TOWARDS A SECURITY SCIENCE THROUGH A SPECIFIC THEORY AND METHODOLOGY

Thesis submitted for the degree of
Doctor of Philosophy
at the University of Leicester

by

Maj. (Res.) Giovanni Manunta

Scarman Centre for the Study of Public Order

University of Leicester

1997

ABSTRACT

TOWARDS A SECURITY SCIENCE THROUGH A SPECIFIC THEORY AND METHODOLOGY

by Maj. (Res.) Giovanni Manunta

Chairperson of the Supervisory Committee: Doctor Martin Gill, CSPO

This research discusses the adequacy of the present body of knowledge of security in business and industry. It offers a set of concepts and a methodology by which the existing approaches can be organised into a scientific discipline and upon which further research can be based. Three main reasons are submitted for undertaking this task. First, academic approaches to the study of security are scarce and disagree on basic security concepts. Second, operational approaches originate from a multitude of actors responding to specific problems. Hence, security activities tend to be contingency-focused and to lack vision. Third, security is widely interpreted as an all-embracing topic covering all negative aspects of life. Thus, the attribution of responsibility and blame is subjective, where interest and emotion may prevail over rationality and justice. All these limitations raise problems of theorisation, explanation and justification. These can be addressed only by scientific methodology. This is the starting point of the research.

The research examines the evolution of security concepts and outlines the general and operational features of security in business and industry. The main problem areas (definition and methodology) are identified and related to the principles and methods of science. The scientific reliability of the present security reasoning is examined against a framework of scientific methodology. It is found wanting. A new approach is offered conforming to the principles of scientific methodology, in order to establish general principles applicable to all security situations, and to facilitate further study. It starts with a definition of security, identifies the components of a security context and analyses its processes. It reviews the impact of management and decision-making processes upon security decisions, and offers a general methodology. It examines whether a model can be induced through which to interpret, and reasonably explain, the majority of cases in security management. A model is offered, on whose basis a security problem can be addressed, and which can be used for verification and further studies.

Thus, the research seeks to contribute to the foundation of a science of security.

ACKNOWLEDGEMENTS

This research has required the author an appalling effort of concentration. At the age of 50 it becomes hard even to think, and expressing Italian thoughts in English language has not been painless. Without the help of family and friends, such an effort would have been impossible.

I wish to thank all those who have contributed to this study, and more particularly those who have had the patience of examining and criticising hundreds of pages of which I seemed to be the only enthusiastic reader.

My first thanks go to the academia, for having opened its ranks to an out-sider:

Dr. Martin Gill, CSPO, Leicester University, for having offered me this fascinating opportunity and for having been my supervisor.

Prof. Augusto Balloni and D.ssa Roberta Bisi, Bologna University, for having opened my mind to the Lewinian approach and for having been my Italian supervisors.

Dr. Roger Eatwell, Bath University, for his friendly and sapient support.

Dr. Sally Leivesley, for her encouragement and suggestions.

My special thanks go to the '*Pugnaces Britanniae*', for having provided me with valuable criticism and fair-play:

Omar Malik, St. Andrews University, for his time, criticism and help, and for having been such a meticulous interlocutor.

John Powell, Cranfield University, RMCS Shrivenham, for helping an ex soldier to understand management.

Anthony Slinn, International Security Review, for his overall support and advice.

Peter Timothy, RMCS Shrivenham, for his British pragmatism and his patience in controlling my Italian exuberance.

A particular thanks to Glenn Whidden, on the other side of the Atlantic, for friendly advice and precepts.

Finally, special thanks to my family:

Roberto, my son and *aide de camp* in such a difficult campaign. Without his criticism, suggestions and models, my army would have lost most of its batteries.

Lidia, my wife, for having made my dreams possible, for her loving attentions and for the patience in tolerating years of boredom and mental absence (which, I guess, have not yet come to the end).

Needless to say, the responsibility for the faults and errors in what follows is only mine.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

GLOSSARY

One of the problems in the study of security is that important concepts are defined in different ways, according to their context, application (scientific, technical, professional, colloquial, etc.) and viewpoint. The following definitions are used in this research (italics refer to other definitions in the list):

Asset: any entity (people, property, valuables, information, image, market-share, credibility, etc.) which is considered *damageable* and worthy of protection.

Damage: any change in the state of the *asset,* which is not desired by its *proprietor.*

Environment: set of general conditions and/or circumstances affecting the *situation.*

Event: any occurrence that may result in a *damage* to the asset (defined 'undesired' or 'adverse' when ambiguous).

Hazard: the set of conditions that in particular circumstances could lead to unintentional damage.

Proprietor: the person, or organisation, who possesses the *asset,* establishes its desired state, and has the will to protect it.

Protector: the person who is responsible for, and in charge of, the preservation of the state of the *asset.*

Risk: a potential *damage,* or the possible occurrence of an undesirable *event*, or a possibility of failure. Within this research this term is used as a concept which includes all three different meanings. The interpretation will depend on the context of discussion: those which refer to damage *'possibility of damage'*, to vulnerability *'possibility of failure'*, and to decision *'possibility of a wrong decision'*.

Safety: the contrived condition of absence of danger relative to the *asset* and its *environment.* It results from the implementation of measures aimed to avoid, prevent, minimise or protect from, the occurrence of *damage* which may be caused to the *asset* by unintentional sources.

Security: the contrived condition of absence of, or freedom from, danger and worry, relative to the *asset.* It results from the implementation of measures aimed to avoid, prevent, minimise or protect from, the occurrence of *damage* which may be intentionally caused to the *asset.*

Security Context: the state of affairs where *asset*, *protector* and *threat* are present and interacting, so that the definition of *security* is applied, or applicable.

Situation: the set of specific circumstances which configures the 'here and now' of a *security context*.

Threat: any living entity considered by the *protector* to be capable of causing intentional *damage* to the *asset*.

Vulnerability: any intrinsic, induced or provoked weakness of the *asset,* the *protector* and the *situation*, which could be exploited by the *threat* to produce a *damage*.

PREAMBLE

Seventeen years ago, on leaving the Army, I was offered an important opportunity as a security consultant. Initially, I did not expect to find private security too difficult. In my fifteen years as an officer, mainly in the 'Folgore' (the Italian Parachutist Brigade) often in the presence of terrorist activity, I had frequently dealt with numerous facets of security, ranging from personal to information, from transport to territorial and physical security. Having spent my service commanding or training operatives and regular officers in special courses and in the Italian Officer's School, I assumed that I had acquired considerable knowledge in both the defensive and offensive aspects of security.

However, the civilian security market was unique in its problems, requirements and, most important of all, its constraints. Some of the problems were indeed caused by terrorist activities, for which I was prepared. The discovery that the vast majority were of a more petty nature (such as vandalism, pilferage, burglary and theft) was discouraging, since it exposed my ignorance of private security priorities and constraints. Security began to appear to me to be a confused concept. It was not driven by the simple military 'defend till the last' or 'eliminate the enemy' objective. This was compatible with my view, that there are many ways of winning a battle. I shared Musashi's opinion, that 'the best warrior is the one who does not need to fight'. Nor was security a simple question of budget, as many commercial managers saw it. It seemed that an answer was required to the Socratic questions: 'What is security? What constitutes a good security? How does it differ from security which is bad?'

The scholars did not provide a clear answer. In many academic works, solutions were given to 'security problems' without having first offered a definition of security. Furthermore, in the 1970's security attracted few scholars, and in some academic circles it was considered to have suspect political implications (both conservative and fascist). [1] Consequently, many scholars were reluctant to involve themselves in the subject. Much academic attention was directed at its conceptual opposites of risk and threat, such as crime, political violence, terrorism, insurrection and war. Some useful material was provided by political philosophers (Debray,

[1] 'La proprieta' e' un furto' (property is a theft) was a favourite slogan in Italian universities

Marx…), guerrilla leaders (Guevara, Marighella…) and by others with first-hand experience (Clutterbuck, Trinquier…). Modern scholarly examination of the subject was beginning to produce useful studies of crime (Young, Wilson…), of terrorism (Laqueur, Wilkinson…), of guerrilla warfare and of insurrection (Kitson, Laqueur,…). Such works made valuable contributions to understanding with their subject areas, but rarely addressed the issue of security as a whole. Most of the theoretical approaches to their understanding and solution used one of three main paradigms: 'crime prevention theories', on bases ranging from sociology to policy objectives; 'risk theories' founded on probability theory originating in the engineering of safety, and 'game theories', mainly in the area of international relations, and particularly in the simulation of nuclear war-games. These different methodologies were often valuable in the conception and implementation of security measures. However, none of them appeared to address the fundamental issue of the concept of security.

I therefore turned to the operational approaches. I bought all the relevant books and subscribed to all the specialist magazines and journals (Italian, British, French, Swiss, Israeli and American) I could find. I attended many international courses and seminars in Italy, Switzerland, England, Israel and the United States. It was clear that most of the publications and courses were prepared by operational or technical personnel to meet their own needs. Journalistic and anecdotal accounts of events were by their nature even more closely confined.

Operational approaches were diverse and often had a narrow, specialised view of their subject. There were various definitions of security. Explanations were often little more than to a list of important points and tips. Technicians tended to reduce security to their field of expertise, without any attempt to re-interpret and/or adapt their technical knowledge to a wider issue. Indeed, whilst there was disagreement on the definition of security, there was a general consensus on its tools and functions, and particularly on a 'magic formula' which could be easily identified as: 'avoid the trouble, reduce the losses, keep people and problems out, maintain secrecy, and ...find a scapegoat, if you cannot hide the troubles and losses from those who pay the bill'.

The Socratic problem 'What is security?' was under-researched. Remarkably, security remained an indefinite concept applied to very definite situations and problems. Experts and professionals suggested many tactical solutions, which apparently aimed only to answer Aristotle's first two questions on the material and formal causes: 'How is security made? What is its formal aspect?' There was general agreement and a surfeit of information on its material and formal aspects. Authoritative sources of reference such as standards, technical details and codes of practice were available. Systems, procedures, planning, training, and methodologies were covered in great detail by many sources. However, they were far from satisfactory in their answers to Aristotle's remaining questions on the efficient and on the final causes: 'What is the source of security? What is it for?' Many different answers were given, based on different premises and for different purposes. Many were often of value at the tactical and specific level, but none of them appeared to address the general concept of security.

Thus, in 1979, it appeared that there was no sound and accepted definition of security, and that there was no easy solution. It was clear that no progress was possible until the problem of definition had been addressed. In view of the substantial confusion on the nature of security, it was difficult to see on what basis a security consultant could advise a client that an asset was *secure*. The concept of security meant different things to different people in different contexts. The enigma was usually answered by the opinion that '...*security, like beauty, is in the eye of the beholder*'[2]. In these circumstances, it was impossible to provide clients with what I had wished to offer: security, in the sense of a well-defined condition obtained through a rational, demonstrable approach. All this for the lack of a single, unifying concept. A single concept, from which to derive a model within which all the existing techniques and incomplete ideas would then constitute the *how*, not the *why* of security reasoning.

It seemed that a fundamental re-think was needed. This suggested a top-down approach, commencing with a philosophical examination of the whole idea of security and its surrounds. From this could be derived the basic concepts and definitions, upon which to build a strategy, from which - in turn - to reassess tactics. It was an enriching journey, which took me from Plato to Descartes, Hume, Russell and Popper; from Sun Tsu and Machiavelli to von Klausewitz and Liddel Hart; from the Haga Kure and Musashi to Ueshiba. The philosophers explained the nature of science, and how it may be conceived, formulated and explained. Strategists gave insight into the complexity of a decision making process in the presence of an antagonist, and why and how goals, choices and constraints influence decisions and operations. There was evidence that security is a philosophical idea, linked to the daily struggle for life, and consequently dependent on mental factors, such as awareness, will, determination and morale. In contrast with the quantitative approaches derived by

[2] Sutherland, G.E.: Answering the question: What is security? June 1992, *Security Management*, p.59.

insurance and statistics, these broader approaches suggested that security is a complex, not fully quantifiable topic, but one dependent upon the integration of both its physical and psychological aspects.

It is submitted that this situation still pertains in 1996. The physical aspects are relatively easily understood and learned; there is abundant reference to them in both literature and practice. These involve physical defences, such as fences, doors and safes, electronic alarms, access controls and closed circuit television (CCTV). By contrast, the psychological aspects - well researched in other fields of human activity - appear to be relatively neglected, with the exception of studies of risk perception, offender's motivation and victim's behaviour. Yet, since psychological aspects involve thoughts and emotions, and since behaviour is influenced by cultural and cognitive factors, security decisions ultimately depend on beliefs, fears and desires. This finding infers that security decisions are not exclusively rational, but are affected by human choices, desires and constraints. This is the starting point of the research.

INTRODUCTION

OBJECTIVES

There appears to be a widely accepted belief that security is an organised complex of specialised functions, which complies with well-identified principles, means and methods, whose validity and consistency derive from millennia of experience and sound methodology. [3] This research examines whether the formulation and application of these principles, means and methodologies warrant a more disciplined approach. It identifies the basic components of a security context and analyses its processes. It also seeks general principles and laws applicable to diverse security situations. It examines whether a model can be induced by which it is possible to interpret, and reasonably explain, the majority of cases. Thus the research seeks to contribute to the foundation of a 'science' of security.

This research has the objective of offering a framework of understanding on which such a discipline may be built. This is an ambitious goal. It is therefore prudent to observe that primary sources are scarce, and are mainly focused on subjects related to security, rather than on security itself. This research can aspire only to suggest the first foundation of a security science, and to prepare the ground for debate. Thus each step of the reasoning is clearly identified, to permit further analysis and facilitate criticism. The aim is to provide scholars with a broader spectrum for research, and operatives with the necessary, albeit modest, theoretical background. It is also relevant, before outlining the structure of the research, to explain the reasons underlying its objectives.

[3] For example: Kluwer Handbook of Security, 1991; Simonsen, 1996; Walsh, T.J., and Healy, R. J, 1996

JUSTIFICATION

Security is a topical subject of political [4] and economic [5] significance. Parliamentary disputes, election speeches, press and TV provide daily evidence that security is a major issue. Unfortunately, security is also a most confused subject. Notwithstanding numbers of conferences, seminars and courses held every year all around the world, the evidence is that there is still disagreement on the nature of security and consequently on which facts or events are truly security matters, and on what security should or should not do, in terms of performance and liability. [6]

There is evidence of mutual distrust between the principal actors: security advisers, providers and users, each one blaming the others for situations deemed unsatisfactory. Recurrent claims of the misuse, abuse or even futility of security measures (such as, for example, access controls, vetting, CCTV, alarm systems, dogs and armed response) may be found both in the media and in specialist literature. There are many examples. Senior management's perception of commercial and industrial security is sometimes unflattering:

> *'Security is a non-productive, a highly expensive capital item, extremely costly to install and maintain, always seems to need updating, is forever giving false alarms, and, since we have insurance, who really needs it anyway?'.*
>
> (Handbook of Security, suppl.25: 8.2-01).

Security professionals, in their turn, confess to doubt about the capacity for decision of senior management:

> *'Corporate executives who are skilled at making profits often appear to be naive consumers when it comes to decisions about security expenditures.'*
>
> (Jenkins, 1985: xxiii)

[4] An estimated 49% of the voters in UK is influenced by political proposals about security, according to a MORI poll 23-26 June 1995 (Riddell P., *The Times*, 30 June 1995)

[5] The estimated market for security products and services by 1996 is worth more than £ 2,500m in UK, and £. 14,000m in the five major EC markets (Germany, UK, France, Italy, and Spain). (McAlpine, Thorpe and Warrier Report, as quoted by Saunder Narayan, *International Security Management*, Spring 1994).

[6] Hawthorne, 1996; Manunta, 1996b; McInerney, 1997; Nichter, 1996.

Professionals also complain that security has become a playing field for unscrupulous salespersons:

> *'The word security is widely abused, in the context of crime prevention. Some companies, although specialising in but one facet of security, say alarms, describe themselves as security companies when in fact they are not so. They then compound their felony by describing their salesmen as security experts or even consultants.'*
>
> (Kluwer's Handbook of Security, suppl.. 26, 2.3-01)

There are also arguments about performance and liability. Performance is the modern Sword of Damocles suspended over the head of security managers. They are increasingly confronted by their superiors, posing questions, the answers to which hinge upon agreement on definitions:

> *'What is the company paying for when it pays for security? Does security mean everyone is safe while on company property? Does security mean every risk has been identified and reduced to the lowest level?...What is security? Only when security has been defined can a security manager begin to develop a security program that will satisfy company requirements.'*
>
> (Sutherland, 1992:59)

Blame and liability are increasingly accompanying security responsibilities both in the public and the private sector. Additionally, the public sector is transferring a part of its responsibilities to the private sector through legislation and legally binding regulations:

> *'In 1991, Chapter Eight was added to the Federal Sentencing Guidelines (Title 28, ss. 994) to provide for sentencing of business whose employees commit crimes because the companies are "vicariously liable for offenses committed by their agents"... Chapter Eight describes in detail that culpability shall in part be determined by "the measures taken by the organisation prior to the offense to prevent and detect criminal conduct, the level and extent of involvement in or tolerance of the offense by certain personnel, and the organization's actions after an offense has been committed"'.*
>
> (Chovanes, 1994:64).

Similarly, the private sector is increasingly placing responsibility and legal liability on those undertaking the security function.

> *'The security industry has faced many claims of negligent hiring because of the unique duties security firms undertake, their relationship with clients, and their access to property and people'*
>
> (Ingber,1993:63)

Blame and liability are becoming 'the problem', particularly on the other side of the Atlantic. Evidence is given by Kahn:

> *'…liability case statistics compiled by Jury Verdict Research, US Courts have handed down 342 guilty verdicts awarding $1 million or more since 1962. Several times that number of million-dollar settlements have also occurred. Of the premises liability cases going to trial in 1990, the plaintiff won 55 percent of the time, up from 52 percent in 1989'.*
>
> (Kahn, 1994:61)

These demands, expectations, claims (and spurious claims) are burdening security with increasing obligations and duties. An utopian view that damage and injury should not occur is manifest in the tendency to allocate responsibility for any event, including Acts of God. The security sector is often made a convenient scapegoat. Such expectations, which have been fostered in the past by some in the security industry in order to improve sales, cannot be realistically met. This has the dangerous consequence that security may be considered inadequate or negligent.

Different reasons have been offered to explain the 'inadequacy' of security in meeting expectations. Most refer to lack of professionalism in the private sector and impute it to weakness of regulation. [7] It is frequently lamented that too many people are entering security to the detriment of quality, and the necessity for a better knowledge and a sound methodology permeates the entire spectrum of professional security. Others refer to more general causes, such as background [8] and education. [9] Wright admits, with some discomfort, that

[7] George and Burton, 1996

[8] There is a body of opinion who holds that a background from the military or police does not produce good security 'managers'. For a contrary position, see Juliano, Sept. 1996

[9] Borododzicz, 1996; Hearnden, 1995; Manunta, 1996b

> *'Everybody who knows anything about security is aware that he does not know everything about security. The field is a huge one, and the problems are always changing...'*

(Wright , 1972: XI)

Security managers criticise their own level of education:

> *'Changes in the world are increasing our responsibilities and challenging our competence as security directors. To fulfil these responsibilities and meet these challenges, we must learn skills for our expanded roles...The key to our future success as security professionals can be summarized by three words: education, education, education'*

(Beaudry, 1992:104),

The possibility is that risk managers do not all have a clear idea of what they are doing. According to Broder,

> *'a recent poll by the Risk Management reported that 85 percent of those polled indicated that risk identification and evaluation is their number one priority'.*

Broder, 1984: XVII

To the critical mind, this result may as well be a fair indication of the ignorance of those polled regarding the planning, implementation and management of their own security measures. This suspicion appears to have foundation. Daily evidence suggests, and recent research confirms, that these measures have not always been attentively conceived:

> *'Preventing or reducing crime is dependent not just on knowing why and how people offend, but also the appropriateness (and limits) of different measures designed to deter, reduce, or prevent crime. At the present there is a lack of research evidence on each of these factors, and therefore policies are likely, at best, to be only partially successful. All too frequently, insufficient attention is paid to managing security projects'* (researcher's emphasis)

(Gill, 1994:8-9).

Another reason offered is that of the fallibility of defences in the presence of a resolute attacker. There is evidence that carefully controlled projects and well executed plans may not be sufficient to guarantee success in security. Indeed, most authors stress the point that even good physical defences may not provide adequate security.

> *'A false sense of security can leave an organisation open to serious and unexpected vulnerabilities. Security practitioners can develop a feeling of invulnerability and overconfidence in their actions and plans... a controlled access point can actually attract a shrewd offender. If perimeter security is strong, the offender can perceive the access point as the weak point in security. As a result, entrances often have increased protection. To avoid suspicion, however, a skilful and resourceful offender can manipulate what is considered legitimate and normal at an access point'.*
>
> (Purpura, 1991:124)

It is submitted that the reason for security deficiencies are more fundamental. Analysis of the above findings suggests that something substantial may be amiss at both the conceptual and decisional levels, and indicates misunderstanding between the different actors operating in security. These hypotheses find further evidence in the specialised literature [10] and public enquiries. [11] What emerges is a confusion of concepts between safety and security, and a difference between approaches based on the physical sciences and on the social sciences. This cultural dispute has repercussions in relation both to methodology and to the basic definitions as, for example, those of hazard, threat and risk. This disagreement is long-standing. Whilst in 1983 the Royal Society, discussing safety, recognised that

> *'One problem which the Study group was faced with concerned the difference between technical or scientific use of terms such as risk, hazard, risk assessment and risk management and the colloquial use of these terms. The Study Group found difficulty in agreeing a common set of definitions to be used by each sub-group.'*
>
> (The Royal Society, 1983:22),

In 1992 was still forced to concede that:

> *'In the course of the study, it has become clear that these (terms) have limitations, but serve the purposes of the group of scientists and engineers concerned with putting numbers on risk*

[10] e.g., The Royal Society, 1983 and 1992, Borrelli & Pacilio, n.a., Adams, 1995

[11] e.g., the Exxon Valdez and the Lockerbie cases

(The Royal Society, 1992:.2)

However, on the following pages, the report acknowledged that

> *'the terms discussed above do not meet the needs of social scientists'*
>
> (Ibid.: 7)

The same text offers discouraging evidence of conceptual and definitional discrepancies, which have reverberated in the literature of security. The following selection is an example (emphasis added):

> *'Hazards are defined here, following Kates and Kaspersons (1983) as "threats to people and the things they value".' (Ibid.:89)*
>
> *'Hazard is seen as the situation that in particular circumstances could lead to harm' (Ibid.: 3)*
>
> *'Risk is the probability that a particular adverse event occurs during a stated period of time, or results from a particular challenge' (Ibid. :2)*
>
> *'Risk is a combination of the probability, or frequency, of occurrence of a defined hazard and the magnitude of the consequences of the occurrence' (Ibid.: 5)*

What is worse, in academia the definition of security appears often to be assumed, if not seen as an irrelevance. No wonder then, if:

> *'In comparison with risk management, academic approaches to the study of security as a discipline are at their infancy'*
>
> (Borodzicz, 1996: 138)

This assertion invites further scrutiny. At the operational level, the term 'security' is used with different meanings in different circumstances and, ironically, to define conditions that are all but secure. An example may be found in the following statement:

> *'No system, however, can be made completely secure....Maximum security is a concept; the end to the means used to achieve it. ...all the...components of a security system do not individually achieve maximum security...there are no known universally accepted standards by which a security professional may evaluate a security system...this book considers the following five levels (or generic categories) of security systems: minimum*

> *security, low level security, medium security, high level security, maximum security'* (emphasis added).
>
> (Gigliotti and Jason, 1984:1,2)

Defining security is a difficult task, and a tendency to evade it is not uncommon in specialist literature. An example of such circumspection can be found in Post and Kingsbury's *Security Administration*:

> *'The term security is often used loosely and in different contexts. For example, national security, international security, internal security, private security, retail security, physical security, and industrial security are all used in daily conversations. The definitions of these terms are not often clear and are often used interchangeably'*(emphasis added).
>
> (Post and Kingsbury, 1991:1)

The different meaning of the word 'security' to different people in different contexts has been emphasised by many authors. A synthesis has been attempted by Golsby:

> *'The term security has a different meaning to different people. For example, to a brash teenager it might have something to do with birth control; to a 70-year-old woman it might mean being able to sleep comfortably at night without being awakened and beaten for the change in her purse. To employees it may mean returning to their cars at the end of the workday and finding them where they were left. On the other hand, to an organisation security means being able to continue its business activities without disruption. Security can also be defined as protection, assurance, a state or sense of safety or certainty, and not being exposed to danger. Security implies a stable, relatively unchanged atmosphere in which individuals or groups may pursue their ends without disruption or harm and without fear of loss or injury'* (author's emphasis).
>
> (Golsby, 1992:53)

The ambiguity of the definition produces the further problem of delineating its context. While Post and Kingsbury [12] feel the need of identifying 9 basic characteristics and 8 categories of security, Write's approach to definition is not obviously helpful:

> *'Security is not a non-productive, negative concept'.*

[12] Post, Kingsbury, 1991: 3

(Write , 1972: XI)

Little wonder that the word 'security' may still perplex careful readers. They may feel, with Kant, that 'whenever a dispute has raged for any length of time, there was, at the bottom of it, never a problem about mere words, but always a genuine problem about things'. A early assessment of this problem was made by Socrates. In Plato's dialogue *Cratylus*, Socrates attacks Hermogenes' thesis that names are given or changed by acts of individual volition:

> *Socrates: It may be that you are right, Hermogenes. but let us see. Whatever name you decide to give to each particular thing is its name?*
>
> *Hermogenes: Yes.*
>
> *Socrates: Well, then, suppose I give a name to something or other, designating, for instance, that which we now call 'man' as 'horse' and that which we now call 'horse' as 'man', will the real name of the same thing be 'man' for the public and 'horse' for me individually, and in the other case 'horse' for the public and 'man' for me individually? Is that your meaning?*
>
> *Hermogenes: Yes, that is my opinion.*
>
> *Socrates: Now answer this question. Is there anything which you call speaking the truth and speaking falsehood?*
>
> (Plato: Cratylus 385)

Inasmuch as everybody seems to have definitions of their own, an unprejudiced reader may find it arduous, with Socrates, to distinguish 'truth from falsehood' in the culture and practice of security. Indeed, the problems of definition reverberate on those of cognition, which appears to be affected by the same level of ambiguity. Research on cognitive perception [13] and on public perception or 'mis-perception' of crime and risk [14] identifies a general tendency to make judgements according to previous knowledge and habits. [15] In particular, reference is made to the difference between the opinions of the so-called 'experts' and 'lay persons', about which a caveat is appropriate:

[13] *inter alia*: Allport, 1954; Gregory, 1973

[14] The British Crime Survey, 1983:22-27; Williams, 1994:34-59

[15] This area of research is frequently influenced by existing studies on safety.

> *'It is imprudent, though common, to attribute the difference between risk perceptions and statistical estimates of risk wholly to the ignorance or errors on the part of the public. The converse is a public mistrust of 'experts' which is not without justifying evidence'.*
>
> (The Royal Society, 1983: 14)

and

> *' the view that a separation can be maintained between "objective" risks and "subjective" or perceived risk has come under increasing attack, to the extent that it is no longer a mainstream position'.*
>
> (The Royal Society, 1992:89)

nevertheless, it is generally accepted that

> *' risk perception involves people's beliefs, attitudes, judgements and feelings, as well as the wider social or cultural values and dispositions that people adopt, towards hazards and their benefits'*
>
> *'...the perception of risk is multidimensional, with a particular hazard meaning different things to different people (depending, for example, on their underlying value systems), and different things in different contexts'*
>
> (The Royal Society, 1992:89).

If threat, vulnerability and risk have 'different meanings to different people in different situations', as the evidence suggests; if there is no agreed definition of security, then, the same reader could argue: what should be supposed to be the utility - and the objective value - of 'National Standards' and 'Codes of Practice'? What kind of judgement can be expected, when definitions, knowledge and customs are acknowledged as relative, or not always appropriate?

A disturbing answer comes from daily evidence, which shows the tendency of both security 'experts' and 'lay persons' to fall prey to prejudices and clichés and, consequently, to the possibility of confusing the causes and effects of a security system. For example, there is a general tendency to consider a strong, well lit, man-guarded building secure, and a dark, empty street insecure. However any judgement of 'security quality' should take into account not only the presence of a security system, but also the existence of a threat, from which to derive then the effective capability of *that* system in coping with *that* threat in *that* situation.

Security is a vital field of human activity. Any failure, whether of judgement or of approach to a security problem may have disastrous consequences. Threats and risks may be under/over estimated, or simply neglected, and investments in security measures may be applied in the wrong direction. Lives and valuables may be lost due to inappropriate assessment, planning or decisions. Security problems can be increased by an erroneous appraisal or behaviour. For instance: strong physical security at a cash point may provoke an increase in armed attacks on personnel outside the premises, or the behaviour of a close protection team may attract the attention of an aggressor to a new and unexpected target and even facilitate his planning and operations. Again, without a clear definition of security and of its objectives, there are no clear premises and constraints, thus no method of making a rational examination of decision and actions. What is worse, decisions and actions cannot be defended against smart claims based on the ambiguity of definitions. This is considered in professional circles to be a very severe handicap, because it refers to an activity of practical relevance, where blame and liability are becoming a problem needing careful prior assessment.. Evidence is offered (see: The Existing Approaches) that the above problems emerge primarily from a proliferation of targets and a confusion of roles, in the absence of a theoretical frame of reference.

A number of problems in contemporary security are identified and addressed in this research. The most important are: the absence of an overall approach and, consequently, that of a common ground of definitions, the ambiguity of the concept of security, including its goals and scope and finally, the rigidity of the methodology, which often dismisses the non-measurable, to formulate easy and 'precise' responses which by-pass the complexity of the problems.

A scientific examination of these problems is long overdue. There is an urgent need for security to evolve from empiricism and formalism into a more scientific discipline. In order to be rational, acceptable and defensible, security concepts, plans and activities must be based on clear definitions, explanation and methodology. As Socrates argued, definitions are needed to provide a solid and common ground of understanding. Philosophers of science assert that explanation is the fundamental distinction between science and pseudo-science, and assign to methodology the task of providing it in a sound, verifiable way.

The need for scientific discipline can be illustrated. When facing the necessity of making a security decision on a particular situation, the initial problem is to assess the present 'quality and quantity of its security condition'. This simple question: 'Is this asset, or situation secure or not?' inexorably prompts the question: 'How do we know if this (asset, situation) is secure or not?'

In the absence of a methodology the only possible answer is: 'by experience'. But this is only an apparent answer, since its credibility depends upon an act of faith. The simple fact is that a security condition cannot be assessed without a sound methodology. This leads to the next question: 'How can we prove that this (asset, situation) is secure?' The capability to assess the existence or non-existence of a security condition, to measure its extent, to provide solutions, and the ability to state that these solutions are the best possible, pre-supposes that there is an answer to the question: 'What is security?'

There is no agreed definition of security or of a security context. However, only after the identification of a security context is it possible to answer the further basic questions: 'What is security for?' 'What are its elements and how are they related?' 'How does security work?'

The elements, relationships and effects of a problem, are the building blocks of a formula (not necessarily mathematical); such a formula offers the possibility of a rational solution. The existence of a formula postulates the existence of a science. Only science can provide the ability to measure, test, decide and explain solutions to a given situation. Thus the provision of a reasoned answer to the most basic question: 'Is this (asset, situation) secure or not?' depends upon the existence of a science, which, only, can provide the methodology for assessment, measurement and decision within a security context. This conclusion leads to the central question of this research:

'Does a security science exist, and if so, how can it be considered a science and what are its paradigms?'

A science, as such, does not exist. This research submits that its foundations can be laid, by formulating an appropriate scientific methodology by which to re-organise the existing knowledge and approaches.

STRUCTURE

This research starts with the investigation of the contents of the existing body of knowledge about security and proceeds towards its reorganisation into an overall theory in accordance with the accepted principles of science. From the theory an operational model and methodology are derived, to satisfy the exigencies of test and application. The research has the following structure:

Section I: contains a short account of the evolution of security and a survey of the existing approaches to security in order to identify its specific features and the main problem areas. After reference to the relevant schools of thought, a definition of science is offered, with a short account on the methodology by which to build, apply and explain a scientific theory. The concept of science being founded on the principle of reliability, the criteria of rationality, proof, and validity are discussed. The final focus is on methodology, explanation and prediction. The aim is to establish the applicability of the criteria and principles particular to science to the existing body of knowledge of security. The process of verification exposes inadequacies in present reasoning, and supports the necessity for an approach based on the scientific methodology. To conclude, the possibility of formalising the existing body of knowledge into a 'security science' is examined.

Section II: offers a formal definition of security, and contains a detailed analysis of the security context. It postulates a framework which contains an identifiable asset, threat and protector, all inter-related, and offers an analysis of their relationships, dynamics and processes. The relevant dimensions of a security process are identified as time, psychological, political and administrative, and their pertinent aspects are discussed. The verification of the existence of a security context is used as the criterion of demarcation between security and other states of affairs. The process for translating the conceptual framework into practice is analysed and the following four conclusions are reached. One, this framework is useful in the identification and explanation of the fundamental mechanisms of a security context, but it is too simple to be translated into a security decision-making process. Two, each security context is different, and peculiar to its particular Situation. Three, if the parameters of the Situation are known, then the resulting effects can be identified and evaluated. Four, it is, therefore, possible to analyse a security context according to general laws and principles, and to apply this methodology of analysis to a specific security context. The analysis follows the scientific method outlined in the first section. Both academic and operational evidence for and against a scientific theory of security is reviewed, as a part of the validation process. Reference to the existing works in security or related subjects is made when relevant to the explanation and verification.

Section III: The practical phase of the validation process requires the definition of a coherent working model and that of a specific methodology. This starts with the investigation of the relevant management and decision-making theories, and continues with a discussion of problem-solving theories and techniques. After examination of the implications of management and decision-making process issues upon the security reasoning, a methodology for analysing and solving a security problem is provided. Discussion follows on the possibility of inducing a model through which security problems in the context of business and industry can be interpreted and reasonably explained. This requires the analysis of the relationships between the decision-maker and the model builder, and of the difficulties of translating thoughts into mathematical models. A procedure for formulating requirements into models with minimum distortion is outlined. A model of a security process is offered, on which security problem can be discussed, and which can be used as an experimental set-up[16] for research and verification. Reference to the most common security approaches and verification by comparison with the existing body of knowledge are provided when relevant.

METHODOLOGY

This research is, perhaps, unorthodox. It offers a philosophical and eclectic analysis of the concepts of security, with a view to the application of that analysis to the academic and operational fields. It is based on literature, professional experience and reasoning, and follows a scientific methodology. Its structure differs from that of many theses submitted to Anglo-Saxon universities. These often begin with a literature survey and follow with a new piece of empirical research. This established approach is unfortunately inappropriate to security in its present state of development. The absence of theory, the scarcity of scholarly literature on the subject, the disagreement on definitions and approaches, combined with the complexity of the issue and the researcher's Latin culture, have prompted a different approach, hopefully to the benefit of creativity. Therefore, the survey of the existing literature is distributed throughout the research.

Because security can assume different aspects and shapes, case studies are not offered. Scientific methodology requires a credible test to be based on the analysis of a substantial number of cases, in an experimental set-up. This is not possible within the constraints of

[16] Popper, 1980: 415

time, resources and goals of this research. The study concludes with a model on which such task may be undertaken by future students. It is therefore confined to proposing, with the foundations of a science of security, a possible instrument for their investigation. The testing and validation of its results are possible tasks for further research.

SECTION I

CAN SECURITY BE A SCIENCE?

1.1 INTRODUCTION

The objective of this research is to formulate foundations for a science of security. This requires a multiform and ambiguous state of affairs to be organised into a framework. It is submitted that this framework must meet the requirements of a scientific discipline. Therefore the existing body of knowledge must be formalised into a 'systematic and formulated' coherent whole. [17] The task is to apply the discipline of scholarly rigour to operational knowledge, in order to interpret it with academic knowledge, to verify its reliability and to fill the cultural vacuum between these two worlds, by offering an overall theoretical approach.

The fundamental questions are: whether such a theory can be formulated, and according to which methodology; what its paradigms should be; and whether there is any *real* necessity for scientific rigour on this subject. These are examined in this Section.

It has already been suggested first, that contemporary security is a largely indefinite topic with controversial boundaries; second, that this state of affairs is partly due to a lack of an overall theory and formal definitions; and third, that security is an emotional subject (in that it depends on perception, fear, worry, and danger), influenced by strong political and economic interests. Evidence is offered that the first of these deficiencies has been caused by the increasing number of actors approaching operational security problems from different angles and with different goals, and that the second is largely due to the neglect of the subject by many in the academic circles. For the third (the emotional, political and economical contents), factual evidence is available from several sources: coverage in newspapers, opinion polls, political programs and pertinent economic figures. Conceptual evidence on this subject will be presented in Section II of this research.

This Section lays the groundwork for the formulation of the theory in next Section. It is divided into three sub-sections. The first seeks to identify those problems facing security which should be solved by an adequate overall theory. An historical account of the evolution of security helps to outline the general and specific features of security. The existing approaches are surveyed, and the case for formalising the existing knowledge about security

[17] Concise Oxford Dictionary, p.1081

into a scientific discipline is made. The second sub-section offers a definition of science by means of the identification of its aims, features, properties and principles. It discusses the scientific premises of criteria and methods to be used for the formalisation of a new approach. The third sub-section applies these criteria and methods to the existing body of knowledge, in order to evaluate their reliability. This is found inadequate; the main problem areas are identified and discussed as the absence of theory and the unsoundness of the methodology. The case for formalising the existing knowledge about security into a scientific discipline is confirmed. The Section concludes with a discussion on the possibility of formulating a theoretical approach to security. A positive answer is given, provided the essential issues of definition and methodology are addressed in accord with the scientific criteria of explanation, testability and falsification.

1.2 WHAT IS SECURITY?

Defining security has proven elusive. The task has been practically ignored in the academic world[18] and there is no agreement, at the operational level, on the definition of security. In the absence of a more scholarly reference book, general definitions as: *'Freedom or protection from danger or worry'* [19] have to be accepted. Encyclopaedia Britannica does not offer a definition of security, but defines the subject 'Security and Protection Systems' as:

> *'Any of various means or devices designed to guard persons and property against a broad range of hazards, including crime, fire, accidents, espionage, sabotage, subversion and attack'.*

This definition implies that security is "the condition of persons and property, which results from the appropriate use of 'security and protection systems', i.e. the above means or devices".

As will be seen at the end of this sub-section (The Problem of Definition), neither of these definitions is satisfactory. The first is too wide; the second is too narrow. A formal definition is provided in due time (Section II).

In its broadest sense, security is an attempt to reach and maintain a state of *'absence or freedom from danger and worry'.* In the operational sense, it is a set of functions and activities aimed at preventing unacceptable losses and damages to those tangible and intangible assets considered worthy of protection.

This sub-section surveys the contents of the present body of knowledge about security, to give a solid base for the theory of security which is presented in Section II. This base is constructed by means of the analysis of the evolution of security concepts, and the identification of the main approaches and features. Surveys and sources on this subject being incomplete, this analysis is descriptive; it does not purport to be definitive.

[18] Some attempts have been made in International Relations Studies (e.g., Mc Innes et Alia, 1992)

[19] Oxford Advanced Learners Dictionary, from now OALD

1.2.1 <u>The Evolution of Security</u>[20]

There is evidence that the concepts of security and war (a more modern activity covering only the last six thousand years of history) may have developed from the same root. In antiquity the principles of security tended to be identified with those of war. Without underestimating the importance of those concepts deriving from law and order, study of the available sources (see following paragraphs) make it clear that the original contribution to the security culture came from the military sciences, such as command and control, information, camp discipline and fortification. In present times, the concepts seem to converge. Contemporary writers consider war (or the menace of war) as an aggressive and more sophisticated version of security, directed against rival states, and the objective of war is changing from conquest to peacekeeping [21].

The contiguity of the concepts of war and security and the fact that security tended to be limited to private matters may explain why literature on security is scarce, and generally confined to the latter half of this century. In the past, personal security was part of the daily struggle for survival, and a sort of 'innate' culture. The source of expertise could only be found in past experience and tradition, and the basic knowledge was transmitted via training and imitation. Furthermore, until recent times, literacy was rare and domestic matters tended to be regarded as ordinary. It is therefore probable that writers would not have found interesting what was considered as a basic, common-sense, subject. On a more general level, history and literature indicate that security tended to be considered mainly an instrument for the preservation of power and facilitate government. Consequently, security-related literature was confined to issues of law and order, and to specific aspects of military and political problems.

Security being concerned with the preservation of life and possessions, it appears to be as old as life. Security concepts are found from the beginning of writing. The earliest written evidence of security-related concepts is found in codes of law, such as the Sumeric (3,000 BC) and Hammurabi's (2,000 BC). Later, it appears in works generally referring to the art of war and government. The Bible, Homer, Sun Tsu, Cicero, Virgilius, Caesar, Suetonius, Joseph,

[20] Surveys of the evolution of security may be found in Post and Kingsbury's *Security Administration* (1991, pp. 31-40); *Encyclopaedia Britannica*: Security and Protection Systems; La Mont. (1982): *Understanding Electronic Security Systems*. Texas Instrument Inc.

[21] Dougherty and Pfaltzgraff ,1990; Gallie (1991); Keegan, 1994.

Vegetius, Sanshiliu Ji (36 Stratagems), are relevant examples of works and authors where certain evidence of security topics and principles can be found.

Other evidence can be found in archaeology and in anthropology. For example, we can reasonably assume that the security culture and skills recognisable in to-day's primitive cultures are very close to those of our primitive ancestors. As anthropologists report, primitive social organisations reveal deep understanding and sophisticated application of the basic security principles and functions. [22] From birth, people are instructed via tradition and trained via imitation in basic security skills. The new-born are taught not to cry in the proximity of an enemy and are trained from early childhood to recognise and avoid dangers, to give alarm, hide and shelter in case of danger. When physically stronger, boys and (sometimes) girls are required to help erect, guard, maintain and defend physical barriers. Settlements are reinforced with fires, moats and primitive palisades (made of branches of thorned plants), which are frequently adorned with the heads of dead enemies, magic signs and taboos in order to increase their deterrent value. Primitive people domesticate animals to provide alarm and support, and react as organised teams according to well planned and rehearsed tactics when the fight is considered unavoidable, or the potential loss unbearable.

Evidence of security measures accompanies nearly every archaeological discovery. Locks, strong doors, barred windows, traps, safes, alarm systems, physical barriers and shields were known and used from the very beginning of civilisation. [23] The oldest known lock is wood-made, dates from 4000 BC, and was found in Sargon Palace, Khorsabad, near Nineveh. In the same period, a painting of a lock was made in Karnak Temple, in the Nile valley. As long ago as 1000 BC, the Egyptian god Anubi was represented with a key in his right hand. The oldest known safe was found in Pompei and dated II C. AD; it is wooden-made with iron bands and is provided with a very sophisticated lock. It is very similar, in its conception, to the safes used until the last century. [24]

According to the above evidence, there is little doubt that the concepts of awareness, avoidance and reaction are as old as life itself, being an essential part of the daily struggle for life, and founded on the basic instinct of survival. Early human beings were certainly aware of

[22] Keegan, (1994): *A History of Warfare.* Random House Inc, New York; Mails, T.E.(1995): *The Mystic Warriors of the Plans.* Aurum Press Ltd, London.

[23] Literary evidence of security systems (mainly, safes, seals and locks) are found in the Bible, Homer and old Chinese legends.

[24] Maggioni, 1993

the dangers and, before any defensive methods evolved, they could only react as animals do, trying either to avoid the most feared threats, or to eliminate their source, in the well known 'flight or fight' pattern of behaviour.

It appears that security principles and concepts have followed a pattern of evolution within that of social organisation, from individual family to band, tribe, chiefdom and state. It soon became clear that groups were less vulnerable to threats than single persons: they provided a deterrent by their mere number; they made the organisation of sentries and patrols possible and facilitated basic defensive tactics. The institution of the family and the discovery of basic agricultural techniques brought about an important limitation to the fundamental principle of escape: the exigency of defending family, residence and means of survival (children, food reserves, crops and vital portions of territory) from both animals and enemies. In order to preserve their margin of survival, persons limited in their possibility of escape had to conceive a way of resolving the now unfavourable equation of 'flight or fight'. This was achieved by counter-balancing its negative element (limitation of movement and space) with some factors of efficiency, notably the concepts of organisation, protection, detection and alarm. One of the consequences of these arrangements was the recognition of the concept of deterrence. Human beings learnt quickly that the mere existence of protective measures was frequently enough to discourage adversaries from actuating their aggressive intentions. Painful experience taught the attackers seeking to penetrate organised defences that losses were often unacceptable and frequently dissuaded them from further attacks.[25]

The probable next stage on the evolution of security was the emergence of specialisation, first by the division of external and internal security, [26] then between public and private security. [27] With the appearance of the state and the entrustment of its defence to a properly organised army, the responsibility of internal security shifted gradually from a military to a civil force.

The state approach to internal security (i.e., concerned with threats against the institutions of the state) was mainly based on the principle of deterrence through ferocious sanctions. Public security [28] was rudimentary (it seems that the concept of investigation only came to light in

[25] La Mont, 1982: 1-5, 1-6

[26] Protection against attacks from outside the state (e.g., war) cf. attacks from within (e.g., subversion).

[27] Private as 'proprietary, or contractual' differs from public, or 'government', in that belongs to, and is for the use of, one particular person or group only.

[28] From now, in the sense of that part of internal security related to Law and Order.

the imperial Rome) and based on the same principles. Private disputes were generally solved by arbitration and according to the principles of proportionality and compensation. [29] Domestic matters were under the rule of the head of the family, which included the power of death over family members and slaves. [30]

The literary evidence cited and history in general indicates that, in the ancient world, public security was mainly considered by rulers for the role it could play in the stability of government, that is, in their own, personal security. It seems that public security in modern terms (as a responsibility for the public and individuals as well as an instrument of government) emerged only when the complexity of the state and the increasing demands of the citizen [31] obliged the rulers to address it. A possible explanation is that security was generally interpreted through the centuries more as a private than as a public good. This has relevance later in the discussion of the utility of security (see: General Features of Security). The interpretation of security as a public good (and not as the Ruler's own, or Ruler's peace) seems to have only come to light with the advent of democracy in Athens and Rome and, after centuries of oblivion, in the City-States of the Renaissance and in the so-called 'modern' state. Aristotle's distinctions among different forms of government (tyranny, oligarchy, democracy) [32] can be translated into different ways of interpreting public security. This was still closely related to the Ruler's Peace and internal security. In Plato's *Phaedo*, the Athenians' notion of public security seems to include protection from bad example, impiety, and … philosophers. It was in the name of public security that Socrates was sentenced to die by the Athenian Assembly in 399 BC.

Evidence of a mature security culture and organisation comes from the examination of the documents and archaeology of republican and imperial Rome. In the Roman administration *cives* (citizens) were considered to be not subjects, but participants and owners of the *Res Publica* (the State). *Disciplina Publica* (public security, in the sense of enforcement of law and order) was described in a detailed body of laws and edicts, derived from *XII Tabulae* (the Twelve Tablets, 550 BC.) and lately collected into the *Corpus Iuris Iustineaneus* or Justinian's Code. Police records were kept, and a special law, *Lex Julia de Vi Publica*, was designed in

[29] Sumeric and Hammurabi's Code; The biblic precept: eye for eye, tooth for tooth

[30] Carcopino, 1995: 92-5

[31] This term came to use after the French Revolution. Here, reference is made to persons who consider themselves participants of the 'Κοινε', or 'Res Publica', and not subjects, of the State or Ruler.

[32] Aristotle, The Politics

order to control the exercise of authority and to prevent its abuse. *Securitas Publica*, in the sense of 'the safety or immunity of the state' acquired political prominence and occurred in mottos, emblems and coins. [33]

Public security was guaranteed by well organised agencies and bodies, whose functions were similar to their modern equivalents. *Praetor Urbanus, Aediles, Censores, Praefecti, Tresviri Capitales* (Magistrates), *Quaestionarios* (Investigators), *Delatores* (Spies) *Cohortes Urbanas* (City Police), *Lictores* (Military Police), *Vigiles* (Night Watchers and Fire Brigades), *Annonarios* (Custom and Administrative Police) enforced law in urban and country territories. The protection of coasts and naval traffic from piracy was ensured by a powerful fleet, which preceded Britain in 'ruling the waves' surrounding the Empire. However, not even such a strong governmental shield, unprecedented in antiquity, could provide the citizen with full security. Evidence can be found in Plautus, Cicero (the latter, however, applauding assassination when it suited his own interests [34]) and Dio, who records the Senate voting in AD 32 that senators should be searched for hidden daggers. [35] The utilisation of security guards, bodyguards (trusted slaves, retired soldiers or gladiators), guard dogs, safes, locks and bars, and the recourse to private organisations such as the confraternities of '*trivia*' [36] made the arrangement of private security in ancient Rome remarkably similar to that of contemporary times.

The fall of the Roman Empire brought a period of political instability to western civilisations, which was to endure until the Middle Ages. The endemic state of war between cities and districts, aggravated by plague, pestilence and ignorance, made security an important problem of daily life. Where roads were abandoned, bands of outlaws ruled and security could no longer be enforced in the countryside. Both in town and rural areas, security became a semi-military undertaking, relying on weaponry, armours, physical defences and savage sanctions. Public security became a sort of personal affair of the ruler, who acted in the same time as legislator, judge, guard and executioner. It was confined to rudimentary laws and edicts and mainly trusted to night-watchers [37] and walls, moats and drawbridges, but - essentially - to the

[33] Robinson, 1994: Chapters 7, 8, 12, 13.

[34] *Cicero ad Atticus*, 14.4

[35] Dio, 58.18

[36] Organised groups who put themselves in charge of ruling the *trivia* (crossing of roads), later a source of mercenaries for those who needed 'security services', including assassination.

[37] An interesting description of night-watchers' operations may be found in Shakespeare's 'Much Ado About Nothing', Act 3, Scene 3, when Dogberry explains the watchers their duty.

ability of people of taking care of themselves. In these conditions, private security was entrusted to physical defences, to the ability to raise private militias, to the strength of the family and to their ability to handle weapons.

