management*. London: Wiley and Sons.

Leslie, S. 1994. The Cold War and American Science: The Military-Industrial-Academic Complex at MIT and Stanford. Boston: Massachusetts Institute of Technology. [Course Notes Online]. Available: http://web.mit.edu/course/other/esd.83/www/notebook/The%20Cold%20War%20and%20American%20Science.doc [29 April 2008]

Liebeskind, J. 1996. Knowledge, Strategy, and the Theory of the Firm. *Strategic Management Journal*, 17(Special Issue): 93-107, Winter.

Longenecker, J. & Broom, H. 1972. *Small Business Risk Management*. Cincinnati: Thompson South-Western.

Lowry, J. 2001. Observations on the Effects of Defence In-Depth on Adversary Behaviour in Cyber Warfare. *Proceedings of the 2001 IEEE Workshop on*

Information Assurance and Security, West Point, 5-6 June 2001, 187. New York: Institute of Electrical and Electronics Engineers.

Maier, R. & Lehner, F. 2000. Perspectives on Knowledge Management Systems – Theoretical Framework and Design of an Empirical Study. *Proceedings of ECIS 2000*, Vienna, 4.

Malhotra, Y. 2000. *Knowledge Management and Virtual Organisations*. Hershey: Idea Group Publishing.

Martin, A. 2002. *Harnessing the Power of Intelligence, Counterintelligence and Surprise Events*. Cambridge: Executive.org

Mark, D. 1997. Competitive Intelligence and the Corporate Jewels. *Competitive Intelligence Review*, 8(3): 62-70.

Masuda, Y. 1981. *The Information Society as Post-industrial Society*. Washington: World Future Society.

McCrie, R. 2006. *Security Operations Management*. Oxford: Butterworth-Heinemann.

Meijer, H. & Meijer, F. 2007. [Personal Communication]. June 21.

Mellon, J. 2001. *Assessment of KGB's Intelligence-Gathering Successfulness in the West During the Period of 1954 to 1991*. Salford: University of Salford. (Bachelor of Arts).

Melody, H. 1991. Manufacturing in the Global Information Economy, *CIRIT Newsletter*, 3 (1), February: 2.

Miller, H. Competitive Intelligence – An Overview. *Society of Competitive Intelligence Professionals.* [Online]. Available: http://www.scip.org/Library/overview.pdf [25 May 2007]

Morgan, G. 2006. *Images of Organisation*. London: Sage.

Moule, G. 1996. *A Study of Security Countermeasures to Reduce Economic Espionage in the United States from 1975 to 1996.* Michigan: Lake Superior State University. (Bachelor of Science).

Murphy, D. 2008. *Understanding Risk*. New York: Auerbach.

Nahapiet, J. & Ghoshal, S. 1998. Social Capital, Intellectual Capital, and the Organizational Advantage. *The Academy of Management Review*, 23(2): 242-266, April.

Nasar, S. 1999. *The New Dollars and Dreams: American Incomes and Economic Change*, by Frank Levy. Reviewed in: Russell Sage Foundation. [Online]. Available: http://www.milkeninstitute.org/publications/review/1999_3/Q1_99bookreviews.pdf [22 May 2008].

Nasheri, H. 2004. *Economic Espionage and Industrial Spying*. Cambridge: Cambridge University Press.

National Counterintelligence Centre. 1997. *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*. Washington: National Counterintelligence Centre.

Neef, D., Siesfeld, G. & Cefola, J. 1998. The Economic Impact of Knowledge p 175. Oxford: Butterworth-Heinemann.

Nolan, J. 2001. Confusing counterintelligence with security can wreck your afternoon. *Competitive Intelligence Review*, 8(3): 53, January 3.

Nonaka, I. & Takeuchi, H. 1995. *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation*. New York: Oxford University Press US.

Nye, J. & Owens, W. 1996. America's Information Edge. *Foreign Affairs*, 75(2): 21, March/April.

Olsen, R. 2002. Professional Investors as Naturalistic Decision Makers: Evidence and Market Implications. *Journal of Behavioural Finance*, 3(3): 161-167.

Olson, D. & Wu, D. 2008. *Enterprise Risk Management*. London: World Scientific.

Pattakos, A. 1998. Threat Analysis: Defining the Adversary. *Competitive Intelligence Review*, 9(2): 53-62.

Peltier, T. 2002. *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. Boca Raton: Auerbach.*

Perkin, H. 1989. *The Rise of Professional Society: Britain Since 1880*. London: Routledge.

Pfleeger, C. & pfleeger, S. 2003. *Security in Computing*. Prentice Hall.

Podbregar, I. 2006. Some Patterns of Industrial Espionage. *Journal of Criminal Justice and Security*, 8(3&4): 179-402.

Ponzi, L. & Koenig, M. 2002. Knowledge Management: another management fad? *Information Research: An International Journal,* 8(1): 145, October.

Porat, Marc (1978). *Communication policy in an information society, in Robinson, G. (ed). 1978. Communication for Tomorrow: Policy Perspectives for the 1980's*. New York: Praeger Publishers.

Powell, W. & Snellman, K. 2004. The Knowledge Economy. *Annual Review of Sociology,* 30: 199-220, February 20.

Prescott, J. & Miller, S. 2001. *Proven Strategies in Competitive Intelligence: Lessons from the Trenches.* New York: Wiley.