This parochial existence was changed by the Crusades, which opened roads and minds to the world outside. The advent of this trading and commercial era in the presence of piracy, but in the absence of institutional protection, re-raised old security problems (the protection of the transport and storage of large quantities of goods). Those problems had been already solved in the past by previous and stronger governments, such as the Roman. Caesar's and Pompeus' fleets had exterminated pirates and rendered Mediterranean sea '*Mare Nostrum*'. Such solutions were not available to their successors, due to the fragmentation, belligerency and intrinsic weaknesses of States. They were, more often than not, restricted to their own territory. No State could afford the means to control maritime routes. In the absence of governmental strength, private and commercial security had to be reconsidered by those involved. The traditional recourse to prevention, protection, alarm and intervention had proved inadequate against armed bands, which had military training and sometimes consisted of hundreds of men. In such circumstances, no private organisation (nor public power) could afford the cost of effective security measures. Hence, a different approach was required. New solutions were found in medieval guilds, linked to private insurance, and enforced by the establishment of the principle of collective responsibility for compensation, of which there is evidence in the medieval edicts. The concept of <u>loss reduction</u> (and/or <u>transfer</u>) was adopted in security. This principle originated from private problems and was mainly solved through private initiative. It is submitted that it constitutes the first modern security principle, and that it also marks the emergence of a commercial (cf military) concept of security. Public security still remained the 'King's rule', and was often more a threat than a shield to the subjects. An attempt to limit the abuse of power was made in England with the Magna Carta (1215). The scholastic philosopher Aquinas (c. 1225-74) went so far as to justify popular rebellion against tyranny and assert that the constitution of a community should be determined by people. [38] This, however, was considered utopical (men are not angels) and a series of internal wars and civil disorders suggested the necessity of a 'strong hand'. Political philosophers as Machiavelli (1469-1527) and - to an extent - Hobbes (1588-1679) provided the Prince with both the

[38] Aquinas, *Summa Theologiae*

principle that the power is *ipso facto* just [39] and the techniques for achieving power and maintaining it through wickedness and despotism, to keep 'them all in awe'. Both, however, acknowledged that the Sovereign could never act unjustly, being obliged by Law of Nature and by their rendering account to God. [40]

Since the 17th century, scientific discoveries and the spread of knowledge resulting from the invention of printing have brought new contributions to the security culture. Laplace and his principles of probability, Bayes and his theorem of predictability, Gauss and Kolmogorov's theories of measurement, have given a more scientific basis both to the concept of loss reduction and the predictability of damages or failures within a system, including a security system. The craftsmanship of locksmiths and *'serruriers'* (normally: gifted clock-makers) gave a new impulse to private and domestic security, to the point at which it was acknowledged as having scientific value [41] and considered 'the art of the kings'. [42].

It is widely assumed that modern security originated during the Industrial Revolution. With its advent, the fear of fire, common crimes (theft, robberies) and labour movements (strikes, violent mobs) led to the development of industrial security. [43]. Interest in social progress, initiated by Locke (1632-1704) [44] and fostered in the 18th and 19th century by Hume (1711-76), Bentham (1748-1832) and Mill (1806-73), caused a re-thinking of the concepts of justice and, consequently, public security. Thanks to these liberal political thinkers, the concept of public security begun to change from private (the Ruler's) to public good. The English 'Bill of Rights (1689) was followed by a series of similar statements, as the Virginia Declaration of Rights (1776), the French Declaration of the Rights of Man and of the Citizen (1789). The rights to life, freedom, security and property (even happiness, in the American Constitution) were from now on stated as fundamental and in-suppressible.

An important component of security, crime prevention, became an issue in governments. After the Metropolitan Police Act (1829), a major revision of police organisation was brought

[39] Machiavelli's '*Il fine giustifica i mezzi*': the end justifies the means. (Researcher's translation)

[40] For a discussion, see: Wilkinson, 1977: 8-11 and Sommerville, 1992: 100-104

[41] see: L'Enciclopedie Diderot et D'Alembert, 1770: Serrurerie

[42] This art was practised by various sovereigns, for example Louis XVI of France.

[43] Differently from commercial security (mainly interested in the protection of goods), industrial security was mainly focused on the protection of the means of production (e.g., from the Luddites)

[44] Locke maintained that every individual has a right to life, liberty and property.

about in Britain by the Police Act of 1835, thanks to Sir Robert Peel's enquiry into the state of crime, and his proposals for creating a modern metropolitan police. This Act is a pivotal point in the birth of modern policing[45].

At the end of the last century, security had already found its specific identity and had achieved some cultural, political and commercial importance. With public security being increasingly involved with controlling crime and understanding its causes, new areas of study were opened by research made by Lombroso (1835-1909) and his fellow criminologists. Very active locksmiths and manufacturers (Fichet, Bauche and Chubb) established an industry manufacturing safes, strong doors, and locks. In 1858, Edwin Holmes inaugurated the first central alarm station (basically, via metallic wires and bells), and began to organise the first alarm company, Holmes Protection Inc. The foundation of the first telegraph companies made it possible to send an alarm to distant stations, and after the spread of electricity, the first electric alarm circuits (basically, an electric circuit with hidden switches, connected to an electric bell) appeared in New York in 1889 [46]. Two private security organisations (Pinkerton in USA, Sorensen in Sweden and Europe) began to provide services to individuals and governments. Insurance companies sold contracts to an increasing number of private clients, and provided expertise on security topics. The first manuals dedicated to personal security appeared in Europe, firstly in France and England. Some were technical manuals provided by manufacturers; others were manuals on armed or unarmed combat (Savate, Boxing, Wrestling, and the new art of Jujitsu) with suggestion of relevance to the field of personal and domestic security. Security topics were generally related to crime and considered only in the context of a technical solution (i.e., alarms, locks and safes) or of a possible confrontation. Consequently, advice was directed mainly towards technical matters and tactical behaviour (awareness, positioning and reaction).

The advent of world-wide conflicts brought serious government attention to industrial security (where it remains), initially, due to fear of military sabotage, espionage and subversion (First and Second World Wars), and currently through fears of terrorism and industrial espionage. Industrial security being an essential component of war efforts, its programmes were integrated into nations' security systems. Created in response to a temporary

[45] It is widely considered (see: Livingstone, 1996, and Johnson, 1992) that, until then, policing was referred to as a 'broad social function that embraced government, morality and economics', while the term 'police' was used to denote this function rather than a 'body of state-funded officers'.

[46] Cunningham, 1989:1

contingency, a substantial part of this system endured after World War II because of the advent of new international tensions, the Cold War and the appearance of sensitive governmental programmes, for example in the communication, nuclear and space industries.

In 1919, a mine engineer and management theorist, Henry Fayol, identified security as one of the fundamental activities of industrial undertakings, and defined its objective:

> *'...to safeguard properties and persons against theft, fire and flood, to ward off strikes and felonies and broadly all social disturbances liable to endanger the progress and even the life of the business....It is, generally speaking, all measures conferring upon the undertaking and requisite peace of mind upon the personnel'.*
>
> (Fayol, 1954:4)

Though far from today's sophistication, there is little doubt that Fayol can be considered the pioneer of the most recent of security concepts, that of management, which after Fayol can be thought of as including those of organisation and loss reduction.

In the latter part of this century, the appearance of non-conventional forms of war (guerrilla, insurgency, and lately low-conflict operation, peace-making and peace-keeping) and the revival of terrorism have provoked a fundamental re-thinking of security. This has included governments, scholars, professionals and individuals. Opponents who were ideologically motivated, para-military organised and trained, and - frequently - state-sponsored could not be easily neutralised or deterred by the existing security functions. Their preference of 'soft' targets and their activities against unprotected civilians and organisation obliged to a spreading of the security culture, systems and activities throughout the population. New laws, policies, strategies, procedures and tactics were adopted to deal with the problem. The industry invented and produced new security equipment, and new professional profiles appeared on the market. Though not as serious as it was in the 1970's and 1980's, this situation still pertains in 1996.

Security is now at the forefront of political topics, encouraged by the media and by the lobbying activities of a fast-growing security industry. A massive process of education through many books, specialised magazines and articles and TV coverage have inculcated the security culture in the public. It has created a substantial market for the security industry and made security and its issues (crime prevention, counter terrorism, etc.) a permanent entry in the political and electoral agenda. [47] Many universities offer post-graduate courses in a subject that was not thought of 20 years ago; numerous exhibitions, conferences, seminars, courses are held world-wide.[48]

This cultural and communicational process has achieved very important results, more in the security-related areas of crime prevention, counter terrorism and risk than in general thought about security. In the United Kingdom, for example, co-operation between scholars, the government and the security industry has, in the last 30 years, produced a number of academic and governmental research studies (e.g., the 'Crime Prevention Unit Papers'); annual Crime Statistics; National Standards and Codes of Practice. Public security is a major concern to any government. Security systems and activities operate in many organisations, from government agencies and industrial plants to hospitals, churches and schools. Large companies have their internal security organisation, and security services from private organisations are available to everybody. All of these factors have contributed to a greater public, business and government awareness of security as an important issue, and one which has permeated throughout 'normal life'.

Security nowadays is a professional complex of specialised functions. New communication systems, biometrics, detection and computer technologies have added tools to a security arsenal that, until recent times, was based (as in the Pharaoh's era) on weapons, traps, locks, safes, strong doors and bars. All the new paraphernalia that human ingenuity has conceived ('electronic' safes and locks, computerised and centralised alarm systems, close circuit television, counter-surveillance equipment, etc.) are now the ingredients of security programmes. Security systems are becoming increasingly automated, particularly with respect to sensing and communicating hazards and, to a lesser extent, with respect to assessment, decision and reaction. Advances in miniaturisation are reflected in security equipment that is smaller, cheaper, more easily installed and maintained, and more reliable. Yet, it should be recognised that technology, however important and synergetic to the application of the security principles, has not added any new concept to those already identified. On the contrary, it seems to have opened new vulnerabilities and provided new possibilities to the attacker.

[47] A survey of the most relevant aspects of this issue can be found in Jenkins: Home Office Crime, Sunday Times 16 X 1994

[48] Manunta, 1996b; Ortmeier, 1996; Simonsen, 1996.

A new idea has emerged from what may be regarded as the oldest of the security branches: behaviour in personal security. This part of the millennium has seen the welfare and culture of the individual growing increasingly important, and more widespread. Hence, the security culture has rediscovered the concept of unity between body and mind, so as to improve awareness, behaviours, and decisions in a security context. The 'new idea' came from the discovery of the importance of psychological preparedness not only to increase awareness, but to 'win without fighting' (an old Sun Tsu concept, but previously limited to intelligence and subversion). Ignace of Loyola (Exercicios Spirituales) in the West, Takuan Soho (The Unfettered Mind) and Musashi Myiamoto (The Five Rings Book) in the Far East - though starting from different positions, and with different purposes - have helped those with security responsibility to give impulse to the new interpretation of <u>prevention</u> as a philosophical integration of awareness, decision, avoidance and reaction.

These cultural premises, together with the explosion of individual interest in security topics and some attempts at generalisation, have given birth in this part of the century to an original philosophy that takes into account personal security and life: Aikido. According to its founder, Ueshiba Morihei, security does not necessarily need to be achieved through fight, because "'*'the restoration of harmony is the goal of all conflict and the best 'victory' is the one in which everyone wins".*[49] Therefore, personal security (and security in general) is no longer seen as an exclusively egotistical concern, but as a means of restoring harmony, i.e. peace and tranquillity, not only in a personal microcosm but also, Ueshiba suggests, in the Universe.

Having concluded its pilgrimage from practice to philosophy, security needs to proceed along the road of understanding to complete its evolution into a science. In order to rearrange all the existing concepts and methods into a discipline, the next step is to conduct a systematic analysis of its main features and to identify its problem areas.

1.2.2 <u>The Existing Approaches</u>

A survey of the existing approaches to security offers a starting point for analysis. No such survey appears to have been made previously, and it is likely to be incomplete.

[49] Ueshiba, as quoted by Dobson and Miller, 1993: IX.

It is not necessary to examine minutely every approach to security and the supporting theories. It is their general focuses which are relevant, to point out the reasons why an overall theory has been felt to be missing. The identified approaches have been classified into groups by generalisation. With security being a complex fact of life, any approach suggested hereafter embraces numerous aspects, not only that which has been identified as the principal.

In order to conduct the analysis on theoretical and empirical levels, the identified approaches are subdivided into 2 different categories: academic and operational.

1.2.2.1 The Academic approaches

No mention of a science, or theory, of security is to be found in dictionaries of sciences or philosophy, nor in academic syllabuses. A survey of the existing courses given by academic institutions in 'Security' or 'Security Management' has not revealed the presence of such issues[50]. There are, however, several areas of study which make reference to security as a subject; the most important are International Relations, Politics, Military Studies (including Low Intensity Conflicts, Terrorism and Peace-Keeping), Law, Law Enforcement, Crime Prevention, and Risk Studies.

The literary evidence is that Military and Law and Order were the first to touch on security, largely interpreted as 'the King's order', often in the guise of public security and focusing on the prevention and repression of unlawful activities. Modern Law and Order studies extend to cover both personal and private security. The potential encroachment of security measures onto democratic freedoms and civil liberties are also extensively studied under a range of headings and with varying degrees of objectivity and competance.

Both Crime Prevention and Law and Order are based on deterrent, prevention, conviction, punishment and re-education. They contribute the concepts of:

> *'**opportunity reduction**, which attempts to reduce opportunities for offending; **social prevention**, which attempts to counteract criminal motivation; and **legislative prevention**, which aims to reduce crime by reinforcing legal prohibitions'*
>
> (Home Office Research Studies: Co-ordinating Crime Prevention Efforts, April 1980: 7).

[50] Manunta, 1996b

Current policy is that *'prevention is better than cure'* [51]. Legislative and social prevention are directed by government, but opportunity reduction is generally delegated to the private sector. This last activity centres on

> *'making offences physically more difficult to commit ('target hardening') and the usefulness of this approach is widely accepted by the police and others'.*
>
> (Ibid.).

However, according to the same source:

> *'there has been little hard evidence of its efficacy...But opportunity reduction goes beyond physical measures'*
>
> (Ibid.)

An interesting area of research has been devoted to the subject of 'Public Order and Policing'. Here, the complexity of interrelations between crowds and police are analysed, together with the theories and techniques of control. [52] Contributes to security concepts come in terms of communications, negotiation and pro-active activities intended to 'defuse' and 'channel' the 'threat', rather than confronting it.

A set of 'security theories' has been found in International Relations Studies, related to defence and defined as 'balance of power', 'deterrence', 'deterrence and détente', 'balance of terror' [53]. Perhaps their titles and contents suggest that they should be better called 'theories of insecurity'[54]. The term security has the general meaning of a state of affairs between states where warfare is *'so highly improbable as to be practically out of question.* '[55] It does not cover security-related activities as, for example, political and industrial espionage between allied states. On the contrary, too frequently appears a cosmetic cover of terms and activities related with hegemony and pursuit of national interests, germane to military and political power rather than to a genuine concept of security. Because of the dimension involved, and considering their focus, goals, scope and methods, these theories are not applicable in this research. There are signals, however, that approaches in this area of study are no longer

[51] Ibid.

[52] King and Brearley, 1996

[53] Mc Inness et al., 1992:4, 10-11, 38-39

[54] Dillon, 1996: 1-11, 113-128

[55] Stoessinger, 1993: 310

defined in pure military dimensions and are moving towards more easily recognisable security aspects. [56]

Studies about Terrorism have abounded since the 1970's. Volumes of research, often commissioned by governments, have been produced, which have analysed in detail the terrorist's motivations and behaviour. Many books have been produced, considered to be authoritative or conclusive. [57] Close attention has been paid to terrorist methodology, such as assassination, kidnapping, bombing and hijacking, and to the possible responses, both at the government and the individual levels. In particular, it is submitted that the studies of counter-terrorism have influenced and, to some extent, energised, the study of security concepts [58].

Risk Studies are relatively new (late 1950's). They have mainly been prompted by the necessity of rendering safe such potentially dangerous hazards as the nuclear power stations, and, lately, all main threats to population and environment. Thus, they mostly address safety hazards, both technological (biological, chemical and nuclear) and natural (flooding, earthquakes and fire). The main focus has been clearly stated by The Royal Society:

> *'Governments are now seen to have a plain duty, which they do not deny, to apply themselves explicitly to making the environment safe, to remove* ***all*** *risks or as much of it as is reasonably possible'.*
>
> (The Royal Society, 1983: 95).

Given such an ambition, it seems incredible that security has not received the attention of risk scholars. Possibly, this is a manifestation of academic snobbery, with security having been considered by risk students, until recent times, a rather practical topic of cultural irrelevance. As a matter of evidence, there is a body of opinion in academia [59] and in the industry that professional security is

> *'…that part of risk management which seeks to reduce the chance by preventing, detecting, or dealing with fire, crime, accident and waste (often called "loss prevention")'.*

[56] Mc Inness et al., 1992: 38-39, 84

[57] For example, the works of Clutterbuck, several; Laqueur, several; Wilkinson, several

[58] Derrer, 1992; Flynn, 1979; ICPO-INTERPOL, n.a.; Jenkins et al. 1985; Kobetz and Cooper, 1978;

[59] CSPO MANUAL ed 1996: Module I, Unit 3

(Group 4, 1992: 13)

If the attention of risk students to security may be considered marginal, the contrary is not true. Risk concepts have largely influenced security thinking. 'Risk analysis' methodology, originating in the area of safety studies, has been widely adopted in security assessments. This is now an essential part of security studies, generally included under the subject topic 'Security Management'. It covers also concepts of 'Loss Reduction' derived from insurance and finance. Moreover, 'Risk Perception', is now a part of post-graduate security studies, and its concepts are beginning to influence the way security reasoning are conducted.

However, risk studies are considered far from mature, and are not fully translatable to security. Firstly, because there is no agreement between physical and social scientists even on the definition of risk. Secondly, because the old favourite paradigms of the identification, assessment and management of risk, which were derived from insurance and based on statistics, are coming under increasing attack, mainly from social scientists, and are considered of limited use by a number of security students. More is offered on the subject at the conclusion of the Section.

Generalising, academic approaches to security fall into categories:

- Political (maintaining and protecting *the power* of the State)
- Governmental (maintaining *public order* for the public good)
- Juristic (the legal consequences of *unlawful* behaviour).
- Criminological (the causes and dynamics of *criminal* behaviour).
- Sociological (the social causes and dynamics of *deviant* behaviour).
- Social (where the interactions with *society* are the main concern)
- Psychological (the cognitive and behavioural aspects in a situation of *fear*).
- Mathematical: (the probable impact of a *damaging* event).
- Economic (*economic* aspects of choice and actions, as causes and consequence of a *damaging* event).

Each of them constitutes a study of the security aspects of a particular discipline. None treat security as a discipline in its own rights. It is not relevant, here, to discuss each of these areas in detail, but to point out their conceptual differences.

1.2.2.2 The Operational Approaches

The operational approaches to security are numerous and different, and, because of the complexity of life, are more difficult to classify than the academic ones. Problems stem from their application at different levels (i.e. governmental, public and private), their cultural dependence from diverse academic approaches and paradigms, and their typical responses to different, specific needs. Nevertheless, in the course of the research, it has been possible to identify some general trends useful to a general classification, depending both on the typology of the particular asset to be secured and on the general goal each approach aims to achieve. Broadly, we can distinguish the following categories:

- Military (the opponent is seen as an *enemy*, and the confrontation as a *battle*).

- Police-like (the opponent is seen as a *criminal*, and the activities as *investigation* and search for *evidence*).

- Engineer-like (security is seen as a *technological system*, where the opponent and potentially the managers are considered to be *interfering entities*).

- Managerial (where the respect for the *budget* prevails over the needs of security).

- Social Responsibility (priority of *people* over other considerations)

Each of these approaches has objectives and activities which relate to security. However, they are focused on particular aspects: the source of risk, the perfect functioning of technology, the economic consequences of loss, or on the sanctity of human life. None constitutes a generalised treatment of security, per se.

1.2.2.3 Summary

In summary, the evidence suggests that there is a number of different approaches to security, both on the academic and operational levels, each one characterised by different assumptions, aims, definitions, focuses and methodologies. The results of each approach vary, depending on the assumptions made on the actors, the nature of events, their causes and effects. Each has a different aim: a search for consensus, a neutralisation of the causes of unwanted events, a reduction in the effects (social, criminal or economic), or keeping within a budget. The activities of each are dependent upon the focus: social policy, law enforcement, confrontation, loss prevention, risk management or crime prevention. Last, but not least, the operational definitions are affected by the cultural biases, which also influence the choice of the methodology and the focus of the scrutiny (crime, threat, cost-benefit, vulnerability, opportunity, motivation, risk analysis, or other).

The methodologies yield different cultural and operational profiles, which in turn lead to partial solutions. For example, the 'military approach' profile may see the opponents as enemies as actors; war and other military activities as the nature of events; conflict of interest as a cause, and defence, conquest or disruption as effects. The primary aim is the neutralisation of the hostile actors. Definitions are derived from experience and enforced in military manuals. The approach focuses on fighting the threat and the methodology is one of threat analysis. A similar analysis could be made of each of the approaches, and specific profiles could be built.

None of the approaches offer a basis for a general structure, though they do contribute to it.. They assist with strategic and tactical decision-making, but cannot be used in articulating a security theory. Alas, it is submitted that none adopts an overall security approach, since stems from different definitions, focuses, approaches and scopes, and covers partially different fields of interest.

This assertion may well be challenged. More substantial evidence could reasonably be demanded. However, such a debate in the absence of agreed definitions can only be sterile. This research offers definitions (next sub-section) with a view to providing the common ground essential for productive discussion. For the moment, the assertion rests upon the analysis which has been offered.

1.2.3 General Features of Security

Having identified the main problem areas, (absence of theory, confusion of definitions and multiplication of approaches) it now seems appropriate to identify those areas which may offer common ground for the subsequent analysis. This can be found in those features specific to security and which distinguish its body of knowledge from other issues or activities. A preliminary review of the historical evolution of security suggests a common theme which underlies security concepts and activities:

'I must take care of this (person, asset, etc.), because somebody has the intention of, or is acting to, steal, spy upon, damage, or destroy it. I must do it personally, because I will suffer the loss or damage, and nobody else (not even the State) is undertaking the task.'

From this theme preliminary considerations can be drawn. Security emerges through history and literature as a concept initiated by worry, [60] based on antagonism, [61] driven by egoism [62] and inspired by conservatism. [63] Worry (and the associated states of fear and anxiety) is the initiating factor leading to security considerations and activities; this point is further discussed in Section II (Genesis of a Security Process). Security activities are prompted by and subject to another person's initiative. This leads to antagonism, that is, opposition to somebody intending, or acting, against someone else's object of interest. This feature of antagonism explains why security is characterised by a degree of uncertainty. The feature of egoism derives from basic self-preservation, and leads to self-interest. Self-preservation and self-interest give security its particular characteristics. Firstly, conflict is deemed to be a last resort and a risk to be avoided; security is therefore risk-adverse. Secondly, security is directed at preservation of existing assets, not at the acquisition of the attacker's assets; it is therefore conservative. Thirdly, security is, as far as possible, defensive, not aggressive; pro-active attacks on the antagonist are not within its normal methodology; this concept has always been recognised by laws. Fourthly, security is self-centred in that it seeks to safeguard the holder's assets by protective measures which may (and are often intended to) encourage the antagonist to direct his attention elsewhere. [64] Hence, security concepts are based not on a 'defend to the last', but on a 'defend as long as justified' principle.

[60] *'state of being anxious, or troubled'* OALD

[61] *'active opposition or hostility, esp. between two people'* OALD

[62] *'a state of mind in which one is always thinking about oneself and what is best for oneself'* OALD

[63] *'tendency to resist great or sudden change'* OALD

[64] The effect of displacement as a consequence of deterrence has been immediately understood, and rationally exploited in the choice of security measures.

In philosophic and economic terms, the principle of justification of security activities may be seen in terms of interest and utility. Adam Smith's theories on self-interest and John Stuart Mill's theories on the human tendency to pursue 'utility' [65] may give a good explanation of the function of security. This reasoning may even lead some authors to think of security in terms of utilitarianism. [66] These positions, which have widely been adopted in 'Security Management' and 'Crime Prevention', are not completely clear in security practice. For a start, interest and utility may be difficult to define. The interest of the private sector are relatively apparent: peace of mind, money, personal integrity, etc. On contrast, those of the public sector are less obvious. A variety of interests is served: political popularity, party policy, budgetary targets, minority pressures, department and personal interests are amongst those within the dynamic which is contained within, or concealed within, the public good. These different viewpoints may lead to conflicting priorities and constraints during the decision-making process, a point further discussed in Section III. Even assuming that interests and utility are clearly definable, the position suggested by utilitarian theories that private security contributes to general security is not supported by evidence. As each private security programme (which may pertain to a criminal, spy or terrorist) is designed to meet a particular self-interest, the impacts of the different programmes may conflict and not combine usefully. [67] Furthermore, the interests of private security may also conflict with the common good, raising issues of civil liberties. Equally, public security may be designed to further the interests of those in government, to the detriment of the interests of the public. The extreme examples are dictatorships and totalitarian regimes. On the other hand, there is common ground which accounts for a convergence of interests. The majority of security related subjects agree on identifying the majority of offenders as acting on the basis of opportunism. In this line of thought (i.e., 'administrative crime prevention'), each private activity is a restriction of the offender's area of choice and action. This may result in a number of them abandoning their nefarious activity because of the diminution of their marginal utility. In this perspective, utilitarianism may be seen as a driving force towards improving public security via the improvement of private security activities. [68]

[65] *'quality of being useful'* OALD

[66] a set of theories *'based on or supporting the belief that actions are good if they are useful or benefit the greatest number of people'* OALD

[67] e.g., 'Displacement Theories' in Crime Prevention.

[68] for an approach to this position, see Goodin, 1995

Balancing the pro and contra, the researcher submits that the conclusion that bona fide security activities will supplement or complement each other and thereby further the common good is not justified by the evidence. While there is little doubt that security is driven by self-interest, it seems difficult to infer that it conforms to the principle of utilitarianism.

This analysis is central to the research. It is debatable and therefore further evidence will be provided later. It is appropriate, before proceeding to the more controversial concepts of security, to outline its operational features.

1.2.4 Operational Features of Security

As most consideration of security has been at the operational level, this outline reviews *how* security operates, through which means and methods, and *why* these means and methods are applied. This is made through the discussion of the 'tools', 'functions', 'principles' and 'methods' of security.

Since security is largely empirical and not based on scholarly literature, both the distinctions and the exposition of concepts are arbitrary. They respond to the researcher's personal conception and are only made for the purpose of exposition. The absence of agreed definitions and the number of the approaches make it obvious that this description may be subject to different interpretation.

As an example, there is evidence in existing literature that planning, organisation and conduct of security measures and activities (the 'tools') is lead by a number of specific ideas, or 'principles', which their exponents consider to have been validated by their own past experience. These 'principles' depend upon the particular approach, and while there is a general agreement on the fundamental concepts, the interpretation of their operational facets tends to be parochial. For instance, at the academic level it is possible to find positions based on the (previously mentioned) concepts of 'balance of power', 'deterrence', 'risk reduction', 'opportunity reduction', 'social prevention', 'legislative prevention', etc. At the operational level, two examples of different conceptions are found in the Kluwer's Handbook of Security, and in the Group 4 Manual.

The Kluwer's Handbook of Security supplies the following list of principles:

Protective measures must be so designed that, when a breach of security occurs, this fact is known as quickly as possible.

The first breach of security occurs when it becomes known that a target exists.

Protection of his property and of the workpeople is the responsibility of the proprietor or his manager.

Security measures should be commensurate with the threat

Concentration of risk.

If sabotage is a threat, bottlenecks must be eliminated.

The criterion of access is need.

Security must have a good image.

It is not one measure that will give security, but the sum of all practicable and possible measures.

That which protects must itself be protected.

All security systems should contain an element of surprise for the criminal.

Co-operation.

Maximum complicity.

Guilt must be pinned.

While the strongest barriers should be that closest to the target, the most effective burglar alarm is that which gives the earliest warning.

Security measures of whatever kind must ultimately defer to the concept of human freedom.

(Kluwer's Handbook of Security' :1.3 Principles of Security)

Group 4's Security Manual (1992:3) describes what are called 'key principles':

Informed

Directed

Independent

Co-operation

Monitored

Consistent

Unpredictable

Concentrated

Appreciated

Acceptable

(Group 4 Security Manual, 1992:3)

These 'principles' appear to be used as a check or quality control list, to refer to when solving a security problem:

> *'In considering any security problem and the possible ways of providing the correct solution, a constant referring to the above principles should ensure that the suggested solution will be the right one'*

(Group 4's Security Manual, 1992:3)

Moreover, it is not clear if the concepts above described are 'principles', 'functions' or 'activities', and an agreement on such concepts seems far from reached, with it depending on the approach. Following in the example, authors do not agree on the necessity of such detail. A very condensed synthesis of security 'principles' may be found:

> *'...three general principles ... are broadly applicable to all security problems: the removal of temptations, defence in depth, and concentration of protection'.*

(Wright, 1972:26)

There are authors, who think of security as the positive result of a conflict and identify its principles as those classic of war: alertness, decisiveness, aggressiveness, speed, coolness, ruthlessness, surprise, etc. [69]. Others, who think of security as a system, tend to refer to the mechanics of security activity, such as the well known equation of physical defences [Time of Penetration (TP) must be greater than the sum of Time of Alarm (TA) and Time of Intervention (TI)]: [70]

$$Tp > Ta + Ti.$$

[69] Cooper, 1972

[70] Biasiotti, 1991

Authors from military security tend to refer to principles such as C3 I (Command, Control, Communications, Intelligence), while those from governmental security (counter intelligence, anti-terrorism, subversion, sabotage) or from the police tend to refer principally to the intelligence and investigative phases. The private sector approach is generally related to management and loss prevention:

> *'Security, in its generic form, and the security survey audit, in its specific application, are essential elements of the total risk management function. The precise role that security plays will depend on the particular business at hand'.*
>
> (Broder, 1984: xvii)

The above references are a sample of the existing literature. In general, those concepts are not clearly expressed, and the evidence for them can be deduced only by analysis. Therefore, no further examples are offered. The very fact that existing literature is largely written by operational and technical people for their own use, and in the absence of an overall theory, leads to its limitations.

It has already been said that both the distinction and the exposition of concepts are arbitrary. Each application has, in practice, overlapping aims and effects, and could be considered a principle[71], an effect[72], or a function[73]. For example, it is possible to hear or read that *'in order to prevent a burglar entering the window, we must protect it with security shutters, which may also deter or stop him'*, or that *'the principle of prevention requires the use of security shutters, in order to impede, delay, or deter a potential burglar'*, or, equally, that *'the principle of protecting the window with security shutters against an assailant will result in an effect of deterrence, so as to fulfil the primary function of prevention'*.

In the example, security shutters may be considered to have primarily a protective function, or to accord to the principle of deterrence, or, because they both protect and deter, to accord to the principle of prevention. Each term will be discussed on the basis of its primary purpose, not on its causes or effects.

[71] *'basic general truth that underlies something'* OALD

[72] *'change produced by an action or cause; result or outcome'* OALD

[73] *'special activity or purpose of a person or thing'* OALD

1.2.4.1 Tools

The condition of security is attained through specific activities, which need specific tools to fulfil their security function. The identification of these tools makes it possible to understand their basic functions and goals.

The evidence of existing security measures, and a survey of the existing literature, show that the condition of operational security is achieved through specific activities and tools, which are identified in the following diagram: [74]

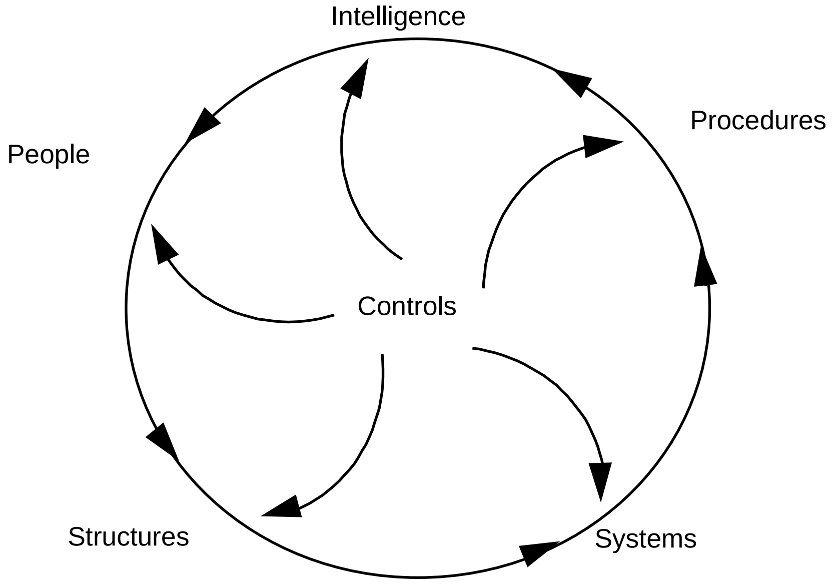

Figure 1 A Security System

The above diagram shows that the condition of security results from the interaction between Intelligence, People, Structures, Systems, Procedures and Controls. The Controls are seen as 'the source of synergy', by their direction and co-ordination of the others.

I<u>ntelligence</u> is, generally speaking, a specialised process related to the collection, analysis and dissemination of information. This activity is frequently confused with that of espionage, which relates only to that part of the collection phase where covert means are used. In security, intelligence ranges from governmental (which is mainly directed against foreign states, terrorism and organised crime) to private (from external threats and competitor

[74] CSPO Course notes, 1996, module I, unit 1: 18 (fig.1: Manunta's Security System)

intelligence to basic internal investigation e.g. vetting). The activity of intelligence and its concomitants (deception, secrecy, early warning, surprise...) is of prior importance in security, where the old proverb '*To be forewarned is to be forearmed*' holds good.

Intelligence (processed information) allows prediction, pro-activity, better use of tools and methodologies, optimises functions, and helps decision making processes. The goal of intelligence in security is that of assisting decision-making and providing the necessary evidence.

> *'The key to winning this kind of warfare[*terrorism*] is accurate intelligence on the capabilities of the opponent. Only when this is available it is possible to deploy appropriate countermeasures, such as jamming, deception, and the whole range of electronic countermeasures (ECCM) can be utilised.'*
>
> (Wilkinson, 1993: 7)

Traditionally, this theme has three facets: information, counter-information and disinformation. Its basic features are: to know everything about the opposition, to conceal everything about ourselves, and to deceive the opposition so as to provoke incorrect assessment and decisions, whilst not being deceived ourselves. Security being the result of a rational activity, good information reduces the risk of a wrong decision. On the other hand, denying information to the opposition, or deceiving them with false information increases their risk of wrong assessment and decision. Imaginative use of technology and tactics may help to achieve surprise, to entrap, and to deceive or unbalance the counterpart. With information playing such an essential part, imagination and its fruits (creativity, ingenuity, surprise, opportunism) is one of security's most powerful tools.

People are the subject, the object and the antagonist of security. As a subject (security managers and personnel), people require, decide, plan and execute security policies, programmes and projects; control, manage and guard structures, defences and systems, and intervene when and where necessary, according to proper training, plans and instructions. As an object, people are protected, assisted and controlled by security practitioners, assisted by security structures and systems. As antagonist, people are opposed, challenged, impeded, intercepted and restrained. It is an axiom in security that people are the weakest link in the security chain. Apart from negligence, the possibility of internal complicity, or negative activity, should never be dismissed as implausible, particularly today, when white collar crimes, work crimes, internal assaults, sabotage and espionage represent a large part of the threat.

Structures are a fundamental part of any security system, and can have different features, which may be summarised as: containers, barriers and shields. As containers of people, properties and activities, they should be designed to assist in control and intervention. As physical barriers they have the task of deterring, impeding or delaying an eventual attacker. As shields, they have the task of interfering with a disruptive attack (e.g., chemical, electromagnetic, bomb, bullet or knife), by impeding or stopping it, or minimising its effects.

Systems have the role of assisting intelligence, people and structures, in that they can control, detect and verify any undesired presence or activity in a given volume, space or access. If necessary, systems can be designed to give evidence of specific events, or to provide information about presence, movement and activities. It is an axiom in security that systems are only as good as their operator. 'Smart' maintenance (so to neutralise sensors or interfere with their correct functioning) is not uncommon in security systems. The researcher' experience indicates that security personnel are increasingly system-oriented. This is thought to be to the detriment of awareness, attention and analysis, and to produce 'administrative' rather than 'intelligent' security.

Procedures have the role of linking people, structures and systems, to obtain a fully integrated security system. Procedures are needed to activate or deactivate an alarm, to open or close a safe, to control accesses, people, cars and equipment, and to deal with a specific problem or a situation of crisis or emergency. It is an axiom in security that procedures are the second weakest link in the security chain. This postulate may induce security managers to confuse complexity with security and to produce a punctilious list of operations to be performed. However, too close procedures (typical of bureaucratic organisations) tend to alienate people, and to limit their sense of responsibility and initiative. Conversely, too loose procedures (typical of non-hierarchical organisations) tend to produce superficiality and inattention. A balance may be very difficult to achieve.

Control is viewed as 'the source of synergy', which provides direction and interaction with and within the others. The very concept of security (as a network of activities) is based on control and ascertaining in sufficient time that something undesirable is happening, or is going to happen. Control is assisted by procedures; it maintains and improves system performance, and manages the response. Control may take different forms depending on its timing, but in security should be essentially pro-active. To achieve and maintain a security condition in a given state of affairs, all the relevant spaces, structures, accesses, volumes, people, activities and properties must be kept under control, so that it becomes clear in sufficient time when, where, how and why to intervene to restore the desired condition. In security, control is assisted by sophisticated methodologies and technologies, the former being essentially related to the use of compartments and profiles, and the latter being essentially based on hi-tech forms of detection. This activity, which covers all the aspects of the security system (e.g., intelligence, people, structures, systems and procedures) must extend to both internal and external threats.

1.2.4.2 Functions

In order to achieve and maintain a condition of security using these activities and tools, certain security 'functions' have to be fulfilled. Their identification clarifies *what* security is intended to do and *why* a specific security measure is used. These 'functions' have already been identified and defined as: *prevention, protection, deterrence, detection, alarm and response.*

As stated earlier, security is based on prevention: being risk-adverse, its measures and activities are primarily intended to ensure that the undesired event will not take place. This result may be achieved in a number of ways, by avoiding, impeding, dissuading, neutralising or deterring a potential attacker. Preventative measures cover both non physical measures - such as awareness, avoidance, secrecy, deception, behaviour- and physical measures, such as detection, alarm, relocation, impediment, use of filters and deterrence. Examples of pure preventative measures are given by secrecy (e.g., the object of security is secretly relocated in an unknown place, and that secret is preserved), avoidance and pro-active neutralisation of the threat. The researcher's experience indicates that preventative measures on their own, not supported by protection and response, are rarely successful. This is because secrecy is difficult to maintain, awareness is limited by human factors, and not all threats are known or may be neutralised in advance. Therefore, prevention has to be considered to be a part of a security system. It should always be used hand in hand with protection, detection and response.

The fundamental security measure, protection, dates from the earliest human activities. Experience taught people that vulnerability was greatest at times when they were static, when involved in routine activities and during the combative phases of their life. Hence, the idea of providing for two necessities: the first one related to impeding, or delaying, the approach of an enemy when awareness and ability to respond were reduced. The second need was to shield persons or valuables from attack. Consequently, protection involves both the activities intended to keep the attacker at a safe distance by impeding, or at least delaying him until a response can be given (barrier, impediment), and the activities intended to interfere with the attack, in order to impede, or minimise, the damage (shield). In security, protective measures are generally aimed at prevention and at interfering with hostile processes such as choice, reconnaissance and planning, rather than to assist in combat. This explains why protective measures are often displayed, to deter (in their effect of dissuasion and influence on motivation) a potential attacker. However, a resourceful attacker may not be deterred, but make use of this evidence to improve her/his plans by exploiting the visible vulnerabilities. For example, a terrorist who knows that her/his intended victim uses a bullet-proof vest could decide to shoot him in the head. Thus, recourse to deterrent through display of protective measures must be carefully thought of; and the partial ostentation of protective measures may be used to deceive or entrap an attacker. Professional experience suggests that there is real value in protection when it is supported by detection, alarm and response. Prevention and protection may be insufficient to avoid, stop or deter a resourceful aggressor, whether s/he makes use of deception or overwhelming power. The necessity of safeguarding protective measures appears to be a matter of common sense. If defences are attacked or circumvented unknown to the protector, then there is a good chance that both the asset and the protector will be caught exposed. Consequently, the protector should uncover (detect) a potential aggressor as far as possible from the defences, to give the response force enough time to react in the best possible conditions.

Detection (and the immediate communication of what has been detected, i.e. alarm) is essential to make the best use of the protection, and to provide the most efficient response. Detection in security responds to a series of requirements. It should be made as far as possible from the defences; it should be communicated immediately and unambiguously; finally, it should be ascertained in the shortest possible time. The time needed for approaching and attacking the defences may then be used as a delay, which provides the response with the opportunity of reacting in the best tactical conditions (e.g., from an unexpected direction and with the support of the defences). In the case of local alert (for example, by using a siren), the alarm consequent to detection may as well have an effect of deterrence and thus, in a general sense, of prevention. With security being risk-adverse, detection must discover any sign of suspicious activity; therefore is, by its nature, overzealous. This calls for procedures and control, particularly where detection is largely entrusted to technological sensors who cannot distinguish intentions, but only work in the range of their programmed capabilities. This creates problems of false and improper alarms, and the necessity of verifying each alarm by ascertaining its real cause. When the rate of false alarms is high, the detection systems are distrusted by the response forces (police, security guards, etc.) with consequent lack of commitment. This human vulnerability could be exploited by a resourceful attacker, who may provoke a series of false alarm, until the security system is disconnected or distrusted.

Security is the result of a precarious equilibrium of activities necessary to impede its alteration or to restore the desired condition. When prevention has failed, but detection and alarm have worked, an effective response is not only due, but unavoidable, in order to restore the desired condition of security. To be effective, the response has to be timely and decisive. To achieve these results, provided that both detection and alarm occur in good time and that the resistance of the defences is effective (see the equation of physical defences: $Tp > Ta + Ti$.), the response has to be prepared in advance, adjusted to the possible requirements, and forewarned.

Response, both on the physical and logical levels, may be pro-active and/or re-active and have different aspects, according to the context. Clearly, a problem of intervention during an armed robbery requires different operatives, equipment, and methods of operation than those that would be required in the case of a leakage of information. It is important to note that, though operationally possible, the perfect response (one which neutralises the threat before damage is suffered) can rarely be made. This is because the range and effectiveness of the possible measures may be limited (and normally is) by situational constraints (e.g. of a moral, social, legal or political nature) or by criteria linked, for example, to a wider aim (political consensus, budget, legal and social considerations, etc.). A discussion upon the dilemma between technical effectiveness and general expectations and constraints in the field of national security and terrorism may be found in Wilkinson's '*Terrorism and the Liberal State*' [75].

[75] Wilkinson, 1986: Part I, 3-50 and pp. 103-109.

1.2.4.3 Principles

Given the above tools of security and the functions to be ensured it becomes possible to describe the 'principles' of security. Careful examination of operational literature indicates some generally agreed 'principles': *avoidance, opportunity reduction, denial, time delay* and *defence in depth*. A brief explanation of these terms may help.

The basic aim of security is avoidance, as, by nature and definition, security is risk-adverse, not risk-prone. Avoiding a danger, or a threat, thereby avoids the necessity for confrontation, which is, in terms of security, an insecure condition, since it implies the possibility of defeat. Avoidance is derived from awareness, which is based upon information of the threat (it being illogical to avoid, evade or escape, what is not known) and the detection and control of possible sources and situations of danger.

Opportunity reduction is based on the idea that *'prevention is better than cure'* [76] and is conducted at both the physical ('target hardening'[77]) and the psychological ('removal of temptations'[78]) levels. This principle is based on three assumptions: that the majority of attacks are made by 'opportunists' (who are also considered to be 'the least skilled of criminals'[79]); that a 'soft' target will be preferred to a 'hard' one' [80]; and that the attacker's choice of targets will be amongst those s/he identifies as such[81]. These assumptions confirm some of the general features of security (risk-aversion, self-interest) and its tendency to displace, rather than oppose, the threat.

The principle of denial is used in security as a more active interpretation of avoidance. It is derived from information and control, and aims at ensuring that the right people, goods and activities are in the right places and at the right times. Security is ultimately based on denial, i.e. on preventing something undesired from happening; this result may normally be achieved by denying the potential sources of danger the opportunity of reaching the object of protection. If denial of the sources of danger is impossible, or impractical, then this principle

[76] Home Office Research Studies: Co-ordinating Crime Prevention Efforts, April 1980: 7.

[77] Ibidem

[78] Write, 1972: 26-28

[79] Ibid: 27

[80] See: 'Rational Choice' and 'Displacement Effect Theories' in Criminology.

[81] 'Low Profile approaches' in personal security. See: Derrer, 1992; Flynn, 1979; Jenkins, 1985; Siljander, 1980; Shaw, 1993.

must be applied to the object of security (for example, a person in danger will be denied a place, an itinerary, an activity...etc.).

The concept of time delay is concerned with extending the time of exposure of the attacker, using space, procedures and barriers as a way of delaying the attacker and the actions s/he needs to accomplish, in order to be successful. The basis of time delay is the realistic assessment of time from perimeter to target. Time delay is achieved physically by setting of the most sensible targets in the most distant and protected place from the access, or perimeter, and logically by setting procedures. Each element of the programme is designed to increase the time necessary to penetrate defences, approach the target, execute the attack and leave. This has a strong effect of deterrence, as it increases the attacker's time of exposition to defender's response. The most important tools of time delay rest in architectural design, physical barriers, policy rules and regulations.

Defence in depth is also linked to time delay, but is mainly concerned with the use of protective measures. It aims to interpose a series of physical barriers (such as fences, doors, locks, cabinets, safes, and people) that must be penetrated by the attacker in order to attain her/his target. The idea is to reduce opportunity and capability by multiplicity, i.e., by requiring different accomplices, abilities and tools, while increasing the defender's opportunities.

1.2.4.4 Methods

The description of security's, 'tools', 'functions' and 'principles' is useful in circumscribing the context of its activities. The identification of the 'methods' helps to understand *how* security measures are conceived, planned and implemented. An example of the existing methodology in security may be found in Martin Smith's *'Common-sense Computer Security'*, in which he states that security entails:

1. Identification and valuation of the assets to be protected.....

2. Recognition of peculiar vulnerabilities and weaknesses....

3. Identification of all the threats...

4. An assessment of the likelihood -the risk- of a particular threat occurring or weakness emerging, and the consequences that would result.

> *5. The development, implementation, and enforcement of a cost-effective security policy to reduce as necessary the risks against the system...*
>
> *6. The preparation of suitable plans to recover from any disaster...*
>
> *7. Monitoring and reviewing periodically the effectiveness of the security arrangements.*
>
> (Smith, 1989: 4,5)

Indeed, this process is common in security literature, normally in a simplified version and often under various names:

> *'For a large organization or any enterprise serious about security, a professional method can be followed in assessing security needs. This method is known by various titles, including security survey, protective security risk review, security audit, and security review. The security review consists of the following four stages: resource appreciation; threat assessment; risk analysis; identification of weaknesses and recommended solutions'.*
>
> (Golsby, 1992: 53)

All security decision-making processes aim to identify, evaluate and assess at least these four elements (i.e., asset, threat, risk and vulnerability). Once the asset has been identified, effective responses are given to those threats and vulnerabilities defined as the most credible, or the worst possible, so to avoid the undesired potential impact (risk), or to reduce its effect to a more acceptable level. This is achieved by way of a series of operational steps, discussion of which now follows.

Security is a rational activity, therefore a professional survey (that is, an assessment of the present state of affairs) has to be made before any other step can be carried out. According to the problem, the survey may be made at different levels (general or specific), and by different methods (physical survey, technical inspections, interview, collection of data and use of simulations). The examination covers the threat, all the identified components of a security system and the examination of the existing (and foreseeable, if any) policies and programmes. The first step is the collection of data by appropriate methods, but particularly by statistics, interviews and the analysis of reports. This helps the planning and the execution of the subsequent step, physical inspection. Any information obtained from the survey are considered to be 'raw data', and subjected to analysis according to the identified purposes and priorities. The study of logs, incident loss reports and case studies is an invaluable tool for identifying where, when, how and at what cost it is necessary, and cost-effective, to take action. A careful examination of reports over a significant period of time will identify vulnerabilities (of assets and defences), frequency, times and duration of attacks, costs and losses, quality of intervention, areas needing more attention, procedures needing implementation or modification. A professional analysis elaborates these data into 'managerial' tools, such as matrixes, trees, flow-charts, indexes and models. Data collection and processing is always necessary. Existing data may be incomplete or its conclusions may be wrong. Nor should the possibility of disinformation ever be excluded.

Any security assessment should be the outcome of the collection and analysis of data, and review all the identified factors in relation to its policy and objectives. A security assessment may be required to find evidence, to find faults and leaks, to improve an existing programme, or simply to test whether the system is functioning correctly. The assessment is the groundwork for the planning of improved, better justified and properly costed security programmes. Assessments should always be presented in a way acceptable to persons without a security background (tables, models, flow-charts, matrixes). This format will also assist in the process of analysis.

Planning follows the principles of security. It contains the main aspects and tools of security (strategy, tactics, design, structures, systems, methods, procedures, etc.), to ensure the performance of the necessary functions. As mentioned previously, security is the product of an intelligent and rational activity, which are conducted mostly in routine conditions and with limited resources. Planning in security has four aims: optimise use of the resources by minimising interference and duplication and thus reducing wastage of time, money and labour; to assist, justify and control the decision making process; to ensure that the security programme is put correctly into practice and to control its implementation; finally, to guide and assist intervention in case of emergency.

Literature offers evidence that the assessment and planning phases are accomplished by borrowing qualitative and quantitative methods from other disciplines. For instance, surveys, audits, interviews (military, statistics, engineering); threat analysis (military, criminology, psychology); risk analysis (psychology, mathematics, statistics, engineering); risk management (management, econometrics). However, a caveat is appropriate. Agreement on a general methodology and the operational tools does not come from unanimity on the basic principles and definitions [82].

Preparation at all its levels includes moral, psychological and physical factors, such as selection, education, training, morale, awareness and determination. Consequently, preparation in security has many different aspects: educational, technical, tactical, and behavioural. All variety are needed because security covers a wide spectrum of activities and meets different requirements in the prevention, protection, detection and response phases. The preparation of a close escort team is as different from that of a TSCM team (Technical Surveillance Counter Measures), as the training of a guard is different from that of a control room supervisor.

In general terms, management is professional administration. Security management is an overall concept, covering all aspects of the planning and administration of security, including risk analysis and the choice, planning, organisation, administration and control of the security functions. Management is the key to the proper functioning of a security system. Because of its dependence on human activities, and of its vulnerability to even trivial errors, a well managed, even if inferior system will give better results than a badly managed, albeit hypothetically superior, one. In management, control of the activities is essential to meet the requirements of efficacy and efficiency. Managerial control should not be confused with security controls (previously discussed). Here, control is basically concerned with measuring progress and correcting deviations. The basic functions of managerial control are: to establish standards of performance, to measure actual performance against standards and to take corrective actions. It is a widely accepted opinion that

> *'Control activities act as the feedback mechanism for all managerial activities. Their use is, therefore, crucial to the management'.*
>
> (Cole, 1993: 7)

Given the importance of management in modern security activities and its influence on the operational methodology, the subject will be analysed more in detail after the presentation of the general theory.

[82] inter alia: Balloni, 1993; Broder, 1984; Gigliotti and Jason, 1984; Gill, 1994; Handbook of Security, The Royal Society, 1983 and 1992.

1.2.5 <u>The Problems</u>

Having identified the ground for the future reasoning, the next step is to analyse the two main areas which have been identified as problematic, those of definition and methodology.

1.2.5.1 The Problem of Definition

The previous investigation has shown that the problem of definition is closely linked to the broad range of approaches to security. Indeed, there is reciprocal influence between these issues: the different interpretations of security may be seen as the origin of different approaches to security, and vice-versa. The evidence is that security remains relatively unknown to the academic level and presents itself on the operational level as a concept with indefinite limits, covering uncertain quantities of insecurity.

Previous reasoning has shown that the reunification of this fragmented body of knowledge within an overall approach first requires a solution of the problem of definition. Different attempts have been made to reduce the dimension of this problem, generally via the discussion of the existing definitions, the identification of both the facts or events considered as object of security, and of the reasons why a need for security has been felt..

Booth and Wheeler, writing on international politics, make an excursus on the concept of security since 1945. They recognise that in the period 1945-1980 there was a shared understanding of the concept of 'security' between most observers of international politics, though no generally accepted definition. Security and defence were 'virtually synonymous' and implied some or all of the following:

> *"…that a state is free from the threat of war; that is able to pursue its 'national interests' and preserve 'its core values'; and that it feels safe against potential aggressors…"*
>
> (Booth and Wheeler, in McInness, 1992:4)

This concept was to change in the 1980s. Unease with the established concept of security, which privileged the state and military power, led to the growing recognition of a 'more holistic and dynamic concept' which, according to the authors, implies:

> *'first, a concept of security which focuses not just on the state, but which includes individuals and the world community as a whole; second, a concept which is not status quo oriented, but which is future oriented and seeks progressive change; and third, a concept which is not synonymous with military problems, but which encompasses a broad agenda of threats (economic, environmental and human rights for example) which prevents peoples and groups living full and free lives'*
>
> (Ibidem)

The conclusion is that security has become 'an essentially contested concept'.

A study of the various definitions of security and their logical meanings has been essayed by Post and Kingsbury. After having identified in the word *securus* (the Latin adjective from which the term security is derived) nine basic characteristics:

safe

free from danger

feeling no care or apprehension

protected from or not exposed to danger

providing guardianship

free from risk

satisfying

protective

taking effective precautions against,

the authors admit that *'Since definitions tends to be arbitrary, any attempt to classify them may result in overlap'* and, accordingly, classify these definitions of security into eight categories:

historical-a narrative of past events

psychological- the study and interpretation of human mind

sociological- the study of human social behaviour

functional-the procedural aspects of social controls

management-the organisational context of security

normative-the presenting of norms and standards

> *structural-security viewed in terms of its parts and relationships*
>
> *descriptive-a collection of different classification of elements of security.*
>
> (Post and Kingsbury, 1991: 3-13)

The identification of both scope and quality brings the investigation to a diverging dilemma: that of widening or narrowing too much the field of speculation. On one hand, the scope of security, such as that identified by the dictionary: *'freedom or protection from worry and danger',* seems to encompass all the problems of human life, worry and danger including, inter alia, psychological problems interesting more the field of medicine and psychiatry than that of security as we currently interpret it. On the other hand, the condition of security, resulting from the appropriate use of 'Security and Protection Systems' such as those identified by the 'Encyclopaedia Britannica' seems too reductive, in that it excludes, for example, behaviours. Yet, it is widely assumed that behaviours play a large part of prevention, management and reaction of and to security problems.

A different attempt to define the field of speculation has been made via the identification of those facts and events that are currently interpreted as being the object of security. For example, according to the Encyclopaedia Britannica, these facts or events pragmatically encompass:

> *'...a broad range of hazards, including crime, fire, accidents, espionage, sabotage, subversion and attack'.*

Some authors appear to consider this explanation to be 'reductive' and look at security as the ultimate answer to 'all types and kinds of losses':

> *'Taken in its broad context, security, at any level, attempts to accomplish two things: it must provide protection against hazards both manmade and environmental; and it must prevent all events, which have been defined as unlawful by society, from occurring to nations, states, municipalities, and individuals. Security's primary objective is thus to provide protection against all types and kinds of losses'* (researcher's emphasis).
>
> (Post and Kingsbury, 1991: 2).

This statement could be interpreted as an own-goal for professionals who could be considered liable in the case of *any* failure. It may have some relevance as the authors later limit their ambitions (but not their ambiguity) in admitting that security:

> *'... can ensure a* <u>*reasonably reliable protection factor*</u> *against disruptive influence'.* (researcher's emphasis.)
>
> (Ibid.: 11)

Utopia appears to be the inspiration for many good professionals, when they feel themselves obliged to give a justification of their work. Some authors appear to be unrealistic:

> *'Security being those measures which are necessary to maintain a state of well-being within a facility and to prevent loss, damage or compromise due to crime; espionage, sabotage, fire, accidents, disasters, strikes, riots.'*
>
> (Paine, 1972:23).

Other authors view security as a mission:

> *'Security functions are essentially protective (not punitive), preventive, and precautionary through the systematic organisation of normal operating relationships. Security's ultimate reliance is not in power nor the fear of power but in an understanding of the ethos of a society and the production of a climate in which functional responsibilities that affect the destined are discharged'.*
>
> (Knight, Richardson, 1963:98).

And

> *'Security provides those means, active or passive, which serve to protect and preserve an environment that allows for the conduct of activities within the organisation or society without disruption'.*
>
> (Post and Kingsbury, Ibid. :10),

others remove human factor and reduce security to common-sense warehouse management:

> *'the protection of property of all kinds from loss through theft, fraud, fire, and other forms of damage and waste'*
>
> (Oliver, Wilson, 1972:3)

The above quotes are a few examples, chosen to illustrate the current confusion in security. Further reference would confirm the trend towards two main positions. The first one is identified by Encyclopaedia Britannica (we may call it 'pragmatic'), which specifically limits the field to protecting people and property from fire, accidents, criminal and terrorist activities, such as theft, arson, sabotage and espionage. The second one (we may call it 'philosophical') is derived by the dictionary's definition, and assumes that security (by and large) should protect people, assets, the environment and the quality of life from all man-made and natural hazards and accidents. These include, *inter alia*, financial frauds, disasters, strikes, forgery, negligence, insolvency, accidents, riots, labour problems, war, acts of God and sexual harassment. In simple terms, security should protect the world from all the problems of life. Examination of specialist literature shows that the first position (the 'pragmatic' one) is losing ground to the second (the 'philosophical' one) in the last decade. Hence, the conclusion is that the current written evidence indicates that security is generally focused on the avoidance of, or protection from, *any* unwanted occurrence.

This is the *quid* of the problem, which prompted this research. The philosophical point of view, although fascinating, does not yield concrete results. The theory of security would then become as wide and as indefinite as a theory of beauty or happiness. Its concepts could not be transferred into an operative context. Its boundaries could not be defined. Without clear definitions and limits, security could not be considered to be a rational, let alone 'scientific', activity. In the absence of definite boundaries, how could it be judged whether *'someone, or something, is secure or not'*? How could a particular case or situation be assessed and performance measured? How could essential matters such as blame, liability, responsibility be decided?

However, a preference of 'pragmatism' over 'philosophy' can lead to the opposite error, that of narrowing the field too much, thus excluding areas and activities undoubtedly pertaining to security. Most of the written references on 'intentional' acts focuses on unlawful or antisocial events, their perpetrators, and connected causes and effects[83]. The voluminous literature is largely influenced by concepts from the Crime Prevention, and Law and Order areas of studies. This leaves out some events that most certainly pertain to security as, for example, a range of 'unlawful' government activities in the field of international and national security. It presumes security as a 'bona fide' activity performed by law-abiding citizens and organisations against spies, terrorists and criminals. More evidence for this position is offered.

The first argument is the absence of definition. Security is not included in dictionaries of sciences or philosophy, and challenges even semiology scholars. Dictionaries consider it an all-embracing concept, covering both psychological and physical conditions (freedom from

[83] For example, Post and Kningsbury, 1991: 3

worry, and protection from danger), and the activities intended to achieve them. Academic approaches range from international security to risk, including safety of people and environment. None of them provides a definition of security as a discipline in se. Therefore, a restriction of the field of study to unlawful or antisocial facts or events appears to be premature.

The second argument is more substantial. Freedom from worry or protection from danger are not considerations limited to crime, nor are they exclusive to the righteous. A patrol bivouacking in enemy territory, a spy, terrorist or criminal barricading himself against a police raid, are securing themselves from facts and events that they certainly consider to be 'worry and danger', but that cannot be defined as crimes. To conclude, no such discriminating position is to be found in Law. Security is a human natural right; and no law limits the right to security to a particular category of persons, no matter how defined[84]. Concern with security is not restricted to the law-abiding.

1.2.5.2 The Problem of Methodology

As has been seen, the literature of both the academic and operational fields reveals differences in priority, sphere and focus. These differences do not apparently recur in the framework of methodology, where there is a consistent agreement on its basic steps.

The origins of security methodology lie perhaps in a standard military procedure, the so-called *'solution of the problems'*. This procedure was created in the 1920's in Fort Leavenworth (General Staff School), USA, in order to give an ordered path of reasoning to the officers faced with military problems[85]. It was based on six steps: 1) statement of mission; 2) analysis of the enemy; 3) choices of action; 4) solution; 5) decision and 6) plan. This procedure, improved through the years and the experience of three wars (W.W.II, Korea, Vietnam) is still being used by NATO today, and a similar version is known to be in use in the East European Armies.

Today, military officers are taught 'military appreciation', a qualitative approach to decision-making, based on comparison between the enemy's and their own possibilities. It has seven

[84] Declaration of the Rights of Man and of the Citizen, 1789, art.2; Universal Declaration of Human Rights (UN General Assembly, 1948, art.3;

[85] Tuchman, 1991:90-91

main steps: 1) Study the existing situation. 2) Specify the aim to be attained. 3) Examine and draw reasoned conclusions on all relevant factors. 4) Consider all practicable course of action. 5) Decide on the best course to attain the aim. 6) Make a plan to implement that course. 7) Check all the reasoning and the practicability of the plan. A detailed description of this methodology may be found in military manuals[86].

Over the years, similar versions of the military process have been formulated by government departments for analysing specific security problems. According to Jelen, the present USA official methodology, National Operation Security Procedure (OP. SEC.), involves the application of a systematic analytical process consisting of five phases or steps[87]. These can be summarised:

1. Identification of the asset: the target the adversary needs to reach in order to achieve her/his goals.

2. Analysis of the threat: the identification of adversaries, their goals, intentions and capabilities.

3. Analysis of vulnerability: the examination of the total activity for factors that can be exploited by the adversary.

4. Risk assessment: an estimate of the potential effects of the exploitation of a vulnerability, and a cost-benefit analysis of possible corrective actions.

5. Identification and the application of appropriate countermeasures.

This formal process has been widely adopted in corporate security, and has certainly influenced safety reasoning. Probably, this is the result of national security controls over key strategic industries (for example, the nuclear) and the military background of many security professionals. Evidence of this process occurs throughout security literature[88]. All security processes aim to identify, evaluate and assess at least the focal elements (asset, threat, vulnerability and risk), in order to find efficient responses to those threats and risks deemed the most credible, so to avoid the undesired impact, or to reduce it to a sustainable level.

[86] S.M.E. -Italian Army-: IL METODO PER LA RISOLUZIONE DEI PROBLEMI OPERATIVI, 1987 (n.a.)

[87] Jelen, Security Management Oct.94: 67

[88] Golsby, Security Management, Aug. 1992:53

However, and perhaps not surprisingly considering the difference in priorities, focuses and scope of the various approaches, disagreement on the basic definitions and the operational tools has led to methodological differences. This is particularly evident when it comes to the calculation of the potential damages (risk). Here is where incongruities become apparent.

A variety of techniques, or 'tools' is employed. No consensus on the decisional criteria for ranking the operational issues is to be found. Criteria described by Orlandi [89] as 'probabilistic'[90], 'competitive' [91] and 'organisational'[92] are applied by different authors to similar situations in different formulae [93]. It is not clear when, and where, a particular criterion should be preferred and applied. To take 'Risk' as an example:

Opportunity + Target = Risk [94]

Threat + Vulnerability + Impact = Risk [95]

Probability X Magnitude = Risk [96]

Probability = Risk [97]

But also

$\mathbf{R = f \times M}$ [98]**,** which may become: $\mathbf{R} = \sum_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{R_i}$ or: $\mathbf{R} = \prod_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{R_i}$ [99] and even:

$$\mathrm{R} = \sum_{i=1}^{i=n} p_i D_i * \prod_{j=1}^{j=k} \left(1 - \varepsilon_j\right)$$ [100]

[89] Orlandi, 1989: 72-103

[90] Based on statistics. Measures are taken against the most probable event, threat, vulnerability, etc.

[91] Based on a comparison between 'protector' and 'aggressor', considered in terms of quality and quantity

[92] Based on the identification of 'paths', both physical and logical, that the attacker is likely to follow in order to reach his target.

[93] Baratte (1986: 374-375); Bound and Ruth (1983: 102-115); Courtney (1977: 97-104); Guarro (1987: 493-504); Makila (1985: 225-231); Miguel J. (1984: 307-311); Nielsen et al., (1978).

[94] Post and Kingsbury, 1991: 91

[95] Smith, ASIS Conference 1994, London

[96] The Royal Society, 1992: 5

[97] The Royal Society, 1992: 2

[98] Risk= frequency x Magnitude. Orlandi, 1989, Ch.4, AIPROS, 1984: pp. 8-15.

[99] Total Risk= the Sum or Product of single Risks, calculated as above. Ibidem

The ALE (Annual Loss Expectancy) formula is widely used in the USA. It has similar building blocks (frequency and magnitude), but on a logarithmic base:

$$ALE = \frac{10^{(f=i-3)}}{3}$$ [101]

This brief description of the above formulae shows that the different approaches based on the same framework of methodology have different system of calculus and, therefore, produce different results. This leads to different, but equally arguable, decisions. A more detailed explanation of the above formulae would be futile at this level of discussion, considering their world-spread usage in the last three decades. The point is:

> *'...the perception of risk is multidimensional, with a particular hazard meaning different things to different people (depending, for example, on their underlying value systems), and different things in different contexts'*
>
> (The Royal Society, 1992:89)

Evidence of this 'multi-dimensionality' is offered in Table 1 (below), where 'some formal definitions of risk or 'riskiness' (sic), quoted from Vlek & Keren (1991), are listed in a number of 10 different mathematical approaches, some of them have been described above in their mathematical formulae:

[100] Total Risk= the Sum of single risks, calculated as above, by the product of the probability of failure of each system, according to a factor of efficiency. Marcello, 1989:1

[101] Federal Information Processing Standard Pub. 65

Table 1: Definitions of Risk

Some formal definition of risk or riskiness

(1) Probability of undesired consequences

(2) Seriousness of (maximum) possible undesired consequences

(3) Multi-attribute weighted sum of components of possible undesired consequences

(4) Probability x seriousness of undesired consequences ('expected loss')

(5) Probability weighted sum of all possible undesired consequences (average 'expected loss')

(6) Fitted function through graph of points relating probability to extent of undesired consequences

(7) Semivariance of possible undesired consequences about their average

(8) Variance of all possible consequences about mean expected consequences

(9) Weighted combination of various parameters of the probability distribution of all possible consequences

(10) Weight of possible undesired consequences ('loss') relative to comparable possible desired consequences ('gain')

Source: Vlek & Keren (1991) [102]

Similar evidence can be gained from the analysis of the definitions of threat and vulnerability. This raises the important question: "if threat, vulnerability and risk have 'different meanings to different people in different situations', and if their assessment is subject to different methods and formulae, what can then be the utility - in terms of objectivity and explanation - of suggesting a 'Standard Decision Making Process' to those who disagree on 'standard' definitions and models?" It may also be argued that the methodology is far from satisfactory. Criticism in this sense may be found among social scientists [103]. These disagreements may stem from weaknesses in reasoning:

Firstly, without a prior identification of the context, there can be no clear premises and constraints and, therefore, difficulty arise in defining the objective. Secondly, analysis which starts from the prediction of potential damages, tends to produce solutions with regards to the effects, rather than to the causes. Thirdly, this kind of process is deterministic in its nature, because it considers the threat, the protector and the situation as rigid entities leading to quantifiable damages, thus not taking into account the dynamics of the antagonism. Fourthly, it tends to disregard reality, e.g. political choices in the setting of goals, priorities and constraints, which are prompted by interests that may differ from those of security. Finally,

[102] The Royal Society, 1992:95

[103] Adams, 1995; Borodzicz, 1992; The Royal Society, 1992

evaluation and assessment being mainly based on quantitative methods (i.e., on statistical weights and priorities), this process tends to omit those factors which are impossible to convert to numbers. In the security literature some of the situational, organisational and motivational implications, as visibility, choice, interference, capability, will and determination, are frequently neglected. These limits and deficiencies can help to explain why decisions stemming from such a process can be extraneous to the system to be protected, and why true security should not be confused with the simple activity of introducing barriers and controls.

There are two fundamental flaws in this approach: firstly, a security system conceived in such a manner tends to become complicated and contradictory, and to interfere too much with normal activities to be respected; secondly, that such a system is easily penetrated by a reacting threat, capable of rapidly changing targets, methods and tactics, and flexible to the point of creating new threats, vulnerabilities, and unthinkable damage.

1.2.6 Conclusions

The evidence is that the conception and application of security principles and methodologies are a disputed subject which would benefit from a more disciplined approach. The substance of security remains highly empirical. Its practice is still striving to emerge through a painful trial-and-error process from instinctual to rational operation. A multitude of actors operating in a multitude of fields have produced a plethora of approaches which only add to the general ambiguity.

It is submitted that the differences have historical and cultural causes. The main historical cause is the meagre interest paid in the past by governments to individual problems. The cultural cause is the widespread academic neglect of a subject which, until recently, was generally regarded mundane and without cultural significance. These factors have led to the current empiricism of security.

The practice of individual security was the product of necessity. It has emerged laboriously through a trial-and-error process from instinctual to rational operation. Individual security having evolved from a multitude of different efforts with limited interests, it is not surprising that the attention has been directed to ad hoc solutions of contingent problems, and not to speculation on theory. Starting from different premises and being driven by the exigencies of different needs, the different approaches have followed different paths of specialisation and have arrived at different positions and definitions. Different methods of calculus are used which reach different results and lead to different solutions to the same problem. These differences, whose reconciliation within a single concept is difficult, are the origin of cognitive, communicational, and decisional interference. This in turn produce conceptual and operational errors. Explanation, attribution of responsibilities and the measurement of performances become contentious, or even unrealistic. It is hard to see how this rationale can be attained when the prevalent attitude tends to a philosophical, all-embracing concept of security. This field of speculation is the most essential, since further progress depends upon it. On the one hand, security expectations should refer to reality, not to utopia. On the other hand, reality should not be confused with numbers. Security should not remain limited to a technological interpretation based on common-sense and empiricism.

There is no immediate answer to this need. The problem is not that of offering another approach, or attempting a reconciliation of the existing ones. The primary exigency is that of ensuring consistency, credibility and capability of control to the reasoning, so to permit constructive criticism, suggestions and progress. Any further discussion must stated in a way which allows both explanation and experimentation, conform to a sound methodology, not presently available. It is submitted that this methodology can be found in science. Hence, the next step is to identify, by means of a review of the concepts and principles of science, the approach and methodology by which the existing body of knowledge may be formalised into a theory. Without this step, further progress towards a science of security cannot be made.

1.3 WHAT IS SCIENCE?

1.3.1 Introduction

To investigate the scientific validity of the existing body of knowledge of security and the possibility of formalising it into a 'scientific discipline', a definition of science is needed. This is not easy, because no school of thought is accepted as definitive.

It is not within the scope of this research to discuss the many viewpoints on what is, perhaps, the most debated theme in the human intellectual activity. It is, however, necessary to explain, through a broad description of its principal paradigms, the positions adopted for the purposes of this research[104].

In order to present each step of the reasoning, this sub-section offers a definition of science by means of the identification of its main features, properties and principles. This starts from the generally agreed position[105] that science is, in essence, 'organised and reliable knowledge[106]'. The discussion covers the central criteria and paradigms. It seeks to identify that part of knowledge which is generally accepted as a science. The nature, derivation and scope of knowledge are analysed and, in particular, the justification of claims to knowledge. The concept of science being founded on the principle of reliability[107], the criteria of rationality, proof and validity are discussed. The final focus is on methodology, explanation and prediction.

The aims are: 1) to outline the methodology for undertaking and explaining the theoretical part of this research; 2) to establish the applicability of those criteria and principles particular to science to the existing body of knowledge of security.

[104] Encyclopaedia Britannica, 1986, vol. 25: Science; A Dictionary of Philosophy, 1983 (2nd ed.): pp. 319-321; A Companion to Epistemology, 1992: Scientific Knowledge; The Blackwell Companion to Philosophy, 1996: Chapters 1, 2, 9, 10, 11; Ayer, 1956; Popper, 1980; Pitt, 1988; Quine, 1993; Russell, 1980; Pasquinelli, 1970; Wolpert, 1992

[105] Science as: *"Organised knowledge, esp. when obtained by observation and testing of facts, about the physical world, natural laws and society; study leading to such knowledge; branch of such knowledge'* (OALD)

[106] Knowledge as*: 'understanding; all that a person knows; familiarity gained by experience; everything that is known; organised body of information.'* (OALD)

[107] *"being consistently good in quality or performance, and so deserving trust"* (Oxford Advanced Learner's Dictionary)

Consistently, the methodology outlined is immediately applied to verification whether security knowledge fulfils the conditions necessary to ensure its reliability as a science. Thereafter, the possibility of defining, or organising, security into a scientific discipline is examined, and a conclusion is offered.

1.3.2 What is Science?

This apparently simple question is Socratic. It challenges the fundamentals of knowledge and no conclusive answer has yet been found (and, conceivably, never will be). The nature of science has long been disputed, and the discussion of what can be considered as 'knowledge' or 'science' is as old as philosophy. Since Plato (c. 427-347 BC), different schools of thought have discussed whether Science is a branch of Knowledge or if it is Knowledge, starting their arguments by debating the very nature of the Knowledge[108]. This leads to dispute of the nature of the 'Knower' and of her/his objectives. It ultimately demands a definition of 'justification', that is, the criteria and methods which should be accepted in the process of 'scientific inquiry'.

What is 'science'? What is 'knowledge'? Any academic answer to these questions would certainly be controversial, and would most likely involve disciplines such as *'epistemology'* [109], the *'philosophy of science'* [110] and even the *'science of science'* [111]. These highly sophisticated disciplines attempt to provide a framework of understanding within which a science may be defined as such, and to evaluate its content of 'validity'. In order to define, analyse and evaluate the various branches of study, these philosophical theories of knowledge essay:

> *'...first, to elucidate the elements involved in the process of scientific enquiry - observational procedures, patterns of argument, methods of representation and*

[108] e.g.: Locke's distintions between knowledge and belief, 1975, chapter 1; Russell discussions on 'knowledge of truths' and knowledge of things', and on 'philosphical and scientific knowledge', 1990 chapters 5 and 14

[109] *"The branch of philosophy concerned with the theory of knowledge. Traditionally, central issues in epistemology are the nature and derivation of knowledge, the scope of knowledge, and the reliability of claims to knowledge"* (Dictionary of Philosophy)

[110] The branch of philosophy concerned with the rationality of knowledge. *"The philosophy of science seeks to show wherein this rationality lies; what is distinctive about its explanations and theoretical constructions; what marks it off from guesswork and pseudo-science and makes its predictions and technologies worthy of confidence. above all, whether its theories can be taken to reveal the truth about a hidden objective reality."* (Dictionary of Philosophy)

[111] A branch of science, which enables *"the study of its own development and history to be put upon a quantitative basis...society has increasingly needed reliable ways to judge the performance of science itself, particularly as science has demanded ever greater state funding. To meet these needs, science indicators have been devised."* (The Fontana Dictionary of Modern Thought, 1988: 761)

> *calculation, metaphysical presuppositions- and then to evaluate the grounds of their validity from the points of view of formal logic, practical methodology, and metaphysics'*
>
> (Encyclopaedia Britannica, vol.25: 661).

Answers are derived from different, and sometimes opposite, premises. 'Logical positivists' argue that science is the only form of knowledge, and that scientific arguments depend only on formal logic, and in particular on mathematics. 'Rationalists' refer the concept of science to that of 'rationality' (the logical deduction from hypotheses and induction by data), and rely on formal logic to test the 'truth' of their conclusions. 'Relativists' declare that science is unavoidably subjective, because the very setting of premises is the expression of creative individuality, and no datum or measurement can be absolutely precise. 'Sociologists' stress the fact that the collector of data is biased by her/his own social environment, and that the contamination of scientific language by everyday associations deprives even science of its most important quality, precision. 'Anarchists' deny even the existence of a 'scientific' methodology, and observe that

> *'the history of science reveals not a single rational method but rather a series of opportunistic, chaotic, desperate (and sometimes even dishonest) attempts to cope with immediate problems'.*
>
> (Searle, 1996:11)

Even the continuity of scientific knowledge is disputed: logical positivists see it as an accumulation of truths over time; Gestalt theorists affirm the contrary: since new theories involve new perceptions, knowledge proceeds through a series of 'radical discontinuities'. Revolutionary scientists think of it as 'paradigms' which are successively destroyed by new ones, through a series of 'revolutions'.

According to the evidence[112], the spectrum of opinions on the topic at hand ranges between two extremes: at one end, the general philosophical view identifies science with knowledge [113]; at the other end, the specialist, and prevailing, opinion restricts the definition of Science

[112] Encyclopaedia Britannica, 1986, vol. 25: Science; A Dictionary of Philosophy, 1983 (2nd ed.): pp. 319-321; A Companion to Epistemology, 1992: Scientific Knowledge; The Blackwell Companion to Philosophy, 1996: Chapters 1, 2, 9, 10, 11; The Fontana Dictionary of Modern Thought, 1988: 760); Ayer, 1956; Popper, 1980; Pitt, 1988; Quine, 1993; Russell, 1980; Pasquinelli, 1970; Wolpert, 1992

[113] *'Science defined simply as knowledge of natural processes is universal among mankind, and it has existed since the dawn of human existence'.* (Encyclopaedia Britannica, vol. 27:33). See Searle, 1996: ch. 3

to that branch of knowledge that can be measured and calculated [114]. The discussion from the former position revolves around the degree of rigour to be used in accepting 'knowledge'; the latter discussion focuses on the impossibility of measuring all that is considered to be 'known'. Both lead to a debate on the criteria to be used for dividing 'general' from 'scientific' knowledge. This debate is central to this research, therefore the next step is to review the principal paradigms of both positions.

The debate on knowledge is founded on insubstantial ground, because, despite highly evolved 'scientific' instruments, *"...it is not clear what we mean by knowledge"* [115] and, despite millennia of philosophical speculations, *"Concern with the theory of knowledge is very much a matter of taking this difficulty seriously"*[116]. This debate is probably as old as philosophy. First literary evidence is in Plato's *Theaetetus*, generally considered to be the first essay on epistemology.

Epistemologists dispute three fundamental questions: the cause, the scope, and the reliability of knowledge. The first question (what is the nature of knowledge and how it is derived) has an essential philosophical value, since the *quid* of the problem is a metaphysical dilemma (whether we have any sort of innate knowledge, or whether all our knowledge is derived by experience), which ultimately leads to debate the unsolved question of free-will and determinism and, thereafter, the divine nature of humans. These ideas have been extensively explored by different schools of thought, which have revealed a tendency to polarise into two opposite positions, rationalism and empiricism. Compromises have periodically been attempted. These viewpoints are summarised in the following quote:

> *"Rationalists (for example, Plato and Descartes) have argued that ideas of reason intrinsic to the mind are the only source of knowledge. In opposition to this view, empiricists (for example, Locke and Hume) have argued that sense experience is the primary source of our ideas, and hence of knowledge...But Kant took the view that the concept of cause is not empirical but rather a pure category of the understanding, required to make sense of the relation of events within experience...a sort of 'a priori' knowledge which is not derived from experience, but is a condition of the comprehensibility of experience."*

[114] *'...only natural science forms the normal, even the only, mode of true knowledge...'* (The Fontana Dictionary of Modern Thought, 1988: 760)

[115] Pitt, 1988: 3

[116] Ayer, 1956: 78

(A Dictionary of Philosophy, 1979: 109)

This debate continues, with fuel being added to its flames by contributions from specialised areas of study (cognitive psychology, problem-solving and artificial intelligence.

The second question (what is the scope of knowledge) raises definitional and teleological [117] problems. In the former area, distinction is made [118] between knowing things (which involves experiential knowledge), and knowing about things (which require propositional knowledge, i.e. the result of inference [119], reasoning, and communication). The teleological area of problems relates to what is expected of science: explanation, prediction, or both. Any discussion of either the definitional or the teleological issue ultimately returns to the original unsolved question: what is knowledge, and how is it derived.

In the absence of agreement on the first two questions, the debate moved to the third and apparently more pragmatic, question: the reliability of claims to knowledge. This issue is central to science. By encompassing the conditions of proof, explanation and predictability, it is widely considered the boundary which separates scientific from general knowledge. An agreement on this subject is far from reached, as it raises important philosophical and theological considerations. The most important is: what do we mean by 'reliability'? Does reliability mean certainty?

Most philosophers and scientists reject the pretension that reliability can ever reach the absolute value of certainty, with the possession of such a criterion being considered beyond human capabilities. Theologists argue that certainty would entail that biblical knowledge of the Good and Evil which was denied to humanity with the banishment from the Garden of Eden. According to Plato, Socrates would merely assert that only one thing is certain to him: 'to know nothing' (a certainty which, like that of Descartes on doubt, was immediately disputed, on the very ground of its formulation). Bertrand Russell would simply appeal for an answer to the question:

[117] *'The theory or study of purposiveness in nature'* (A Dictionary of Philosophy, 1983: 350)

[118] Russell, 1980: chapter 5.

[119] *"The process or product of reasoning or argument. In a piece of reasoning or an argument a conclusion is inferred or derived from a premise or premises; it is asserted as true, or probable, on the assumption of the truth of the premise or premises."* (The Fontana Dictionary of Modern Thought)

> *"Is there any knowledge in the world which is so certain that no reasonable man could doubt it? This question, which at first sight might not seem difficult, is really one of the most difficult that can be asked"*
>
> (Russell, 1980:1)

Yet, even accepting its 'natural imperfection', the question of reliability cannot be ignored without disputing even the possibility of science. The nub is the nature of the criterion to be used for judging, if not the absolute, at least a 'satisfactory' degree of reliability. Philosophers argue that such a criterion is based on a circular reasoning, since, to define 'reliability', it should already possess the quality of being 'reliable', and ultimately must base its validity on an 'act of faith' [120]. Scientists reply (after Galileo and Bacon) that science, being humanly imperfect and perfectible, is not grounded on faith, but on proof deriving from experiment, test and evidence of facts. Philosophers retort that empirical 'proof' cannot verify the complete evidence (all the possible cases past, present and future); hence, also scientists rely, soon or later, upon an 'act of faith': that on the principle of induction [121]. Since the validity of the criterion of inference by experience (induction) is not absolute, and verifiability[122] proved to be

> *'...a very strong condition....One was justified in claiming to know that x if x was verified. Unfortunately, as it turned it out, the condition created problems because it was too strong.',*
>
> (Pitt, 1988: 4)

the efforts to make sense of verification separated along two different paths of reasoning. One, associated with Descartes and Popper, was directed at the proof of its contrary: *falsification*. The other one*,* associated with Plato's tripartite theory of knowledge[123] and the paradigm *'justified true belief'*, was directed to a weaker condition, that of *confirmation*. These positions have been held in epistemology with alternate fortunes, with occasional attempts at reconciliation.

[120] Kant, 1781; Russell, 1980; Popper, 1990

[121] *'Induction is the process whereby scientist decide, on the basis of various observation or experiments, that some theory is true'* (The Blackwell Companion to Philosophy, 1996: 290)

[122] from Latin: *'verum facere'* = to make true

[123] According to Plato, for epistemic validity, a proposition has to be true, to be warranted (supported by evidence) and to be believed.

René Descartes (1596-1650) identified the criterion of reliability as the ability of knowledge to survive scepticism, or 'doubt'.

> *'Descartes' epistemology, indeed, was to pivot precisely upon the sceptic's method of doubt in his setting aside any claim that was open to doubt until he discovered some indubitable truths, for example,* *cogito, ergo sum'* (I think, therefore I am. Researcher's translation)
>
> (A Dictionary of Philosophy, 1983: 109)

The investigation then shifted to the question of doubt, which revived the basic questions of cause and scope: What is doubt? How it is derived? How do we know we have a doubt? What is the scope of doubt? How do we know a doubt to be *true*? These questions, being complementary to those on knowledge, are only a reformulation of the main problem: what is knowledge? Moreover, it was soon argued that even the belief in doubt is a certainty, which, following the Cartesian principle, there are strong reasons to doubt. Doubt, it was generally agreed, cannot be used as a criterion, but only as an impelling force disputing the reliability of knowledge and opening new fields for speculation. Consequently, a second path of reasoning (that leading to *confirmation*) was explored. The necessity of satisfying this requisite by way of incomplete evidence shifts the problem from confirmation to *reliability*, which opened a different and more practical set of questions: To which degree has 'reliability' to be 'reliable'? Can 'reliability' be measured, and how?

These questions raise two different problem areas: (1) it is not clear how much evidence is needed and (2) the non-physical phenomena would be excluded from having the 'dignity' (reliability) of science. In the first problem area,

> *'The fundamental issue here is the construction of a strong enough relation between an hypothesis and the evidence for it to allow asserting the hypothesis, that is, to claim it as knowledge. Basically, the problem is one of determining what it means to say you have enough evidence.'*
>
> (Pitt, 1988: 4)

Moreover, there is a body of opinion that holds that:

> *'If by 'knowledge' we mean something like 'have evidence in support of theoretical claims that the world is populated by such-and-such entities and is governed by so-and-*

> *so laws,' then we have a different sort of difficulty. The problem here is that we do not have enough control of the evidence-giving relation to know when we are in a position to claim that having evidence entails we are justified in our cognitive claims'*
>
> (Pitt, 1988: 4)

The second problem area is associated with the fact that empirical proof (as proposed by natural and physical scientists) is considered unsatisfactory -or non generally usable - by scientists dealing with less-measurable areas of research, e.g., the non-physical sciences, and philosophers. Empirical proof would not explain most of their work, as, for example:

> *'The proof of a philosophical statement is not, or only very seldom, like the proof of a mathematical statement; it does not normally consist in formal demonstration. Neither is like the proof of a statement in any of the descriptive sciences. Philosophical theories are not tested by observation. They are neutral with respect to particular matters of fact.'*
>
> (Ayer, 1956:7)

Consequently, some philosophers (for example, Wittgenstein and Ayer) attempted to redirect philosophical attention

> *'...from the defence of claims to knowledge against doubt to the analysis of their meaning. For instance, it would now commonly be held, in A.J. Ayer's standard formulation, that what is meant by the claim to know proposition P is that at least (a) P is believed, (b) P is true, and (c) there are good reasons for believing that P is true.'*
>
> (A Dictionary of Philosophy, 1983: 110)

This is only a reformulation of Plato's tripartite theory of knowledge, which Gettier (1963) demonstrated to be inadequate [124]. Neither the principles of belief nor that of truth can be used in science as a criterion of reliability. The content of relativity and uncertainty implicit in the concept of belief [125] weakens its validity for the assessment of the reliability of knowledge, because:

> *'It is indeed true that one is not reasonably said to know a fact unless one is completely sure of it. This is one of the distinction between knowledge and belief.'*
>
> (Ayer, 1956: 16)

[124] Gettier considered the case where an epistemic object was true and warranted but believed for the wrong reason.

Truth may be very difficult to prove in philosophical and scientific terms, since it is not clear when truth is satisfied. There is no agreement on the nature of the truth, nor on the criterion for defining truth. Quine's assertion that *'Pilate was probably not the first to ask what truth is, and he was by no means the last'* discourages the use of truth as a criterion of reliability[126]. He also observed that truth may sometimes be considered a *quality* rather than a relation.

Hence, it seems that only Ayer's condition 'c' (notably, the existence of 'good reasons') is accessible to philosophers and scientists. Quine offers evidence for this conclusion and defines the most common criteria for establishing a truth condition: *correspondence, similarity* or *resemblance* between the proposition and the fact, or state of affairs; or a relation of *coherence* between propositions; or even a *satisfactoriness of belief* [127]. To be satisfactory, since Hume (1711-76), philosophers and scientists have required belief to be *'justified and true'*, i.e. supported by 'good reasons'. This requisite has proved to be difficult to attain, being linked to the unsolved areas of confirmation and induction.

> *'On examination, keeping Hume's problem of induction in mind, it appears any degree of support short of invoking total evidence (all evidence past, present and future) is arbitrary'.*
>
> (Pitt, 1988: 4)

Thus, the problem became: "when can we say that inductive reasoning (i.e. a generalisation based on incomplete evidence) has the reliability of a 'justified true belief'"? One important contribution to this issue has been conveyed by Bayesians, named after Thomas Bayes (c.1701-61). They hold that our beliefs (including scientific beliefs) come in degrees, which are based on the axioms of the probability calculus [128]. Thus, for example, a person can believe to degree 0.7 that a given event will take place, since statistics indicate a probability of 70% for that event. It is important to note that

> *'...while Bayesians think of degrees of belief as probabilities in this mathematical sense, they still think of them as subjective probabilities. In particular, they allow that it can be perfectly rational for different people to attach different subjective probabilities to the*

[125] see Locke's notions of knowledge and belief (1975, chapters I , IV)

[126] Quine, 1993:93

[127] Quine, 1993, cap. V

[128] Papineau, 1996: 295-8

> *same proposition - you can believe that it will rain today to degree 0.2, while I believe this to degree 0.5.' (Author's emphasis)*
>
> (Papineau, 1996:295).

At first, Papineau says, this acceptance of subjectivity might seem to invalidate Bayesianism as a solid ground for scientific credibility. However, Bayesians maintain that this initial prejudice does not matter, because this belief will be revised in a 'rational way' until will correspond with the evidence. This rationale is offered by Bayes' theorem, which suggests a procedure for revising existing degrees of belief in response to new evidence (confirmation). If, for example, H is some hypothesis, and E some newly discovered evidence, then the degree of belief in H is adjusted in line with the right-hand side of the following equation, which states[129]:

$$\text{Prob (H/E) = Prob (H) x Prob (E/H) / Prob (E).}$$

According to the above equation, the probability p tends to 1 (certainty) as more evidence adjusts the hypotheses. Bayesians maintain that the application of this theorem can justify belief in scientific generalisations, because it leads to convergence of opinion, since, *'given enough evidence, everybody will eventually end up in the same place, even if they have different starting points'* [130]. This line of reasoning is based on the assumption that events are regular; it tends to exclude that which is not measurable and infers the belief that, given evidence enough, this process will converge, sooner or later, towards the perfect knowledge. To date, neither the assumption nor this belief have been supported by the history of science. Bayesians, says Papineau, *'fail to solve the principle of induction, since they do not show why all rational thinkers must expect the future to be like the past'* [131].

Thus confirmation is a perilous predicament, since a 'justified true belief' is only valid as long as the 'good reasons' maintain their validity. There is the further problem that, when these 'reasons' are empirical (based on a *finite* number of observations and tests), this condition is derived by induction.

[129] This theorem was originally proved by Bayes in 1763. A discussion upon this theorem can be found in Papineau (1996: 295-298).

[130] Papineau, 1996: 296

[131] Ibid:297

The paradigm of confirmation by induction has been challenged by Popper, who affirms that an explanation *'a posteriori'* (the inductive method) is scientifically unacceptable[132]. He states that science should then live by faith in some kind of *'uniformity of nature'*, which is hard to define satisfactorily, and seemingly impossible to prove without circularity (i.e., faith in the principle of induction itself). History of science shows that no scientific theory is ever conclusively *verified*, no matter how many tests it has survived, and it is always eventually proved *false* and transformed into, or replaced by, new theories, that pass not only those tests passed by the initial theories, but also additional tests. No run of favourable observational data, however long and unbroken, may be considered logically sufficient to establish the truth of an unrestricted generalisation. Since unrestricted generalisations could not be *verified*, he pointed out, they could be *falsified,* that is, *refuted by experience.* And *falsifiability*, not *confirmation*, is for Popper the *criterion of demarcation* of science. Scientific theories are always liable to be discarded or modified if the observations fail to fit their expectations. Hence, their scientific value lies not in the principle of induction (*verifiability*), but in their capability of surviving criticism, attacks, and tests (*falsifiability*). There is no reason why a scientific theory should not be proposed *'a priori'*, free from the constraints derived from inductive methods.

Popper's reasoning has the merit of having clarified the human fallibility and explained the role of scepticism in revealing the numerous errors of science, but leaves part of the problem unsolved. His principle of *falsifiability* shows when a scientific theory is wrong, but not when a scientific theory is valid. Yet, it is positive knowledge that makes science trustworthy. How much can science be trusted, if its validity cannot be proved? Not too much, the evidence suggests:

> *'Science, then, is to be considered in this article as knowledge of natural regularities that is subjected to some degree of skeptical [sic] rigour and explained by natural causes.'*
>
> (Encyclopaedia Britannica, vol. 27:33),

This definition, though elegant, leaves science on thin ice, with the basic questions unanswered: does 'regularity'[133] in nature exist? Is science only concerned with regularities? To which extent a 'regularity' has to be 'regular', in order to satisfy the condition? How, and

[132] Popper, K. The Logic of Scientific Discovery, 1990: 27-48

[133] *'state of being regular, i.e. conforming to a principal or standard'* OALD

to which extent, can ‘scepticism’ be reconciled with confidence on ‘rigour’? Many scientists and philosophers view this position as a compliant way of giving chaos an (only apparently) rational shape.

> *‘The mere recognition of regularities does not exhaust the full meaning of science....In first place, regularities may be simply constructs of the human mind. Humans leap to conclusions; the mind cannot tolerate chaos, so it constructs regularities even when none objectively exists...Science, therefore, must employ a certain degree of skepticism [sic] to prevent premature generalisation’.*
>
> (Encyclopaedia Britannica, vol. 27:32)

They further argue that, even when measure and calculus can be used to achieve some degree of belief and prediction, their mere formalisation does not assist explanation, since

> *‘Regularities, even when expressed mathematically as laws of nature, are not fully satisfactory to everyone. Some insist that genuine understanding demands explanation of the causes of the laws, but it is in the realme [sic] of causation that there is the greatest disagreement’.*
>
> (Encyclopaedia Britannica, vol. 27:32)

The importance of causation (i.e., the postulate that each phenomenon, or effect, has a reason, or cause) is that it allows for the formulation of general laws, hence for inductive inference. According to Hume (1711-76), causation is simply a matter of constant conjunction. One event causes another if and only if events of the type to which the first event belongs regularly occur in conjunction with events of the type to which the second event belongs. Hume said that the earlier of two causally related events is always the cause, and the later the effect[134]. The problem, says Papineau, is that *not all regularities are sufficiently lawlike to underpin causal relationships* [135]. There are two underlying difficulties: that of distinguishing genuine *causal laws* from *accidental regularities,* and that of giving a *direction* to causation, so to distinguish causes from effects. They are not easy to resolve in analysing physical phenomena, difficult in non-physical sciences, and particularly difficult in social sciences. Physical scientists observe that social sciences are reflexive (in the sense that they are part of the system they study), highly complex (the high number of variables, not all of them

[134] Hume, 1739

[135] Papineau, 1996:308-310

exactly identifiable, impedes mathematical modelling) and inconstant (their largely unforeseeable results depend upon human decisions, beliefs, desires, passions and caprice) [136]. Therefore, there are too few regularities to underpin either the law of causation, or the principle of induction.

All of which raises a set of very difficult questions: are sciences which do not pertain to the physical domain of nature 'scientifically' explicable? Which methods should they adopt, would they be considered 'reliable'? How far should the search for a cause be pursued? Must all causes be natural?

According to the Anglo-Saxon tradition, which has mainly been concerned with the problems of investigation and validation, *"only natural science forms the normal, even the only, mode of true knowledge (as distinct from received authority or mere subjective assertion)"* [137]. This is because natural science is derived via the principle of cause/effect from the observation of facts, according to an 'objective' methodology (i.e., based upon quantitative measurements), and it allows for tests and explanation (it may be repeated, therefore demonstrated and predicted), thus ensuring reliability. In this line of thought, measurability is generally considered the scientific criterion *'par excellence'*. Indeed, the well known Kelvinian approach is generally accepted: 'anything that exists, exists in some quantity, and can therefore be measured'. Science, it is assumed, goes hand in hand with technology: science leads to better technology, which in turn supports the progress of science. The invention of 'scientific' instruments such as the microscope, telescope, oscilloscope and spectroscope has brought an increased range of phenomena within the scope of our senses. Thus, the progress of science depends on technology, which provides the capability to make more phenomena perceivable through more sophisticated instruments of investigation. This assumes that, since science helps the invention of more precise instruments, and the instruments help, through more precise measurements, to achieve a more 'precise' science, this spiral will converge, soon or later, with the perfect knowledge. However, some scientists and philosophers disagree with this interpretation[138]:

[136] see: Stuart Mill's opening remarks in: A System of Logic, 1961, Book VI, Chapter 7

[137] The Fontana Dictionary of Modern Thought, 1988: 760

[138] for a discussion, see: Pitt, 1988: chapter 1; Wolpert, 1992: chapter 2

> *'Unfortunately, the line from science to technology is not a straight one, and it is not always obvious what the role of science has been with respect to any given technological innovation'.*
>
> (Pitt, 1988:3)

and

> *'...it is essential to distinguish between science and technology, particularly since the two are so often confused....Technology is very much older than science, and most of its achievements - from primitive agricolture to the building of great churches and the invention of the steam engine - have in no way be dependent on science. Even the mode of thought in technology is very different from that of science.'*
>
> (Wolpert, 1992: xii)

There is another problem. The criterion of measurability goes hand in hand with experimentation, observation and description of physical evidence. This leads to a dispute of the scientific status of non-physical sciences, notably social sciences. Physical scientists say that the 'scientific' principles of causation, measurability, experiment and induction cannot be applied in this area of study. Others disagree. This view was firstly suggested by Hume in his discussion of human actions, motives and causes:

> *'were there no uniformity in human actions, and were every experiment which we could form of this kind irregular and anomalous, it were impossible to collect any general observation concerning mankind, and no experience, however accurately digested by reflection, would ever serve to any purpose'.*
>
> (Hume, 1748, VIII, as quoted by Jones, 1996: 573)

More recently, Hempel and Oppenheim maintained that:

> *'...individual events may conform to, and thus be explainable by means of, general laws of the causal type... all that is needed for the testability and applicability of such laws is the recurrence of events with the antecedent characteristics, that is, the repetition of those characteristics, but not of their individual instances...there is no a priori reason why generalisations should not be attainable which take into account ...dependence of behaviour on the past history of the agent'*
>
> (Hempel and Oppenheim, as quoted by Pitt, J.C., 1988:14,15):

Their reasoning follows from two premises: that 'the determining motives and beliefs of the individual are classified among the antecedent conditions of a motivational explanation'; and that 'there is no formal difference on this account (researcher's emphasis) between motivational and causal explanations'. However,

> *'A potential danger of explanation by motives lies in the fact that the method lends itself to the facile construction of ex post facto accounts without predictive force. ...While this procedure is not in itself objectionable, its soundness requires that (1) the motivational assumptions in question be capable of test, and (2) that suitable general laws be available to lend explanatory power to the assumed motives.'*
>
> (Pitt, 1988: 16)

As stated earlier, the criterion of induction is criticised, since it assumes, on the basis of a *finite* number of experiments, that the world conforms to deterministic laws, which may therefore be inferred by induction. However, the same critics have offered no resolution of Hume's dilemma which states that *'if... the past may be no rule for the future, all experience becomes useless, and can give rise to no inference or conclusion'* [139]. Besides, scientists seem happy to agree that any theory may be accepted as reliable until supported by 'good reasons' and subject to a degree of 'sceptical rigour'. Within the limits already discussed, the criteria of proof via experiment, test and observation, supported by induction and Bayesianism, is an acceptable - admittedly, not conclusive - positive definition of scientific knowledge. After all, they argue, these principles have provided a ground solid enough for the conception and flourishing of science.

If this position is accepted, the problem becomes one of questioning the credibility of proofs and data coming from evidence, e.g., from experiments, tests and observation. This introduces Russell's elegant arguments on sense-data, judgement and knowledge [140], and invites the controversy of relativists, sociologists and anarchists. The logical positivists' position that formal logic and mathematics are the only acceptable base for investigation may be too restrictive. However, it is clear that the benchmark of experience should be subject to some form on discipline, and a great majority of scientists agree with Popper that data should only come from an *'experimental set-up'*[141].

[139] as quoted by Jones, 1996: 574

[140] Russell, 1980, Chapters. 1, 5

[141] Popper, 1990: 205, 206, 415

This shifts the question from the reliability of claims to knowledge to the reliability of methodology [142] and explanation. Given this approach, the definition of science emerges from a circular logic: a given body of knowledge may be defined as a *science* if it is derived via a *scientific* methodology, and if it can explained via a *scientific* demonstration. Hence the question: what are '*scientific'* methodology and explanation?

Scientific methodology has been studied by philosophers of science from two different premises: *"description (an account of what scientists actually do) and prescription (what scientists ought to do to advance truth)"* [143]. Scientific methodology should therefore represent '*the logic of the scientific discovery'*, and the most accepted criterion of evaluating *'scientific activity'*[144]. Whatever its goal, it may be broadly defined as a procedure by which scientific laws and principles are established.

> *'A defining quality of the scientific method, especially as it was understood in the late 1940s and early 1950s, is that a scientist must be a dispassionate, disinterested, detached, objective observer of a system. He must not interfere. He must simply observe, record, model and report'*
>
> (French, 1989, p.17)

There is little agreement on what can be accepted as a *'sound methodology'*. However, two phases of scientific activity have been identified as essential: the initial formulation of hypotheses, and the confirmation (modification, or rejection) of these hypotheses. The first is widely considered to be a 'creative inspiration' that, according Popper, cannot be restricted by rules or 'mechanised' via a fixed set of steps. This explains why no scientific discovery has, so far, been made by computers[145]. The second, confirmation, is generally viewed as the phase of demarcation. With absolute confirmation having proved impossible, this phase rests on the principle of validity, that is, on the criteria which define the proof as 'scientific'. Thus the question returns in a circle to the matter of the 'reliability' of scientific knowledge. If the

[142] a set of methods, or ordered steps, usable to investigate, analyse and evaluate a given problem.

[143] The Fontana Dictionary of Modern Thought, 1988: 760

[144] Popper, 1990 (14 Impr.)

[145] Simon and his colleagues (1987) have developed a computer program which they claim that, using their problem-solving approach, can make 'discoveries' over a wide range of subjects. For example, they have shown that, given the information available to Newton, the computer has discovered universal gravitation. However, we should not forget that their demonstration has involved the invaluable wisdom of hindsight, and that scientific research involves more than just problem-solving: there is also the formulation of both the problem and the theory , data-gathering, description, explanation, and theory-testing.

earlier criteria are accepted, then confirmation is considered satisfactory when it conveys a *'justified true belief'*, and until its *falsification*.