Raval, V & Fichadia, A. 2007. *Risks, Controls and Security*. Danvers: John Wiley & Sons.

Robinson, R. 1999. *Issues in Security Management*. Oxford: Butterworth-Heinemann.

Roper, C. 1999. *Risk Management for Security Professionals*. Woburn: Butterworth-Heinemann.

Rouach, D. & Santi, P. 2001. Competitive Intelligence Adds Value: Five Intelligence Attitudes. *European Management Journal*, 19(5): 552-559.

Ryan, J. & Jefferson, T. 2003. The Use, Misuse, and Abuse of Statistics in Information Security Research. *Proceedings of the American Society of Engineering Management National Conference*, St Louis, 2003, 1-10. ASEM.

Saettler, P. 1968. *A History of Instructional Technology*. New York: McGraw-Hill Book Company.

Samiotis, K., Poulymenakou, A. & Doukidis, G. 2002. Organisational Reflections on the Introduction of Knowledge Management Systems: Evidence from Supporting (E-) Banking Activities. *The Third European Conference on Organisational Knowledge, learning and Capabilities,* Athens, 5-6 April 2002, 1. Athens: Athens University of Economics and Business.

Samli, A. & Jacobs, L. 2003. Counteracting Global Industrial Espionage: A Damage Control Strategy. *Business and Society Review,* 108(1): 95-113.

Schweizer, P. 1996. The Growth of Economic Espionage. *Foreign Affairs*, 75(1):9, January.

Shade, L. 1996. Data Trash: The Theory of the Virtual Class. *Canadian Journal of Communication*, 21(2). [Online]. Available: http://www.cjc-online.ca/viewarticle.php?id=369 [13 May 2008]

Shapiro, C. & Varian, H. 1999 *Information Rules: A strategic Guide to the Network Economy*. Cambridge: Harvard Business School Press.

Sharma, R. 2004. *Industrial Security Management*. New Delhi: New Age.

Slay, J. & Koronios, A. 2006. *Information Technology Security and Risk Management*. Milton Old: John Wiley & Sons.

Smith, B. 1990. *American Science Policy Since World War II*. Washington: Brookings Institution Press.

Soliman, F. & Youssef, M. 2003. The Role of Critical Information in Enterprise Knowledge Management. *Journal of Industrial Management & Data Systems*, 103(7): 484-490.

South Africa. 1995. *Government White Paper on Intelligence.* [Online]. Available: http://www.info.gov.za/whitepapers/1995/intelligence.htm [22 January 2008]

Stallings, W. 2006. *Cryptography and Network Security: Principles and Practice*. 4th ed. Upper Saddle River: Pearson Prentice Hall.

Sulc, L. 1997. Law Enforcement Counterintelligence. *Trends in Organized Crime*, 2(4), June.

The American Heritage Dictionary, Roget's II: The New Thesaurus. 3rd ed. 2003. Houghton Mifflin Company. [Online]. Available: http://thesaurus.reference.com/browse/Knowledge [28 May 2008].

Teece, D. 2003. *Essays in Technology Management and Policy: Selected Papers of David Teece.* Hackensack :World Scientific.

The Oxford English Mini-Dictionary. 3rd ed. 1994. Oxford: Oxford University Press.

Trauth, E. 2000. *The Culture of an Information Economy: Influences and Impacts in the Republic of Ireland*. Dordrecht: Kluwer Academic Publishers.

Trim, P. 2002. Corporate Intelligence and Transformational Marketing in the Age of the Internet. *Marketing Intelligence & Planning*, 20(5): 262.

Tuomi, I. 2002. The Future of Knowledge Management. *Lifelong Learning in Europe (LLinE)*, 2(2): 69-79.

U.S. Marine Corps. 2007. *Counterintelligence*. New York: Cosimo.

Vellani, K. 2007. *Strategic Security Management*. Oxford: Elsevier Butterworth-Heinemann.

Volberda, H. 1996. Toward the Flexible Form: How to Remain Vital in Hypercompetitive Environments. *Organisation Science*, 7(4): 359-374, July-August.

Walsh, J. 2003. *Asset Protection and Security Management Handbook*. New York: Auerbach.

Waters, M. 2001. *Globalisation*. New York: Routledge.

Webster, F. 2006. *Theories of the Information Society*. New York: Routledge.

Wenner, L. 1998. *MediaSport*. London: Routledge.

West C. 2001. *Competitive Intelligence*. London: Palgrave.

Whitehead, S. 2007. [E-mail to the author with reference to counterintelligence masters research]. June 25.

Whitehead, S. 2007. [E-mail to the author with reference to opinions concerning counterintelligence]. September 6.

Whitehead, S. 2001. The Counterintelligence Page: Part 1. *The South African Security Professional*, Sep/Oct: 32.

Whitney, M. & James, G. 1999. Why Spy? An Inquiry into the Rationale for Economic Espionage. *International Economic Journal*, 13(2): 103-123.

Williams, R. 1990. Television: Technology and Cultural Form. London: Routledge.

Winkler, I. 1996. Case Study of Industrial Espionage through Social Engineering. *Proceedings of the 19th Information Systems Security Conference*, 1-7. Davis: Department of Computer Science University of California.

Zack, M. 1999. *Knowledge and Strategy*. Boston: Butterworth-Heinemann.