Returning to the first phase, leading schools of thought (mainly the positivists and the inductivists) state that even the hypotheses should pass the test of 'demarcation' by the analysis of existing data. These schools hold that scientific hypotheses cannot be the product of intuition, but must derive from data, which should be collected and analysed without prejudice. However, it has been shown that even the 'unprejudiced' collection of data is influenced by an initial idea, which, in order not to be 'prejudiced', must come exclusively from the 'imagination of man'. The objections then are that 'imagination', is influenced by existing ideas, and that judgement is the consequence of psychological and situational factors. This is why the 'scientific value' of the hypotheses is not seen by philosophers of science as essential an issue as that of the 'scientific value' of the conclusion. Many philosophers and scientists agree with Popper that:

> *"...There is not such a thing as a logical method of having new ideas, or a logical reconstruction of this process. My view may be expressed by saying that every discovery contains an irrational element or a creative intuition in Bergson's sense. In a similar way Einstein speaks of the 'search for those highly universal laws...from which a picture of the world can be obtained by pure deduction. There is no logical path leading to these ...laws. They can only be reached by intuition, based upon something like an intellectual love of the objects of experience"'.*
>
> (Popper, 1990: 32).

On the same grounds, the majority of scientists would refuse to be constrained by an inflexible methodology.

> *'Science does not consist merely in making timid generalisations from wide collections of data, for the scientist's selection of data is dictated by some theoretical interest, and his results are not simply inductive extrapolations, but rather explanations, models, and theories'.*
>
> (A Dictionary of Philosophy, 1984: 320)

Thus it may now be submitted that the value of science lies in its capability to explain and predict. These capabilities are closely related, since explanation must be based upon general laws, which, to be scientifically valid, should be predictive.

Explanation is the beginning and the end of science: science is explanation, but science itself must be subject to explanation. There is no escaping this circularity.

> *'To explain the phenomena in the world of our experience, to answer "Why?" rather than only the question "What?" is one of the foremost objectives in empirical science. While there is rather general agreement on this point, there exists considerable difference of opinion as to the function and the essential characteristics of scientific explanation'*
>
> (Hempel and Oppenheim in Pitt, 1988:9)

Besides,

> *'Whether or not science discovers how the world works or how some version of the world works is not the issue....What is crucial is the insight that the kind of knowledge science produces, whatever form that knowledge takes, permits the development of explanations, and it is those explanations which are the real pay-off....By putting the emphasis on explanation we make a criterion of adequacy for scientific progress. All the research in the world counts for nothing if it fails to generate explanations of the domain under investigation'*
>
> (Pitt, 1985:6,7)

This explains why, according to Papineau, *'Many philosophers of science this century have preferred to talk about explanation rather than causation'* [146]. The question is: when should an explanation be considered as satisfactory in science? Scientific reliability in explanation must be achieved both in *descriptive* and *predictive* terms. The distinguishing features of description are generally accepted to be given in the classical 'Laws of Thought'[147], in mathematical formulae or in formal logic [148]. Therefore, a description may be objectively tested both in its propositions and in conclusion.

In contrast, prediction is founded on less stable ground, since:

[146] Papineau, 1996: 309

[147] *"(1) The law of identity: 'Whatever is, is'. (2) The law of contradiction: 'Nothing can both be and not be'. (3) The law of excluded middle: 'Everything must either be or not be'"* (Russell, 1980: 40)

[148] Hodges, 1977; Lemmon, 1965; Quine, 1986; Pasquinelli, 1970.

> *'Ideally, scientific laws are strictly universal or deterministic in form, asserting something about all members of a certain class of things, but they may also be 'probabilistic' or statistical, and assert something about a methodically estimated proportion of the class of things in question.'*
>
> (The Fontana Dictionary of Modern Thought, 1988: 761),

With the ideal criterion of certainty having been excluded, prediction either infers faith in the principle of induction described by Russell as supporting

> *'the belief in the reign of law, and the belief that every event must have a cause...Thus all knowledge which, on a basis of experience, tells us something about what is not experienced, is based upon a belief which experience can neither confirm nor confute'*
>
> (Russell, 1980: 38),

or it is based on a 'justified true belief', in turn founded on probabilistic or statistical inferences supported by Bayes' theorem and defined by Russell as 'probable opinion'[149],

> *'... which, at least in its more concrete applications, appears to be as firmly rooted in us as many of the facts of experience.'*
>
> (Russell, 1980: 38)

It has been shown above that both alternatives have been attacked by Popper. Yet, if the Popperian logic of falsifiability has to be accepted, then,

> *'The possibility of indefinitely challenging the successive grounds of an explanation has suggested to some people....that a complete explanation cannot be given within science.'*
>
> (Scriven, in Pitt, 1988:70).

A different opinion has been offered by Hempel and Oppenheim with their 'Covering-Law Model of Explanation' [150]. By this model,

> *'...something is explained if it can be deduced from premises which include one of more laws. As applied to the explanation of particular events, this implies that one particular event can be explained if it is linked by a law to some other particular event'.*
>
> (Papineau, 1996: 309)

[149] see: Bayes' theorem and Bayesianism.

In its simplest form, the model has been formalised as [151]:

a has C

for all x, if x has C, then x has E

a has E

According to Papineau this model (originally called deductive-nomological [152]) has also been interpreted in a predictive way, according to a variant which allows for non-deterministic explanation as well as deterministic ones. This variant is named the 'inductive-statistical' model. Papineau gives an example of its application in the following [153]:

a drinks 10 units of alcohol per diem

For p per cent of xs, if x drinks 10 units of alcohol per diem, x has a damaged liver

a has a damaged liver.

Here the '*explanandum'* (the statement that has to be explained) cannot be *deduced* by the '*explanans* '(the statement that explains), but only follows with an *inductive* probability of *p*; and the inference appeals to a *statistical* regularity rather than an absolute (*nomological*) generalisation. Most of the modern scientific research is based on the 'inductive-statistical' model. Pharmacology, medicine, rocketry, aviation and security are presently based on this model for both explanation and prediction. Clearly, the assumption is that the initial belief inferred by this model will converge, with Bayes, to a 'statistic certainty' as more evidence is available. This reasoning seems to work better where regularities are easy to be found, e.g. in the technological rather than in the human domain. However, the author warns,

> *'... while they are often treated as separate theories, the covering-law account of explanation is at bottom little more than a variant of Hume's constant conjunction of causation. it ...faces essentially the same difficulties as Hume: (1) in appealing to deductions from 'laws', it needs to explain the difference between genuine laws and accidentally true regularities; (2) it omits the requisite directionality, in that it does not tell us why we should not "explain" causes by effects, as well as effects by causes...'*

[150] Hempel, and Oppenheim, 1948, 15, 135-175

[151] Papineau, 1996: 309, 310)

[152] Nomological is a law of nature that must always be in some sense necessary and cannot be broken (A Dictionary of Philosophy, 1979: 198-9)

(Papineau, 1996: 309)

To conclude, there is no agreement on a criterion of reliability whether in the matter of definition, methodology, proof or of explanation. With the debate on knowledge and science being as old as philosophy and leading to fascinating propositions on the nature of mankind and his relationship with the Divine, an increasing number of epistemologists is contributing new hypotheses and theories to 'the question of the questions': what is Science?. Popper has observed: '*Even the analysis of science -the 'philosophy of sciences'- is threatening to become a fashion*'[154].

The question remains: 'what is Science?' This debate is a unending spiral of arguments with alternating, but not definitive, outcomes, and the researcher has no intention to join the 'fashionable' army of epistemologists. However, a definition of science and a frame of scientific methodology is needed, to define the premises and the limits of this research.

No school of thought can, so far, claim to have established the absolute truth of its position. Therefore, each (provided it is supported by evidence and a rationale) must be considered to be equally acceptable (or refutable). For the purposes of this research, and in conformity with the view generally accepted, science is taken to be a 'justified true belief', produced by

> *'Any of various intellectual activities concerned with the physical world and its phenomena and entailing unbiased observations and systematic experimentation. In general, a science involves a pursuit of knowledge covering general truths or the operations of fundamental laws'.*
>
> (Encyclopaedia Britannica, vol. 27:32)

Compatible with this definition and with previous findings, the following definition of Scientific Theory is adopted for this research:

> *'A systematic ideational structure of broad scope, conceived by the imagination of man, that encompasses a family of empirical (experiential) laws regarding regularities existing in objects and events, both observed and posited -a structure suggested by these laws and devised to explain them in a scientifically rational manner'.*
>
> (Encyclopaedia Britannica, vol. 27:33)

and

[153] Ibid.:310

> *'A theory may be characterised as a postulational system (a set of premises) from which empirical laws are deducible as theorems. Thus, it can have an abstract logical form, with axioms, formation rules, and rules for drawing deductions from the axioms, as well as definitions for empirically interpreting its symbols. In practice, however, theories are seldom structured so carefully'.*

(Ibidem)

The frame of methodology and explanation used in the research is contained in the second part of the definition of a Scientific Theory:

> *In attempting to explain the things and events that he experiences, the scientist employs (1) careful observation or experiments, (2) reports of regularities that he has found, and (3) systematic explanatory schemes (theories)'.*

(Ibidem)

There is support for the acceptability of this method for the scientific explanation of non-physical sciences (within the paradigms of the motivational and teleological approaches) in Hempel and Oppenheim. A synthesis of the above concepts may be found in Scarman CSPO Course notes[155].

In Popper's terms, the truth-condition of the offered theoretical approach is not claimed; it is asserted on the basis of a 'justified true belief', that is on having, so far, passed the tests of inference and evidence. Its 'scientific property' is grounded on the most accepted paradigm (which bases the definition of Science on the reliability of its methodology and on its ability to explain its phenomena), whereas its 'scientific value' is based on its ability to surviving 'falsifiability'.

Accordingly, the choice is made to base the methodology of research and experimentation on the following steps:

- establishment of a *set of premises* through a *postulational system*,
- deduction from them of *empirical laws* as *theorems* by reason of an *abstract, logical form, with axioms, formation rules, and rules for drawing deductions*,

[154] Popper, 1980: 23

- validation of the findings via *observation* and *experimentation*,
- explanation of the results in clear, logical, *falsifiable* steps.

The next task is to investigate the reliability of the body of knowledge on security, by the application of these criteria and principles.

[155] Scarman Centre for the Study of Public Order MSc in Security Management, Course notes, 1992, Module 1:15,16.

1.4 IS SECURITY A SCIENCE?

To investigate the scientific validity of the existing knowledge about security, the preliminary step is that of ascertaining which type of science may the existing body of knowledge be referred to. Different rigour of test and precision is required in scientific demonstration of, for example, physical sciences or social sciences. Thus, the process of verification is undertaken in three steps: firstly, positioning the identified approaches to security within the whole body of knowledge and in relation to the main branches of science; secondly, investigating whether any part of security knowledge has already been organised according to a scientific methodology and explanation; and thirdly, verifying whether this identified set of knowledge fulfils all of the necessary conditions required to establish its reliability as a science, when applied to a real security situation.

The first step starts from the assumption that 'security' is a concept within the whole of Knowledge (indeed, it exists because of Knowledge). This assumption presumes the inter-disciplinarity of knowledge, here considered an *'organised body of information'* [156]. Thus, any given concept (including security) should be seen as related to all other existing concepts, in any other branch of Knowledge.

Because of the multi disciplinarity of each discipline, there is no agreement on the definition of these branches. It is however possible to classify the content of knowledge of each discipline by its history, nature, methods and principal focus. For diagramatic purposes, these disciplines are grouped in three arbitrary branches by their educational and cultural role: natural (e.g., medicine, biology, chemistry), physical (e.g., mathematics, logic, engineering) and social sciences (e.g., politics, economics, psychology, sociology).

[156] OALD

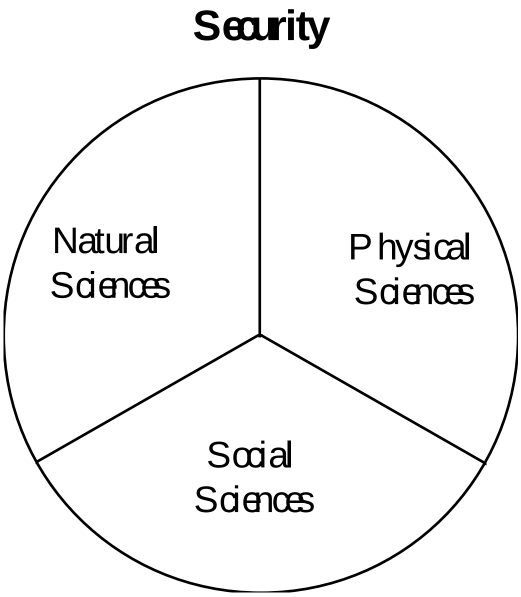

Figure 2: Security as a multi-discipline

The assertion that security is a concept drawing on each branch of knowledge raises the question: how strong, and how close, a relationship is there between security and each different branch? Some hypotheses can immediately be forwarded. The obvious link to the social sciences is through disciplines as law, sociology and criminology. The link to the physical sciences is through disciplines as mathematics and engineering, in the topics of, for example, risk analysis and security systems. Security is linked to natural sciences by aspects which include physiological processes, as fear, learning, motivation, behaviour and decision.

The verification of these hypotheses comes from the analysis of the existing literature. The contribution of each discipline to the existing body of knowledge of security has been identified and the relevant existing approaches have been pinpointed in the following diagrams.

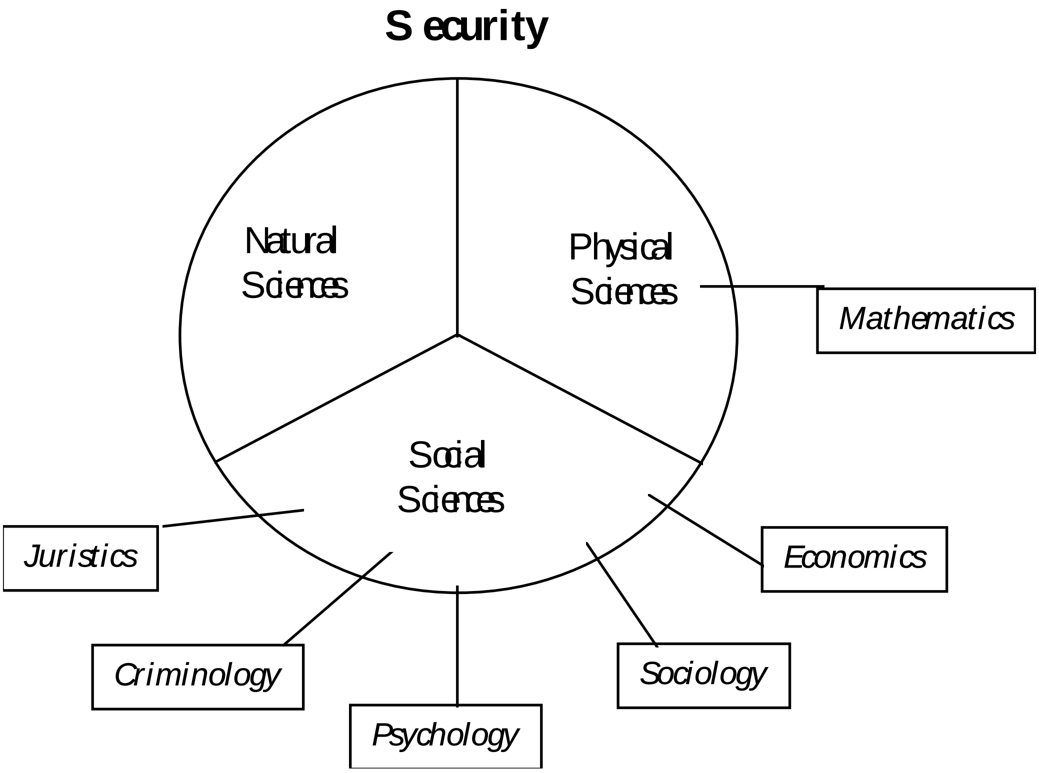

Figure 3 The Academic Approaches

Having identified the academic approaches, the operational approaches are located:

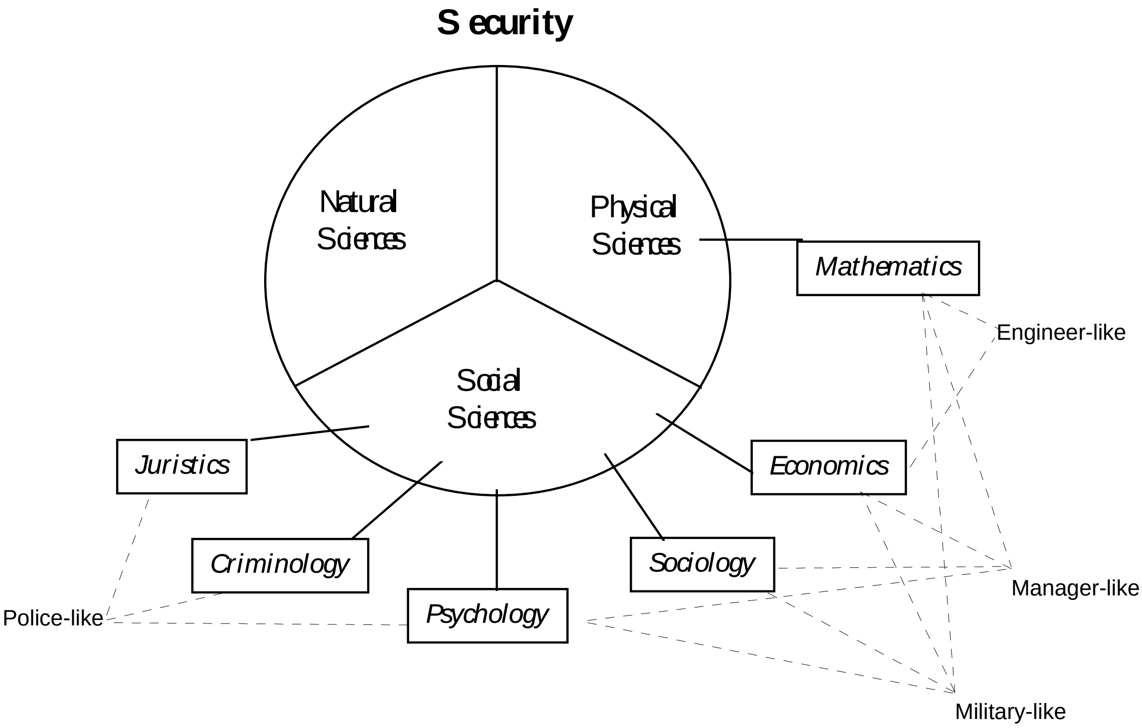

Figure 4 The Operational Approaches

The above diagram suggests that the *existing* body of knowledge of security presently depends only upon the Physical and the Social Sciences. The initial hypothesis that (because of the assumed inter-disciplinarity) the present concept of security is also linked to the Natural Sciences appears not to be supported by the evidence of the approaches. The diagrams suggest that no *existing* approach to security (not those to risk, or related subjects) is directly linked to the Natural Sciences. Yet, there is evidence to the contrary. It has been shown that security is an outcome of human activities largely motivated by fear and self-interest. Hence, at least one Natural Science (physiology) has relevance to both mental and physical processes of security. The absence of a direct Natural Sciences approach to security is a lacuna in the current thinking about security, which merits more attention and research.

It is now time to rearrange the various existing approaches with regards to the related branches of Science. The previous diagram shows too rigid a separation between the different branches of the science, and does not represent the concept of inter-disciplinarity. Considering that the described approaches are inter-linked by direct relationships and feed-backs, the 'fluctuating' boundary in the following diagram suggests a better graphical explanation:

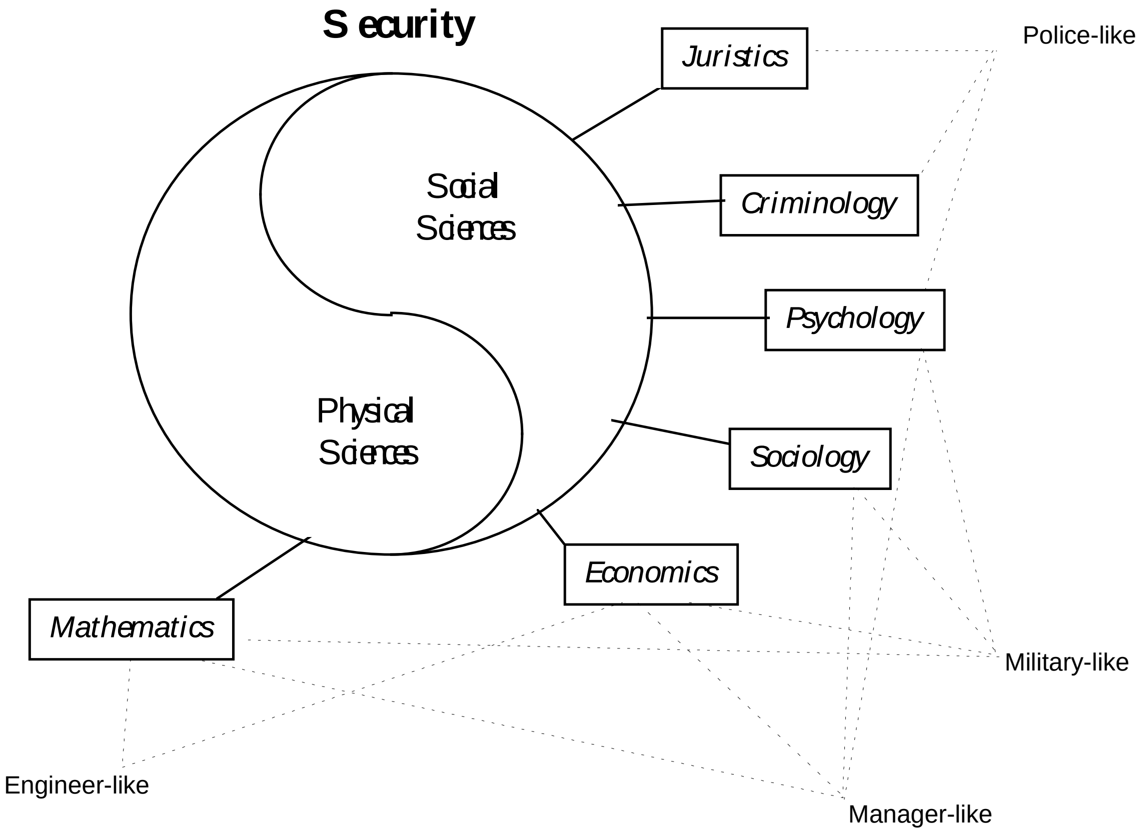

Figure 5 The Existing Security Approaches and their position to Branches of Knowledge

The relationships between the physical and social elements of security and the difficulty of positioning some discipline appear now more perceptible. As a matter of fact, they are interactive and overlapped. Whilst the physical sciences effectively support the social sciences, it is the latter which, with the power of imagination and thought, provides decisions and solutions where the rigours of the physical sciences are not enough.

The question of classification (i.e., to which branch of science should security be referred) is now relevant, because the proof of validity requires different degree of rigour in dependence of its position. Previous definitions portray security as dependent on human sentiments and behaviours, and the above diagram shows a prevalence of approaches linked to Social Sciences. These seem good reasons to accept for the purposes of this research the largely non-physical character of security. Further evidence is provided during the presentation of the theoretical approach.

The next step is to consider whether any part of the body of knowledge of security, as found in literature and as taught in academic and professional courses, has scientific grounds and could have a scientific explanation. Earlier findings indicate that science stems from a *'systematic ideational structure'*, which may be conceived *'a priori'*, mainly from the *'imagination of man'*. To have 'scientific validity', the initial statement, the reasoning and the conclusion must each be formulated in such a way as to allow logical and empirical testability. This requires them to be examined *'a posteriori'* within an *'experimental set-up'*, through the *'careful observation or experiments'* in order to submit *'systematic explanatory schemes'*.

At the academic level, no evidence of a formal 'Science', 'Theory', or 'Discipline' of Security is to be found, since the necessary analysis has not been attempted. Academic disciplines exist (in particular, law and order, crime prevention and risk) which include security, or components of it., as a part of their studies. Courses in "Crime Prevention" and "Security Management" are taught at postgraduate level in many Social Sciences Departments, in a number of countries [157]. However, the meagre evidence available suggests that more research needs to be done on the two forces driving security, fear and interest. It is submitted that the paradigms 'risk perception' and 'risk management' are still incomplete from a security point of view, and do not cover the whole subject area. Evidence is provided in the following Sections.

At the professional level, 'tools' adopted from the above disciplines are to be found both in literature and practice. There have been engineering considerations of technological systems, criminological analysis of offender's and victim's behaviour and motivations, and mathematical calculation in the assessment and management of risks. Research and literary evidence show that security professionals can produce standards, data, cost/effectiveness evaluation, indexes and estimates. In a given situation, they can also predict the *technical* functioning of a system (e.g., the resistance of a door or of a safe, the false alarm rate of an alarm system, the fault rate of a control system), and its technical effectiveness against a given attack. It is also believed possible to explain, *a posteriori,* behaviours, reactions, motivations, criteria of choice, modus operandi, of the identified actors in most security circumstances.

The third step of the inquiry requires verification that the identified scientific foundations of security apply and satisfy all the conditions necessary to establish security as a scientific

[157] Manunta, 1996b: The case against: is Security a Profession?

discipline. As stated, the fundamental issues of definition, methodology and explanation need to be examined.

1.4.1 Test I: Definition

The inadequacies of existing definitions of security have been demonstrated. They constitute a primary cause of confusion. Discussion of the principles of science makes it clear that, in the absence of clear definition, none of the requisites of science can be fulfilled, neither the formulation of a set of premises, nor the preparation of an 'experimental set-up', nor the collection, analysis and evaluation of data. This lack of definition is the fundamental weakness which underlies most of the difficulties discussed below.

1.4.2 Test II: Methodology

The second phase of the test is directed at methodology, which has been defined thus:

> *'A scientist, whether theorist or experimenter, puts forward statements, and tests them step by step. In the field of the empirical sciences, more particularly, he constructs hypotheses, or systems of theories, and tests them against experience by observation and experiment.'*
>
> (Popper, 1990: 27)

The application, or applicability, of the issues of theory, experience, observation and experiment to security must be examined. Here the significance of the absence of an overall theory is revealed. No problem can be formulated and tested. No hypothesis from which derive deductive inference can be formulated *a priori*. No experiment can be prepared. No general explanation of observed security phenomena can be induced *a posteriori*. Thus, in the absence of definition and theory, experience has no scientific validity, and explanation is only opinion. This is demonstrated by the different methods of calculus which lead to different decisions about the same problem, all of which equally acceptable, or refusable.

The contrary, and current, position is that: 1) security draws scientific validity from other sciences; and 2) there is enough experience of security matters to allow the construction and formulation of hypotheses on the basis of statistics.

The first argument is based on right premises, but reaches a wrong conclusion: it is not the scientific validity of 'borrowed' disciplines in themselves which is refused, but the fact that they may confer *ipso facto* scientific validity to something which, from a scientific point of view, does not exist. The reasons for this statement have been provided above.

The second argument is wrong in both the premises and conclusions, and requires a more detailed discussion. The issue of experience is easily dismissed. No matter how much experience exists, if it is collected outside an 'experimental set-up', if it is not interpreted according to 'general laws and principles' and if it is not organised by a set of hypotheses so to reach generally valid (and falsifiable) conclusions, it adds nothing to scientific knowledge. The resulting knowledge remains confined in the mind of the individual, it is not transmissible, it is not falsifiable, it remains an opinion. The issue of the possibility of drawing scientifically valid conclusions from existing statistics and data needs a more detailed examination.

There is evidence that most of the security reasoning is based upon hypotheses supported by a 'justified true belief', which is induced through statistics from 'natural regularities'. Protective measures are generally designed on the basis of this principle, which is considered to be an 'educated guess' based on statistics, Bayes' theorem and Hempel and Oppenheim's 'Covering-Law Model of Explanation'. Faut de mieux, these 'educated guesses' are based on the 'best expert's estimate' [158]. This position (which is borrowed from the calculation of insurance and engineering risks) is widely accepted in security as allowing reliable prediction. [159] However, this line of thought is not validated by the existing data, apart from technical reasoning referring to structures and systems. The reasons are: first, in the absence of definitions and theory, methodology has no base to start, thus no scientific validity. Second, this approach assumes the reliability of a linear (cause-effect) predictive reasoning. For example: 'if we have a valuable asset and a thief, and if we secure this asset in a safe inside a closed and alarmed room, then we will have a justified true belief that a theft will not take place'. Apart from epistemic considerations (e.g., previous criticism to bayesianism and the 'Covering-Law Model of Explanation'), the validity of such reasoning has been frequently disproved. The recent thefts from some of the most protected museums in the world (notably, the Louvre, and the Musei Vaticani) are powerful evidence that in security

[158] e.g.: The Royal Society, 1993; cap. 2

[159] Broder, 1984; D'Addario, 1989; The Royal Society, 1983, 1992; Walsh and Healy, 1996

theoretical hypotheses cannot be based upon linear reasoning. Third, there is no agreed method of using these data: if different conclusions can be reached starting from the same data, then it is hard to see how a prediction can be trusted. Finally, not enough regularities to allow reliable predictions are to be found in fields involving opposing actors, as does security. In such fields results depend on surprise, imagination and secrecy, and regularities are dangerous vulnerabilities to be immediately exploited or avoided. Any time a trend is identified by one actor, her/his consequent actions will substantially modify it to the point of being unreliable for prediction. There is evidence for this statement in, for example, chess (a much simpler activity than security, being performed within definite limits and rules, and dependent upon the actions of a single opponent), and in the more complex financial market.

This re-raises the issue of the reliability of experience in security matters. The issue is whether there is, in security, any power of prediction. As previously stated, prediction requires the formulation of general principles based on the discovery of regularities (which depends on observation, thus on methodology), and it is closely linked to explanation. The evidence suggests that, at current state of security, a prediction (or an explanation *a priori*) obtained by inductive inference can only accepted as scientifically reliable in the case of technological systems.

Apart from epistemic considerations of definition and theory, a major reason for ‘scientific’ scepticism is that data do not come from an ‘experimental set-up’, i.e., one where probabilities have scientific validity and are interpreted after specific hypotheses. This has two negative consequences: there is neither sufficient and reliable data, nor have enough regularities been identified on which to base reliable predictions.

Information is considered insufficient and unreliable by many authors. The basic argument is that the available statistics do not include all relevant data as, for example, the situational, motivational and managerial factors affecting all the actors in the process[160]. Many known figures are based upon incomplete data and surveys, do not come from uniform formats, do not include all the events, and do not take into account all of the relevant factors of a security process [161]. Additionally, the accuracy of some conclusion has been criticised in different

[160] Adams, 1995, Chapter 2

[161] Malik, 1995: 37

occasions. For instance, it has been suggested that crime statistics have been manipulated to meet private or political interests [162]. Thus, the possibility that some researchers may be politically biased, or funded by the security industry, seeking support and credibility for their aims or products cannot be dismissed.

Given such a basis for reasoning, it is hard to accept that 'justifed true beliefs' can be induced. For example, a statistic showing that 78% of intrusions are made by forcing the door, is frequently used to infer that, by reinforcing the door, security will be improved. This inference is scientifically inconsistent, because: a) it is based on a linear reasoning, b) it is drawn by incomplete evidence collected outside a scientifically controlled situation. The former argument has already been discussed. The reasons for the second follow. Firstly, the statistic above does not consider the whole of the universe, i.e., it does not consider the number and nature of all the other doors which were not forced in the same period, nor does it say which of the forced door had been previously reinforced, and at which degree. Secondly, no evidence is included on the nature and location of the door and the house, nor on the valuables that are contained, nor on the capability, motivations and choices of both the intruder and the dweller. It is unknown if the house was empty or its dweller present, what happens to the houses provided with 'normal' doors, or what happens after 'reinforcing' the door. From a scientific point of view, the only inference that can be made is that, in an unclear state of affairs and within the limits of the survey (which are not perfectly known), 78% of unknown intruders with undefined motives have forced doors of unknown quality, breaking into undefined properties of undefined value, situated in an undefined context, and under undefined circumstances. Whilst this information shows a marked preference for a door as an easy access for an intruder, and has undoubted relevance to the seller of reinforced doors and locks, it gives the owner no help in the prediction of the vulnerability of her/his house. A purchaser of a reinforced door could be led to infer that her/his house is now secure since it has been provided with a strong door or lock, whilst in fact only the door has been made stronger. It has not been made more secure, a different quality depending, for example, on its installation (reinforced hinges, frame, etc.), maintenance and use. The same purchaser cannot reasonably infer on the basis of statistic evidence that houses without a strong door or lock are insecure, since a great number of houses without particularly strong doors and locks are not broken into. Nor can s/he predict that, once the door has been

[162] see: Burrell and Leppard, Sunday Times, 16 October 1994; Leppard, Sunday Times 23 October 1994.

reinforced, s/he will not suffer intrusion. An intruder impeded by a door may use tools to force it, or break in through a window, a roof, an adjacent wall, and even persuade the householder to open the door by ringing the bell, or force the householder when s/he is entering or leaving her/his house. Conversely, the non-buyer of a reinforced door or lock could infer that her/his house is secure, since statistics show that, for example, only one house in one thousand is burgled per annum, but her/his prediction on the security of her/his house would be equally inconsistent. Daily evidence shows that houses that are well provided for with security systems have been burgled, and that houses totally unprotected have not. Finally, and perhaps conclusively, the inference that a security system makes *ipso facto* a house more secure is not supported by the evidence: notwithstanding the installation of tens of thousands of new security systems every year, crime rates are unchanged, or even increasing. The contrary argument that, without these systems, more houses would have been burgled sounds reasonable, but cannot be proved.

The above reasoning can be applied to comparative statistics: if, hypothetically, the average rate of violent crimes is 1,250 cases per 100,000 people per year in the UK, and 1,400 in France, what prediction or explanation can be derived from their comparison to establish whether a particular Mr. Jones is in less danger than a particular Monsieur Cotillon? Yet, the evidence is that most present security methods are based on this methodology of prediction[163].

The question of regularities is also essential. Science requires that, in order to be reliable, a 'justified true belief' must be grounded on general principles derived by inductive inference from the observation of regularities. This is possible in security only for specific technical matters (rates of failures, false alarms, or factors of resistance against a given agent assumed as constant). Outside the technical domain, current security statistics do not reveal (even assuming their completeness and correctness) enough regularities for the derivation of general principles upon which to base reliable predictions. This assertion could be disputed on the basis that it is not the principle that is false, but the data which are unreliable, hence the methodology used for collecting these data. It could be argued that, provided that the collection of data is adequate and the methodology is sound, then a 'justified true belief' can be induced. Reference could be made to specific and carefully investigated cases. For example, separate researches have shown that the installation of CCTV systems in public

[163] D'Addario, 1989; Flynn, 1979: 40-50; Shaw, 1993: 20-23

places has reduced the crime rate in the area [164]. Important security policies are now undertaken on the basis of inference from this evidence. Earlier reasoning suggests that this inference is invalid because of the manner in which it is formulated. This formulation assumes as true the relationship cause/effect (installation of CCTV = diminution of crimes) which has been demonstrated to be false on other occasions [165]. Even assuming the accuracy of the data, this evidence is not enough to infer the validity of this cause-effect relationship. Causes and effects do not appear to have been thoroughly investigated, therefore the principle of causation cannot be proved [166]. It is not clear whether the reported diminution in crimes has resulted from the installation of the CCTV system or from other causes. The data do not reveal the role played in the diminution in crime by the increased awareness of security forces and public, by the severity of the local magistrates, or by a temporary displacement of criminals to safer places while waiting to understand how the new system works and what impact it will have on their business. Nor are the possibilities of seasonal variations in trend, or of chance combinations of factors considered. The strongest argument for the rejection of the above reasoning is its invalidity for prediction. Even assuming the occasional validity of the relationship, no prediction can be made that the same system, adopted on a larger scale and over a longer time, will produce consistent results. This is because no long-run collection of data is available to establish scientific reliability, and because the particular character of security dynamics does not allow regularities to settle for enough time. In science, the reliability of a given hypothesis for a prediction comes from its proven repeatability. If the same experiment cannot be repeated and achieve the same result, then its hypotheses or results cannot be used for prediction. On the contrary, there is evidence of crimes committed in spite of CCTV systems, either for indifference to punishment or for experience of leniency. [167] Nor can extreme but not unique cases be ignored, e.g. that of a teenager arrested 80 times for 130 offences for burglaries and criminal damages[168].

To conclude, the test of repeatability and the volume of contrary evidence indicate that the present methodology does not allow for a general application of the principle of inference to

[164] see: Hobson, The Times, 16 Feb. 1994, Sharrat, The Guardian, 6 July 1994.

[165] see: Gill, 1994: 37, 61.

[166] see earlier reference to Hume, Oppel and Oppenheim

[167] Gill et al., 1994; Erickson and Stenseth, Oct '96

[168] Wilkinson, The Times, 23 Nov. 1994

security. Thus, no inductive inference can be made from experience (observation and test), since

> *'we do not have enough control of the evidence-giving relation to know when we are in a position to claim that having evidence entails we are justified in our cognitive claims'.*
>
> (Pitt, 1988:4)

The above considerations bring in the issue of testability. The data discussed above were not collected in an experiment designed and controlled for the purposes of security analysis. If they are to achieve scientific reliability, security hypotheses must be testable within an 'experimental set-up'. Science gives to the principle of inductive inference the validity of a 'justified true belief' only when the following conditions are ensured: 1) variables can be isolated and modified one at the time, keeping the others constant, and 2) experiments are repeated in large numbers and over time in identical circumstances. At present, neither condition is met in security methodology, for a number of reasons. Firstly, not all the variables are known, and those known cannot be isolated from the social context; secondly, there are difficulties in predicting human reasoning, behaviours and actions; thirdly, the conditions of research modify the experiment itself; finally, the conditions of real life cannot be reproduced at will:

> *'The laws of the phenomena of society are, and can be, nothing but the laws of the actions and passions of human beings united together in the social state. Men, however, in a state of society, are still men; their actions and passions are obedient to the laws of individual human nature'.*
>
> (Stuart Mill, 1843, book VI, introd. to chapter 7)

1.4.3 Test III: Explanation

The previous comments on methodology suggest difficulty in finding a scientific basis for explanation in security. At the present, only technical matters can be explained. The absence of agreed definitions impedes the identification of the problems. There is no 'postulational set of premises', or theory, thus hypotheses cannot be formulated. Methodology is unreliable. Available data are unsatisfactory. The relationship cause-effects is hard to establish. Observations and tests are not the product of an experimental set-up. There is not enough evidence to infer general principles by induction, and to allow 'justified true beliefs'. Problems have been identified in the area of causation and in that of testability. So far, the effect of chance and deterrence on choices, motivations, and behaviours cannot be properly ascertained and tested. For example, the important concept of deterrence (a desired effect of a security system) is frequently used to explain the positive effect of a new security system and justify its installation. A measure of 'deterrence' is offered by comparison between *ex-ante* and *ex-post* figures of undesired events. However, this measure is not clear enough to attribute to deterrence the absence of an attack, which may simply be the result of absence of intention to attack. Therefore, if a house is not burgled, it may be because of a new security system, or because no burglar was interested, or because the only interested burglar was temporarily unavailable (in prison, on holidays, unwell). In the current state of security knowledge, there is no basis for positive conclusions, predictions or explanations as, for example: 'if you adopt this system, then your losses from shoplifting will be reduced by this percent', nor: 'if you install this fence, then intrusions will be stopped', nor 'if you do not use such a system, you will be burgled'. Similarly, neither 'if you meet a murderer, then you will be killed', nor 'given a local yearly murder rate of 1 per 100.000 inhabitants, you will not be murdered next week', are a valid judgement.

'*General principles and laws'* of security cannot be induced by operational data without *a priori* definitions and models and explanations of general processes, principles, and laws. Therefore, the definition of *'systematic ideational structure of broad scope,...that encompasses a family of empirical laws'* cannot be applied to the existing approaches, because no evidence of such a *'systematic ideational structure'* has been found. It follows that some of the requirements of the Encyclopaedia Britannica definition of science are only partially met at the empirical level:

> *'Any of various intellectual activities concerned with the physical world and its phenomena and entailing unbiased observations and systematic experimentation. In general, a science involves a pursuit of knowledge covering general truths or the operations of fundamental laws'.*

The conclusion are as follows. The current 'scientific' content of security lectures, reasoning and application is merely 'borrowed' from other disciplines, without genuine 'systematic explanatory schemes'[169]. The scarce research on security-related topics holds minor validity, since data are collected without a reliable set of assumptions and outside a specific 'experimental set-up'. Even where well-established methods and rules of practice, governed

[169] Encyclopaedia Britannica, Scientific Theory

by precise regulations and standards exist, this does not constitute evidence of scientific reasoning. With Wolpert, it is presumable that security has followed the technological, rather than scientific, way of reasoning[170]. Thus security is often confused with its technologic aspects. Treated as a 'machine', a security system is conceived, used and repaired as necessary. Inadequacies are understood, predicted and rectified as technical failures are. However, the understanding is not based on scientific theory, nor follows a scientific methodology. This is not enough to explain security as a whole; to make sense from experience, a theory is indispensable, because:

> *'Scientific laws and theories have the function of establishing systematic connection among the data of our experience, so as to make possible the derivation of some of those data from others'.*
>
> (Hempel and Oppenheim in Pitt,1988.: 32).

[170] Wolpert, 1992, Chapter 2

1.5 CONCLUSIONS

The central question of this research is: can Security become a Science? Any answer must involve the problems of definition, theory, methodology and explanation. So far, these issues cannot claim scientific reliability. Most seriously of all, in the absence of an accepted definition, security is an arbitrary concept. However, the provided evidence does not negate the possibility of formulating a 'scientifically reliable' theory of security. The fact that no such approach has yet been undertaken, is not a sufficient reason to dismiss it as impracticable. Two reasons for affirming the possibility of a scientific approach have been identified. The first is derived *'per existentiam'*. Security is regularly taught in courses and seminars at the highest academic levels throughout the world. Its activities are ruled by laws and regulations, enforced by well-defined bodies and authorities at various levels (government, public, private), and conducted in accordance with settled methodologies, most of which are derived from existing sciences. A great number of books, manuals and specialised articles on many aspects of security are to be found in specialised libraries. The existence of security concepts, methodologies and activities derives from millennia of practice. The protection of innumerable assets over a wide spectrum in all circumstances is a reality that cannot be denied.

The second reason is the demonstration '*per absurdum*'. Security professionals make (though cannot always explain) decisions on the personnel, structure and systems appropriate to the problem at hand, and on how, where and why they should be employed. It must be assumed that the above studies, activities, regulations, persons, methods, systems, conform to some general principles and are organised according to some rational tenets[171]. The alternative, '*per absurdum*', is to conclude that all security activity is random response inspired by faith.

This is not to say that, because some order exists, security can presently be considered as a discipline. Evidence has been provided that it cannot. It is merely to point out that, providing more academic attention, this ambitious goal can, presumably, be achieved. Previous reasoning has highlighted the importance of scientific methodology for explanation and prediction; even more important is its contribution to the progress of knowledge. Scientific methodology must assist the organisation and interpretation of the concepts within the

[171] Simonsen, 1996

existing body of knowledge into a genuine security theory. It must direct the reasoning from clear premises to unambiguous conclusions along a clear, ordered way, as to allow for each step to be criticised and eventually - with Popper - *'falsified'* and improved. Considering the largely non-physical character of security, scholarly evidence has been provided of the possibility of a scientific explanation in non-physical sciences. The possibility of finding '*general truths'* in the existing security concepts and of identifying the '*fundamental laws that operate or rule them'* can therefore be considered.

It is submitted that this attempt must start *ab ovo*. Building such a discipline on existing definitions and approaches appears to be impracticable, because of the differences of premises, assumptions and goals. Rationalisation must come through a process of identifying the general framework (the security context: actors, processes, range and limits), before moving on to a discussion of more particular issues (the objective value[172] of decisions and actions within the defined context). The former point is, fundamentally, a problem of definition, or (in agreement with Popper) demarcation. The latter, is a problem of explanation.

The problem of definition is crucial, and the *sine qua non* to the explanation. The definition is not simply a linguistic problem: it involves the placement of exact boundaries around a concept, or idea, in order to outline and distinguish it from others; thus it provides the foundation of a scientific approach. Science could not exist without this essential step. Philosophers and scientists agree that its importance consists in its ability to demarcate that which is known from that which is unknown, and, within that which is 'known', what can or cannot be explained, to what extent and by which method. The non-existence of a clear definition of security, signifies the non-existence of these boundaries. If such boundaries are not defined, or, at least, sketched, how can a *security* problem be defined, how can its presence be detected, what value can be attributed to a *security* decision? Indeed, how can the possibility of such decision even be conceived? Until clear limits and scopes are set, rational activity will not replace wishful thinking and security will remain a useful scapegoat.

Once a criterion of demarcation is agreed, the next step requires the provision of a reliable explanation. A set of pragmatic obligations, such as those of justification, performance, blame and responsibility, oblige security decision-makers first to determine the context, scope and

[172] Objective as opposed to subjective, the latter being a value influenced by individual factors (such as, but not only, perception and judgement) and the former a rational and demonstrable conclusion from the facts.

rationale of their task. Until the limits of their rationale, findings and decisions are known, all they say and do is merely opinion or, at best, *'an educated guess'* [173]. Explanation starts from a clear definition and depends upon a sound methodology. It requires the previous verification of the existing context, which allows for the subsequent identification, analysis and assessment of decisional criteria, priorities, constraints and goals. Certain realities must be taken into account. Two areas of problem have been identified, which seem overlooked by the existing methodology, and are pertinent to how security decisions are made. One is related to the psychological and political factors that govern the setting of scopes, priorities and constraints on security. This includes a better understanding of the influence of perception, fear and self-interest on security processes. The second problem area relates to the fact that in emergency such a process must be accomplished in minimal time and under exceptional pressure. Both require the understanding and the analysis of the cognitive, motivational and situational inferences of both aggressor and protector, and an acknowledgement that they inter-relate. It is suggested that only after the identification of all of these factors, can the capabilities of a security system in terms of flexibility and reaction versus its settled goals and priorities be evaluated, the effect of a new system on the problem as a whole be predicted, and the whole process explained. This formidable goal is not immediately attainable. Human activities, particularly those which involve conflicting actors, cannot be easily constrained within a framework of rationality. However, it is submitted that the groundwork for this ambitious attempt can already be prepared.

[173] Wright, 1972:26

SECTION II

THE THEORY

2.1 INTRODUCTION

The discussion of the existing body of knowledge of security has shown that there is a need to organise security into a scientific discipline. The examination of the nature and characteristics of science has indicated that it may be possible to provide *reliable* definition, methodology and explanation. The first, the definition, would establish the premises of the reasoning. It calls for the knowledge and the proof of whether there is, or is not, a security context, *id est*, in a set of circumstances where security is the main problem and goal. This step is necessary to define the decisional context and to prioritise both the decisional criteria and the constraints. The second issue, methodology, would substantiate the rationale of the reasoning, i.e., whether decisions and actions made in a security context may, or may not, have an objective value, and, if so, to what extent. This step is necessary to permit explanation, measure performance and attribute blame and responsibility. The third issue, explanation, would justify solutions and assist the correction of faults and errors. It would permit the establishment of the degree of reliability and thus the credibility of a security decision. This step is necessary to convert decisions into actions with minimum friction and maximum efficiency. The problem of definition relates to the theoretical level and must precede the investigation of methodology and explanation, which are considered of a more practical relevance and will be discussed in Section III.

This Section investigates the problem of definition and contains a detailed analysis of the security context. It is divided into four sub-sections. The first offers a formal definition of security. It postulates a framework containing identifiable asset, threat and protector, all inter-related, and offers an analysis of their relationships, dynamics and processes. The second sub-section identifies the relevant dimensions of a security process as time, psychological, political and administrative, and discusses their appropriate aspects. In the third sub-section, the verification of the existence of a security context is used as the criterion of demarcation between security and other states of affairs. The final sub-section analyses the process for translating the conceptual model into practice, by adding to the basic formula the factor 'Situation'. The following conclusions are reached. The formal definition of security and its conceptual model are useful to identify and explain the fundamental mechanisms of a generic security context. If the parameters of the Situation are known, then the dynamics within a specific security context and their resulting effects can be identified and evaluated. It is, therefore, possible to analyse a security context according to general laws and principles, and to apply this methodology of analysis to a specific security context.

The analysis follows the scientific method outlined in the Section I, which requires the following steps:

- statement of the *'set of premises'* bearing a security theory, through a '*postulational system*',
- deduction from them of '*empirical laws'* as '*theorems'* by reason of *'an abstract, logical form, with axioms, formation rules, and rules for drawing deductions...',*
- validation of the findings via '*observation* and *experimentation*',
- explanation of the results in clear, logical, '*falsifiable'* steps.

Both the formulation of the premises and the deduction of a postulational system will be validated by adherence to the following rules. The validation rule within a postulational system (i.e., *'imagination of man*') is included in the definition of scientific theory. Although the logic of the scientific discovery is not incompatible with this extreme [174], the nature of security requires limits to be set on imagination. Therefore, the number of non demonstrable premises and assumptions will be limited as far as possible and will be assumed as constraints. This procedure will distinguish them from the deductional structure of the reasoning and the conclusions. Validation will come from a comparison of the theoretical analysis and the empirical findings. Both academic and operational evidence for and against a scientific theory of security is reviewed, as a part of the validation process. Reference to the existing works in security or related subjects is made when relevant to the explanation and verification. The 'verifiability and falsifiability' of each step, from the premise to the conclusions, will thus be obtained.

[174] see Popper on intuition, 1980:32

2.2 A DEFINITION OF SECURITY

This sub-section seeks to formalise a definition of security by which to demarcate the subject area. The argument has been divided into different steps of analysis with increasing level of detail. The first step investigates the possible approaches to a definition of security and identifies a number of general features of security. This allows a second step of investigation through a process of approximation leading to the concept of practical security, i.e., the circumstances where security activities have both sense and utility. Having identified the main traits of security, conclusion are drawn in the third step of investigation in the form of a set of premises, which states the limits of the future reasoning. The final step formalises the whole argument into a definition of security on which to base a workable criterion of demarcation of the subject area from similar activities.

2.2.1 How can Security be defined?

The earlier examination has suggested that the current concept of security is so wide-ranging as to be impracticable. There is no agreed definition of security. There is conflict between *philosophical* security as an ultimate goal (absence and freedom of worry and danger) and the factual evidence, which shows that *operational* security is a precarious condition characterised by different approaches, different aspects and different goals.

A discussion of philosophical security would only divert this research from its practical objectives to the unsolved paradigms of certainty, free-will and determinism. The focus is therefore on finding criteria for the attribution of responsibility, liability, blame and for the measurement of performance. Such criteria can only be derived from a practicable definition of security; one will be offered.

The definition of security must be consistent and clear. To be consistent, the definition is developed from the conclusions drawn from the examination of the existing evidence. To be clear, the methodology requires each proposition to be expressed in such a way to facilitate falsifiability. The test of consistency between the conclusions of the abstract reasoning and those of the examinations of the evolution of security and of its features will be made after the formulation of the conclusions. The test of clarity is made at each step of the reasoning, starting at the first, the meaning of 'definition':

> *'a process or expression that provides the precise meaning of a word or a phrase. A definition (definiens), correctly made, will be logically equivalent to the word or phrase being defined (definiendum)'.*
>
> (A Dictionary of Philosophy, 1979: 86)

The definition of a concept involves the identification of its essence [175], i.e. the consistent set of its defining properties, judged to be a necessary and sufficient condition to understand its meaning and to separate it from other, though similar, concepts. A definition may have two different goals:

> *"Definition may be either of a present established meaning or of a meaning proposed for the future. In the former case the definition is said to be descriptive, in the latter prescriptive, or stipulative."*
>
> (A Dictionary of Philosophy, 1979: 86)

Both description and prescription are essential to the identification of a practicable concept of security. Consequently, the definition of security will be given in both *descriptive* and *prescriptive* senses. This formal definition will provide the basis for the subsequent formalisation of the theory.

The initial process of identification of the 'set of defining properties' of security has been structured on the same basis as existing literature and practice. This has required a series of attempts, according to the different viewpoints. The first is that, if (according to previous definitions) security's main focus of interest is the avoidance of adverse occurrences, the identification of these occurrences should then enable its empirical definition to be induced. However, this attempt has immediately revealed problems. The compilation of a list of unwanted occurrences raises questions on their association, causes, and effects. Any answer to these questions (*in relation to what? caused by what? causing what?)* would necessitate investigation of the typologies of the assets, threats, and impacts. These are spread over a wide range, and each is specific to its circumstances, which raises the dilemma of either

[175] Essence: '*The set of properties of a thing or of instances of a kind of thing which that thing or those instances must possess if it is to be that particular thing or they are to be instances of that particular kind. The essence can also be said to be the* defining properties *of a thing or a kind.'* (The Fontana Dictionary of Modern Thought, 1988: 283)

specialising to such a degree that no theory could be formulated, or of abstracting to the point of losing operational relevance. Besides, this exercise would be illogical: without a previous definition of security, any list would be arbitrary. This is no way to enhance understanding of the subject.

The second attempt moves from the identification of all the possible events to the investigation of their qualities: *'What criterion does security literature and practice use to classify an occurrence as unwanted?'* The immediate answer is: *'that which may lead to a loss, or damage'*. However, not every occurrence which may lead to this is security related. A badly placed bet, bad practice, absence of mind, forgetfulness, an accident or a financial loss are examples. The criterion of potential loss or damage, though necessary, can hardly be considered sufficient for a definition of security. Nevertheless, this attempt has been useful, by identifying the focus on security in avoiding a set (not yet definable) of potential losses or damages.

The next attempt originates in the idea that the need of security pre-supposes the existence, or perception, of worry and danger. A definition of security based on this would be (loosely): *'the opposite of non security'*. The problem becomes: *how can non-security be defined?* This approach is more promising, because an important feature of security can be identified by the following reasoning. The concept of non-security is not the exact converse of security. It is more definite, being closely related to the concepts of *'danger and worry'*, which are described in dictionaries as the causes of the need for security. At this stage and for the purposes of this study, *'non-security'* may be defined, independently of its causes, qualifications and typologies, as: '*a feared and dangerous condition, which provokes the need for security'*. Consequently, a definition of security could be *'that activity which limits (impedes, restrains, etc.) the condition of non-security'*. There would be no need for security if non-security was not felt as present. This finding infers that the concepts of security and non-security are not neatly separated, but coexist.

None of the above attempts has provided conclusive results. However, they have led to a first approximation of a concept of operational security, consistent with that in existing literature and daily experience. Security, in the operational sense, is the response to the desire to avoid losses and damages, whose anticipation creates a feared and dangerous condition. This preliminary definition is useful, because it highlights the existence of a 'grey' area, where security activities and feelings of non-security coexist and which can be considered to be the domain of operational security. However, it cannot be considered sufficient for this research, since it does not address the problems of justification, performance, blame and responsibility.

In order to define this 'grey' area where security and non-security overlap and conflict, the research must identify its essence, or 'set of definitional properties'. This investigation is attempted below via two steps of reasoning, one systemic, the other one analytic. The former requires the discrimination of the entire set of definitional properties from the remaining whole, or Universe. The latter demands the description of any particular property. Consequently, a criterion of demarcation between 'security' and 'non-security' and a reliable means of analysis are needed.

The evidence has not yet suggested a reliable criterion of demarcation. However, the scientific methodology permits its identification through the *'formulation of hypotheses'*, which may result in the *arbitrary* definition of a boundary, or limit, around the field of investigation. Although the methodology allows *arbitrium* at this stage, the validity of the criterion of *arbitrariness* may be rejected as non-scientific by those without a philosophical or mathematical background. The crucial point lies in the interpretation of its meaning. The researcher submits that, in scientific terms, arbitrary does not mean dictatorial, or capricious; it means the most credible approximation[176] to the measure of an entity which is not exactly measurable. With nothing having in nature this quality of perfection, physics, engineering, statistics and ...the science of measurement are based on this basic principle[177]. Accordingly, the arbitrary criterion of demarcation will be identified within the area of uncertainty by means of an instrument of analysis based on the principle of approximation.

2.2.2 <u>The Process of Approximation</u>

The steps of approximation starting from the findings of the preliminary analysis are made: firstly, by establishing a general criterion of demarcation between security and non-security. Secondly, this criterion not having the required precision, by restricting the 'grey' area where both sets coexist within two boundaries: the lower including that which is certainly contained in the set 'absolute security', and the upper excluding that which is certainly contained in the set 'absolute non-security'. Thirdly, by setting between these boundaries an arbitrary 'best limit' (as defined earlier) through the identification of a set of operational criteria. This 'best

[176] *'Amount or estimate that is not exactly right but nearly so'* (OALD)

[177] A mathematical representation of this principle is given by the choice of a point, or a segment, within the bell-shaped curve of the Gaussian distribution.

limit' will then be assumed as the 'postulational set of premises' for the definition of security. The analysis follows.

Different methods of approximation exist, which are generally based on mathematical and statistical formulae and, therefore, are not directly applicable at this qualitative phase of the reasoning. However, their basic logic may be utilised, as an introduction to their (eventual) quantitative application. This logic derives from philosophical reasoning such as the Cartesian process of analysis, which suggests in its 'second golden rule': '*to divide each of the difficulties* under examination *into as many parts as might be possible and necessary in order best to solve it*' [178]. The rationale leading this philosophical rule to mathematical calculus consists in the observation that each time an area or problem of indefinite limits is divided, the limit drawn by the division is identified. Therefore, by dividing the problem area, each defined piece of the problem is 'measured' between two identified limits. This process continues until the non measurable, but less relevant fringes (those which cause the problem to be 'fuzzy') are arbitrarily excluded. This logic, applied to human reasoning and to operational research methodologies, constitutes the foundation of the decision-making process.

The process of approximation starts from the wide definition of security: *'Freedom or protection from danger, or worry',* [179]which the earlier survey suggests as a generally acceptable start point. The analysis is assisted by two disciplines of epistemology, logic[180] and linguistic analysis[181]. In this research, logic is interpreted in its broader sense and is used to provide a graphical explanation of the reasoning and of the successive steps of approximation. Linguistic analysis is used in its most basic form to provide an understanding of the meanings (both direct and inferred) contained in the concept of 'security', by the examination of its contents.

[178] Descartes, 1968:41

[179] OALD

[180] Logic has been defined as: *'a science that deals with the canon and criteria of validity in thought and demonstration and that traditionally comprises the principles of definition and classification and correct use of terms and the principle of correct predication and the principles of reasoning and demonstration'* (Webster Third new International Dictionary, 1986), and, according to the Dictionary of Philosophy, has a double meaning: *'In its broader sense logic is the study of the structure and principles of reasoning or of sound argument. Hence it is also a study of those relations in virtue of which one thing may be said to follow from or be a consequence of another.....However, in its narrower sense, logic is the study of the principles of deductive inference, or of methods of proof and demonstration'*

[181]The analysis of the meaning of words and sentences in a given language, in order to identify their content of knowledge. This methodology of reference has a long history (medieval philosophers, John Locke and others have shown interest) and in its modern paradigm was initially formulated by Frege, and developed by Wittgenstein.

Both logic and linguistic analysis have been shown to be capable of providing a powerful, though not conclusive, tool for explanation and '*falsification*'[182]. In linguistic analysis theory

> *'the meaning of an indicative sentence is given by its truth-conditions. On (*sic*) this conception, to understand a sentence is to know its truth-conditions'*

Nevertheless,

> *'The conception of meaning as truth-conditions need not and should not be advanced as being in itself a complete account for meaning'.*
>
> (A Companion to Epistemology, 1993: 250)

This latter point is accepted. Therefore, the truth-condition of the premises so derived is not claimed. Furthermore, the methodology does not require verification of the premises, which have already been settled as arbitrary and fixed as constraints. What is methodologically important is to have authoritative support for this method of proceeding. Thus, its concepts are used only where they are appropriate, that is as a tool for reducing the degree of uncertainty of a definition, by assisting the identification of the component of certainty, i.e. the less disputed contents. To avoid the *minutiae* of epistemology, the use of these sophisticated tools is restricted to the basic exploration of the problem. However, this research suggests that this field of investigation merits study in more detail. It suggests that future research making more scholarly use of these instruments of analysis would further advance understanding.

The first step of approximation uses Venn's diagrams[183]. These provide a graphical representation of the basic idea: taking the whole of the Universe (U) and the whole of Security (S), then the Universe can be divided into two fields: security (S) and non-security (No-S):

[182] The scientific value of linguistic analysis as a criterion of demarcation has been disputed, for instance, by Popper.

[183] A pictorial representation of logical statements, useful for clarifying and checking logical arguments, presented by John Venn, an English logician

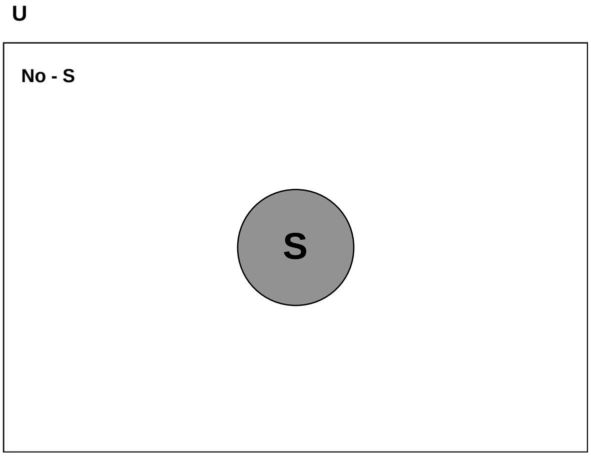

Figure 6 The Ideal States of Nature

The diagram represents the logical separation between these two concepts. It also demonstrates the need for a definition (here represented as the boundary separating the two fields), which can be drawn here only when the contents of each set are known. Hence the problems to be investigated are: what is S? What is No-S?

The dictionary helps to answer the first question, by establishing what has been here defined the 'philosophical' condition of security, i.e., the one where danger or worry are absent. Therefore it can be inferred that the remaining set No-S is defined by *'the presence of danger and worry'*. This criterion (the presence or absence of danger and worry) is useful in that it separates two *ideal* states of affairs: the *perfect* state of security concomitant to the absence of fear and danger, and the *perfect* state of non-security characterised by their presence. However, it cannot be considered sufficient for the purposes of this research. There are two reasons. Firstly, there is no 'perfect state of affairs' in nature, and previous reasoning have shown that both states may coexist. Secondly, professional security is not concerned with the ideal states of affairs, since in perfect security there is no reason for 'freedom or protection', and in perfect non-security there is no utility in trying to achieve this impossible result. A first conclusion can now be drawn by previous attempts to define security. The aggregation of these two *ideal* states of affairs does not comprise the whole of the Universe. Literary evidence and experience confirm the existence of an intermediate state, where security activities coexist in the presence of 'worry and danger'. Philosophers, scientists and the majority of observers may go further and argue that this intermediate area is the normal state of the nature[184].

It is therefore possible to identify between these two ideal states an area of instability, where security and non-security coexist. This concept is graphically explained below by adding to the above diagram a second set (?S), here defined as insecurity. This set is comprised within a lower limit, including what is certainly 'security' (S) and an upper limit, excluding what is certainly 'non-security' (N-S). This set (?S) sees the contemporary activity of forces leading towards security or non-security. Within it, the characteristics of (S) and (No-S) coexist, in proportion dependent on chance and on the efficacy of the security activities. Therefore, the set (?S) has been subdivided into two areas, according to a limit representing the occasional balance of the opposite forces. The grey area of instability, or 'indeterminacy', is the field of speculation because it is, the researcher submits, the domain of security activities. Here the activities aimed at transforming, and maintaining, the largest possible area of insecurity (?S) into a state of *practical* security (P-S) have both sense and utility.

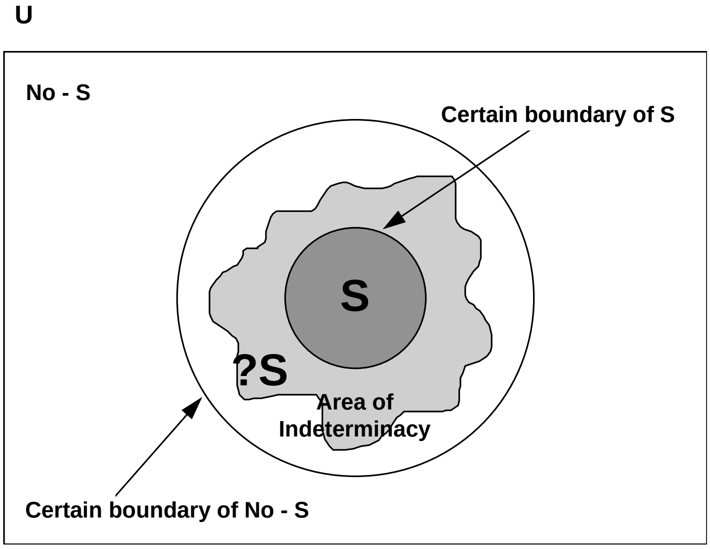

Figure 7 The Existing States of Affairs

The varying limit of the grey area of 'instability' cannot be defined, because of the dynamics of the processes. However, by the principle of approximation, the area of instability can be arbitrarily subdivided into two sets, one (?S) where insecurity is dominant; the other (P-S)

[184] see: Clarke, 1993: X and 57

where chance and specific activities (when they occur) maintain a prevalent state of security. This concept is represented below:

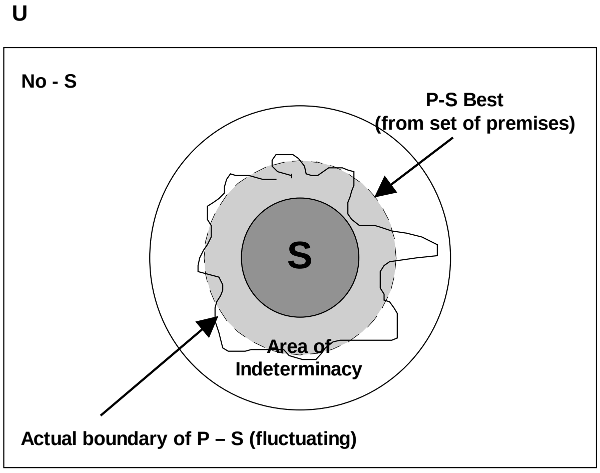

Figure 8 The Area of Indeterminacy

The problem now consists in identifying that part of (?S) around (S), which comprises the area of practical security, or (P-S). The extent of this area depends partly on chance and mostly on a range of 'protective' activities and systems to counter causes, or sources, of non-security, according to an upper limit depending on their dynamic balance. Chance cannot be considered. Operational necessities, notably those relating to justification, performance and responsibility, require the limit of (P-S) to be identified and defined. This is done by means of the analysis of the contents.

The contents have been investigated by applying to the operational body of knowledge[185] a methodology based on Aristotle's doctrine of four causes[186]. These are described in *Metaphysics*: *material* ("that from which, as constitutive material, something comes, for example the bronze of the statue"), *formal* (that which represents, for example, "the goddess Minerva"); *efficient* ("the source of the first beginning of change...for example...the father is the cause of the child"); *final* (the purpose, "that which is done for the sake of something, as health is for walking around")[187]. The *material* and *formal* causes of security are represented by

[185]see: Chapter 1

[186] In English the word cause would probably apply only to the third. Therefore, the aristotelic term 'cause' can be here thought of as distinguishing four fundamental questions and answers.

[187] A Dictionary of Philosophy, 1979:59

structures, systems, people and methodologies. In this research, they are seen as tools, whose choice, installation, and employment is governed by circumstances; as such, do not add to our knowledge. By contrast, it is submitted that the definition of (P-S) can profitably be investigated on the basis of the *efficient* and the *final* causes.

Linguistic analysis of the word '*security'* as described in dictionaries infers that security is that state of affairs, or condition, which is identified by the '*freedom or protection from worry and danger*', where worry is *'a cause of anxiety, or apprehension'* and danger comes from *'the chance of suffering damage, loss, injury'.* Hence, whilst the presence of *worry* and *danger,* regardless of their origin, are sufficient to identify the state of non-security, the key components of the concept of security are the words *freedom or protection.* Indeed, these two concepts may represent two distinct states of affairs. While the state of freedom (i.e., the condition of *absence* of bonds) may *occasionally* exist in nature, the state of *caused* freedom (in the sense of being the result of intentional *activity*) and, more obviously, that of protection, must be constructs. Both freedom and protection presume a previous state of captivity, threat, coercion or compulsion, and a conflict with those provoking this unwanted state of affairs. Accordingly, the condition of security (identified by the non-existence of worry and danger) may result from a *natural* [188] or an *artificial* [189]state of affairs.

Discussion of security as an activity does not include the natural condition, which may be considered a product of chance, and not of rationality. This research focuses on the artificial condition and only on those *worries* based on the perception of *dangers*, i.e., connected to the *'chance of suffering damage, loss, injury'.* This choice is assumed as a premise to the forthcoming reasoning, and stated as: *Security is a contrived condition, intended to avoid, prevent, or protect from, the possibility of a perceived damage, loss, injury*.

Although its contents have been identified, the limit of the set (P-S) cannot yet be drawn, since it has not been found in the evidence. Nor, in the absence of a theory, can it be derived by induction or deduction. However, it is submitted that this limit can be drawn arbitrarily by the method of approximation. For instance, it can be identified by studying the relative capabilities of those defensive and offensive forces aiming at achieving S or N-S. By this logic, a limit can be arbitrarily delineated and maintained in professional security by the

[188] *'produced by nature, not by man'* (OALD)

[189] '*made or produced by man in imitation of something natural*' (OALD)

approval and implementation of a security programme. It is submitted that the establishment of a limit is possible in a specific case, and would enable a rational decision to be made, but it is understood that this limit is dynamic. It must be re-examined in the light of that decision, and of the response to that from the sources of non-security (in a feed-back mechanism). This procedure permits the assessment and justification of security decisions. Accordingly, the issue will be discussed under operational methodology.

In the absence of a definition (which, so far, has not yet been provided) and of an overall theory, the analysis cannot be taken further. Scientific methodology permits its conclusion (the existence of an area of practical security where the antagonism between opposite forces creates a dynamic limit which can be identified) to be stated within the 'postulational set of premises'.

2.2.3 The Set of Premises

Having identified via Venn's diagrams and linguistic analysis the main traits of security, two initial premises have been stated:

Security is a contrived condition, intended to avoid, prevent, or protect from, the possibility of a perceived damage, loss, injury.

A practicable concept of security has boundaries, which can be defined and, perhaps, measured.

From these initial premises, the following secondary premises can be derived:

Security is the outcome of will and rational action. The definition of security as an artificial condition acknowledges the existence of a conscious will capable of contriving it according to a rationale. Both will and rationale have limits. Security is not a spontaneous initiative, but a forced response to someone else's initiative. Besides, its rationale is characterised by a significant degree of uncertainty, since decisions are based on incomplete information.

The state or condition of security is a product of antagonism[190]. Choice of the word 'antagonism' is deliberate. The more general 'conflict' would include conflict with nature and chance. These

[190] Conflict is *'An extremely broad term used to refer to any situation where there are mutually antagonistic events, motives, purposes, behaviours, impulses, etc.'* . (Penguin Dictionary of Psychology), and may have different meaning to different people. It is submitted that the key word for interpreting its meaning in a security theory may be considered antagonism, which may be defined as the: *'active opposition or hostility especially between two people'*. (Oxford Advanced Learner's Dictionary) and *'Generally, a state of affairs*

conflicts do not fall into the same framework of rationality as conflicts between opposite wills, thus are not considered in this research. Hence the use of the more specific term 'antagonism' for explaining a conflict between (at least) two wills, the first seeking *'freedom or protection from worry or danger '*, the second being the cause of *'worry and danger'*.

The driving forces behind security are the perception of a danger and/or the fear of a damage, loss and injury. Security is the result of rational activity aiming to avoid damages, losses and injuries. Previous findings show that the level of activities relates to the level of perception and fear. Two common assumptions at the basis of the concept and activities of security were identified. The first is a need, which has been loosely described as: *'there is someone or something to be taken care of, because someone has the intention of, or is acting to, stealing, spying, damaging, or destroying it'.* The second is the pragmatic appreciation of the impossibility of eluding the task: *'I must personally perform this activity, because I will suffer the loss or damage, and nobody else (not even the State) will undertake it.'* Both link the decision of protecting to the will to protect and to a rationale.

2.2.3.1 Analysis of the premises

The analysis of the premises highlights two identifiable limits, or criteria, which contribute to a qualitative definition of security. One criterion is focus, the other is antagonism.

The criterion of focus is clear (i.e., '*avoiding, or protecting from, damage, loss, injury'*), and helps to understand the limits of security activities. Security conflicts are not intended to conquer or destroy, but to preserve; they are risk-adverse and thus a decision may be changed, or an activity interrupted if a greatest risk arises from the conflict. However, the criterion of focus does not assist progress to a better definition of that area of fuzziness which includes damages originating in accidental and intentional events. This clarification, which is considered important to the measurement of performance and responsibility, is offered via the criterion of antagonism. Further discussion at this level is not considered essential, because it would direct the reasoning to the operational field, in that it links the rationale of security activity to the dimensions of the possible '*damages, losses, injuries'.* Therefore, it will be considered later as a part of the operational problem, in the analysis of decisional criteria and constraints.

between two processes, stimuli, structures or organisms such that their effects are in opposition to each other' (Penguin Dictionary of Psychology).

The criterion of antagonism (within the limits imposed by the focus) draws a clear demarcation between accidental and intentional events, thus brings a decisive contribution to the problem of definition. However, the implications deriving from the acceptance of this criterion must be examined. A number of prejudices or biases to the reasoning may exist, which must be clearly identified and analysed before proceeding further, to accord with the methodological requirement: the *'settling of clear premises'*. The first is that of the purist, who argue that the concept of antagonism is inconsistent with that of (pure) security, which is ultimately seen as the 'perfect state of tranquillity'[191]. The second bias is moral: there is a tendency to identify antagonism in security as a struggle between Good and Evil, Law and Crime, Order and Disorder, in which security possesses the positive connotation of a moral crusade. The third bias is cultural, an inclination to identify antagonism with 'war' or 'fight' between two 'armed enemies'. The final bias is political: security has been seen by some left-wing thinkers as the product of a conservative ideology, and therefore antagonism is anti-social[192]. Evidence and discussion of the relevant issues may be found in the previous discussion of the existing approaches. Here, the research is only interested in practical security, and the concept of antagonism is neutral with regards to legal, social and political considerations. It is only used to define a circumstance where opposite wills have the goal of provoking, or impeding, a damage, independently from their personal motivations.

In addition to those derived from linguistic analysis, there are good grounds, theoretical and practical, for the use of antagonism as a criterion for demarcation. The theoretical ground is its power of explanation. The existence of antagonism (hence, of an antagonist) assists the understanding of the dynamic, ever-changing balance of every security condition, and explains the fallibility of security. Conflicting, interacting and mutable actors give rise to an infinite number of possibilities and concomitant problems of prediction, which only antagonism can explain. The practical ground is its inescapability. Without the concept of antagonism the need, claimed by many authors (mainly criminologists) to understand the motivations and behaviours of 'offenders' would not be explained. Nor the difficulty that security professionals encounter in making a threat assessment, and the need for intelligence would be explained. Evidence in support of this assertion may be found in most reputable

[191] The English term 'security' derives from the Latin '*securitas*', which in turn comes from '*sine cura*', i.e., free from troubles. Andrews, 1875: 1380

[192]'La proprieta' e' un furto' (property is a theft) was a favourite slogan of left-wing extremists in the '70s.

works on Threat Analysis, Motivation and Procedures. The importance of understanding this peculiar aspect of security has been stressed by Whidden:

> *'It is important for the reader to realize that the defence...is a matter of detecting and defeating the attack by a person using technical devices, not just the technical devices themselves. Therefore, the person to be defeated must be caused to do things that will reveal his activities, and certainly not be allowed to know, too soon, that there is a threat to his operation. If he does become aware of a threat, he may take counter actions such as abandoning the operation for a while'*
>
> (Whidden, 1994: 4)

It may be argued that a similar condition also applies when responding to accident and chance. Actually, we are in continuous 'conflict' with nature, and seek to force her to submit to our wills. Similarly, there is 'conflict' with accidents: we try to avoid them, to prevent their happening, and to react when they happen. However, a conflict that originates from, and is conducted by, an antagonist is different, both in terms of processes and predictability, from a 'conflict' that originates in accident, or chance[193].

If the antagonist is non-deliberate and non-reactive, the 'conflict' originates from a set of adverse circumstances which are not deliberately provoked and have no specific motivation. The outcome of the 'conflict' is decided by the relative weights of the actors, who may be inanimate and frequently 'automatic', as a door or an extinguisher against a fire. Assuming a limited number of variables, these relative weights may be measured and compared. An example is the resistance of a specific material of a given weight and thickness against a specific factor capable of a given output (heat, acidity, pressure, etc.) in a given situation. In such conditions, the outcome of the 'conflict' may be predicted and quantified by quantitative methods.

Conversely, if the antagonist is thoughtful, motivated by intent and reactive (or pro-active), the conflict originates in a choice, is driven by a will, motivated by gain and supported by a rationale. The antagonist adapts her/his course of actions to suit her/his interests according to the circumstances, and creates new opportunities and vulnerabilities when s/he cannot exploit the existing ones. The results are not the simple products of measurable forces, but

[193] Chess (a very simple game with a limited number of variables and rules, compared with security), with its almost infinite variety of contingency moves, depending on the activities of only one antagonist within limited dimensions in space and time, underlines the difference.

depend on a 'battle' between a number of non-mechanical factors including wills, intellects, perceptions, sensibilities, knowledge, quick thinking, morale and adaptability.

> *'Experienced terrorists develop sophisticated 'cover' to protect themselves against detection and infiltration. They are adept at disappearing into the shadows of the urban and suburban environment. They increasingly tend to acquire the funds and resources necessary to shift their bases between cities and across frontiers. Modern internationally-based terrorist organisations take full advantage of the mobility afforded by air travel, and are adroit at shifting their bases of operations when things become too hot for them.'*
>
> (Wilkinson, 1981: 169)

With these ever-changing conditions, no quantitative measurement is possible or, even where possible, particularly useful for explanation and prediction. This is because antagonism with a intentful, pro-active and reacting opponent creates a context where non-measurable variables proliferate. Space, time and psychological dimensions may be altered by a change of a variable, thus the resulting state of affairs. Since the security reasoning cannot be supported - at the state of the art - by quantitative methods of assessment, the outcomes are unpredictable in quantitative terms. This, of course, does not include the purely technical aspects of 'conflicts' as, for example, those deriving from the utilisation of a given tool against a given target, or, in some case, the prediction of damages in the event of a positive attack.

One of the most interesting consequences arising from the application of the criterion of antagonism is the sanction of an operationally important demarcation between Safety and Security. Both describe activities aimed at avoiding, or protecting from, '*damages, losses, injuries*', and are frequently used interchangeably, and at times confused, in research, literature and colloquially. Security is often intended as an all-embracing concept[194], which includes safety, and vice-versa. However, the terms are distinguished in all dictionaries. Safety is clearly related to the accidental events, which may be provoked by Acts of God, pure accident, or negligence. Security is, admittedly less clearly, related to intentional events i.e., those intending damage contrary to the will and at the expense of another person.

[194] *'In a general sense, "security" is an individual or collective feeling of being free from external dangers or threats, whether physical, psychological or psycho-sociological, which could jeopardise the achievement and preservation of some objectives considered essential, such as life, freedom, self-identity and well-being. This notion implies freedom from uncertainty. Such a state of affairs has an ideal existence only'.* (Tapia-Valdes, 1982: 11)

Distinctions between philosophical and practical security, and between security and safety are overdue. Security is not only a theoretical or a philosophical study unlike 'the sex of angels', or the nature of truth, good or beauty. Decisions which may involve the lives of people and massive expenditure of money must be justified on a sound basis. The confidence with employers, clients and the public must be earned. Legal claims of blame and liability must be pursued, or opposed. A number of reasons support this distinction of roles. Those relating to the distinction between philosophical and practical security have already been discussed; those relating to the distinction between security and safety follow.

The first difference is in the matter of prediction and, consequently, problem-solving. While the probable outcomes in a safety context can reasonably be predicted because the opponent is not reactive, those in security cannot, because of the antagonism between opposite wills, minds and actions. While safety decision making processes are mostly made in conditions of risk (in its statistical meaning, as 'known probability of outcomes') those in security are mostly made in condition of uncertainty (as above, as 'unknown probability of outcomes').

The second difference is in the methodology. Safety reasoning is focused on hazards, while security is on threats. In safety, the assessment is damage-oriented and comes from statistics, case studies, technical investigations, measurement and risk analysis methods. In security, it is threat-oriented and derives consistency from intelligence, surveillance, vetting and investigation. No evidence of need for intelligence has been found in safety literature. Differences in prediction require different tools in decision-making and planning[195]. No equivalence between a VIP security programme and a safety programme intended to protect lives from fire or flood has been found in any of the above areas.

Finally, the most obvious difference is in operation. While safety knowledge and procedures must be disseminated and known by people as widely as possible, security procedures and sensitive data must only be known on the basis of 'needs'[196]. Some mental processes and operational conditions that are prompted by antagonism are particular to security and are not met in safety. Motivation, will, mental processes, procedures, controls, behaviours, activities in security are different from those in safety, because of intelligent reaction and intentional

[195] This subject is discussed in detail in their specific chapters.

[196] This does not mean, of course, that a 'security culture' should not be diffused. On the contrary, its diffusion is widely seen as a means for obtaining 'security' consciousness, and awareness, in order to reduce opportunities for crime. However, it is undisputed that the operational issues should be kept as secret as possible.

use of violence[197]. In safety, the opponent does not react to a response, nor to the installation of a system, by protecting itself or changing its method of attack. A safety system will never provide a proper response to a security problem (or vice-versa), because it is designed with different priorities, purposes and capabilities. A safety response is inadequate against a burglar or an assassin, in the same way that a tactical response team cannot replace trained firemen. This is not to deny that a safety system may be of some assistance to a security problem (and vice-versa), though this is more likely in detection than in prevention and reaction. Sensors designed to detect heat, smoke, water or gas, may also detect the operation of some burglary equipment, and vice -versa. An example is the smoke detectors installed outside strong-rooms to detect the use of a thermal lance. Similarly, CCTV systems installed for purpose of crime prevention may give an alarm in case of accidental fire. The difference lies in the existence of an intentional and reacting counterpart, which influences each stage of a security process: perception, analysis, evaluation, assessment, planning, management and reaction. This difference is reflected at the professional level, by the completely different approach to wilful or accidental sources of danger. Besides, it imposes a different criterion for judging responsibilities in safety and security, which is sanctioned at the institutional level, by the differences (both in subjects and in responsibilities) in the laws relating to security and to safety. To conclude, it is submitted that all the authors of security works quoted in the bibliography may occasionally confuse security with safety in the introductory pages, but clarify the distinction in their operational chapters, which are explicitly focused on the acts of an antagonist.

Therefore it is offered that the essential criteria of demarcation of the concept of security are antagonism and focus. This modifies the frame of reference found in many existing works on security and drastically diminishes its 'fuzziness', by putting definite limits to both the actors and the events which are proper to security.

It is now possible to explain why the identified approaches are considered unsatisfactory. Firstly, because they are incomplete. Secondly, because objectivity requires to avoid the Scylla and Charybdis dilemma posed by the acceptance or refusal of their cultural premises. Finally because, whatever the causes, security is primarily focused on the avoidance of a perceived

[197] In Wilkinson's meaning: *"...the illegitimate use or threatened use of coercion resulting, or intended to result in, the death, injury, restraint or intimidation of persons or the destruction or seizure of property. This definition has several advantages: it does not confuse the capacity to inflict violence with its actual infliction, and it implies a clear distinction between physical violence and aggressive and emotive rhetoric. In my view, it is vital to make these distinctions clear if there is to be serious public discourse or scholarly investigation concerning the problem of violence."* (Wilkinson, 1986: 23,24)

negative event rather than on solving social, political, military, legal or economic problems. These are specific problems, which pertain to their specific areas; they may overlap with security, but have different goals and priorities.

Evidence has been offered that the concept of security is neutral with regards to moral, legal, social or economic paradigms. Consequently, none of these considerations should dominate a theory of security. To start from clear premises, one point must be re-emphasised: if social, political and economic considerations dominate a problem, then the issue is not one of security. It is social, political or economic, and has to be seen and solved as such. This is not to deny that there are social, political and economic influences and consequences to every security decision, at a certain level, or vice-versa. Their analysis, however, pertains not to the definition of the security context; they take the form of criteria and constraints at the decisional level, which is discussed in the specific sub-section.

2.2.4 A formal definition of security

Having stated the premises and defined the most identifiable limits of the security concept, their analysis has laid the foundations for a formal definition of security, and thus for the formalisation of a theory. These are as follows.

It is assumed for the purposes of this research that in security 1) the focus is the avoidance of intentional loss, damage, injuries; 2) the antagonism is intentional, and relative to an 'object of conflict'; 3) decisions are influenced by interest and fear, which in turn are caused from the perception of a source of potential danger or worry; 4) the achievement of security is within the limits of opposite human perceptions, wills, needs, interests and capabilities, and that, being the product of dynamic antagonism, is unstable.

2.2.4.1 The Basic Components

The identification of the basic components of a security process comes as a consequence of both the premises and limits. These identify antagonists within the process: one, the originator of the process, fears an undesired event and acts to avoid it (Protector), a second is the entity that is considered capable of provoking the undesired occurrence (Threat [198]). The existence and antagonism of both is explained in security terms by the presence of an object of dispute (Asset).

It is submitted that a security situation does not arise unless there is an Asset, a Protector, and a Threat to that Asset. This statement is assumed as a constraint and explained as follows. The mere existence of an asset does not constitute a security situation. Neither protector nor threat can exist without an asset. The existence of a protector without the perception of a threat has no sense, and its activities cannot be defined as 'security'. The mere presence of a threat will not start a security process if it is not perceived, and dealt with, by a protector. The verification of this statement will be offered after the general discussion of the security context.

The security situation arises only when the owner of the asset recognises the existence of a threat and makes the decision to protect her/his asset.. The issues of perception and decision are crucial. The media offer daily evidence of people not giving consideration to security, because they do not perceive the existence of threats. Pick-pocketing in friendly crowds, and many cases of espionage, rape, kidnapping or physical assault are explained by the lack of perception of the victims. There is also evidence of people with perception (or mis-perception) of threat who do not take any security action, and consequently suffer damage. A frequent explanation (confirmed by subsequent interviews) is the absence of fear, that is the supposed harmlessness of the perceived 'threat' to that particular asset. One possible reason for this absence of fear could be the absence of interest (or responsibility) by the protector, in that asset. As a result, no need for protection was felt. The explanation is: either the asset is not perceived as an Asset, i.e. something worthy by definition to be possessed and, consequently, protected, or the protector is not a Protector (i.e. does not feel responsibility for the Asset), or the threat is not perceived as a Threat. A corollary is represented by the phenomenon of 'fear of crime', where people protect themselves in the absence of a threat. This case may be related to a wrong assessment (imaginary Threat), or to an exaggerated fear for the Asset and, consequently, to an exaggerated perception of the role of Protector (or vice-versa). This case cannot be defined one of security. The absence of a rationale derived from the (missing) assessment of a perceived Threat suggests that this case is more a subject

[198] From now on, the antagonist of the protector is defined Threat. The incomplete knowledge of English idiom has not allowed the researcher to find a more precise term. This reason holds for Protector and Asset. Capital letters are used for defining the basic elements of a security process, so to distinguish their use as such from the colloquial.

for psychology than for security. It follows that only after an assessment of the perceived problem has been made, and the consequent actions undertaken, will a security situation be established.

2.2.4.2 Genesis of a security process

According to the premises and definitions, a security condition is not the result of chance, but of a rational and perhaps scientific, human activity, based on perception, cognition and decision. It is submitted that the security process does not arise until the possessor of an asset has both perceived a threat and acted upon her/his perception. Until the possessor of an asset feels the perception of the threat (which assumes the concern about a possible damage to her/his asset), s/he will remain in a condition not definable from a security point of view ('neutral'). In such a condition, there is no fear[199] of damage, hence no interest or motivation in any security decision, or action. The state where only the perception of a threat and the fear of a damage are present, but no security activity is undertaken, is one of total 'insecurity'. In the absence of, or impending, a decision, the possessor remains in a state of expectation of a damage.

This research propounds that a process leading an individual from the state of 'insecurity' to initiate security activities is made in three separate stages. These stages are: the perception of the evidence of the possible existence of a threat (a noise, a shadow,…), the cognition that this evidence may constitute a security threat[200], and the decision of acting upon this cognition. This decision marks the moment of entering the security process.

A different case arises when the threat has been perceived and the possibility of a damage has been accepted. In this case, the decision to do nothing has been taken (in risk management terms, the risk has been retained). Thus, the asset is not perceived as an Asset i.e., worthy of protection, but to be expendable. This infers two possibilities: the threat has not been perceived as a Threat, or the protector is not a Protector. This state is 'neutral' (i.e., not definable as security, insecurity, or non-security).

It is now possible to summarise the process leading to a full security context:

[199]In its general meaning of concern, anxiety, etc

[200] This reasoning conforms to the so called 'threat perception', and to the scholarly paradigm 'risk perception'.

Table 2 Genesis of the Security Process

GENESIS OF A SECURITY PROCESS		
EVENTS	*ELEMENTS*	*CONDITION*
Tenure of an Asset	Asset, Possessor	Neutral (not definable)
Perception of a Threat Danger ⇨ Fear	Perception + Asset + Possessor + Threat = Fear	Insecurity
Assessment Evaluation	Fear + Situation + Cognition = Need for Security	Insecurity
Decision	Asset + Threat + Protector + Fear = Decision to Protect	Security **Security Context**

More details may be derived from the following example:

You, the reader, are walking in the street, taking in the beauty of a splendid summer night (neutral). Suddenly, you see a person approaching (perception). Immediately, you start being more attentive and careful. A man is staring at you. He is huge, unshaven, his shoulders are tightened, his fists closed, and a strange grin appears on his mouth (cognition). The street is dark and empty. You immediately suspect he intends to rob you (threat perception, insecurity). In that case, should you resist, or comply? (assessment, evaluation). You decide to give him the small sum you have in your wallet (decision, return to neutrality).

Perhaps he is not interested in the money? (re-appraisal of the situation, and new state of insecurity, leading to new decisions) He looks stronger than you, he has put his right hand in his pocket, perhaps he is armed. You begin to reproach yourself for entering such the deserted alley. Maybe he is a maniac who derives pleasure from assaulting, or even killing, innocent passers-by? The media are full of such examples. If that is the case, you will have no choice but to defend yourself. How to? Could you flee before he gets too close? Could you deter him by displaying resolution, or perhaps shouting? Is help available? No, there is no choice, you will have to confront him. Can you resist his attack? No, little chance. What can you do to improve your chances?. Perhaps, if you attack him first...

Then, out of the blue, comes a perfectly innocent question from the supposedly menacing stranger: "Excuse me, Sir, could you tell me where the 'King's Arms' is?"

How many times does this happen to us? For this very reason, the above is a good example of the concept of security previously mentioned. To analyse this simple story for its security aspects: the mere possession of an 'asset' (the purse) was not a sufficient condition for thinking about security; only when a potential threat was perceived, were the possible dangers considered. Instinctively, a process of assessment started. The likely nature and potential seriousness of the threat and its possible targets were analysed. The possible damage to each of the identified targets was evaluated: it was the fear of the damage that prompted the decision process. Once identified the asset as the purse, potential profits and losses were balanced. The decision was taken on the basis of fear and interest. There was no will to protect a small sum.

A new process started when unacceptable damage was feared. The purse was expendable, but life and health were not. In that case, our will to protect was excited by our survival instincts, and we prepared ourselves to fight back. Accordingly, a security context arose, not for money, but for life. Life and health were the real asset which motivated the 'security' decision. Why, one could ask, were we not in a full security context when we decided to give up the money without reacting? It could be argued that the decision not to fight for the money was taken in a security context and was based on the principle of avoidance. This objection raises a very interesting point, which highlights the difficulties in defining security and explains the exigency of the arbitrary criterion of antagonism.

The subject is not philosophical, but operational security. If the purse is the object of security, no security decision other than relinquishing was taken. The acceptance of damage offers no basis for assigning responsibility and blame, nor measuring performances, from a security point of view. The acceptance, being based on motives not actions, renders explanation of the actions very difficult, if not impossible. The key lies in the absence of any action: there *was* a security context, a security decision *was made*, but was *discarded* the very moment we realised we no longer had any will to protect the purse. Otherwise, there would at least have been an attempt to escape the perceived threat. *Ergo*, the equation is: passive acceptance of a potential damage, therefore no will, no action, no security context.

A different case arose when the asset was life and health. Then, the decision was to act, and possible tactics and actions were analysed and planned. Luckily, in this case, the threat was not real, and only perceived. However, until it was revealed that there was no threat, we were faced with a security problem, the product of the perception of a threat and fear of the potential damage to an asset. The solution to the problem arose at the same time as the perception of the threat disappeared.

What if there had been no awareness of the threat, and the asset had been lost? Then, we would simply have had to suffer the damage, perhaps the worst of all, the loss of life. However, and according to the definitions given in this research, this would NOT have been a security problem, as there was no perception, no fear and no will to protect. In the absence of decision, no security activity and no security context can be identified.

This example is intended to illustrate that all three components (asset, protector, threat) must coexist in order to create the defined 'security context'. Other examples may show different situations, more or less complex, and on different scales. In all circumstances, the interaction of these three components is the necessary and sufficient condition to define the security context. Otherwise, the context is the rich pageantry of life, not the science of security.

2.2.4.3 Antagonism and the security process

It has been suggested that antagonism is the product of opposite interests in the asset. However, a simple contrariety in interest is not enough to lead to that special form of antagonism peculiar to security, which by definition is influenced by 'worry and danger'. It would be impossible to contemplate the existence of antagonism without considering the reasons for avoiding worry and danger. In security, written evidence and experience indicate that the concept of 'worry' is relative to the possibility of a 'danger' which is considered unacceptable. Thus, the issue is about the degree of unacceptability which provokes antagonism.

There is no easy answer to this question. Long-running arguments permeate the risk literature about what risks[201] and what level of risk are acceptable[202]. Similarly to security, the disagreement on definition and the variety of approaches leads to contrasting conclusions. Positions vary from those who maintain that no risk is acceptable, to those who say that a certain level of risk is 'physiological' in nature, thus when a solution to a risk is offered, a new one is created [203]. The current position in security admits voluntary risk-taking and accepts a certain level of risk when balanced by positive outcomes, or, simply when protection is non-affordable. This opinion challenges the position of this research and contradicts the general definition of security. The researcher submits that only one of two possibilities can derive from the acceptance of a risk (possible damage): or this decision creates no worry, in which case there is no need for security, or it creates worry, in which case the absence of any attempt to attain 'freedom or protection' configures a mere state of insecurity.

This research is not interested to go further in the debate, particularly in the issues about the measurement of the acceptability of risk. The discussion of the relevant operational issues is postponed to that about the assessment of criteria and constraints within the decision-making process. At this level of discussion, it is only relevant to submit that acceptability is linked to considerations about the amount of fear and the amount of damage which are considered unacceptable. These thresholds are relative to the owner of the asset and influence her/his will to protect and, ultimately, the degree of commitment of the protector. Both thresholds depend upon the perceived value of the asset, and upon the credibility of the perceived threat. Fear or worry occur if there is a *'chance of damage, loss or injury'* to somebody or something considered to deserve security*,* i.e., *freedom or protection.* No study about the threshold of fear provoking the will for protection has been found. Existing research and experience indicate that the key point in instigating security lies in fear or undesirability of damage, which in turn is derived from the perception that a threat may exist (the so called *perception of the threat*), and originally, from the interest in an asset. Any security reasoning identifiable in the existing literature relates the credibility of a threat to its assessed capability

[201] In the sense of 'possible damage'.

[202] Adams, 1995: 58; Broder, 1984: 29-33; The Royal Society, 1983: 102-4; The Royal Society, 1992: 135-7

[203] See: risk 'compensation' and risk 'thermostats' in Adams, 1995, Chapter 1-2

of inflicting a damage (Threat Analysis). The evaluation of the negative outcomes (or damage) of a possible adverse event (Risk Analysis) underlies every decision, and the degree of unacceptability of the potential damage depends upon a cost/benefit analysis. These processes are fundamental to security planning.

It is therefore submitted that the need, the will and the decision to proceed into a security context depends upon a fear, which is presumably commensurate to the quantity of 'perceived damage'. It does not arise by financial, moral, political or social considerations.

2.2.4.4 A formal definition of security

All of these considerations, originated by the analysis of the existing literature, have been drawn by logical inferences by means of Venn's diagrams and from the examination of the linguistic contents of the Dictionary's definition of security. The premises, their consequences and the conclusions are consistent with the findings from the investigation held in the previous analysis. It is on these premises that the following definition is based, and from the definition the theory follows.

$$S = f\,(A, P, T)$$

Security is a function of the interaction of its components: Asset (A), Protector (P) and Threat (T). This logic formula summarises the concepts inspiring this research: Security is the contrived condition of an Asset. It is created and maintained by a Protector in antagonism with a reacting counterpart (Threat). It aims to protect the Asset from unacceptable damage.

This is the premise and foundation of the proposed theory of security. It will provide a framework of reference consistent with the definition, and capable of being tested. This framework of reference is defined as the 'security context', that is the circumstances in which the formal definition of security is appropriate.

2.3 DIMENSIONS OF SECURITY

2.3.1 Introduction

Before proceeding further in the formulation of the theoretical approach, it is methodologically relevant a) to analyse and clarify the consequences of the above premises, reasoning and conclusion; b) to undertake a phase of verification of these issues against research and evidence. Both steps necessitate a discussion of the different aspects, or dimensions, of security.

Security has been presented as the outcome of a rational activity which itself, stemming from perception and being influenced by fear and interest, is not of exclusively rational origin. This is not to say that rational criteria and assessment are absent in security, but that the choices are also influenced by personal factors, which are not measurable, or definable as rational. Moreover, these choices are characterised by a degree of uncertainty, since they are subject to someone else's initiative, and are the outcome of 'confrontation' between opposed capabilities. Security concepts and activities have been described as driven by egoism, inspired by conservatism and based on antagonism to a person acting against one's own object of interest. These assumptions and considerations were considered to have essential consequences on the reasoning.

Some of the consequences of this viewpoint may now be more apparent. Entering a security context is a decision initiated from the fear of a given undesired occurrence, and aimed to avoid that occurrence. Decisions and actions need a motivation and a scope, and are referred to a particular occasion, or event. These issues emerge in daily operational necessities, and are recurrent in research.

The level and width of a security context are related to both *fear* of a specific undesired event and the *will* to avoid it. Experience and research in cognitive psychology and criminology indicate that *fear* and *will* are not simple quantities. Fear is related to *'the individual's appraisal of threat, rather than the real nature of threat'* [204]. Will, originating from considerations of *interest* and

[204] Holmes, 1985: 141.

utility[205], is related to the *value* that both Protector and Threat confer on the Asset. The assessment of *value*, *fear* and *will* depends on cognitive, cultural and situational factors. These factors, in turn, are also influenced by consideration of interest and utility made by both Protector and Threat. The security decision depends upon a comparative assessment of these factors.

This has two main consequences on the security reasoning: first, the acceptance of relativity[206] of the judgement; second, the inappropriateness of using fixed values, e.g. financial, to govern a decision making process. Both concepts are interdependent. Both need more thought and research. As for the relativity of judgement, different individual levels of perception, cognition, motivation and decision are the factors that most influence entering the security context and the relationships between its actors. As for the inappropriateness of using fixed values, the traditional justification of recourse to quantitative measurements is the necessity of avoiding qualitative, thus arbitrary, judgement [207]. However, the alleged usefulness of using an objective system of measurement has repeatedly proved false in security. Evidence has been provided by social scientists that perceptions are culturally construed [208]. Further evidence will be offered in the discussion dedicated to management and decision-making.

Another aspect to be considered is that of the circumstance in which the judgement is made. The 'here and now' of a security judgement may be in the tranquillity of an office, under the pressure of a boarding meeting, or under threat of life. It is clear that perceptions, priorities and goals cannot be unaffected by circumstances, which range from administrative comfort to personal combat.

2.3.2 Time

Time is a critical factor in security. It is frequently overlooked in existing literature, which concentrates on the administrative phases of decision-making and routine activities even during emergency. An exception can be found in Sally Leivesley's ORA methodology

[205] Those considerations are constant issues in security literature, and a requirement in 'Security Management'

[206] in the sense of the dependence of these factors on the subjective judgement of both Protector and Threat, cf objectivity.

[207] The Royal Society, 1992:192-4

[208] Adams, 1995: IX, X; The Royal Society, 1992: chapters 5, 6

(Operational Risk Assessment Technique)[209]. In this methodology, different temporal phases identify different states of affairs, as the security problem evolves from its rise to its conclusion. Decision-making environments change from routine to emergency to routine; and mental processes operate at different speeds and under different mental sets[210]. Accordingly, it is submitted that the dimension time is essential in identifying a security condition and assessing the state of affairs, since the dimensions of all its intervening factors could not otherwise be appreciated.

The analysis of each moment of the evolution of a security problem pertains to the operational tasks of planning and post-facto investigation. For the purpose of explanation in this study this process is analysed in its three constituent phases: before, during and after the undesired event.

2.3.3 Psychological aspects

Psychological factors permeate throughout the security process: Perception, Fear, Cognition, Learning, Motivation, Awareness, Behaviour, and Mental processes. It has been assumed, because antagonism is present in the security processes, that these factors govern the outcome of each security activity. This sub-section seeks to verify this assumption, in order to identify its limits and to understand its applicability. This is done in two steps. The first gathers evidence within the relevant paradigms; it is discussed here. The second relates to the influence of psychological factors on decision-making; it is analysed in the Section III. The discussion follows the general 'genesis of a security context' outlined above, and analyses the general processes of perception, cognition, emotion, and decision.

2.3.3.1 Perception

The submission that entering a security context begins from the perception of a danger infers that perception is a key of the security process. Perception [211]is still a largely unexplored field,

[209] Leivesley, 1995a:243-248 (n.a.)

[210] *'Any condition, disposition or tendency on the part of an organism to respond in a particular manner, Note that the term respond here may encompass a number of acts. Thus, one may have an attentional or perceptional set, a task-oriented set for a problem, a functional set, which directs the manner of use of objects (functional fixedness)'.* (The Penguin Dictionary of Psychology, 1985: 689)

[211] *'The most general sense of this term covers the entire sequence of events from the presentation of a physical stimulus to the phenomenological experiencing of it. Included here are physical, physiological, neurological, sensory, cognitive and affective components'.* (Penguin Dictionary of Psychology, 1985: 527)

because *'what is perceived it is not uniquely determined by physical stimulation, but, rather, is an organised complex, dependent upon a host of other factors'* [212]. This research uses 'perception' in its general connotations[213].

The general process of perception has been investigated by cognitive psychologists. Research demonstrate the difference between the perception of a fact and the fact itself[214]. The main factors in the process have been identified as: Attention[215], Attitude[216], Distortion[217], Illusion[218], Motivation[219] and Learning[220]. However, these aspects of the problem are not considered as sufficiently known.

Psychological approaches to risk perception are generally intended to measure the difference between a '*perceived*' risk and an '*actual*' risk, or to analyse its *cultural* construction, or the difference between *expert's* and *lay people's* perceptions. It has already been submitted that, in security studies, most of these approaches are biased by a number of factors. The first is the confusion in the notion of risk, which appears to embrace different concepts, such as Threat, Hazard, Feared Events, Possibility of Damage, and Expected Loss or Damage. This definitional confusion adds to the general ambiguity in understanding the process. There are difference in perception which should be clarified. For example, it seems that the perception of some threats or hazards depends on the primordial instinct of survival, while the perception of others is considered 'culturally construed'. Perceiving a life-threatening circumstance has not the same psychological importance that perceiving the possibility of a theft, or similar financial losses, and has different impact on cognition. These substantial

[212] Penguin Dictionary of Psychology, 1985: 527

[213] *'the faculty of perceiving. The intuitive recognition of a truth, aesthetic quality, etc. An instance of this (a sudden perception of the true position) The ability of the mind to refer sensory information to an external object as its cause'.* (Concise Oxford Dictionary)

[214] Allport, 1954: Gregory, 1973, The British Crime Survey, 1983; Hayes, 1994 pp. 21-62, Williams, 1994 pp. 34-59

[215] *'A general term referring to the selective aspects of perception which function so that at any instant an organism focuses on certain features of the environment to the (relative) exclusion of other features.'* (Penguin Dictionary of Psychology)

[216] *'...contemporary usage generally entails several components, namely: cognitive (consciously held belief or opinion); affective (emotional tone or feeling); evaluative (positive or negative); and conative (disposition for action). There is considerable dispute as to which of these components should be regarded as more (or less) important. Cognitive theorists usually maintain that the undelying belief is fundamental, behaviorally oriented theorists focus on the conative, ...and most other researchers feel that a combination of the affective and evaluative components are the critical ones'* (Ibid.)

[217]"generally, any twisting or contorting that alters the shape of something so that it no longer faithfully represents the object." (Ibid.)

[218]"Basically, any stimulus situation where that which is perceived cannot be predicted, prima facie, by a simple analysis of the physical stimulus" (Ibid.)

[219] *'The most typical use of this extremely important but definitionally elusive term is to regard it as an intervening process or an internal state of an organism that impels or drives it to action. In this sense, motivation is an energizer of behavior.'* (Ibid.)

[220] *'The process of acquiring knowledge or the actual possession of such."* (Ibid.)

differences are not appreciated in most existing literature, where the paradigm perception is normally linked to the concept of risk (in the sense of possible damage) and not to that of threat (source of danger). The second is the quantitative approach to the measurement of risk, which has reverberated on attempts to measure 'risk perception' in the dimension of damage rather than to analyse the effect of such perceptions on motivation and decisions[221]. Social scientists are currently debating this subject. Remarkably, the research is limited to 'risk' (the confusion of terms makes no clear when the subject under discussion is hazard and threat). Little effort is directed to investigating the asset and the situation from the aspect of perception. The third is that some of these studies affect the object of their scrutiny, and loose therefore the necessary objectivity:

> *"It is the Royal Society purpose in studying risk -to manage it- that frustrates efforts to produce predictions. Because both individuals and institutions respond to their perception of risk by seeking to manage it, they alter that which is predicted as it is predicted"*
>
> (Adams, 1995:14)

The conclusion is:

> *'What is clear is that risk perception cannot be reduced to a single subjective correlate of a particular mathematical model of risk, such as the product of probabilities and consequences'*
>
> (The Royal Society, 1992: 89)

The relevance of the perceptive process to this research is in its influence on learning, behaviour and decision. More attention is dedicated to the perception of asset and threat (which influences from the beginning the process) than to the perception of a risk (which influences operational decisions). This last aspect is therefore discussed in Section III. Cognitive studies show perception to be affected by attention, previous knowledge, motivation and expectation. Operational experience reveal that these factors can be improved by experience, as for example in military training and in the practice of martial arts[222]. Correct education, training and procedures may be expected to improve an individual's capability of

[221] Adams, 1995: Chapters 2, 5, 6; The Royal Society, 1992: Chapter 5

[222] A set of exercises conceived for improving perception is described in Manunta, 1990, chapter 1

perceiving a threat. This aspect of security instruction is normally referred to 'awareness'[223]. However, experience indicates that not all the individuals seem to have the same response to this educational process; thus, the selection of the apt person is an important premise to efficient security training.

Perception is a factor which affects the assessment not only of the threat, but also of the asset and the situation. This is a critical issue, which is generally, and inexplicably, considered only in the field of personal security, traditionally separate from other, more technical, forms of security. Since even the most precise assessment is influenced by perception, security assessors should be cognisant that their precise mathematical calculus is a function of this non measurable factor (perception). Perception may then be viewed as a 'factor of efficacy' with regards to the entire process. This 'factor of efficacy' influences all three temporal phases of operational security. Lack of attention to perceptional, and consequently to cognitive, factors may explain some of the most serious errors in security. Perceptional (and cognitive) errors may explain why a given system has failed in prevention, or in detection, as well as wrong decisions during reaction. For example, an attacker may not be perceived as such by bodyguards until s/he starts shooting, a sensor may give an alarm which is wrongly interpreted as 'false'. Some of these failures may be explained as a product of the so-called 'Cognitive Dissonance'[224]. This posits that, when beliefs or assumptions are contradicted by new information, the conflict is resolved by one of several defensive manoeuvres. The person may reject, or ignore the new information, persuade himself that no conflict really exists, reconcile the differences, or resort to other defensive means to preserve her/his conception of the world and of her/himself.

As security originates in antagonism, perception has no fixed value. It is both a dynamic and an effect of relationships between actors. The researcher sees perception not only as a 'passive filter', but also as a powerful 'active' instrument. A person who can manipulate her/his opponent's perception is able to provoke and to assist advantageous changes. This is a very old idea, being associated to war and politics since Homer, Thucydides, and Sun Tzu[225]. Today it is mostly confined to 'information security', where the so-called

[223] *'An internal, subjective state of being cognizant or conscious of something. Alertness, consciousness'.* (The Penguin Dictionary of Psychology, 1985: 76)

[224] *'An emotional state set up when two simultaneously held attitudes or cognitions are inconsistent or when there is a conflict between belief and overt behaviour'* (The Penguin Dictionary of Psychology, 1985: 129)

[225] Starr, 1974. Sun Tzu (c. 500 BC), chapter 13

misinformation, or deception, plays a key role. Both theory and practice of security should start from perception, considered as both a filter and an instrument. Hence, enough resources should be dedicated by those with security responsibility to educate and maintain the perceptional capabilities of their own operatives, and to alter and deceive the antagonist's perceptions of the asset and of the protective measures.

2.3.3.2 Cognition

Psychologists consider perception as leading to cognition. Thus, it influences security decision-making. The nature of cognition and the relationship between the knowing mind and external reality have been discussed by philosophers since antiquity. There are many viewpoints and interpretations of cognition and its development. The relevance of the cognitive process to this research is in its influence on learning, behaviour and decision.

Broadly, cognition refers to the mental processes of knowing, perceiving and judging, which enable people to interpret the world around them. Individuals have a personal view (judgement) of the world surrounding them, which they seem to derive from their environment (perception), and from their frames of reference (knowledge). If cognition, in its general meaning, brings the awareness or appreciation of objects or situations, usually via the senses, and if security decisions start with a perception, then, before embarking on a decision process, one should answer the following questions:

- Is the reality I perceive, truly the exact representation of reality?
- How can I be sure that what I perceive is correct?

These basic questions assume that the education, evaluation and assessment of 'perception' is possible. This involves the acquisition, organisation, and use of knowledge, and affects learning, thinking, problem-solving and behaviour, all of which occur in the security process. It also accords with the earlier 'set of premises', which states that the decision to enter a security process starts from the perception of risk ('possibility of damage') and is justified by its subsequent assessment. Yet, if the starting point of a rational and, possibly, scientific activity, security, lies in a 'perception', then understanding of perception is essential to the formulation of unequivocal premises to the whole process.

Concepts and techniques applied in security about these issues are borrowed from the 'risk analysis, assessment, management' studies. Numerous different approaches have been identified (cognitive, psychometric, cultural and decision-making paradigms). Different models have been defined, mainly in the area of *safety* risks. Their details are not relevant, but it is important to remember that there is no agreement on the definition of risk is, nor on the methodology of its measurement. Since researchers refer more to *technical* (risk of failure, hazards) rather than to *tactical* risks (those arising from intentional and reacting threats), their approaches are restricted to that which is 'measurable' and are thus more appropriate to static than dynamic situations. Previous discussion (Section I) has highlighted the difficulties arising from the application of this methodology to security reasoning.

Social scientists believe quantitative approaches to be narrow and frequently inapplicable. There is an interesting discussion in Adams[226]: '*...many from the scientific and managerial side of the subject are unaware of the anthropological literature on risk'* [227], and *'The literature on risk, measured by pages published, is overwhelmingly dominated by the scientific/managerial perspective'* [228]. The author emphasises that this perspective does not take into account other theories, for instance 'risk compensation', 'cultural theory', 'chaos theory' and 'the propensity to take risks'.

This leads back to the paradigm 'risk perception'. Current positions on perception derive from cognitive psychology. Therefore, the appreciation of risk and, consequently, security decisions, is considered dependent on subjective, non-measurable, factors: perception, knowledge, thinking, credibility, motivation, and interest. An example is the Royal Society list of factors which influence people's perception of risk:

> *'From the perspective of the social sciences, risk perception involves people's beliefs, attitudes, judgements and feelings, as well as the wider social or cultural values and dispositions that people adopt, towards hazards and their benefits' …'What is clear is that risk perception cannot be reduced to a single subjective correlate of a particular mathematical model of risk, such as the product of probabilities and consequences, because this imposes unduly restrictive assumptions about what is an essentially human and social phenomenon'*

[226] Adams, 1995, Preface, and chapters 1, 2

[227] Ibid.: IX

[228] Ibid.: X

(The Royal Society, 1992: 89),

Both the subjectivity and the relativity of risk perception have great importance in daily decisions, and vital importance in security, as they relate to the acceptability of perceived threats, dangers, or risks. Evidence is that different people take different risks in different ways, because of *their* perception of risk in *their* particular circumstance. This has been acknowledged by several authors, and emphasised by Adams:

> *'Risk, according to this perspective* [i.e., Thompson's "cultural theory"], *is culturally constructed; where scientific fact falls short of certainty we are guided by assumption, inference and belief'. (author's emphasis)*
>
> (Adams, 1995: IX)

Cognition is influenced, inter alia, by previous knowledge. Knowledge is, broadly, represented by the body of information possessed by an individual, and the mental components that result from instinctive and learned processes. This individual frame of reference governs and restricts perception and therefore acts as a filter which influences cognition. Judgement[229] is made by weighing the perceived factors against previous knowledge. Individual knowledge is limited. Therefore, an important contribution can be made to good judgement by a well organised process, where external sources with a different basis of knowledge may bring new perspectives and may control the existing ones. This is not always applicable in security, where the dynamics of antagonism may require quick judgement and immediate response, and may even develop to the extreme situation of fight. In potentially emotional security situations, knowledge may help or hinder judgement, dependent on the previous experience and training[230].

2.3.3.3 Emotion

The perception of a threat prompts various mind sets, from interest (including lack of interest) to fear. Both extremes are relevant. Interest alone does not explain the dynamics of antagonism and the emotional involvement typical of the security context. Fear alone would drive the protector to survival, but not protective, processes. The nature of these states of

[229] : *'Generally, the process of forming an opinion or reaching a conclusion based on the available material. The hypotised mental faculty that functions so as to carry out such judgement.... A critical evaluation of some thing, event or person...'*(Penguin Dictionary of Psychology, 1985: 380).

[230] Cooper, 1972; Holmes, 1985; Jenkins et al., 1985; Kellet, 1982; Lev, 1982

mind depends on the nature of the Asset, and on the relationship the Protector has in the Asset.

2.3.3.3.1 Interest

The issue of interest[231] features throughout security literature, and its relevance is easily acknowledged. Security has strong connotations of self-interest, since it stems from a conflict of interests. Interest in the asset is the force that drives both the threat, and the will to protect; fear alone will probably lead to a simple *'fight or flee'* dilemma. The importance of this issue requires an explanation of the concept, the general meaning of which has been defined as 'loose'[232]. Dictionary definitions range from concern and curiosity to a quality or subject exciting curiosity or holding attention, from a financial stake or legal concern, to the selfish pursuit of one's own welfare.

Generally, in security literature, the concepts of attention and motivation are extracted from this 'loose set', and interest is used in the sense of concern, advantage or profit, and stake (financial, or other). In fact, it is more appropriate to speak of self-interest. The difference in approaches, and even the antagonism, may be explained in terms of self-interest, or, better, of the pursuit of different individual visions of utility, rather than in terms of 'cultural profiles'.

The evidence is that utility plays a crucial role in security decisions, and that utility theories may explain the convergence upon the Asset of the opposing interests of Threat and Protector, and their antagonism. In security, utility has both philosophical and economic connotations. Both contribute some pragmatic use, since it is possible to produce a ranking, in order of preference, of decisions and behaviours, even though utility itself cannot be quantified.

Philosophical considerations of utility (notably, those linked to the 'utilitarianism' of David Hume, Jeremy Bentham, and John Stuart Mill) provide a powerful link and a balance between the 'interest' and 'peace of mind', which are widely accepted to be the ultimate goals of security [233]. Utilitarianism is frequently assumed in the widespread opinion that private and

[231] *'one of those terms who slipped unnoticed into the technical vocabulary of psychology, especially educational psychology. Its meaning is loose at best and at one time or another has been used to imply all the following: attention, curiosity, motivation, focus, concern, goal-directness, awareness, worthiness and desire. Most authors merely follow their intuitions in its use, it's hard to go wrong'.* (Penguin Dictionary of Psychology).

[232] Ibidem

[233] for one: Fayol, 1949: 4

public security converge towards a 'common good'. The aggregation of all private security does not amount to public security. The general criticism moved to utilitarianism -notably, the practical difficulties of its application, its unfairness and its one-sidedness -[234] reflects the egotistic vision of security as it emerges from history and evidence. However, there is no supporting evidence for this position. Utilitarianism in security is, indeed, debatable. The 'invisible hand' which, according to Adam Smith's theories, should reconcile self-interest with public interest is far from convincing. Firstly, because self-interest infers a conflict between different entities: one's security may provoke other person's insecurity, public security is always distinct from, and sometimes adversarial to, private security. Secondly, because private security may not have any moral, legal or ethical connotation, whilst (at least in theory) public security has. The outline of philosophical and socio-political differences between private and public security suffices for present purposes, which is only that of identifying the specific features and the driving forces behind and within a security process.

Economic approaches to security are also based on utility. Economic theories of rationality and marginal utility, consumer behaviour, and allocation of resources have provided tools of analysis and explanation for the production of security programmes [235]. Security considerations of the issue are largely depending on 'risk management' approaches, which are essentially based on the principle of utility, and no security report is complete without assessment of the economic pay-off of the proposed measures. However, the widespread recourse to monetary terms to measure the utility of security measures is debatable[236]. The issue of how utility should be measured in security is under-researched, with utility depending from perceptions, interest and expectations, which may be imposed from outside. Apart from reducing losses, security measures can be taken to reduce fear, to ensure peace of mind, to address political and social

[234] A Dictionary of Philosophy, 1984: 361

[235] A.I.PRO.S.: 1984, Broder, 1984, The Royal Society, 1983 and 1992

[236] The Royal Society, 1992: Chapters 2, 5

pressures, to deter an hypothetical potential antagonist, to improve control, or simply to assert a status-symbol. All of reasons may conflict, and overwhelm, pure financial considerations, and challenge the foundations of the current 'Risk Management' paradigm.

As with others, the issue of interest and its constituents is far from explored in security. It is suggested that this is a fertile territory for further research.

2.3.3.3.2 Terror, Fear, Anxiety

Emotions modify perception, cognition and judgement, thus influence the decision making process. The emotions which prompt the will to protect and justify antagonism range between the extreme degrees of Anxiety and Terror[237]. These emotional states of mind are related to the interest which the Protector takes in the Asset. This affects all mental processes (particularly on cognition, perception, reasoning, decision and action), and has different impacts in different temporal phases and situations. Anxiety, fear and terror have a particular weight in security decisions, particularly in conflict situations, when interest involves people and things linked by love, hate, or affects. Dictionary definitions are used in this research: Terror is an emotional state of *'extreme fear'*. Fear is: *'an unpleasant emotion caused by a state of alarm, or anxiety for the safety of somebody/something'* (i.e., the Asset). Anxiety is described as: *"troubled feeling in the mind caused by fear and uncertainty about the future"*[238]. These three states have subjective thresholds; they are more easily aroused by certain experiences, thoughts, and threats than by others. The theme is also linked to cognition:

> *"Much of our experience of terror [and, to a lesser level, fear and anxiety] is the unintended or epiphenomenal by-product of other happenings which are beyond our power to predict or control. Indeed, inability to understand what is happening, say in a sudden automobile collision or a fire, is in itself a cause of more intense fear."*
>
> (Wilkinson, 1986: 50)

Whilst some terrorist acts such as a nearby explosion or shot, or even a loud shout, may induce an 'extreme level of fear', evidence reveals this emotional state to be uncommon in security. Experience shows that, although an element of fear occurs in the majority of the security contexts, few arrive at the extreme state of 'terror'. With the exception of cases

[237] Holmes, 1985:140,141

[238] OALD

involving personal risks and dangers, the level of emotion is generally confined to fear and, most commonly, anxiety. This is because security, being risk-adverse, is inclined to refuse fight. Anxiety, rather than terror and fear, appears to be the most common driving force and, according to the premises, the minimum necessary state of mind in a security context; in combination with interest it arouses a 'will to protect'. Once motivated by interest and emotion, the degree of involvement is governed by the assessment of the threat's capabilities, and of the damage the asset may suffer. It is possible to position Anxiety, Fear and Terror in temporal phases. Anxiety generally occurs in the pre-event phase. Fear and Terror may occur in the event phase, particularly when there is a direct confrontation between Threat and Protector.

2.3.3.4 Decision

Decision connects perception and cognition with action through the process of thinking. It is considered to include choice and commitment[239]. In this sub-section, decision is considered within the whole process of thinking. There is a more detailed treatment in Section III. Thinking is taken to be the mental activity which enables humans to perform both theoretical contemplation and practical deliberation. The former process is directed towards a propositional conclusion (*philosophical thinking*); the latter is directed to reach a decision on how to act (*goal-directed thinking*). Having defined security as the result of a rational activity, this second aspect of thinking is more relevant.

Most psychological research has been focused on the area of *'goal-directed thinking'*, and specifically on problem-solving. Two main approaches may be identified: one was stimulated by scientific methodology and, more recently, by the analysis of existing military approaches to the *'solution of the problems'*; the other has sought to identify similarities between human thinking and computer processes. Both endeavour to improve knowledge of human intelligence and reasoning, and to optimise the use of computers in the so-called information technology.

However, research has provided evidence that human beings do not always think or operate logically (or, rather, according to *formal* logic) [240]. For example, it has been found that, even

[239] Noordhaven, 1995: 7-9

[240] Hayes, 1994: 152-155

when two statements are logically equivalent, humans take longer to process the negative statement than the positive. They tend to attempt the confirmation of known instances, and to make inferences focused on the meaning of the statement, instead of making strictly logical deductions.

> *'It is a matter for debate whether these features of human reasoning should be seen as "errors", or as evidence that human reasoning is far more subtle and sophisticated than a logical system would be, since human reasoning includes the whole social context and the probable actions that people are likely to take as well as the "pure" elements of the problem'.*
>
> (Hayes, 1994: 155).

The problem is that, while the logical functioning of a computer is perfectly understood, the area of cognitive psychology concerned with these processes is large, and not fully explored. Some important issues have emerged from research into problem solving: mental set[241], functional fixedness[242], interference[243], trial-and-error learning[244] and insight[245]. Common-sense psychological theorists assert that, ultimately, people's decisions depend both on their beliefs and desires. This has not been completely accepted:

> *"Some philosophers have been sceptical about common-sense psychological theories (e.g., Stich, 1983). Decision theorists, however, have, for the most part, accepted the common-sense analysis of decision making, and have, furthermore, assumed that beliefs and desires can be completely disentangled from one another (though see Shafer, 1986, for a dissenting view)."*

[241] *'Any condition, disposition or tendency on the part of an organism to respond in a particular manner. Note that the term respond here may encompass a number of acts. Thus, one may have an attentional or perceptual set, a task-oriented set for a problem, a functional set, which directs the manner of use of objects (functional fixedness)'.* (The Penguin Dictionary of Psychology, 1985: 689)

[242] *'A conceptual set whereby objects that have been used for one function tend to be viewed as serving only that function even though the situation may call for the use of object in a different context. For example, a hammer just used for pounding nails may not be perceived as appropriate for use as a pendulum weight'.* (Ibid.: 290)

[243] *'In learning and conditioning, a conflict among associations formed between stimuli and response. In learning and memory, a conflict between information in memory such that either: (a) new information becomes difficult to learn because of previous experiences, or (b) old information becomes difficult to recall because of current information'* (Ibid.: 367)

[244] *'Quite literally, learning that is characterised by trial-and-error responding. The course of such learning is typified by the gradual elimination of ineffectual responses and the strengthening of those responses that are satisfactory'* (Ibid.: 400)

[245] *'Most generally, an act of apprehending or sensing intuitively the inner nature of something....Two additional meanings relate to situational or environmentally stimulated insight: 4 A Novel, clear, compelling apprehension of the truth of something occurring without overt recourse into memories of past experiences. 5. In Gestalt Psychology, the process by which problems are solved. In this sense, insight characterises a sudden reorganisation or restructuring of the pattern or significance of events allowing to grasp relationships relevant to the solution. Here, insight represents a kind of learning and is characterised in an all-or-none fashion'.* (Ibid.: 359,360)

(Garnham and Oakhill, 1994:176)

It is submitted that those findings support the assertion that every security process is affected *ab initio* by psychological factors. Evidence may be found in the model of generalship, from Dixon's stimulating 'Psychology of Military Incompetence':

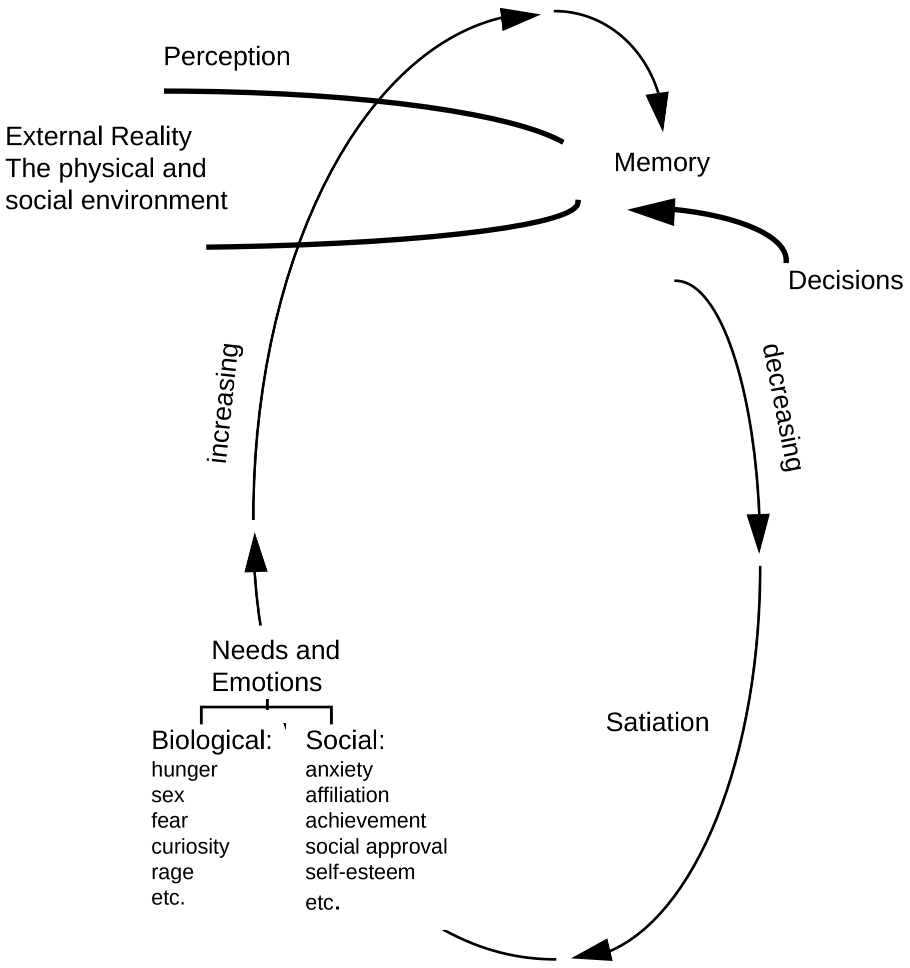

Figure 9 Psychological Factors in Decision Making

> *'The way in which an individual perceives and acts towards his environment is partly determined by the quality and strength of his motives, needs, attitudes and emotion.'*
>
> (Dixon, 1976:.33).

Indeed, all of the above factors interfere with the *'correct'* (better: *ideal*) process. This is relevant to a dynamic concept as that of security, where mental set, functional fixedness and interference obstacle perception and cognition, insight seems to act as a by-pass to decision, and trial-and error-learning appears to be nothing but a inherently erroneous way of making decisions when facing the antagonist. More evidence will be offered later.

Experienced professionals might argue that, with proper planning and preparation, these influencing factors will be capable of balancing themselves out. Both trial-and-error learning and insight may act as a counterweight to the negative influence of mental set, functional fixedness and insight. A 'correct' decision may then be possible, for an actor conscious of these biases, who has made proper planning and preparation and takes all of those factors into account. The researcher agrees with this position, with a caveat which derives from his professional experience. No positive effects can derive from repetitive *clichés,* as those normally encountered in security training; they can only derive from a process based on a sound and coherent methodology, which will be discussed in Section III.

2.3.4 Political aspects

A security process is not self-contained, nor is it a private fact restricted to Asset, Protector and Threat. It happens within people, organisations, in an environment. This obliges to consider other factors besides pure security, which have been summarised, for purposes of explanation, under the generic terms of 'political'. With security being an essentially human and social phenomenon, its choices are inevitably *'concerned with power, status, etc. within an organisation rather than with the true merits of a case'*[246]

There are strong political elements in any security decision. Even when the components of a security process can be quantified (which is uncommon) the setting of rules and standards is intrinsically a political act. That is, the rules and standards must in the final analysis be arbitrary, or must invoke some principle that goes beyond quantification.

Law, image, internal and external relationships, public opinion, social habits, public and personal expectations are just a few of the factors that interact with decisions via rules not perfectly understood, and conventionally known as 'political'. These factors cannot be identified without a previous definition of the specific set of circumstances to be analysed. It is possible, however, to aver with Easton that any security process passes through the 'black box' of the political system, which has been graphically represented as:

[246] OALD: Political

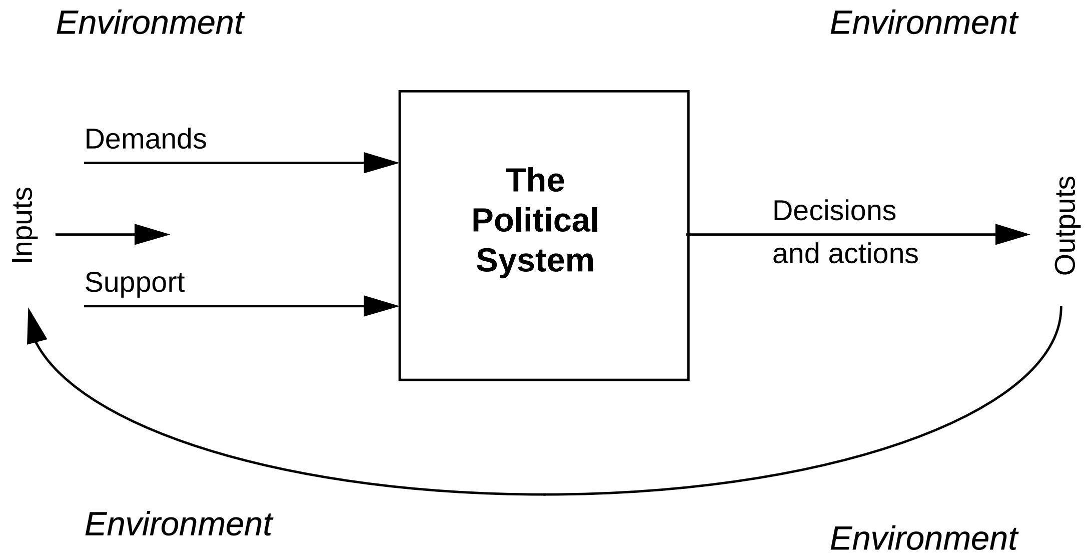

Figure 10 A simplified model of a political system by Easton (1965), as quoted Ham & Hill, 1993: 13

The contents of the 'black box' are not completely known; it is generally accepted that its output depends on the person responsible for the decision-making process. A reference to Meltsner's three types of analysts in the American federal bureaucracy may be helpful:

> ***'the technician, interested in doing good quality -policy oriented- research and essentially an academic in bureaucratic residence; the politician, concerned to achieve advancement and personal influence and interested in analysis only in so far as it furthers these ends; and the entrepreneur, interested in using analysis to influence policy -and improve policy impact'.***
>
> (Ham and Hill, 1993:7)

It is submitted that the political relationships between Protector and Threat begin with their appreciation of the perceived value of the Asset, until now represented under the generic term of 'interest'. The political aspect of decisions helps to explain why the interests of the Proprietor and of the Protector do not always coincide, especially when the Protector considers her/his own personal interest to be part of what s/he perceives as the Asset. This fact may lead to conflicts in security reasoning, activities, and decisions. For example, a guard confronted by a robber may decide to relinquish her/his employer's cash because the gun-point changes her/his perception of the Asset from the cash to her/his life. A security manager selecting security personnel, equipment and methodologies may base her/his decisions on 'political' criteria: private interests of sympathy, personal or economic convenience.

The term 'politic', just because it cannot be exactly measured, does not mean 'irrational'. In a well-defined situation, the most important factors can, at least, be identified. In order to take them into account in a 'scientific' methodology, their 'fuzziness' can be limited to the greatest possible extent, and estimated with appropriate methods. A frame of methodology is set out after the presentation of the security context.

2.3.5 Administration

Administration is an important factor to be considered when discussing security. Security activities are largely routine and are the subject of administrative functions, from planning daily activities to purchase, salaries, control and management. Administration is part of the relationships between Asset and Protector, particularly in routine, non emergency phases, both pre and post-event. Administrative concepts and activities may act as a major hindrance to perceptive, cognitive, decisional and response activities. For example, they may be cause of those 'negative' factors previously identified: mental set, functional fixedness and cognitive dissonance. The prevalence of administration over security may lead to boredom, establish routines which may be exploited by a threat, or create a bureaucratic mentality where formal aspects prevail over security needs. Good management is the essential key to operational security, thus the dimension of management is relevant to the whole process. Its more interesting features will be discussed in the discussion related to the methodology.

2.3.6 Considerations

Detailed analysis of the important subjects presented in this sub-section is not relevant in the formulation of a theoretical approach. Focus on a single factor may cause the loss of the general perspective which, in a dynamic context of antagonism, is essential. For example, excessive concentration on the perceptive aspects may divert the attention from the managerial aspects, and vice-versa. The investigation of detail without loss of general perspective, is a problem without easy solution. It is sufficient, for the moment, to consider the above factors to be qualitative dimensions. However, the experience indicates that, in a given state of affairs, they can be at least comparatively weighted by an expert. This degree of resolution is not relevant to the general theory, but is contained within the decision making process. The influence of these factors (the principal being: time, psychological, political and administrative) on the security context has been grouped under the comprehensive term 'Situation', and discussed after the analysis of the security context.

2.4 THE SECURITY CONTEXT

2.4.1 Introduction

The formal definition of security previously submitted has reduced the 'fuzziness' of security, but does not provide a workable criterion of demarcation from other activities. This criterion should permit measurement of performance and assign responsibility in all possible security-related circumstances. This raises issues of universality and applicability under the control of a scientific methodology. Universality is essential to the validity of the reasoning in all diverse states of affairs that may require security (for example: national security, personal security, commercial security, information security, computer security...). Applicability is similarly essential: the identification of the focus of the reasoning, the establishing of priorities and constraints in the decision making process, and the assignment of both responsibilities and liabilities depend upon it.

This criterion is offered in the verification of the existence of a security context. A security context is defined as the state of affairs to which the formal definition of security [S = f (A, P, T)] applies. The verification of the existence of this state of affairs is considered the *'sine qua non'* of any security analysis. Consequently, the process of explanation derives from the analysis, within the security context, of the constituent actors, of the resultant processes and of dynamics between them.

2.4.2 The Basic Components

The next step in the formalisation of the reasoning is to propound that the basic elements of a security context are the Asset, the Protector and the Threat. A discussion and definitions are offered.

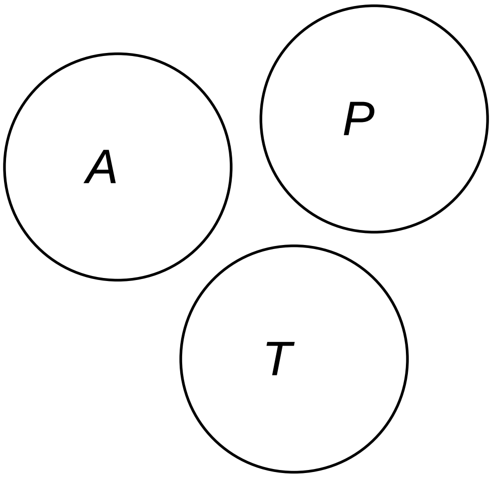

Figure 11 The Basic Elements of a Security Context

2.4.2.1 The Asset

From the security point of view, an Asset exists only when a Proprietor deems it worthy of protection. The mere existence of a threat does not bestow upon its subject the quality of 'Asset', but only that of target.

While the existence of antagonism requires the Protector and the Threat to be living sources, the Asset can be anything or anyone considered worthy of protection. The multi-dimensionality of security is revealed in the multi-dimensionality of the Asset. Examples are persons, life, health, possessions, information, image, accessibility, use, freedom. The term 'Asset' is anything that can be threatened and damaged, and is consequently defended by the Protector. It is not relevant (at this stage) to analyse or define the danger, but only to understand that it originates from the *visibility* and *accessibility* of the Asset to the source of danger, the Threat. The necessity to abstract the reasoning allows the researcher to define damage as the negative outcome of an adverse event; it involves a change in state of the availability, existence or integrity of the asset. The concept of Asset is central to the security reasoning. It is submitted that the security process must start from the identification and the assessment of the Asset; only afterwards can the assessment of Threat and of the possible damages be implemented. There are many types of asset, and there are many reasons why an Asset is considered to be worthy of protection by its Possessor. Financial value is one of the most common, but utility, uniqueness, confidentiality, exclusivity, peace of mind, even pleasure are all possible components of an Asset. For example, a picture may have sentimental or aesthetic value; similarly, a good reputation or a brand name may be an Asset worthy of defence. Hence, the concept of Asset is represented by the sum of its characteristics, material (shape, substance, ...), financial (cost, value ,…) and qualities (existence, utility, reputation, image,...). These elements confer *value* on the Asset, both to the Possessor and to a Threat. The Asset may have different values for the Possessor and the Threat. For example, a heirloom may be a part of the history of a family and therefore invaluable to its Possessor, whilst the Threat may consider only its resale value.

Given the variety of the Asset, and the variety of values that may be conferred upon the same Asset by different people in different times and situations, it is extremely difficult to define Asset in a more specific sense, and impossible to quantify all possible values. However, it is possible to state that the Protector seeks to maintain an Asset in that configuration and state which is desired by the Possessor. Therefore security, in the sense of activity, is directed at obstructing any undesired modification to the configuration or state of the Asset.

2.4.2.2 The Protector

A Protector is someone who, by possession and/or responsibility for the Asset, has the *interest* to protect it and, having the necessary *authority* and *capability*, takes the decision to protect it. Interest and decision, according to the premises, are motivated by fear of an undesired modification to the state of the Asset. Protection, therefore, originates in the will to preserve the desired state of the Asset.

It is very important to understand that security, as both a condition and activity, is not an impenetrable, all-encompassing blanket that protects from all possible dangers. Security is shaped by people, and is limited in purposes and extent by their interests and perceptions. Thus security relates to degrees of will to protect a perceived and desired state of the Asset. It follows that, whilst interest and fear are a necessary motivation, they are not in themselves sufficient to prompt security activity. The decision to protect, as a conscious and rational act, refers not to all the possible threats, but only to those perceived and feared by the Protector. As security originates in, and is influenced by, interest, perception, and fear, it may be seen as a rational activity driven by a value judgement. This is relevant to dynamics of the decision-making process, and is further discussed in the relevant sub-section.

2.4.2.3 The Threat

In a putative security context, a threat exists only if it is perceived as a Threat by the Protector. Given the premises, only intentional threats are considered in a security context. Thus a Threat is a perceived antagonist judged capable of undesired modification of the state of the Asset, as desired by the owner.

In security literature, the concept of the Threat is the subject that mostly needs a clear definition. Evidence of disagreement and confusion on the meaning of threat, hazard, danger, risk, damage, and their respective sources (i.e., source of threat, hazard, danger, risk or damage) has been given.

Threat is, for the Protector, an intentional source of damage. Many attempts have been made to categorise the threat as a source of damage, the act of damage, and the damage itself[247]. Attempts have been made to improve the understanding of the motivations and dynamics of the threat. [248] The analysis of the different types of threat is premature. At this stage it is important only to note that *credibility* is a *sine qua non* of Threat. This necessary condition is the Protector's *perception* and *judgement* that the attributes of Threat (*intention* plus *capability*) constitute a source of potential damage.

2.4.2.4 Note

The three basic components of the security context: Asset, Protector and Threat, may not be physically distinguishable. For example, the Asset and Protector may be one and the same. In this case, typical of personal security, the motivation to protect is, or should be, maximised. Similarly, *per absurdum*, Threat and Asset may coincide, as in the case of a suicide, who is a threat to him/herself. It may also be that the Threat and the Protector coincide[249]. It is therefore always necessary to distinguish the concept and function of each element from its physical manifestation.

[247] Broder, 1984; Gigliotti and Jason, 1984; Flynn, 1979; Nuclear Regolatory Commission, 1979

[248] Abrahamsen, 1967; Adams, 1995; Balloni, 1983, 1993a, 1993b; Beck, 1993; Bennet and Wright, 1993; Gill et al., 1994; Home Office: Crime Prevention Unit Papers; The Royal Society, 1992; Scarr, 1983; Young, 1988, 1992; Wiersma, 1996

[249] An example are the Sikhs bodyguards who were 'protecting' the late Indian Prime Minister Indira Gandhi.

2.4.3 Verification of the Basic Context.

It has been assumed that the presence of all three components is the necessary condition to configure a security context. The chosen methodology requires this hypothesis to be tested. This is done by examining all the possible combinations of the three elements. Some of these combinations are clearly absurd, but their examination is required by the methodology, which demands a test to be complete; this is for allowing falsification and for stimulating further thought. The examination starts from the diagram below:

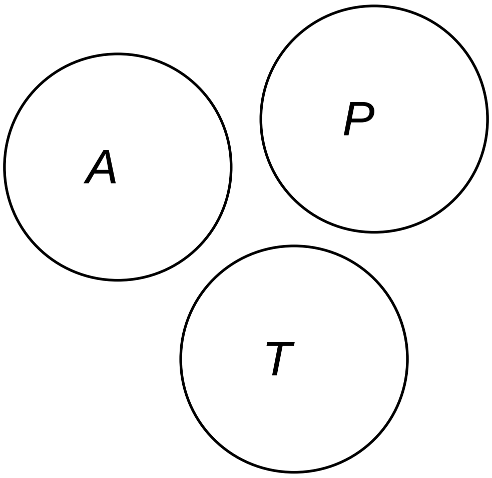

Figure 12. The basic components of a security context

The test must demonstrate that unless all three exist and can be identified, there is no proof of a security context. There are two steps in the analysis: firstly, examination of the general condition arising in the absence of one of the elements; secondly, examination of their possible interrelationships. For simplicity the analysis is confined to the conceptual model. Specific examples of Assets, Protectors and Threats and their related states of affair are not examined.

2.4.3.1 If an Element is Missing

If an element is missing, there is evidence only of a false security context. This will become clear in the studies which follow. For simplicity, the terms Asset, Protector and Threat are still used, but the reader is warned to note their incomplete meanings (with one of them missing, the remaining cannot be fully defined). The extreme cases of two separate and not interacting entities which could be defined as latent components of an incomplete security context are discussed only for completeness.

2.4.3.1.1 T is missing.

If the Threat is missing, the protector cannot be considered as such, but is only the owner of an asset.

2.4.3.1.1.1 First assumption: P and A do not combine.

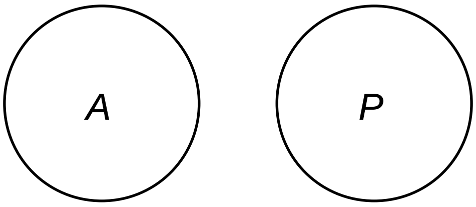

Figure 13: A and P as latent and separate entities

In this case, two entities are represented which have no relationship. Thus, the 'protector' and the 'asset' are not definable as such. A possible explanation may be that 'protector' is unaware of the 'asset' because no 'threat' has been perceived. Thus, 'protector' does not feel responsible from a security point of view precisely because there is no threat (real or perceived), and the 'asset' has not been perceived.

2.4.3.1.1.2 Second assumption: P and A do combine.

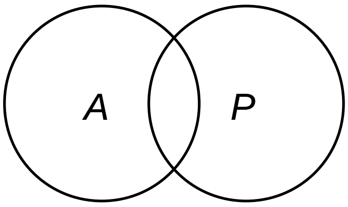

Figure 14: A and P as latent and interacting entities

Here the sense of responsibility from a security point of view is highlighted by the overlapping of 'asset' and 'protector'. The absence of a threat does not account for such a position, unless a distinction between real and imaginary threat is made (see previous notes on 'fear of crime'). This diagram depicts a latent 'protector' who has perception of an imaginary 'threat' and has the potential of becoming a Protector if a Threat were present. This condition may be explained by a characteristic of either the 'asset' or the 'protector'. This is either because the value of the 'asset' is considered so great by the 'protector' that s/he feels it necessary to protect it anyway, or because of an exaggerated 'fear' caused by panic, misperception, or wrong assessment of the 'threat'. This diagram may therefore be considered as the representation of a false security context.

2.4.3.1.2 P is missing.

If there is no protector, then is no asset and no threat. The case only describes the condition of contemporary presence of two potential components of a security context, would a protector be present. In the absence of a protector, no security context exists.

2.4.3.1.2.1 <u>First assumption: A and T do not combine.</u>

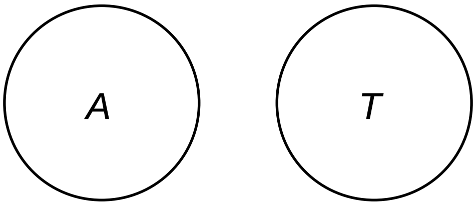

Figure 15: A and T as latent and separate entities

The 'threat' here is not interacting with the 'asset'. All the diagram says is that there are two independent entities, which, if a protector and some degree of interest were present, could be definable as a threat and an asset. The absence of interrelation may be explained by the ignorance of their relative existence.

2.4.3.1.2.2 <u>Second assumption: A and T do combine.</u>

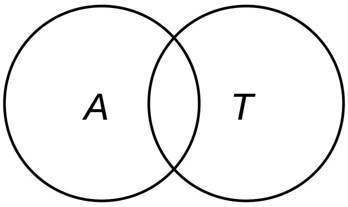

Figure 16: A and T as latent and interacting entities

The 'threat' interacts with the 'asset'. Yet, nothing happens from a security point of view, because no protector is present. The diagram only shows an interrelation between two different entities, one of which, by interacting with the 'asset', is possibly becoming its proprietor.

2.4.3.1.3 A is missing.

Without an asset, there is no reason for security, hence no protector (what could s/he protect?) and no threat (in relation to what?). Antagonism would be irrational and unexplainable from the point of view of security. The case only depicts two potential adversaries, motivated by hate and chance, in the absence of an object of conflict, who do not consider themselves (life, health, etc.) as asset.

2.4.3.1.3.1 First assumption: P and T do not combine.

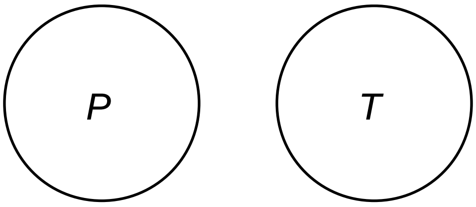

Figure 17: P and T as latent and separate entities

Potential 'protector' and 'threat' exist, but not related to each other. Only two separate entities, which -if an asset and some degree of interest were present- could be definable as a protector and a threat. The absence of interrelation may be explained by the ignorance of their relative existence.

2.4.3.1.3.2 Second assumption: P and T do combine.

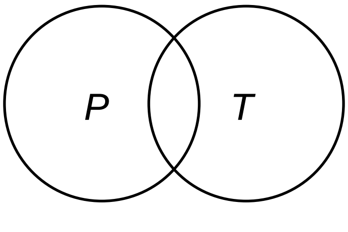

Figure 18: P and T as latent and interacting entities

'Protector' and 'threat' are in conflict. In the absence of an asset, antagonism is unexplainable from the point of view of security. The case only depicts two adversaries, motivated by hate or conflicting by chance, in the absence of an object of conflict, who do not consider themselves (life, health, etc.) as asset.

2.4.3.2 All Three Elements Exist.

The presence of all three components Asset, Protector, and Threat is the necessary condition for the entrance into a security context. The absence of one component describes states of affairs which are not explainable from a security point of view. A false security context has been previously identified in the interaction of 'protector' and 'asset' in the absence of 'threat', which is irrational, or absurd. However, the previous analysis indicates that the existence of the three components in isolation is not a sufficient condition to establish a security context. This requires that they be interrelated. Four possible types of relationship can be identified, of which only one satisfies completely the conditions of the formal definition of security, and consequently establishes the existence of a security context. Each one of these possible circumstances will be tested below.

The first case is represented by the existence of all three elements, but in isolation.

2.4.3.2.1 First case: A, P, T do not combine at all.

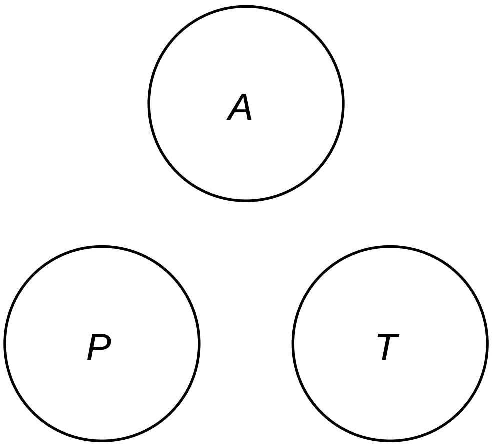

Figure 19: The Three Separate Components of a Security Context

No security context can be identified, since the 'protector' does not feel responsible for the 'asset' and the 'threat' is not interested in the 'asset'. The three entities have the potential to become a 'protector', an 'asset', and a 'threat', should a relationship between them arise. The requirements of the formal definition of security are not completely satisfied.

2.4.3.2.2 Second Case: only two elements combine.

2.4.3.2.2.1 <u>T is isolated.</u>

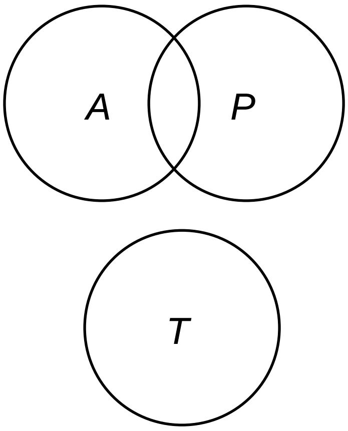

Figure 20: P and A interact; T is isolated

The potential threat exists and accounts for the protector's feeling of responsibility for the asset. However, the potential threat shows no relationship with the other entities. Thus, only the potential for a security context is shown. A possible explanation is linked to the temporal condition. The analysis follows.

2.4.3.2.2.1.1 <u>BEFORE THE EVENT.</u>

The diagram may depict a potential security context in progress. The protector has analysed the possible consequences of interference by the threat with her/his asset, and has prepared a security programme. Different cases can be identified to explain the behaviour of the threat. Firstly, the threat has not yet perceived the existence of the asset. Secondly, the threat is not interested to the asset. Thirdly, it does not consider that the asset justifies an offensive. The case where the threat has been deterred from attack is not considered (otherwise, a relation with the protector would be present).

2.4.3.2.2.1.2 AFTER THE EVENT.

The diagram may depict a past security context. The threat has attacked the asset, but has been unsuccessful. The protection system has been adequate to the capabilities of the threat. The threat has withdrawn and is no longer interested in the asset, nor is engaged or deterred by the protector.

2.4.3.2.2.2 P is isolated.

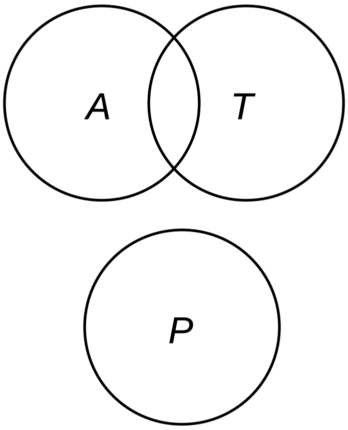

Figure 21: T and A interact; P is isolated

The diagram shows no relationship between protector and the remaining entities. While the protector is absent, the 'threat' is interacting with the 'asset'. In such condition, neither threat nor asset can be defined as such. Thus, no security context exists, and only a potential security context is shown, would the protector take charge of the asset. Other possible explanations are linked to the temporal condition. The analysis follows.

2.4.3.2.2.2.1 BEFORE THE EVENT.

The threat perceives the asset, protector does not. The protector does not perceive a threat (he is protecting other assets), and, accordingly, has not prepared a prevention/protection system. This case is not infrequent in security. For example, the physical integrity of a VIP may be protected, but his/her reputation or communications left unguarded, not having been seen as assets by the protector. Another common example is the internal threat, overlooked by a protector focused on external threats. Another example is a computer virus. It is there, but unless a sensible protector prescribes an attentive check up (or is able to do so), there will be no chance to defeat the virus in time. This diagram may therefore represent a threat, or an asset, either not identified or not assessed.

2.4.3.2.2.2.2 DURING/AFTER THE EVENT

The threat is attacking the asset undisturbed. The protector is absent, not having identified the asset, having a flawed security programme, or having been diverted or misinformed by the threat. This diagram represents defective assessments, programmes or procedures.

2.4.3.2.2.3 A is isolated.

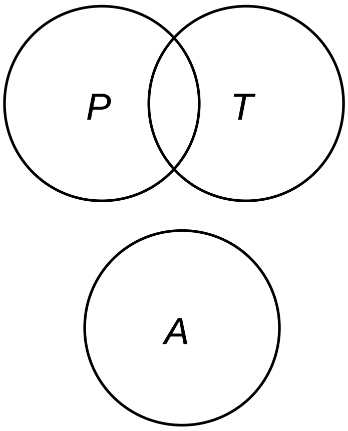

Figure 22: P and T interacting; A is isolated

Here, the asset is not related to the protector, nor to the threat. It is therefore not an asset, from a security point of view. But the 'asset' (real or presumed) exists and leads to a confrontation of protector and threat, who do not really care for it. Such cases of 'unjustified' conflicts are not uncommon, particularly in international security. They are generally, and perhaps absurdly, explained by the contenders as being motivated by security reasons. A possible case was the race to nuclear armaments between the USA and the USSR; their use, by destroying the world, would have left both with no asset at all. Other examples are long-term terrorist conflicts and family vendettas, where the conflict itself supplants and obscures the asset which originated it. Another example is the bodyguard who engages an attacker and looses contact with the person to protect. Other explanations may be given, according to the different temporal phases.

2.4.3.2.2.4 Before/during the event.

This explanation is twofold. The protector makes a pre-emptive attack on the threat before threat relates to the asset. Or the threat attacks the protector, perhaps to clear the way for the identification of the asset, or to search for an asset.

2.4.3.2.2.5 After the event.

Either the protector has repulsed the threat and then decides to pursue it (to arrest/eliminate/repress), or the threat, after an unsuccessful attempt on the asset, decides to attack the protector (e.g., for revenge).

2.4.3.2.3 Third case: A, P, T form an open chain.

In the following three cases, two of the elements are linked to the third, but not to each other. Interactions are incomplete. This configuration may be used to explain the dynamics of antagonism.

2.4.3.2.3.1 A at the centre.

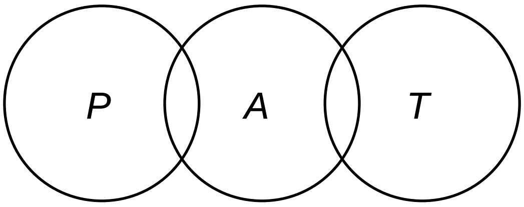

Figure 23: A links P and T

Protector and threat are both linked only to the asset. They have no direct contact or relation each other. This condition represent an example of an incomplete, or unsuccessful, security context. It may occur in two different situations. The protector feels the responsibility for the asset, which implies that s/he perceives a possible threat, but does not fully understand the nature of the threat. As a consequence, prepares and implements an inappropriate security programme, which protects the asset in the wrong direction. Or, the protector understands the threat, prepares an appropriate security programme, but fails to adjust to the development of the threat, which, having surveyed and assessed her/his objective, is able to bypass the security programme, and attacks the asset from an unprotected direction. Or, the threat has used diversion or deceptive tactics, so to make protector respond in the wrong direction.

2.4.3.2.3.2 P at the centre.

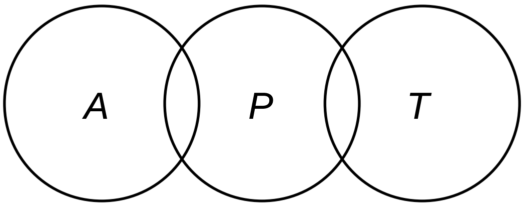

Figure 24: P links A and T

The protector is positioned between asset and threat. Two possible explanation can be found. The protector has been capable to shield the asset from the incoming threat. The threat either elects or is obliged to attack the protector as her/his only means of gaining access to the asset.

2.4.3.2.3.3 T at the centre.

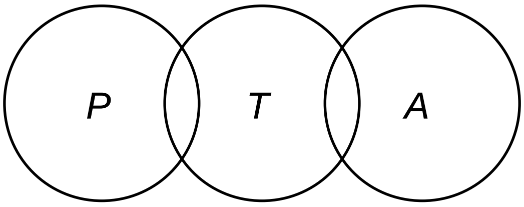

Figure 25 T links P and A

The threat has access to the asset. But is not 'protected' against the protector. The protector is not interested in the asset, but in the threat. This diagram may depict an involuntary condition (protector has been deceived and separated from the asset), or an intentional one (protector is using the asset as a bait to capture the threat). Alternatively, the protector was protecting the wrong asset, and identifies the true target only when the attack is carried out. The protector, then, has no other chance to protect the asset (or limit the damage) than to attack the threat.

2.4.3.2.4 Fourth case: they all combine together.

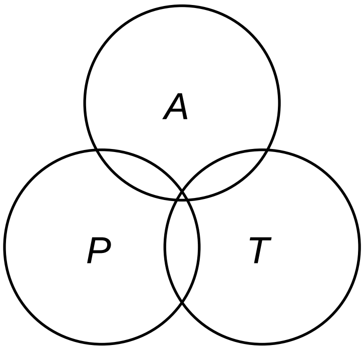

Figure 26 A, P and T are interlinked

It has been postulated, this is the only situation in which a full security context exists. All three elements are present and inter-linked, as required by the formal definition of security. This state of affairs is therefore used as the criterion of demarcation of 'security' from 'non security'.

It is important to note that security contexts are dynamic. Consequently, this diagram can be seen as a momentary representation of a security context in action. The Protector and the Threat are re-adjusting continuously to each other, centred on the Asset. It is now possible, using the diagram, to discuss different possibilities of interaction between the three components.

2.4.3.3 The Basic Model at Work

It has been submitted that the presence of interaction between all three actors is the 'sufficient' condition to configure a security context. Further analysis will show that the model above represents a security problem, which has still to be solved.

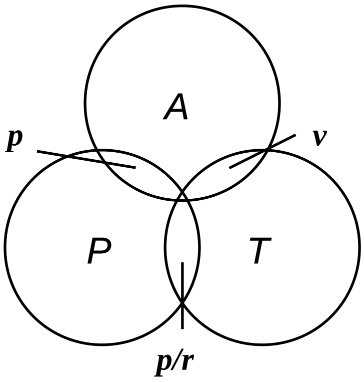

Figure 27: Preliminary analysis of the model

In the figure above, A, P and T are interacting with each other, but there is no area common to all three elements. Each of these areas offers a general representation of the intervening dynamics, which may be defined according to the focus of analysis (i.e., centred on A, or P, or T). For example, an interpretation may be the following. The area common to P and A can be taken to represent the **protection of A by P**. This area is ***p*** (protection). The area common to T and A represents the **extent to which A is vulnerable to T**. Vulnerable does not necessarily mean damaged. It means only that T is in a position to damage A, to an extent represented by the area of vulnerability, ***v***. The area common to P and T represents all the activities of P **to prevent T** from attacking the asset, and **the responses of P** against attack or action by T. It includes all direct or indirect actions of P with regards to T. This area is ***p/r***. (prevention/response). Similarly, if the analysis is focused on A, the area ***v*** may be interpreted as the area of damage, and (if the focus is on T) the area ***p/r*** may be considered to represent the activities of T against P.

The analysis follows keeping the original focus on P. A first observation indicates that the three areas do not overlap. This means that the Protector has perceived a Threat to her/his Asset, and is taking action (***p/r***). Yet, P has not understood T completely, as the lack of interaction between ***p*** and ***v*** clearly show. In fact, P has made a wrong vulnerability analysis, and is protecting A in those aspects (***p***) that are not, actually, under real threat (***v***). Moreover, P has not responded to the real vulnerability where T is/may attack A (***v***). It follows that the diagram represents an impending, unresolved, security problem.

Thus, this diagram helps to understand how the three elements interact, and assists identification of the problem. From this preliminary analysis, it is possible to formulate (or readdress) an appropriate correct security programme, designed to eliminate v and to increase p/r (p/r is at a maximum when T is neutralised via a counterattack). Analysis of this diagram clarifies understanding the strategy behind the security programme. This will depend upon the aims of the Protector. These should derive from clear and definite choices in matters of security policy and management. This reasoning will be further analysed. Continuing the analysis, a number of cases might apply.

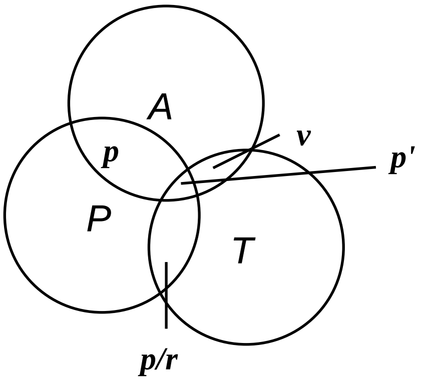

Figure 28: An adjustement of the security programme

In the above diagram, P is more aware of the vulnerabilities of A with regards to T, and has adjusted her/his programme. The area ***p'*** represents the protection intended to reduce the perceived vulnerability. Yet, the way the diagram is drawn, implies that P still has to improve, because at this point, much of its efforts are nugatory. More, the protection has not been able to fully eliminate the vulnerabilities.

The concept can be developed further as the following examples show. This only aims to offer a tool for explanation, and is therefore incomplete. Different shapes have been used, in order to give a graphical explanation of different possible security strategies (more focused assessments, resources, etc.…).

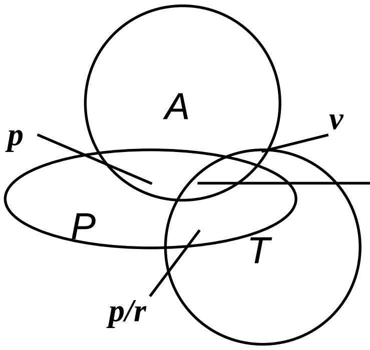

Figure 29 Ineffective protection has been reduced

P has now definitely improved her/his programme. The ineffective protection measures and activities have been reduced, while ***p'*** and ***p/r*** have increased.

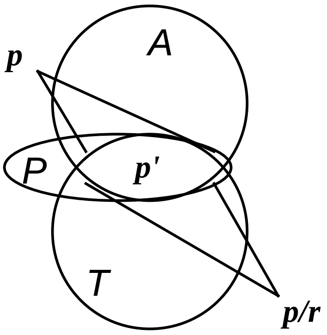

Figure 30 Vulnerability has been eliminated

In the above diagram vulnerability has been eliminated. The Protector has been able to cover all the possible moves of T towards A, while minimising the redundant and the ineffectual protection.

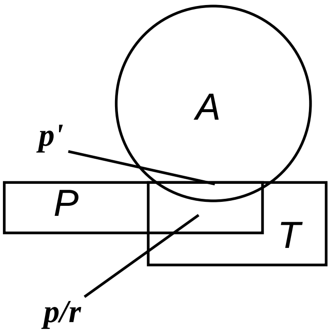

Figure 31 Maximum protection efficiency

All unnecessary protection of A has been eliminated. All of P's actions are aimed at T or A. In this example, the area of P outside the process is intended. It represents a reserve, or additional P related to other A or T. This case illustrates a thoughtful and successful security programme, in which the resources are used to eliminate the vulnerabilities through full protection, while dedicating a part of the efforts to preventive and responsive activities, and to respond to foreseeable possible threats, not yet perceived.

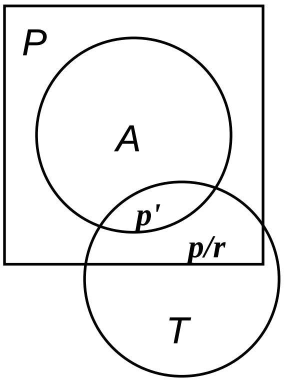

Figure 32 A Probabilistic – Competitive Approach

The above diagram illustrates the case in which security has priority over costs. The Protector values the Asset so highly that s/he decides to cover all possible vulnerabilities against all possible Threats. At the same time, efforts of prevention and response are directed against those Threats already identified and considered more dangerous. The distribution of protection goes all around the asset, but in different strengths in different directions of Threat. This may be an example of a 'probabilistic' or even a 'competitive' approach; different levels of protection are implemented and accord with the different probabilities (or capabilities) attributed to the different perceived Threats[250].

[250] For a discussion on the 'probabilistic', 'competitive', 'organisational' approaches see: Orlandi, 1989

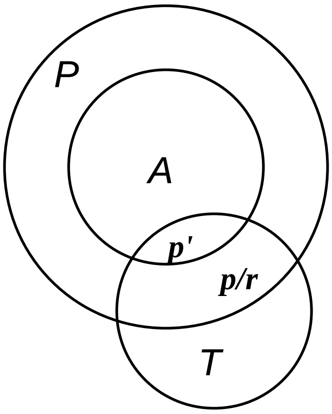

Figure 33 The Organisational Approach

Here, the Protector treats all Threats and vulnerability as indifferent (equally possible). This state of affairs is an example of the 'organisational' approach[251].

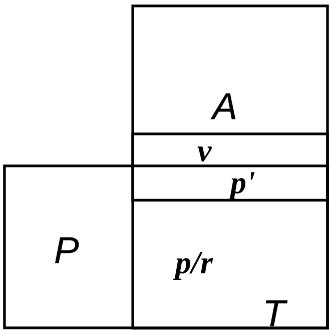

Figure 34 Deciding for Prevention

In the example above, the objective of prevention takes priority over protection. Such decision might stem from the will to eliminate or to deter the Threat. The Protector has decided not only to protect the Asset but also, and particularly, to neutralise the Threat, which is considered too important to remain active. This goal is considered so important that, in sufferance of resources, the decision is made to leave the Asset unprotected at **(v)** and dedicate maximum resources to the certain neutralisation of the threat.

[251] Ibid.

2.4.3.4 Considerations

The basic elements of a security context have been identified, but no definition of the nature of their relationships has been yet offered. Relationships necessarily exist, as required by the formal definition of security.

It has been deduced from the premises and the definitions that the relationships and dynamics are all centred on the *perceived value* of the Asset. The Asset is the fulcrum on which a *security* context is balanced. This simplifies the analysis of a security context, by providing an explicit focus (the Asset) for the identification, analysis and assessment of Threat and Protector. Examination of the above diagrams and formula shows that the relations between the components are three-dimensional. However, if one specific Asset at a time is considered, the examination may be two-dimensional. No precision is lost, at this stage of reasoning, by this simplification[252]. Consequently, it is possible to restate the previous formula with respect to the Asset::

$$S_{(\mathrm{A})} = f(P,T)$$

That is: in a security context, the Security condition (or quality) of a given Asset (S $_{(\mathrm{A})}$) is a function of both the Protector (P) and the Threat (T).

The quality of these relationships depends upon the characteristics of each actor, and -more specifically- from the encounter between each set of properties, as, for example, value, visibility, accessibility, motivation and capability.

It would be premature to analyse these relationships in detail at this stage. Apart from cognitive factors influencing attribution of values, choice, visibility and accessibility, actors are affected in their motivation and capability by the specific situations and by the temporal phases (before, during, and after the given event). There is also evidence that these relations are linked to the pressure caused by the event itself[253]. An extreme example are the differences in intensity and impact of the relationship between Protector and Threat before, during, and after a physical attack. Their resulting effects derive from the confrontation

[252] It is submitted that the concept of precision is relative to the level of analysis, and thus should not be confused with the concept of resolution. At a general level of analysis, a gross level of resolution may be precise enough for the necessity of reasoning. This concept is discussed in the chapters relative to management, decision-making process and problem-solving.

[253] Balloni and Viano, 1989; Holmes, 1985; Kellet, 1982; King and Brearley, 1996; Lev, 1992; Shalit, 1988.

between levels of motivation and of the sum of factors constituting ‘capability’ both at a technical and a tactical level. It is impossible to analyse how relationships will develop, and what effect they will produce, without taking many other factors into consideration. Such analysis is too precise to be relevant at the present general level of discussion. It is postponed to the discussion of an operational model of the security context.

2.5 FROM THEORY TO PRACTICE

2.5.1 Introduction

The security model established to date is an abstract one, where the actors behave 'aseptically' in 'laboratory' conditions, and undisturbed by external factors. It is useful in the identification and explanation of the fundamental mechanisms of a security context, but it is too simple to be translated into a security decision-making process. At that level, the problem is to analyse and understand the effects of identified dynamics in a defined state of affairs. To move from the theoretical to a practical level, it is necessary to introduce the factors which give the uniqueness to each security context. For example: nature and setting of the asset, resources, defences around that asset, local environment, laws, habits, political, social, psychological, managerial and economic conditions.

Any security context is a unique state of affairs, characterised by a set of parameters and variables which influence the processes between the actors. Each state of affair is altered by a change in any of its variables[254]. The number of variables may be infinite. They derive from the combination of the dimensions already identified as time, psychological, political and administrative. At the present general level of reasoning, a systemic rather than an analytic approach is appropriate, as not the single value of each variable is relevant, but their total effect on the basic model. Hence, their influence on the relationships between the actors is considered under the general term 'Situation'[255], and analysed as the resulting balance of all of its factors.

[254] The researcher does not accept in toto 'Chaos Theories', but personal experience in the Special Forces has taught the importance of apparently trivial factors. One moment of distraction of one single person may have disastrous consequences.

[255] *"set of circumstances or state of affairs, especially at a certain time"* (OALD)

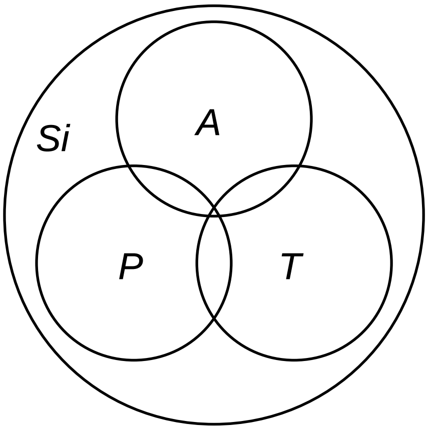

Figure 35: The Operational Security Context

The above diagram has been expressed by adding the factor Situation to the formal definition of security, as:

$$S_{(A)} = f\ (P, T)\ Si$$

The Security of a given Asset ($S_{(A)}$) is a function of the Protector (P), Threat (T), according to their specific Situation (Si).

The way the formula is expressed indicates that (Si) is viewed as a 'factor of efficiency' or, with analogy to the basic laws of motion, as a factor of 'friction', but not as a primary cause of a security process. The fundamental dynamics of a security condition are contained in the 'laboratory' model. Concepts as general policies and strategies, prevention, protection, reaction, vulnerability and damage have been identified and discussed. The analysis of the influence of the situational factors over the process becomes critical when it comes to translate general concepts into practice (planning of a security programme). (Si) is the 'here and now' condition that provides the cardinal parameters (identification, analysis and assessment of a specific case) to specify the operational reasoning. Because it affects perception, cognition, awareness, behaviours and operations within the security process without causing it, (Si) is not an addition to the process, but a characterisation by its influence on the basic actors.

2.5.2 The concept of Situation

Once A, P and T have been identified and assessed, the next step is to assess Si. The correct assessment of the situational factors is widely acknowledged in existing literature to be a vital factor to any security decision. [256] However, the operational evidence is that the Situation is often treated as a fixed factor. One reason is that security methodology makes a large use of quantitative procedures of assessment, with the result that numbers 'freeze' the appreciation. A second reason is that attention is more on its physical aspects (e.g. lay-out of defences) than on time, psycho-dynamics, political and administrative aspects. These are hard to define in numbers, and require specific knowledge not generally available to security professionals. This leads to the fact that, once an assessment's report is submitted, and/or physical defences are installed, the perception of Si tends to be assumed as fixed. The fact that this state of affairs is: (a) *naturally changing* by socio-economic-political dynamics, and laws of nature; (b) *deliberately altered* by both antagonists (P and T), is frequently neglected in security reasoning. This is normally concluded with a report, in which a series of suggested changes in the existing situation is suggested. The concept that these changes will provoke a modification of all the components of the context (A, P, Threat and Si) and that - after this modification - the whole context will need to be reassessed is rarely found in security studies. An attempt to predict how Threat will change after a modification of Si, or which modification of Si will produce the 'best' modification to T (the most suitable to P) is uncommon in the practice of security.

A, P and T are modified by the situational constraints, e.g. legal, social, political, economical, and environmental. P and T tune their plans, program and tactics to the setting of the Asset, and its surroundings. The influence of Si upon P and T is not uni-directional. A modification of Si can be used by P to influence T, and vice-versa. Protector and Threat modify the Situation to their advantage, notably through the installation and use of structures and systems. Each uses these modifications to alter the opponent's perceptions, cognitions, decisions, and behaviour.

[256] Adams, 1995; Balloni-Bisi 1993a, 1993b; Broder, 1984; D'Addario, 1989; Marcello, 1989

2.5.2.1 Relevant approaches

In Psychology, Sociology and Criminology, the influence of the situational factors is considered relevant, because they (a) affect perception, learning, awareness and behaviour; (b) configure the 'here and now' condition which informs reasoning and decision-making.

Of the many themes in these disciplines, those inspired by Lewin's field theories[257]. are the closest to the concepts of this research. The parallel was drawn by Professor Balloni in 1992, on the occasions of the 'SECURINDUSTRIA' conference and of the 'PRIMO CONGRESSO UNIVERSITARIO IN TEMA DI SICUREZZA' (1993). Professor Balloni found interesting similarities between the researcher's work (in security) and his own research (in criminology), common ground being the Lewinian field theories. These theories emphasise the importance of the dynamic and structured elements of personality within its particular environment (the life space[258]), and are used by Professor Balloni and Dottoressa Bisi to interpret behaviour of offenders and victims [259].

It is important to acknowledge that Lewin's theories are not generally accepted. His positions are considered as *'sharply holistic and dynamic, and, as such, somehow esoteric, by scholars with a more specialised approach'*[260]. However, they fit well within this approach, which appears to be the only one in security referring explicitly to Lewin. Evidence of application of Lewin's theories has been found in different disciplines than security, as marketing, cognitive learning and criminology. Some of their concepts are relevant. A description follows.

The Lewinian approach to consumer behaviour is associated with the '*Gestalt*' cognitive theory of learning, which theorises that the perceptual field contains individual stimuli that

[257] *'a broadly based set of theories all of which focus on the total psychological environment and attempt to explain behaviour on the basis of the dynamic interreactions between the forces in one part of the field and the rest of the field....Lewin's theorizing focused more on social psychology and personality theory. The field represented the total environment, including the individual and all significant other people and came to be known as the life space. Behaviour was represented as movement through the regions of the life space some of which are attractive (i.e. those with positive valence) and others unattractive (those with negative valence'* (The Penguin Dictionary of Psychology, 1985: 275

[258] *'The central notion in Kurt Lewin's personality theory. Influenced by the Gestalt perspective, he characterised the world of each individual as a dynamic life space composed of regions representing all the states of affairs, persons, goals, objects, desires, behavioural tendencies, etc., germane to the person. Lewin developed topological models complete with vectors and valences to characterise "movement", "directions" and "force" within the life space and hoped that mathematical models could be developed to formalise the system'.* The Penguin Dictionary of Psychology, 1985: 403).

[259] Balloni and Bisi, 1993a, b.

[260] The Penguin Dictionary of Psychology, 1985: 275

can be segregated from the total field [261]. In Chisnall's opinion, *'the Gestalt theory of cognitive learning the perceptual or cognitive field of a consumer may be of prime interest to the marketer'* considered *'as a problem-solver'*. Chisnall argues that *'By changing or adding to the cognitions held by an individual buyer , the seller is able to influence his choices'* [262]. He quotes Markin:

> *'This change of the cognitive field is, to the cognitive theorists, learning; thus the seller must more or less 'teach' the consumer to prefer his product or brand over those of competitors'*
>
> (Chisnall, 1995: 35).

This supports the researcher's submission that it is possible to 'teach the Threat', i.e., influence it (positively or negatively) by modifying the Situation. This process is caused by the activities of Protection and must be carefully thought of in the strategic phase of planning. The wrong approach may 'teach' the Threat to improve its tactics, or encourage her/his recourse to violence. Security measures should 'teach' the Threat and 'channel' her/his choices in a direction convenient to the Protector[263]. This reasoning can be explained by the offered formula:

$$S_{(A)}= f\ (P, T, Si)$$

Criminological approaches like those of Balloni-Bisi and Abrahamsen (see below) support this positions, and illustrate the relevance of the above formula to behavioural and situational analysis. In Balloni's interpretation[264], Lewin's formula of human behaviour is applied to criminal behaviour:

$$C= f\ (P, A)$$

where (C) stands for criminal behaviour, (P) is the sum of the personal characteristics of the actor, and (A) represents her/his total situation. This allows for a general explanation of criminal behaviour and offers an interpretation of different theories in primary crime

[261] *'The term 'Gestalt' was used to describe the fact that perception of an object involved an appreciation of its total nature. This derived from its part or configurations 'gestalten' and it in turn gave them meaning'.* (Chisnall, 3rd ed. 1995: 35)

[262] Chisnall, 3rd ed. 1995: 35

[263] Crime prevention theories on 'Architectural Determinism' are a good example of this approach. See: Maguire, Morgan and Reiner, 1994: 675, 676

[264] Balloni, 1983: 28,29

prevention[265]. In a wider sense, this view is also applicable in security to any source of danger, or Threat. This interpretation is supported by Abrahamsen, who postulated that

> *'A person's criminalistic inclinations and his resistance to them may either result in an anti-social or criminal act or in socially approved behaviour, depending upon which is the stronger of the two. All people have tendencies and countertendencies. A criminal act can take place only if the person's resistance is insufficient to withstand the pressure of his criminalistic tendencies and the situation'.*
>
> (Abrahamsen, 1967: 37-38)

Accordingly, a potential criminal activity can be assessed by means of a formula in which (H) human behaviour is represented by the sum of the actor's tendencies (T) plus her/his total situation (S), divided by the amount of her/his resistance (R).

> *'This mathematical formula is a concept which can be used in understanding criminal behaviour. Thus, if we substitute H (human behavior) for C (crime) we arrive at the same formula'.*
>
> (Ibid.)

Formally, Abrahamsen's formula is represented as:

$$C = \frac{T+S}{R}$$

This formula has the value of a logical formalisation. It is not intended to have mathematical precision (by which, for example, to forecast the occurrence of a criminal act, or identify the profile of the actor). However, it provides the researcher with a viable tool for understanding behaviour in antagonism, and a powerful explanation of the value of deterrence.

Apart from field theories, abundant reference to situational factors can be found in modern criminology. A summary has been provided in the CSPO Course notes for the Msc in the Study of Security Management [266]. More specifically, the authors state:

[265] For example, 'Lifestyle', 'Routine Activities', 'Rational Choice', 'Displacement', 'Architectural Determinism' and 'Crowd Control' Theories

[266] 'Left realism, and Establishment 'Administrative' Criminology', in CSPO Course notes for the Msc in the Study of Security Management, 1994, Module 1, unit 4

> *'Ron Clarke (1980) was perhaps the first to set out the 'situationalist' case fully; it was he who coined the phrase "situational" crime prevention'*

And follow with explaining Clarke's comments that

> *'...much crime is committed by ordinary people who spend most of their life engaged in lawful activity...He differentiated between the process of becoming capable of offending (on which criminology had concentrated almost exclusively) and the decision to commit a particular offence (a decision made by rational choice which could be influenced by opportunity reduction and other situational methods)'*[267]

Situational factors are seen in different ways at academic and professional levels. This can be explained by their different goals and focus. Academic research is mostly directed to analysing the influence of situational factors on motivation[268]. Situation appears to be related to opportunity, and influences the offender's choice. Operational literature focuses on the influence of situational factors on the vulnerability of defences and on the capability of the attacker[269]. This influence is widely deemed a fundamental security concept, underpinning the planning, organising and implementing of security measures[270]. An essential phase of security activity is the appraisal of the situation through audits, surveys and interviews. No decision making process is considered complete without this preliminary step.

In security the factor 'situation' may have different interpretations. In this research, 'Si' is seen not only as a 'passive' source of constraints and possibilities, but also as an 'interactive counterpart' with the main components (Asset, Threat, Protector) of the security context. It modifies, and is modified by, the actors and their processes, inputs and feed-backs within the given context.

The analysis of the situation from a security point of view leads to the identification of three fundamental environments. They are depicted as areas surrounding the asset and ranked in order of power of intervention and precision in assessment. A graphical explanation is offered below:

[267] Ibid.: 189.

[268] E.g., Gill et al. Crime at work, 1994 and Balloni - Bisi Grande Distribuzione, 1993

[269] E.g.,: Biasiotti, 1991; Broder, 1984; Gigliotti-Jason, 1984; Kluwer's Handbook of Security

[270] E.g., Biasiotti, 1991; Gigliotti and Jason, 1984; Sandia Labs, 1978; Walsh and Healy, 1996.

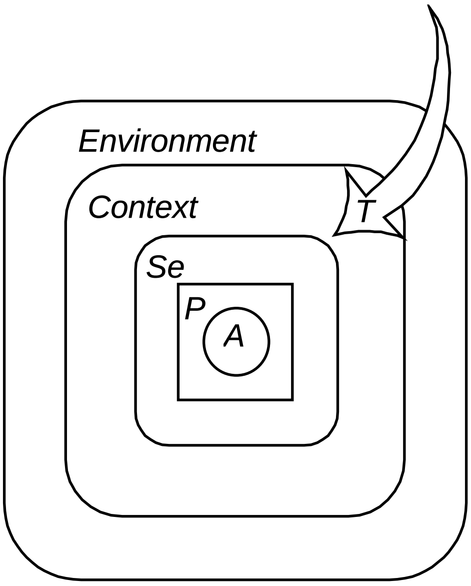

Figure 36 The three fundamental environments

The core of any security condition, is the <u>security environment </u>(Se), made up of the Asset, its setting and the security system (including the Protector, but not normally the Threat) and all which has direct influence on the security activity. It is the area under the Protector's responsibility, control and response.

The intermediate area is the <u>local environment </u>or 'micro-climate', which includes the normal presence of the Threat and all the factors influencing the dynamics of components: e.g. physical distribution, productive and organisational variables, internal and external relations. Its boundaries circumscribe the area where Protector, Asset and Threat interact. It is defined as the 'Context'.

The <u>outside environment</u> or 'macro-climate', is the area external to the Context, but which still influences its processes. It contains the political, socio-economic, legislative, normative and physical factors (morphology, topography, etc.), relevant to the Situation from the security point of view. It is described by the term 'Environment'.

The above diagram is explanatory. It depicts an instant when the Threat is not yet attacking the Asset[271]. The situational factors in security are not static, but dynamic, as the used concept of 'here and now' clarifies. Consequently, the dynamics and processes of a security context must be analysed on a temporal dimension.

2.5.3 The Interrelations

Having identified the main components and features of a security context, the next step is to analyse its dynamics. This phase requires an effort of simplification. It has been said that the interrelation of Protector, Asset, and Threat occurs at a multi-dimensional level, the basic process being influenced by the situational factors. The chosen methodology requires reasoning to proceed from the simple to the complex via demonstrable steps. An analysis at a multiple level is not necessary for understanding and would complicate the explanation. Consequently, the study is confined to the basic relations between Asset, Protector and Threat, and Situation is considered as a 'factor of efficiency'. Conform to the chosen methodology, all possible combinations are analysed. They are six, which can be grouped as following:

1, 2: Asset ↔ Protector

3, 4: Asset ↔ Threat

5, 6: Protector ↔ Threat

2.5.3.1.1 Asset ↔ Protector

The relationship between Asset and Protector is based on interest, and formalised by administration. Part of their relationship is influenced by the perception of the capabilities of the Threat. The quality of relation depends upon the nature of the Asset, and especially upon whether the Asset is a living entity (capable of perception, will, sentiment and communication). If the Asset is a living entity, the Asset/Protector relationship is a two-way process, reinforced through actions and communications. Feed-back causes continuous variation in the intensity (in quality and quantity) of their relationship. These variations are linked to the temporal phases, and become very sharp during the event. An example is the relationship between a bodyguard and the person protected, which not uncommonly develops within a range of emotions, from hate to love. This process of communication and the feed-backs have consequences to security. For example, the visibility and accessibility of the Asset as a target may be increased or diminished. Probably the most important variation is

[271] See: 'Verification of the Basic Context'

in the Protector's perception of the value of the Asset (mainly emotional), and consequently in the motivation to protect.

If the Asset is not a living entity, the relationship is one-way. There is no communication between Asset and Protector, only an appreciation from Protector. The relationship can be then considered to be fixed or constant, at least in the short term. The value ascribed to the Asset is a key determinant of the relationship. It is predominantly rational, though sentiment may increase the perceived value of the Asset.

2.5.3.1.2 Asset ↔ Threat.

The relation between Asset and Threat is based on interest (from the threat) and fear (from the Asset, if living). The Threat acknowledges the existence of an Asset; this implies an appreciation of its value. Most of the relationship between Asset and Threat proceeds through the Protector, and is influenced by the Threat's perception of the vulnerabilities and opportunities presented by the Asset and Protector. The intensity of the relationship depends largely on the nature of the Asset. If the Asset is a living entity (capable of perception and communication), then the relationship is two-way, and is influenced by communication. This leads to different levels of relationship in different temporal phases. At the first stage (before the event) the levels of interest and fear depend primarily on perception and cognition (of the value of the Asset, of the danger of the Threat). At the second and third stages (during and after the event) the relationship is mainly influenced by emotions provoked by the attack and its aftermath. If the Asset is not a living entity, then the relation is one-way, based only on interest. Its intensity increases (or decreases) over different temporal phases, according to the actions taken by the Protector.

The analysis of the relations between Asset and Threat during different temporal phases provides a good example of the importance of time factors in security analysis. One consequence of a successful attack is a change in the nature of the relations between A and T. If the Asset still exists (the attack has not been aimed at destroying, but at taking possession), then it becomes 'property' of the Threat. In this case, Threat transforms itself into Protector. Examples are the booty stolen by a burglar, a captive 'guarded' by her/his kidnapper, an information intercepted by a spy.

2.5.3.1.3 Threat ↔ Protector

The relationship between Threat and Protector is based mainly on fear and conflict. Its intensity is influenced by the perception of their respective vulnerabilities and capabilities. Part of their relationship proceeds through the Asset, and is influenced by the relative perception of the opportunities and vulnerabilities presented by the Asset.

The relation between Protector and Threat is a reactive process. Inputs are sent through actions and communications; their feed-backs (some of which may be highly emotional in the phase of conflict) cause variations in the quality and intensity of their relationship. The fear of the opponent and concern for her/his capabilities plays an important role. Whilst fear of the Threat may often have the effect of increasing the Protector's will of protection, fear of the Protector may deter the Threat, to the point of inhibiting her/his choices, and especially her/his will to proceed. However, this line of reasoning has important limits, which distinguish security from other forms of conflict, for example war. If the will of protection is to be understood, it is important to remember that security is risk-adverse and utility based, and that fear is balanced with interest.

2.5.3.2 The Effects

Once put into play (i.e. in a given situation at a given time), actors and relationships give rise to a vast number of effects. Those most important to a theory of security have been identified by both academic and operational approaches. They include motivation, behaviour, deterrence, capacity, vulnerability, opportunity, damage, and risk.

A short explanation their general interpretation in security is below. It is derived from the reference sources listed in the bibliography.

2.5.3.2.1 Motivation

Motivation is an elusive term, which can be subject to different interpretations[272]. In this research, it is important to distinguish firstly between the motivation of each of the actors,

[272] '*The most typical use of this extremely important but definitionally elusive term is to regard it as an intervening process or an internal state of an organism that impels or drives it to action. In this sense, motivation is an energiser of behaviour*' (Penguin Dictionary of Psychology, 1985: 454).

then between those underlying choice and decision (typical of the pre-event phase), and finally between those underlying action (typical of the event phase). This distinction can also be found in the following reference:

> *'… motivation is not a concept that can be used as a singular explanation of behaviour. Motivational states result from the multiple interactions of a large number of other variables, among them the need or drive level, the incentive value of the goal, the organism's expectations, the availability of the appropriate responses (i.e. the learned behaviours), the possible presence of conflicting or contradictory motives and, of course, unconscious factors'.*
>
> (The Penguin Dictionary of Psychology, 1985: 454.)

Practical experience and military psychologists [273] both highlight the enormous difference in motivation between routine and emergency. In security, this change can be easily seen in the behaviour of guards: routine checks and operations are conducted with a low level of motivation (if there is any at all, apart from salary). By contrast, when there is a state of alert, or an event, motivation is heightened by basic instinct (chase, fight or flee). The former relates mostly to administration; the latter has more relevance to response, especially combat (which plays a large part in intervention, in many security contexts). Further, there is evidence in literature that a change in the 'level' of motivation may interfere with pre-planned operations. For example, 'mental sets' and 'functional fixedness', which are created by training in pre-planned reaction (in specialist terms, IAD: Immediate Action Drills), have different effects on behaviour in test and in a real event. Hence the Threat may seek to exploit routine reactions by surprise attacks. This is often overlooked in security planning, with disastrous results.

Motivation is generally seen as a 'drive'. It was so considered in the preceding paragraphs. Some motivational drives are considered 'innate' (see Maslow's theory below), other stem from bad experiences, media, public debates, etc., and are generally linked to the paradigm known as 'risk perception'. This, and previous discussion of cognition, may explain why motivation can also be an 'interference', in that it may affect perception and reasoning. According to Glucksberg, a high degree of motivation can make people unwilling to alter their mental set..

[273] Kellet, 1982; Lev, 1992; Holmes, 1985: chapter 4; Shalit, 1988

> *'It seems that high motivation can make people unwilling to alter their mental sets - which might account why so many students continue to use old, passive revision techniques even when they know that their knowledge of memory theory and revising in a different way would be likely to produce better results'*
>
> (Glucksberg, as quoted by Hayes, 1994: 157).

Security-related research on motivation done by sociologists and criminologists has generally been in terms of 'drives' and from the Threat's perspective. Criminologists have researched the Threat's motivation extensively. Their scope has been explained by Gill, when he states:

> *'Ultimately, effective crime prevention depends on an understanding of how and why people offend: knowing why someone commits an offence gives clues as to how he or she can be stopped or deterred ... crime prevention measures which fail to take account of these aspects are unlikely to be fully effective'.*
>
> (Gill, 1994:5)

In the last three decades this subject has been frequently related with Threat's Behaviour, in approaches ranging from positivism to idealism [274].

The Protector's perspective is generally categorised by the paradigm 'fear of crime'. It is often stigmatised as irrational and with potentially dangerous consequences. From this viewpoint, motivation appears a source of constraints to security decisions, rather than a factor of improvement. The Protector's Motivation is seen by some as the product of a 'Vigilante' or 'Fortress' syndrome with effects leading to increase insecurity. Evidence may be found in leftish or idealistic sociological and criminological approaches, and in The British Crime Survey:

> *'Increasingly it is being said that fear of crime in Britain is becoming as great a problem as crime itself. Criminologists suggest that preoccupation with crime is out of proportion to the risks; that fear is needlessy reducing the quality of people's lives; and that fear of crime can itself lead to crime -by turning cities at night into empty, forbidding places'.*
>
> (British Crime Survey, 1983:22)

This view is not altogether unfounded, nor is it to be dismissed as simple cultural bias. Security, as Maslow's theories and its self-evidence may demonstrate, is an essential need for

[274] CSPO Course Notes, Module 1, sections 1-4; Maguire et alia, 1994: Part II; Gill et alia, 1994

the human being, since is the *sine qua non* of survival[275]. The basic principles of awareness, avoidance, and reaction are as old as mankind itself, and fundamental to the daily struggle for life. The well known 'flight or fight' pattern of behaviour suggests that they are closely linked to that of aggression. Evidence of this natural mixture of fear, rage, aggression and security may be found in the scientific studies of *'what scientists, perhaps by prejudgement, denote as "the seat of aggression", found in the area of the brain known as the limbic system'* [276]. According to the Keegan, who quotes as reference Groebel and Hinde (1989), three sorts of behaviour have been classified as having their origin in the same area of the brain, and identified as

> *"'instrumental or specific aggression', defined as 'concerned with obtaining or retaining particular objects or positions or access to desiderable activities' and' hostile or teasing aggression' which is 'directed primarily towards annoying or injuring another individual', also include 'defensive or reactive aggression' which is 'provoked by the action of others' "*
>
> (Keegan, 1994: 84)

Evidence suggests that motivation from both the Threat's and Protector's point of view can essentially be seen in terms of needs and drives. As Maslow [277] points out, not all of them are equally important at any given time. Instead, they are organised on a hierarchical scale, in which each different level of needs rests on the assumption that the one underneath has been satisfied. Only as each level of needs is satisfied, does the next level become important. Maslow represents these different levels in the form of a pyramid, at the bottom of which are the physiological needs (essential for body's survival), and at the very top, self-actualisation represents the point where all the needs of human beings are satisfied.

[275] Hayes, 1994: 435

[276] Keegan, 1994: 81

[277] Hayes, 1994: 435

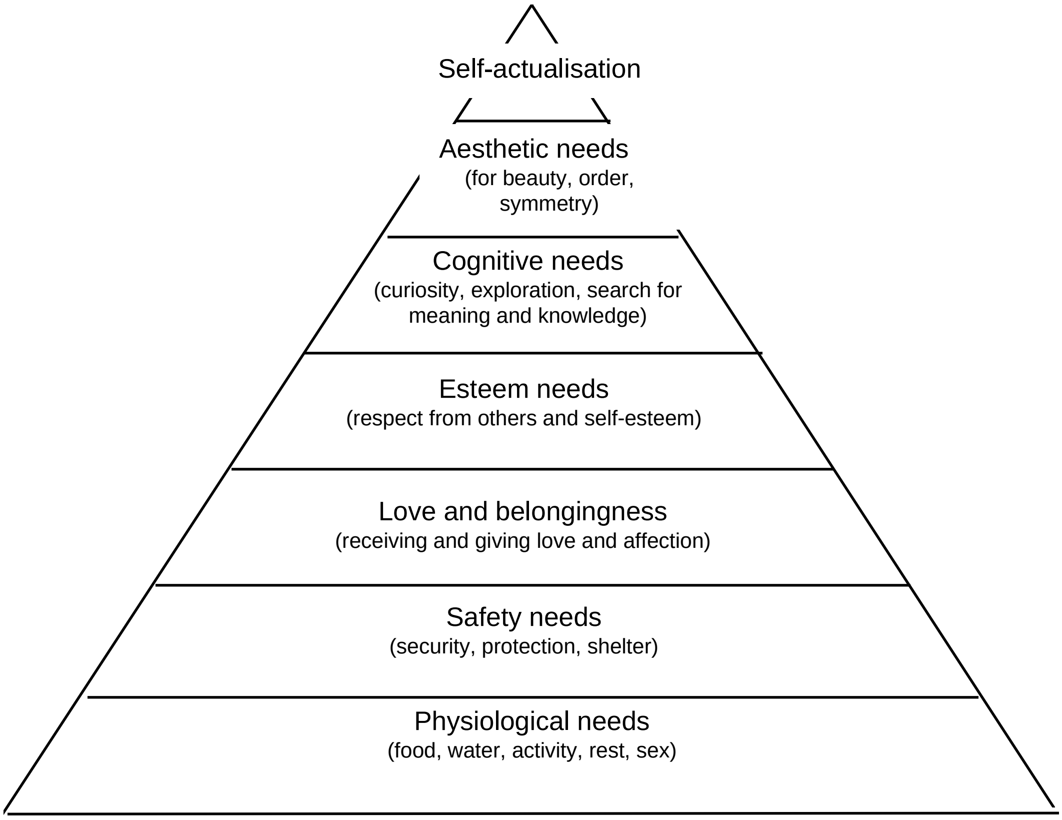
Self-actualisation
Aesthetic needs
(for beauty, order, symmetry)
Cognitive needs
(curiosity, exploration, search for meaning and knowledge)
Esteem needs
(respect from others and self-esteem)
Love and belongingness
(receiving and giving love and affection)
Safety needs
(security, protection, shelter)
Physiological needs
(food, water, activity, rest, sex)

Figure 37 Maslow's hierarchy of human needs, in Hayes (1994: 435)

Safety needs (in sense of security, protection, shelter) are put by Maslow at the level immediately above the basic need (physiological survival) and their satisfaction is considered essential. Interesting results can be obtained by comparing Protector's and Threats needs on the Maslow's scale. In civilised countries and situations (where it is not necessary to steal or rob to survive), the Threat's needs are less essential than those of the Protector. They are normally sited on the 4 top levels of the pyramid (from self-esteem to self-actualisation)[278]. This view is supported by research focused on Threat's needs and by professional experience.[279]

It may be argued that evidence of the non-essentialness of these needs can also be found in those security contexts where security measures are seen as an indication of social importance, or a 'status symbol'. This evidence is an example of an *apparent,* and not a *genuine* security context, being it driven by, and focused on, social, not security, priorities. These areas

[278] Gill et alia, 1994; Erickson and Stenseth, Oct. 1996

[279] Gill et al., 1995: 13, 25, 31.

merit further research. A comparison of Threat's and Protector's motivation could give insights into, for example, deterrence, fear and interest.

Motivating is perhaps as much art as science. The key is to convince security staff and, as far as possible, those they process, that the role is essential and to the general good. The motivation of security personnel is a difficult task for a number of reasons. Security activities tend to be repetitive, petty, poorly paid and unwelcome by other staff, visitors and customers. They involve unsociable hours and isolate operatives for substantial periods of their working time. The implementation of security procedures, for example denying access, searching bags, challenging people or even arresting them, tend to result in a 'vigilante' or a 'fortress syndrome'. Finally, security people are more likely to have a reprimand than an praise for their activity, and as a result most of them develop a cynical attitude towards 'the others', the organisation and the job.

Because of those problems, motivating the wrong people is likely to result in a waste of time and resources. Careful thought should be given to the selection of the right profile of people. Different ways have been found in security for motivating people, and the use of meetings, bulletins and social events is widespread. However, and quite obviously, the issues of salary, career prospects, training and compensation are considered the essential factors.

Motivation within an organisation is achieved by a number of ways. Examples are the careful allocation of tasks and responsibilities within the available functions; education and training; institutional and personal communication; control; and a system for compensation/correction.

2.5.3.2.2 Behaviour

Previously a battlefield for different schools of thought in Psychology and Physiology, the term behaviour is now used without a specific theoretical connotation[280]. A distinction between *'learned'* and *'instinctive'* behaviour is generally accepted. The former is essentially considered typical of the routine activities of security (e.g., those in the pre-event phase), and is mostly conditioned by learning. The latter is considered typical of emergency (i.e., in the

[280] *'A generic term covering acts, activities, responses, reactions, movements, processes, operations, etc., in short, any measurable response of an organism'.* (Penguin Dictionary of Psychology, 1985: 84).

event phase), and is consequently mostly conditioned by emotion, and, in the gravest cases, by a *'fight or flee'* syndrome. Much of the point of training is to prevent reversion to 'instinctive' behaviour under stress, for example in the presence of the threat.

An impressive amount of research has been carried out on behaviour in security-related topics. Threat's behaviour has been researched and analysed by criminologists and sociologists. However, apart from personal security, literature on the 'active' behaviour of Protectors is scarce, and generally relates to 'passive' behaviours that lead to 'insecurity' (victimology), or to 'active' behaviours that lead to 'aggression'. This is a useful initial step. Research and studies in victimology offer important evidence on 'insecurity' subjects, notably those who, having not realised the need to enter a security context, have become victims (because of their behaviour) of a Threat.

Williams gives an interesting summary of victim's lifestyle and behaviours[281]. Quoting Sparks, the author highlights six important factors: *'vulnerability, opportunity, attractiveness, facilitation, precipitation and impunity'*. However, Williams adds that not enough attention has been paid to the exact meanings of these terms. Past experience indicates that these principles, undefined, are sometimes used as a short cut to security through a list of do's and don'ts behaviour based on an imperfect vision of the principles of avoidance and protection. Victimology offers both useful and flawed view points on security. The understanding of inappropriate behaviour highlights the importance of the topic in security, and helps to identify appropriate security behaviour. Williams quotes government initiatives in 1990 aimed to explain high crime rates and to suggest that individuals alter their lifestyle so as to reduce criminality, and warns against a superficial interpretation of the above factors:

> *'Most of Spark's categories carry with them the notion that the victim carries some responsibility for crime. His message seems to be that potential victims should be encouraged to avoid dangerous situations for themselves or their property by staying indoors or keeping their property out of sight. If these cannot be avoided, they should protect themselves by only going out in groups, or in well lit streets, or by securing their property.....These suggestions not only push the responsibility for crime towards its victims, but would also be very restrictive on the liberty of the potential victims.'*
>
> (Williams, 1994 :106)

[281] Williams, 1994: 105

Also in security, behaviour is related to both knowledge (education) and experience (derived from reality, and training). Shaw quotes Diana Lamplugh, OBE:

> *'No one wants to become a victim of crime'. Yet, 'Crimes will and do happen. ...People who have built their judgements and consequent actions on informed knowledge, will consider any necessary avoidance as mature rather than wimpish. If there should be a crisis we find they are better able to react well at the time and recover much more quickly than those who had hidden their heads in the sand and shut themselves away'.*
>
> (Shaw, 1993:7)

The problem seems to lie in the Vigilante and Fortress syndrome, and in the general belief that 'security can be bought', therefore, provided systems and protection are installed, security follows independently of personal commitment. Says Williams.

> *'That is not to say that certain responsible measures such as locks on doors and good neighbourly activities which might reduce crime should not be encouraged, but it does warn against using these ideas ostensibly to protect the individual whilst actually vastly decreasing their personal freedom (see Morgan et al. 1994)'*
>
> (Williams, 1994: 106):

According to Balloni, the behaviour of a victim may be interpreted in terms of Lewin's theories:

> *'becoming a victim is a behaviour (C) that, as every other, is function of the person (P) in relation to a particular environment (A), in a given time'*(researcher's translation).
>
> (Balloni, Viano, 1989:20)

The above reasoning has been summarised in the formula: C = f (P, A). Balloni uses this to interpret the behaviour of any actor within a security context.

In this research, use is made of victimology concepts to help to explain the case where the Asset and Protector coincide, and security has failed because either, there was no perception of Threat, or there was no will (interest, need) to protect, or the Threat and Situation were not correctly assessed, or security decisions and activities were wrong. The explanation of the first two cases is that there was not a full security context. The last two cases, can be explained by failure of the decision making process and/or security operation.

One behavioural trait explored in security literature is awareness. The term has been used in psychology to refer to a wide range of subjective phenomena from simple, primitive detection of very weak stimuli to deep understanding of complex cognitive and affective events. These phenomena refer to different mental processes. However

> *'Although it seems clear that the mental processes involved in being "aware" of the presence of a dim light are fundamentally different from those involved in being "aware" of the underlying psycho-dynamic factors which motivate action, the same term is used to cover them all and the reader should be aware of this'*
>
> (Penguin Dictionary of Psychology, 1985: 77)

The viewpoint of this research is that awareness stems from perception, but is driven by interest and fear. Awareness being at the heart of prevention, it is worthy (together with perception, cognition and motivation) of the most careful attention in security studies.

2.5.3.2.3 Deterrence

The Oxford Advanced Learner's Dictionary defines deterrence as the *'action of deterring'* i.e., one that has the property to *'make somebody decide not to do something'*. Deterrence is an impediment to the Threat. This may be obtained through an appropriate demonstration of strength, awareness, or capabilities. It is important to distinguish the two forms, deterrence of action and deterrence to motivation. In their simplest forms, the former might be an impenetrable physical defence which deters action, but leaves motivation unaffected. The latter may be fear of legal retribution, the Asset being left unguarded. This distinction is important to the understanding and implementation of full-spectrum deterrence. The effect of deterrence is relative and depends on the level of both capability and motivation[282]. At the state of the knowledge, an appreciation of deterrence is necessarily qualitative. The difficulty in assessing the deterrence effect of security and legal measures on possible threats has already been discussed in Section I. Some techniques are offered in Section III. It is suggested that this issue needs further research.

[282] Erickson and Stenseth, Oct. '96; McCrary, 1997; Mc Kay, Dec. '96: 149-150; Wiersma, 1996

2.5.3.2.4 Capacity

In its broadest terms, capacity is a synonym for ability, that is *'the qualities, power, competence, faculties, proficiencies, dexterities, talents, etc. that enable one to perform a particular feat at a specific time'* [283]. In security, capacity is a multi-level concept, mainly related to pre-event and event phases. It represents the physical, intellectual and organisational abilities available to Threat and Protector, at both technical and tactical level. Experience shows that the capacity deployed rarely equates to the total available. The relationship between capacity deployed and potential capacity is a function of motivation and planning. Its effects depends on both motivation and capacity of the Threat, thus the capacity of the Protector must be assessed relative to that of the Threat. This assessment can be done, both from a technical and tactical point of view. Some useful techniques for assessing the technical capability of protective and detective measures have been experimented in Sandia Laboratories, and a set of tests is provided by specific standards prepared at national and international level. [284] Tactical capability can be tested by computer simulation models and field exercises. Penetration tests in sensitive areas are regularly conducted by special forces teams.

2.5.3.2.5 Vulnerability

Vulnerability is the exposure to potential harm or damage. In security, the concept of vulnerability pertains to all the components of the security context. The vulnerability of the Asset relates to the possibility of damage; that of Protector and Situation is an opening to the opportunity of provoking a damage. The vulnerabilities of the Threat relate to his own security. All of them should be considered in planning a security programme.

Vulnerability as a possibility of Damage depends on the characteristics of the Asset (physical, psychological, behavioural...). An Asset can be fragile, readable, exposed, unaware, etc. As a weakness of Protector and, more generally, of the Situation, vulnerability should be referred not only to the technical characteristics of the security system, but also (and mainly) to the tactical aspects that stem from its life and operations. As a weakness of the Threat, vulnerability opens opportunities to be exploited by Protector. Vulnerability is a relative idea, since it depends on the capacity of the antagonist, thus is very difficult to identify and

[283] The Penguin Dictionary of Psychology, 1985: 106

[284] Gigliotti and Jason, 1984; Sandia Labs, 1977 and 1978. Example of standards is BS 5750

quantify. For example, a professional Threat can always provoke or open new vulnerabilities, by means of intelligent diversions, or 'traps'. This peculiarity represents one of the reasons why, conceptually, a clear division between safety and security reasoning must be preserved.

2.5.3.2.6 Opportunity

In general terms, opportunity is defined as a good chance or a favourable occasion. In security, the concept of opportunity is intended as a vulnerability of the security system and an opening offered by circumstances to the Threat. With opportunity essentially being the exploitation of a vulnerability of the security system through a specific capacity, it is important to accept that a professional Threat can always provoke this chance or opening.

The reduction of opportunities is a main concern in security and in crime prevention. However, this assumes that vulnerabilities and opportunities have been identified, and requires the identification and assessment of all the relevant features of the elements of the formula (A, P, T, Si). Whilst the physical aspects can be easily recognised, there are difficulties in appreciating the qualitative aspects. Again, this peculiarity marks a difference between safety and security reasoning.

2.5.3.2.7 Damage

The OALD defines damage as '*harm or injury impairing the value or usefulness of something, or the health or normal function of a person; the loss of what is desirable'*. In security, this term relates to a variety of Assets and covers a wide spectrum of meanings, including loss, harm, injury, disclosure, death, bad image. Their values may not be described in purely monetary terms. Hence, it may be inappropriate to think of damage in terms of cost. This research views a damage as any change in the state of the Asset effected by a Threat and contrary to the wishes of its Proprietor.

The possibility of damage arises from the encounter between the Threat and Asset. This circumstance should be avoided or prevented, or at least should occur in the conditions least favourable to the Threat by means of protection and reaction. The damage inflicted depends upon the relative values of the vulnerability of the Asset and the capacity of the Threat. If the Threat has not the ability to exploit the vulnerabilities of the Asset, or if the Protector intervenes in time to cover, or shield, those vulnerabilities, then the amount of damage is limited, or zero. In security, experience shows that damage is very rarely maximum or minimum, but between the two. Post fact investigations demonstrate that the amount of damage is often influenced by chance . Examples are: a sudden movement of the Asset, a pistol that misfires, or a detonator which fails.

2.5.3.2.8 Risk

Risk has already been described as one of the most controversial concepts; its definition varies according to the theoretical approach and its paradigms. Problems come from the confusion between security, financial and safety concepts. In general terms, the concept of risk contains a combination of uncertainty and the negative consequences of an anticipated, hazardous event. Some of the most common definitions are: *'the possibility of meeting danger or suffering harm, loss, etc.'* [285], or: *'An action that jeopardises something of value. Risk and the role it plays in psychological phenomena have been studied intensively; e.g. "choice shift, game, utility and value"'*[286].. *'the probability that a particular adverse event occurs during a stated period of time, or results from a particular challenge'.*[287] In plain language, the term risk is frequently used to indicate a negative possibility: *'The risk is...'*. In security literature, risk is often used with different meanings: *'the uncertainty of a financial loss'* or '*"the thing insured" in insurance industry'*, or *'the possible occurrence of an undesirable event'* [288].

This research uses all of the above meanings, as appropriate to the context. The interpretation will depend on the context of discussion: those which refer to damage *'possibility*[289] *of damage'*, to vulnerability and opportunity *'possibility of failure or access'*, and to decision *'possibility of a wrong decision'*. These concepts are analysed in detail when it is considered relevant and necessary. The study of risk in psychology and risk analysis is relevant to security. In psychology, the concept of risk is often related to that of fear, and consequently to perception and communication. This issue has already been discussed. In risk analysis and in decision making, the concept of uncertainty is generally transformed, by a Bayesian interpretation, into

[285] Oxford Advanced Learner's Dictionary

[286] (Penguin Dictionary of Psychology)

[287] The Royal Society, 1992:2

[288] Broder, 1984:1

[289] There is an interpretation of risk as a 'probability' of damage, access, etc. This comes from financial and statistic terminology, and is widely used in safety. This line of reasoning has already been described as unsuitable to general security reasoning. Moreover, at this stage, it is not relevant to specify whether the 'possibility' may be calculated as a 'probability'.

one of probability. Risk is seen as an anticipated, negative event whose probability and impact may be calculated through qualitative or quantitative techniques. In this case, it is more appropriate to speak of 'indexes of risk'.[290] These techniques are the foundation of 'Security Management', and are a well-known decision making tool.

2.5.3.3 Summary

Further discussion of these issues is not relevant, at this stage. The essential task is to develop a global perspective, in order to understand the general dynamics of relationship between the actors in a security context. Experience shows that the dynamics relate to the temporal phases; they are influenced by different factors:

Before the event: dynamics are mainly influenced by perception. They are closely dependent on 'organised' decisions and, consequently, on administration. The relationship between Asset and Protector is largely based on an administrative model; that between the Threat and Protector are based largely on a conflict model.

During the event: dynamics are mainly influenced by perception and emotion, and absolutely dependent on actions. They conform to a conflict model, where necessity for speed may impede careful reasoning. In this phase, decisions tend not to be original, but to depend on what has been planned in advance. There is nevertheless a substantial group of real-time decisions (i.e., those taken under the pressure of the events), influenced by perception, emotion and instinct. These also can be assisted by appropriate training and education.

After the event: immediately after the event, the dynamics are greatly influenced by its emotional effects. After recovery time, the administrative model becomes once more the prevailing influence. The activities of this phase are mainly based on an administrative model. The time of recovery depends on the gravity of the event, on training and on precedent planning (crisis or emergency planning).

Two aspects are particularly important. Firstly, not all the possible effects 'automatically' occur in every event, either due to the efficacy of the security system, or because of a chance combination of factors. Secondly, it is possible by proper planning and preparation to

[290] Courtney, 1977; Makila, 1985; Miguel, 1984; Orlandi, 1989

channel dynamics, to avoid or minimise negative effects, and to take the necessary measures to minimise further (secondary) damage.

A general format illustrates the structure, dynamics and effects of a security context. This table is a tool of analysis. It does not purport to be a complete model.

Table 3 A Scheme of a Security Context

Scheme of a Security Context						
The Structure				**The Dynamics**		**The Effects**
Who	***With***	***When***	***Where***	***Why***	***How***	***What***
Asset	**Protector**	*Before the Event* *During the Event* *After the Event*				
	Threat	*Before the Event* *During the Event* *After the Event*				
Protector	**Asset**	*Before the Event* *During the Event* *After the Event*				
	Threat	*Before the Event* *During the Event* *After the Event*				
Threat	**Asset**	*Before the Event* *During the Event* *After the Event*				
	Protector	*Before the Event* *During the Event* *After the Event*				

2.5.4 Conclusions

Before proceeding to more practical issues, related to the application of the theoretical reasoning to practice, a summary of the work done and some conclusions are offered. They are as follows:

Operational security is a complex, unnatural condition. It is a product of antagonism. It occurs within a context where three basic elements are always present: an Asset, a Threat and a Protector and is influenced by the Situation. Both the Threat and the Protector are considered to be living entities. Their valency within the security context depends upon the value they confer to the asset (interest in gain, or fear of loss); it is affected by psychological, political and administrative factors. The will to avoid an undesired event originates in a perception of a source of 'worry and danger', and opens a security context The existence of a security context constitutes the criterion of demarcation between security and other states of affairs. Each security context is different. All the activities within this context are primarily produced by 'people' via specific 'principles', 'procedures' and 'functions'. They are supported by physical and non-physical factors, such as 'structures', 'systems', behaviours and 'intelligence', within a given set of circumstances (the Situation) which influence the whole process, from perception to action. Different dimensions are relevant to application of the 'theoretical' security context to practice, the most important of which have been identified as time, psycho-dynamics, politics and administration. The interrelations between actors and their effects have been discussed. A conceptual structure has been proposed. If its parameters (Asset, Protector, Threat, Situation) are known, then the given security context can be analysed and evaluated.

These findings are the product of a methodology based upon fundamental scientific principles. They came from a set of premises, formulated into hypotheses by deductive reasoning assisted by 'scientifically' acceptable tools, as Venn's diagrams and linguistic analysis, and have been tested against literary evidence. These premises do not come from intuition, but have been derived by the analysis of the existing body of knowledge of security, and by the professional experience of the researcher and selected colleagues. Existing approaches to security have been identified and related to the branches of Science (Section I, fig.4). Evidence is that security requires a multi-disciplinary approach, involving both physical and non-physical sciences. The theoretical approach of this research is positioned within the Social Sciences, alongside Criminology, Politics and Sociology.

Figure 4 identifies the fields where existing theories and disciplines provide (or could provide) relevant contributions, and also help corroborate the findings of this research. The contribution of other branches of sciences, especially the natural and physical sciences, is important to the application of security theory. Evidence has been provided in the course of discussion that this contribution is not always perfectly clear, and some areas have been considered as needing further research.

Methodology requires the testing of these conclusions. The most disputable concepts, particularly the 'psychological' and 'political' aspects of a security context, have been analysed. This analysis has shown the dominance of human over technological factors in security. Human factors and activities - not structures and technological systems - perceive, plan, obtain and maintain a security condition. However, structures and systems are unquestionably necessary, to enhance human capabilities and systemise most of the routine activities of protection, detection, and reaction. Nevertheless, and however important they may be, structures and systems must be driven by security needs and priorities. Most important of all, no system has the capacity of contrasting an imaginative and reactive counterpart.

Therefore, all physical and technical factors are considered to be subordinate factors, or tools. The existing literature stresses that 'software' factors: motivation, survey, analysis, assessments, decisions, planning and behaviours are primary and the 'hardware' factors such as structures and systems are secondary. Accordingly, psychological and political areas are considered at the conceptual level, and the technical and managerial areas at the functional one.

The complexity of including all of these factors in a general explanation of the basic security concepts makes the 'laboratory' model impracticable. They are therefore considered within the concept of 'Situation'.

Having supported this approach with existing theories and evidence, the '*falsification*' process requires this postulational system to be tested by experience. It is submitted that this test can only be done by application to a security problem. This requires a methodology to be designed in accord with the theory. This methodology is offered in the next Section. It consists of two steps, the outline of a decision-making process and then the formalisation of the findings into a model.

One final consideration follows. The crucial tests of the scientific value of this approach are those of explanation and prediction; that is, whether its general principles apply to different security situations. It has been stated in previous discussion that, due to the absence of an overall theory, security cannot be considered as a science. An attempt has been made in this research, by providing a framework of understanding and a security focus to the disciplines identified as relevant. The attempt itself, even if unsuccessful or incomplete, makes a first step towards a security science.

SECTION III

THE METHODOLOGY

3.1 INTRODUCTION

Having set '*a priori*' the general and particular premises, scientific methodology requires them to pass the test of validation *'a posteriori'*. For the *falsification* of assumptions and inferences, two different phases of control have been considered relevant against the literary evidence, and against the experience. The first phase having been undertaken via the discussion of the relevant positions at the theoretical and empirical levels, it should now be the moment to verify the proposed approach against experience. This cannot be done immediately, by using the existing methodology, which has been described as unsatisfactory and considered inconsistent with the offered theory. Thus, the next step is to provide a set of instruments which, by allowing the application of the theory to practice, assist the verification of both the process and the results. Having defined security as a rational process, the most useful instruments are a decision making methodology and a model of a security process. Both instruments derive from the theoretical approach presented in Section II. Decision-making methodology provides a rational path of reasoning to assist the processes of analysis and planning, as well as the control and justification of each step. The model helps to understand where decisions need to be made - or changed - as it assists the understanding and explanation of the structure and dynamics of a security process. Furthermore, it assists the translation of the approach into appropriate computer models, so to allow, for example, the simulation of well structured cases and the construction of 'what if' scenarios.

Field tests have not been attempted in this research. One reason relates to the nature and scope of this research. This is primarily a structured analysis of security related literature, aimed at building the groundwork for further and more detailed study. Moreover, security takes many forms; the scientific treatment of a meaningful number of case studies would be an extensive project, and a research in itself.

Consequently, the analysis is confined to the context of security management. Both the process and the model are delineated only in those characteristics relevant to explain and to evaluate the theory. The test against experience is limited to the discussion of the model, and to offer the academic and the operator with a means of interpreting their work. Reference to the most used security approaches and conceptual verification by comparison with the existing body of knowledge have been provided when relevant and possible.

This Section is divided into three sub-sections: the first defines a methodology, and identifies its aim and scope. This step is made via the investigation of the management process and the analysis of a decision-making process, and identifies their main features in a security context. To conclude, it examines the application of the proposed theory to problem-solving. The second sub-section describes the formalisation of the theory into a model and discusses its application. This requires a discussion on whether a model can be induced through which it is possible to interpret, and reasonably explain, the majority of cases. The nature of the relationships between the decision-maker and the model builder is analysed, and the difficulties of interpreting another person's thoughts into mathematical models are discussed. A procedure for translating requirements into modelling with the minimum of interference is outlined. The third, and conclusive, part discusses a general example of application. A model of a security process is offered, on which security problems can be analysed, and which can be used as an 'experimental set-up' for research and verification. All of the discussion is combined with the explanation of *where* and *why* the existing techniques are appropriate. The utility of the general concept is measured by its capability to supply a security focus and a scope to the existing disciplines. Therefore, the model offers a general check of the concepts submitted in this research.

3.2 THE METHODOLOGY

3.2.1 Premises

To meet the conditions of justification and falsifiability, a security methodology must start from clear premises. In summary, the premises are as follows:

The condition of security is the result of the activities of opposed counterparts; it is aimed to achieve and maintain an advantage over the opposite forces. In a security context the actors are influenced by changes in the security situation. This concept is represented in the following diagram:

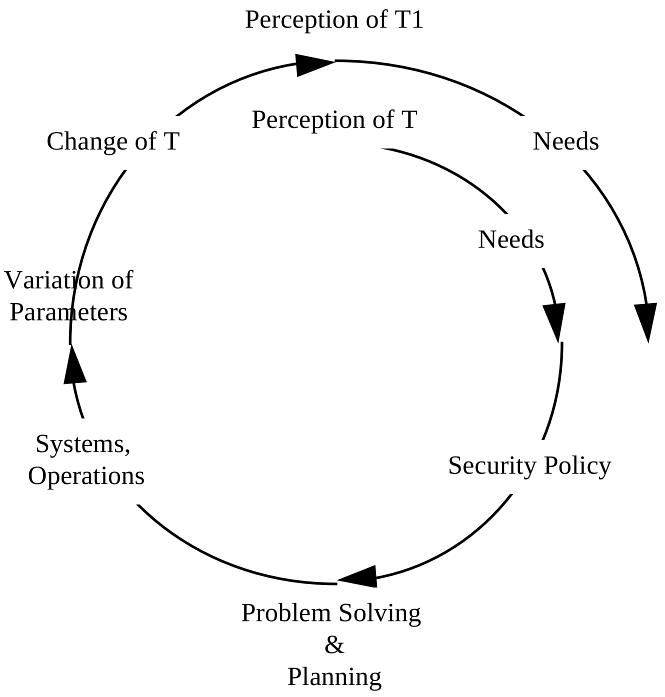

Figure 38 The Security Cycle

In all the phases of a security process the Protector (P) and the Threat (T) follow their own process, relative to the Asset (A). Both the Protector and the Threat endeavour to use the Situation (Si) for their purposes, and react to perceived changes. P strives to maintain control of the context, reacts to new perceptions of T (T1) or to a change of A by modifying Si, and similarly does T. Therefore, a security process comprises two concurrent and conflicting sub-processes, one 'protective', the other 'aggressive', in regard to a particular Asset. Both sub-processes are relevant to the explanation of the dynamics of the antagonism. This is allowed by the analysis of all the components of the formula S(A) = f (P, T) Si.

In the protective sub-process, the perception and cognition of a Threat leads the Protector to the decision to react. In the aggressive sub-process, the perception and cognition of an Asset, which includes those of its Situation and Protector, leads the Threat to the decision to acquire the Asset, while avoiding, or protecting itself from, the perceived Protector.

The intention of the Protector to safeguard the Asset opens a security context and, thus, a security problem. This problem has different focuses and goals, according to the position of the solver. Both P and T are solvers. There is a tendency, in security, to refer to the figure of the solver as the Protector, and to ignore Threat as a solver. [291] Although this line of reasoning has its foundations in both the focus and the purpose of security, two major objections have been identified. Firstly, the concept of security is independent of legal, moral or social considerations. Second, a premise to this research is that in practical security (P-S), both security (S) and insecurity (?S) coexist. Defensive and aggressive processes subsist in both the Protector and the Threat. The Protector's problem is that of restraining, or neutralising, the Threat. The Threat's problem is that of acquiring the Asset without suffering unacceptable damage. [292] The security problem of the Protector is centred on the Asset. That of the Threat (not to be confused with her/his 'aggression' problem) is centred on her/himself (seen as the Asset). Threat's decisions influence, and are influenced by, those of the Protector. A security methodology must take into account both sides of the relationship.

This reasoning has been represented in the following diagram:

[291] see, for example, Broder (1984). For a contrary position in criminology (Rational Choice Theory), see McGuire et al.,1994: 497-498 and Wiersma (1996)

[292] The extreme case of a 'kamikaze' threat is not considered consistent with the concept of security offered in this research, but with that of war.

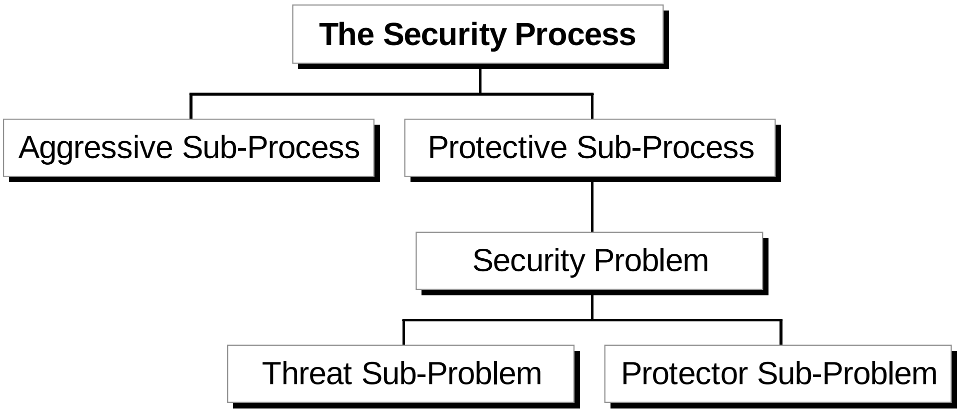

Figure 39 The Security Process

A second set of assumptions is that the solver of a security problem deals with a complex and dynamic condition of uncertainty, based on antagonism and influenced by the situation and the environment, themselves changing. In such a context, a number of features may be identified, such as the existence of different criteria, beliefs and desires, sets of values, multiple levels of analysis and scarcity of information. The questions are: How can a theory be applied in such conditions? Even assuming that the proposed theory is applicable, what can its utility be, if decisions are taken in such conditions?

Different ways of answering these questions are possible, the most immediate being that of identifying the issues to be covered from the rise of a security problem to its solution. This demands the investigation of how a security process actually evolves, the understanding that such process is marked by a series of decision-making exercises within a framework of management, and the identification of how decisions are implemented into practice. This topic issue is commonly described in literature and practice as 'Security Management'. Thus, the next step is to discuss the general principles of management and to analyse how these principles are applied to security.

3.2.2 Management

According to Cole, there is no generally accepted definition of 'management', since the variety of approaches to its theoretical background have produced their own version of what this terms means. Dictionaries reveal it as an extensive concept, including all the activities related to the 'handling' of processes and organisations. Different definitions may be found in management literature, but the classic definition is still held to be that of Henry Fayol:

> *to manage is to forecast and plan, to organise, to command, to co-ordinate, and to control.*
>
> (Cole, 1993: 3)

Management is considered, in this research, as the process of 'handling' a process or an organisation with the intention of achieving a given set of results. [293] This is done by way of a succession of assessments, decisions, plans, implementations, and controls. Results achieved are then evaluated against the efforts, the needs and the expectations, which brings the process to a new cycle.

The concept of management may certainly be applied to individual activities, but it acquires its full sense within the context of an organisation, i.e., *'a group of parts, people, arranged into an efficient system. '*[294] Professor Handy suggests that a manager has to deal with some key variables, identified as People, Work and Structures, Systems and Procedures. [295] He states that these variables cannot be dealt with in isolation, but as an open system within the constraints of an environment. Modern organisations receive inputs such as information, pressures, rules and requirements; their operations produce outputs which have some effect on the environment.

In Handy's systemic vision, three crucial components are identified: the Goals of the organisation, the Technology available and the Culture of the organisation. People interact within a structure according to human relations, operate to achieve a stated purpose, and are influenced by some internal and external interference of social, political and economic nature. This interference is reciprocal, as a change in one part of the system will inevitably lead to a change in one or more others. This systemic vision of the organisation has been adapted to include the security function by an Italian sociologist, Livio Pinnelli. [296] In his system, the security function is both a 'covering umbrella' of the organisation and an interactive function with all departments and the external world.

[293] This is often referred to as 'teleological planning'. Modern management (particularly at the strategic level) may work without a fixed end.

[294] OALD

[295] Handy, 1987. Also Argyris, 1960; Pugh, 1971.

The condition of open system introduces within the process some external criteria and constraints, which must be balanced against those typical of the organisation. For example, management has been criticised for contributing to environmental and social problems because of its narrow definition of a cost-efficient process. The costs of pollution control and the social impacts of policies and production are now added to the traditional costs of raw materials, capital, and labour. Security managers experiment similar problems: criticism to organisations is moved by those who suffer the 'displacement effect' of 'too effective' security measures. [297]

3.2.2.1 The Management Process

The management process is widely seen in shape of a loop, where all factors are balanced in a way that meets the needs and expectations of the organisation, and feed-backs give start to a new cycle. This concept has been represented by Yoder and Honeman: [298]

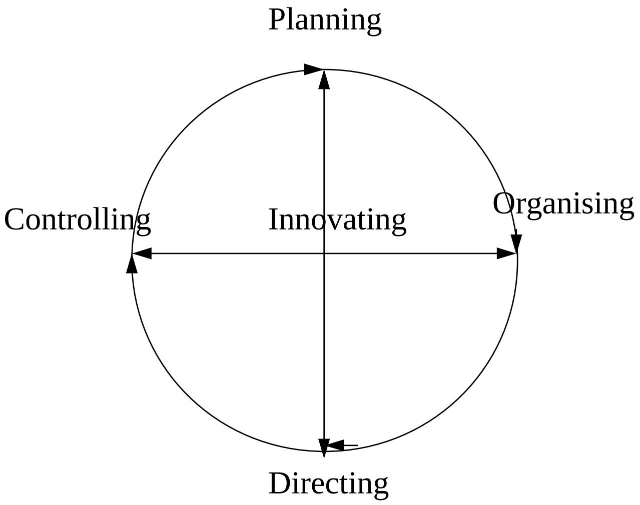

Figure 40 The ASPA Management Cycle

Their model highlights the overall function of a manager, which is that of co-ordinating all the efforts of the organisation. The activities of planning, organising, directing, controlling, innovating are interdependent, so that one weak, or too strong, link affects the result of the

[296] Pinnelli, 1988

[297] Maguire, Morgan, Reiner, 1994: 677-8; Williams, 1994: 407

[298] Yoder and Honeman, 1979.

loop. For the effectiveness of the process, all activities must work well, re-transmit the received impulse and be balanced in their strength and effectiveness. The loop receives impulse from each cycle, which means that important lessons and achievements are not lost in the process. The role of innovating, which affects all other components, is essential to adapt the organisation to change. A brief description of the activities of planning, organising, controlling, innovating follows.

3.2.2.1.1 Planning

The concept of management requires that the organisation:

- Knows why it exists and what its aims [299] are.
- Has a clearly defined mission. [300]
- Knows what its own strengths and weaknesses are.
- Knows what opportunities and threats are posed by its external environment[301]
- Has a set of rules of conduct (policies) to guide its employees in the pursuit of its objectives.
- Has a set of directives,[302] to achieve missions, goals,[303] and intermediate objectives. [304]
- Can identify, establish and control appropriate standards of performance.
- Has the flexibility and the resources to take advantage of changes and to face crises. [305]

This set of requirements is satisfied through a process of planning which, according to Cole, is centred on the key issues of *ends*, *means*, and *conduct*, together with their associate *results* and

[299] A single, unambiguous purpose that must be established before a plan can be developed

[300] An unambiguous, concise statement of the organization's task and its purpose.

[301] A geographical area, including both the area of influence (where the organization is directly capable to influencing operations) and the area of interest (the general area of concern, adjacent to the area of influence, and extending to the area of future operations).

[302] Official instruction containing the strategic goals, conditions for success, political and social constraints, financial limitations, responsibilities, and available resources

[303] An expression of broad meaning embracing aim, mission, objective, and purpose, here used to define the final objective, or goal, of each directive

[304] The series of situations, conditions, or states of affairs, to be subsequently achieved according to specific priorities, in order to attain the goal and eventually fulfil the mission.

[305] Cole, 1993: 109-110

feed-back. The planning process depends on the availability of means and on correct information, and follows a top-down approach. It starts with a consideration of the ultimate aims of the organisation, i.e., *ends*. Once an organisation has established its *ends* and defined its mission, it is necessary to explain how they are intended to be achieved. A prior consideration of *conduct* should be made, in order to define *policies*, or codes of conduct, to be applied to subsequent stages of planning. [306]

3.2.2.1.1.1 Policy

Policy statements are made to indicate to those concerned what the organisation will, and will not, do in pursuance of its overall purpose. Policies are not the same as objectives, plans, or actions. [307] Objectives are *ends*; plans explain which measures must take place to attain objectives, i.e., they are *means*; policies cause people to decide and act in a certain way, but they are not *actions* in themselves. Policies are *statements of conduct*, and may be expressed in a number of different ways according to the organisation's culture and belief-system. Some relate to ethical and philosophical issues, others are more concerned with operational issues. In this research, a policy is both a statement of premises concerning mandates and limits, and a guidance for the use of efforts and resources. With aim and mission, a policy statement is assumed as a constraint to planning and decision-making.

A policy summarises the belief system of the organisation, which on turn is affected by the attitude of the organisation's owners and general managers. International, national, and local laws, regulations and standards; socio-political and cultural aspects; local powers, organisations and customs all play a part in determining an organisation's policies. Given the importance of PR and the pressures of media, lobbies and groups, particularly on matters as community and environment, one important area of modern policies is that of 'social responsibility'. Being 'socially responsible' implies playing more than just an economic role in society and, given the public's expectations, this role tends to be that of 'good neighbour'. [308] Organisations are increasingly expected by society to play, in addition to their roles as

[306] "*Planning is an activity which involves decisions about ends as well as means, and about conduct as well as results. Planning is a process which has to start at the top. Whatever else may be planned at operating and administrative level, the first priority has to be given to the strategic goals (ends) of the organisation*" (Cole, 1993, 4th ed.: 109)

[307] Cole, 1993: 111

[308] Leivesley, 1995b

employers and producers of goods and services, a distinct role in meeting community needs in social welfare, health and environmental matters, and in security schemes. [309]

A security policy is the specific interpretation of the organisation's overall policy. Similarly, it starts from well defined aim and mission and is a statement of conduct, meant to guide -from a security point of view and with security rules of conduct- the organisation's managers and employees in the conduct of its affairs. The systemic vision of this approach means that a security policy is not specific to the security function, but to all people working within, for and with the organisation. External consultants, partners and suppliers are an example. This exigency demands a security policy to be general enough not to interfere with specific different necessities.

Once aim, mission and policy have been determined, a series of controls are necessary, to verify their consistency and congruity. For example, a policy of openness and transparency can be incompatible with a mission which requires covert or clandestine operations. A second reason for this is to be sure that enough efforts and resources can be dedicated to pursue the stated aim within the constraints of the policy and mission. In the case of negative assessment, some or all of the three elements examined (aim, mission and policy) must be changed until congruity and feasibility are ensured. A policy which respects the environment, privileges safety and pursues friendliness with neighbours and customers usually requires more efforts and resources than one which does not. Examples of different policies leading to different costs and effects are the security requirements in commercial aviation and supermarkets in Western and in Eastern Europe.

3.2.2.1.1.2 Strategy

Assuming aim, mission and policy have been stated, the next step is that of implementing them through a consistent strategy. [310] A strategy is concerned with the achievement of goals (*ends*), preparing the framework (*means*) within which actions (*conduct*) can take place. It is :

> *'The practical adaptation of the means placed at a general's disposal to the attainment of the objective in view'*

[309] As an example, see the article: 'MOBILE ARMY AGAINST CRIME, The Star (Bath newspaper), 25 January 1996, where a cooperation scheme between companies such as Wessex Water, British Gas and The Avon and Somerset Constabulary is reportedly aimed to 'encourage staff to use their radio telephones to report any incident they see'.

(Von Moltke, as quoted by Liddel Hart, 1967: 320).

Strategy decisions are typically (though, according to Noorderhaven, not only) undertaken in situation of antagonism, conflict or war, and their outcome has been described by Noorderhaven as simultaneously 'momentous and uncertain'. [311] This circumstance explains the use of military terminology and, to a certain extent, methodology, in decision making and management literature, and in common language. The term strategy has different meaning for different people and contexts. With this being not the place for an exhaustive discussion, the Chandler's position (as quoted by Cole) is accepted:

> *"Strategy is the determination of the basic long-term goals and objectives of an enterprise, and the adoption of courses of action and the allocation of the resources necessary for carrying out these goals."*
>
> *"Strategic management is the process of determining, evaluating, and adapting the aims, or mission, of an organisation and the patterns of decisions that guide the achievement of those aims in the long-term."*
>
> (Chandler, as quoted by Cole, 1993: 102)

Noorderhaven defines a number of features common to strategy and strategic decision-making: the fact that the choice of a strategy does not follow automatically from the ultimate goals pursued; the role of subjective assessment of imperfect or incomplete information; the fact that the actual implementation of a strategy can lead to quite unexpected results, since it deals with surprise and changing plans; and the evidence that strategic decision making is not only based on rational calculation, but also on moral values, and emotions, and possibly also intuition. [312] These characteristics apply to all states of affairs where antagonism exists, from war to security and business. However, relevant differences exist in the level of commitment, use of the means, final ends, approach to the counterpart and, particularly, criteria and constraints.

A business organisation will, in its strategy, typically define in which markets it wants to compete, with which products or services and according to which conditions; a governmental organisation will probably demarcate its duties and fields of competence; an organised group

[310] The word 'strategy' is derived by the Greek στρατεγια: 'strategia', which means military command and has been used since V Century BC in the sense of 'the art of generalship'.

[311] Noorderhaven, 1995:2

[312] Noorderhaven, 1995:2

(as a security department within an organisation) will specify the interests it wants to promote and the means it will use.[313] Two important issues need to be considered in the process: the performance of the organisation and the influence the environment will have on its future actions. Both are generally considered under the technique SWOT Analysis. Performance is then appraised under the headings of Strengths and Weaknesses and the environment is estimated in its Opportunities and Threats. Similar techniques of appraisal are applied, *mutatis mutandis*, in formulating security strategies.

The security strategy within an organisation is intended to achieve the stated mission under the guidance of the security policy and consistently with all organisation's activities. It determines the means and courses of action necessary to ensure the organisation the freedom of action necessary to the fulfilment of its goals and the pursuit of its interests, within a secure environment. Both the concepts of 'freedom of action' and 'secure environment' are equally important. Experience shows that a strategy that is limited to ensure a secure environment tends to become a 'passive' umbrella, and to be criticised by top managers. With ensuring freedom of action to its organisation, security becomes an active part of the organisation's efforts towards success and profit. When the organisation is an open system, the relevant actors and dynamics of the environment, as well as the functions within that environment, must be defined before preparing a strategy. Attention must be paid to all the parts interacting, e.g., competitors, clients, stockholders, employees, local, central and international authorities, the media and the public. This obligation imposes significant constraints upon security decisions. More is offered later.

3.2.2.1.1.3 Programme

Once strategies have been set, the next stage of planning involves decisions about *means* and *actions* . This requires the formulation of a programme. A programme is a detailed plan of what is intended to be done, and is about the correlation of resources with specific activities aimed to achieve certain results within well defined times and costs. Once the programme has been approved, each activity is then analysed in detail and developed via specific projects directed to its implementation.

[313] Cole, 1993: 101-9

3.2.2.1.1.4 Implementation

Once plans have been implemented, their results are monitored and analysed to provide feedback to the relevant stages of the process. The concept of management requires this analysis to be largely focused on the pursuit of efficiency. This concept applies to all phases of planning, and requires rational decisions to be developed through a structured approach (management science), which is assisted by qualitative and quantitative techniques. [314] The possible options are analysed according to different methods, and computations have greatly been facilitated by the advent of computers. This approach is used to establish optimal policies, set production schedules, determine the most profitable mix of products, analysing systemic problems, optimise queuing and searches, assist and calculate shortest-distance shipping patterns. A large part of these techniques is also used in security.

3.2.2.1.2 Organising

The process of organising is closely linked with that of planning.

> *Plans have to be put into operation. This involves detailed organisation and co-ordination of tasks and the human and material resources needed to carry them out. A key issue here is that of formal communication.*
>
> (Cole, 1993: 7)

Management theorists have two different views of organising, responding to the ‘classic’, or ‘bureaucratic’, and the ‘human relation’ approaches. [315] Bureaucrats tend to concentrate their attention on the organisation’s structure and all that is required to sustain it (organisation charts, responsibilities, procedures, communication channels, reporting etc.). Human relation theorists believe that it is people who makes the organisation, and tend to dedicate their attention to issues of groups and individual needs before other issues as structure, authority levels, and decision making. The security function is generally organised according to the ‘bureaucratic’ approach. This is because of the background of many security managers (police, government or military) but also because, more than others, the security function needs well defined roles and rules, immediate action, and requires the exercise of authority

[314] Management science, originated in USA circa 1910, was applied to solve WW II logistic problems. Mathematical models were developed to analyse resource allocation, production scheduling, and logistics problems, and founded the basis for the development of Operational Research, now providing many of the analytical tools used in Management.

[315] Cole, 1993: chapter 24

even at the lowest level. These advantages (which are vital in emergency) tend to backfire in the hands of less trained, or power-motivated people, whose rigidity may be interpreted as trivial, invasive, and sometimes, offensive.

The first step of organising is via the attribution of responsibilities and consistent levels of authorities. This is usually achieved at the strategic level through the definition of the relationship of the security manager to the main board and other departments. This relates to the importance attributed to the security function, and has relevance to the position of the criterion of security within the decision-making process. At the administrative level, responsibilities and levels of authority are clarified through the preparation and dissemination of procedures, which at tactical level takes often the form of a manual. A security manual may be a stand-alone, or independent work, or may be developed as a section or chapter added to other department or functional manuals. The latter solution has the advantage of spreading the security culture within the organisation, and that of gaining credibility and acceptance, being it a signal of its importance within the organisation.

The organisation of a security department includes its position within the organisation, and the definition of its functions. The two are related, since the number and complexity of functions depends on the importance of the department, and vice-versa. The general tendency in those organisations where the concept of security management is dominant, is towards including all functions related to the protection of assets. For instance, business intelligence and counterintelligence, auditing, risk and insurance management, safety, technical engineering, investigation, personal protection and guarding. This concept responds to those of system approach and economy of efforts, attracts highly qualified personnel, and is welcomed by those security managers who see in it the opportunity for being admitted in the boardroom.

Where the concept of security management has not been fully accepted, security functions are normally fragmented and dispersed within different activities, such as accountancy, personnel, plant engineering, R&D, contract administration, fire department, and guarding. This position tends to increase costs, wire-crossing and duplication, and prevents the systemic vision needed for an integrated approach. Besides, it attracts low qualified managers, because of the limits of job contents, responsibilities and career opportunities.

Looking at the structure of organisation, corporate companies with presence in different geographical areas tend to structure their departments according to two extreme positions, centralisation or decentralisation. These positions tend to derive from the culture of the organisation, which may be prone to develop in a vertical, or an horizontal direction. The discussion above of the bureaucratic and human relations approaches is relevant to this. However, even in a decentralised structure a department may have a bureaucratic structure. For example, all security-related matters of a given area could be reunited under a unique local department, and respond to a sole manager. Different pro and contra have been identified for and against these positions: they may summarised as follows. [316]

The main advantage of centralisation is a better position of the head of the security department, who may report to a top manager, or even to the board of directors. Other advantages are unity of concepts and training, freedom from local interference and intimidation, better allocation of resources, a wider base of data, and an homogeneous system for measuring performances. Disadvantages are a tendency to bureaucracy and rigidity, which may bring after time lack of initiative and flexibility, difficulty in motivating and communicating, and limitation of freedom of action and responsibilities at the local levels.

The main advantages of decentralisation are timing, freedom of action, and initiative. However, the attribution of responsibilities at local level means that security managers report locally. Security problems will then be represented to top management by non-security people. Apart from the obvious communicational problems, this situation tends to create too strict local loyalties (a sort of 'us and them' syndrome), imperfect knowledge of local problems from the top management, differences in concepts, vision and training, and some difficulty in measuring performances. Those advantages/disadvantages are not necessarily mutually exclusive. It is possible to organise decentralised departments of security, which receive technical directives from the centre, and report all information also to the centre as a matter of procedure. Advance in information technology allows this arrangement to be made with minimum problems.

The establishment of a standard method of reporting is the second and essential step in organising a security function. This has a number of advantages: computers can collect and store relevant data, reports improve communication within departments, and prepare the

[316] Barefoot and Maxwell, 1987: 19-21

groundwork for formulating budgets, measuring performances and justifying the utility of security by highlighting her/his successes. Thus, the visibility of the security department is improved and those responsible for security gain managerial credibility in their organisation.

3.2.2.1.3 Controlling

Management is largely seen as the art of maximising results. This is achieved by controls, i.e. by comparing the results obtained with those settled, and by assessing the efficiency and efficacy of the process under management. The area of controlling covers two activities: the measure of performances and reporting.

3.2.2.1.3.1 Measuring performances

It is a general assumption in management that, if the output of a function cannot be quantified, or when quantified, cannot show a greater balance than which would be achieved in its absence, then that function is not contributing to the general purpose, and can be eliminated, or minimised. This criterion is considered also true in security. [317] The managerial practice of justification requires that every decision made by the security manager must be assessed economically as well as functionally. There are three questions to be answered:

- Is this (programme, system, measure) really necessary?
- Is this (programme, system, measure) worth its expenditure?
- Is this (programme, system, measure) the most effective option at the stated cost?

The managerial criterion for measuring performances is largely based on the cost-effectiveness concept, which basically means getting the best return for the amount invested. The demonstration of meeting the criterion of cost-effectiveness may be difficult in security, because it requires evidence of tangible and measurable returns against expenditures. However, in the area of loss reduction, this is widely considered possible [318]. The careful recording and reporting of security activities over a period of time may give an indication of what costs have been avoided, what losses have been recovered, and what chains of events

[317] Walsh and Healy, 1996, vol. III, Ch. 23

[318] Hemming, 1996; Kunze, 1997; Walsh and Healy, 1996, vol. III, Ch. 23

potentially leading to a significant damage have been broken by the timely and effective security measures. Under the first area (cost avoidance) the total losses assumed to have been prevented by security are calculated. This cost is normally the total of single losses, considered as occurring either in the 'most probable' or the 'worst possible' scenario. To this, routine 'housekeeping' losses, such as those avoided by plant patrols (e.g., lights turned off, leakage stopped, machinery controlled, tools or materials recovered) are added, as well as an estimate of claims avoided as a result of successful interventions or investigations. Under the second area (revenue generation) are included those successful proof of losses required by insurance to pay the claim, together with the value of recovered assets, and financial recovery from parties other than insurance. The third area (avoided damages) is mainly a matter of speculation. It requires the reconstruction of a 'most probable' or 'worst possible' chain of events that could have resulted in damage had the hazard, or potentially dangerous situation, not been prevented from developing by security actions. An assessment of the cost which would have incurred had the damage not been prevented (particularly when it is made by a 'smart' manager) contributes a further figure to the total sum. With this kind of justification clearly depending upon the largest demonstrable total, a meticulous recording of even trivial events is essential, together with the recourse to a reliable data-base.

3.2.2.1.3.2 Reporting

Managers are interested to this area for a variety of reasons: the need of controlling compliance with standards; assessment of efficiency, efficacy and cost-effectiveness; preparing a basis of data for statistical predictions. The latter is discussed. The whole concept of 'scientific management' is based on the opinion that reporting shows its ultimate value in the area of prediction. The careful analysis of the data emerging from the reports allows for the identification of patterns and trends which may be exploited for future decisions. The analysis is supported by quantitative and qualitative models. In order to have homogeneous and statistically valid data, the preparation, distribution and correct use of specific formats has paramount importance. This reasoning is largely accepted in security, [319] though it is frequently lamented that the available data are incomplete or come from different and irreconcilable formats [320]. The 'raison d'être' of security is to provide a set of adequate countermeasures to foreseeable threats, in order to avoid or reduce damages to well defined

[319] D'Addario, 1989; Placek, 1996

[320] Malik, 1995

assets. This assumes the capacity of making correct decisions, based on the knowledge of facts, supported by reasonable predictions, and implemented by relevant measures. This cannot be performed without reliable data. These data are primarily produced by surveys, interviews, and particularly by the analysis of reports. The use of logs, incident reporting and loss reporting is an invaluable tool for identifying where, when, how and at which cost it is necessary, and cost/effective, to take action. A careful examination of reports over a significant period of time helps to identify vulnerabilities, frequency, times and duration of attacks, costs and losses, quality of intervention, areas needing more attention, procedures needing implementation or modification. Results may be elaborated into 'managerial' tools, such as matrixes, trees, flow-charts, indexes and models. Reports provide the groundwork for improving security programmes, preparing a new budget, installing new systems, and help the security manager to justify his/her proposals for obtaining approval.

3.2.2.1.4 Innovating

Innovation has an essential role in security, in order to adapt plans and activities to the dynamics of antagonism. However, there is evidence that security professionals are not ready to accept this role. According to a recent research made by Hearnden and Travers and based on the Myers-Brigg Type Indicator test (MBTI), security managers tend to be of STJ (sensing, thinking, judging) type, that is a behaviour which favours organised knowledge, detailed planning, and an organised life.

> *'As such, they favour a range of behaviours that can combine to reinforce a major organisational source of resistance to change.'*
>
> (Hearnden and Travers,1995: 193)

3.2.2.2 Summary

The management of security is rarely a self-contained exercise. It takes place inside the general process of management within the organisation, and it is influenced by the internal and external environment. Security decisions are generally subject to the approval of non-security managers, who use their own criteria.

The management of security has some conceptual differences from the general concept of management. For example, the accepted criteria of justification and prediction are not immediately translatable. The position that cost-effectiveness criteria of justification also hold in security is not completely supported by evidence. The problem consists in the incompleteness of the information available and in the difficulty of ascribing monetary values to security results. Not all the areas of security can be clearly defined as, for example, that of the so-called loss-reduction. Here, reference can be made to data coming from previous years, and a 'profit' can be easily calculated by difference with losses antecedent to the adoption of a specific measure, less the cost of the measures. On the contrary, in the areas of terrorism, espionage, and personal protection, the difficulty of calculating potential losses which have been avoided by preventative and deterrent measures is immediately evident. Besides, the criterion of cost-effectiveness does not account for the dynamics of antagonism nor it offers a measure of the 'peace of mind' obtained through security measures, or of deterrence. Results in security cannot always be calculated according to economical criteria. With regard to prediction, it is submitted that knowledge based on the above described methodology is *incomplete* and that further knowledge must be gained by other means. There is no evidence that security predictions based on statistical knowledge are reliable. A discussion on the subject has been offered in Section I, where the limits of a linear reasoning within the dynamics of antagonism have been discussed. More is offered later, along with a possible solution. Another area of problems comes from the resistance to change. This is peculiar to security managers, and is closely linked to their background and education. It is suggested that it can be addressed by proper selection and education. These facts arise problems, which need to be clarified before attempting to model a security process and, consequently, an operational methodology. With the essence of management consisting in a series of decisions, these problems have been located in the way decisions are made.

3.2.3 Decision Making

In its broadest sense, the term 'decision-making' is used to define that particular process of goal-oriented reasoning which is related to making a reasoned choice between different possible courses of actions or states of affair.

> *'Decision making ranges from the administrative procedures by which messages are distributed and filed, to the quality of perception and interpretation, and the degree to which action is guided by adequate consideration of all possible choices. It includes the*

> *execution of the decision, and readjustment to cope with environmental responses to the decision.'*
>
> (Burton, 1968:58)

Decision making is often seen as virtually synonymous with management. [321] Yet,

> *"... focusing on decisions may lead to an overly rationalistic view of management, and may blind us to other aspects of the managerial task. ... managerial action may also take place without decision. At lest, this is true if with 'decision' we refer to a process of deliberate reasoning and weighing of evidence. Many decisions in organizations are 'programmed' by existing procedures, or are made on the basis of routine, without much conscious effort"*
>
> (Noorderhaven, 1995: 9)

The investigation upon this subject evolves around three fundamental questions: 'what is a decision', 'what is it for', and 'how do people make decisions'. A discussion of the most relevant positions is considered an essential premise to the future account on how security decisions are, or should be, made. The first issue is about what is meant by 'decision'. A tendency has emerged, in surveying the specific literature, to confuse at some stage decision with choice and decision making with problem-solving. [322] However, their theoretical paradigms come from different premises. [323] The former tendency has been refuted by White, who states that decision cannot be immediately equated to choice, in that:

> *'...a decision requires some clear logical step from one state of affairs to another, whereas choice did not necessitate any logical steps at all in arriving at the choice'*
>
> (White, 1975:5)

Neither decision-making appears immediately equatable to problem-solving. Firstly, because of their different cultural premises. Secondly, because, contrary to decision-making, problem solving is not considered by theorists as a natural process. [324] Researchers explain that the process of problem solving must be learned.

[321] Barnard, 1938; Simon, 1960: 1

[322] *'That form of activity in which the organism is faced with a goal to be reached, a 'gap' in the route to the goal, and a set of alternative means, none of which are immediately and obviously suitable.'* (The Fontana Dictionary of Modern Thought)

[323] Garnham and Oakhill, 1994: 201, 202

[324] For a discussion on decision-making and problem solving, see:Garnham and Oakhill, 1994, Ch. 10 and 11

> *"In problem-solving (or learning) the animal's natural response is, by definition, the wrong one. Otherwise, it would have nothing to learn and no problem to solve"*
>
> (Garnham and Oakhill, 1994: 5)

In this research, the decision-making process is considered as the overall process of goal-oriented reasoning, and problem-solving as the analytical 'tool' within it which allows for clearing some of the obscure areas of reasoning. [325]. The general position on this process is that

> *"Decision making now simply is the process of selection of and commitment to a purpose, or plan of action. The word 'process' implies that decision making is a series of activities with a certain duration. Although a decision itself may be described as an instant -an essentially timeless phenomenon- decision making inevitably has a time dimension (Harrison, 1987). This is true of the selection process, as well as of the commitment process (the process of implementation may be seen as taking into effects the commitment expressed at the moment of choice)."*
>
> (Noorderhaven, 1995:8)

It has been previously said that three principal decision areas can be identified in organisations: strategic, operating (tactical), and administrative. [326] A description follows. [327]

Strategic decisions are the basic, long-term decisions, which set the principal *goals* and *objectives* of the organisation, including the major policy statements. They tend to be unique, non repetitive and to have an effect delayed in time. They are usually complex, especially in terms of variables (most of them external, and uncontrollable), which have all to be considered before final decisions are made.

Administrative decisions allow for the allocation of strategic and tactical resources. They are essentially concerned with settling *means*, i.e., defining the organisational structure, establishing lines of authority and communication, assigning resources and responsibilities.

[325] A contrary opinion is held by operational research theorists, who consider in their methodology problem-solving as including decision making See: Anderson, Sweeney, and Williams, 1994: 2-4; Bellacicco in SME manual, 1987.

[326] Ansoff, 1969. This position is considered unrealistic in some modern organisation which are project-focused. However, it has been chosen for its consistency with security organisations, which need to be hierarchically organised (so to respect, for example, the 'needs to go and to know').

[327] Cole, 1993, 124-5

Operating (tactical) decisions are contingency based, short-term decisions, which set *actions*. They tend to be routine, repetitive, and to have an effect in short time. They are usually less complex in terms of number of variables, but numerous, and they tend to be contingency-based because of their nature and the immediacy of the effects.

An example of the different levels of decisions in security necessary for the different levels of planning, is the following:

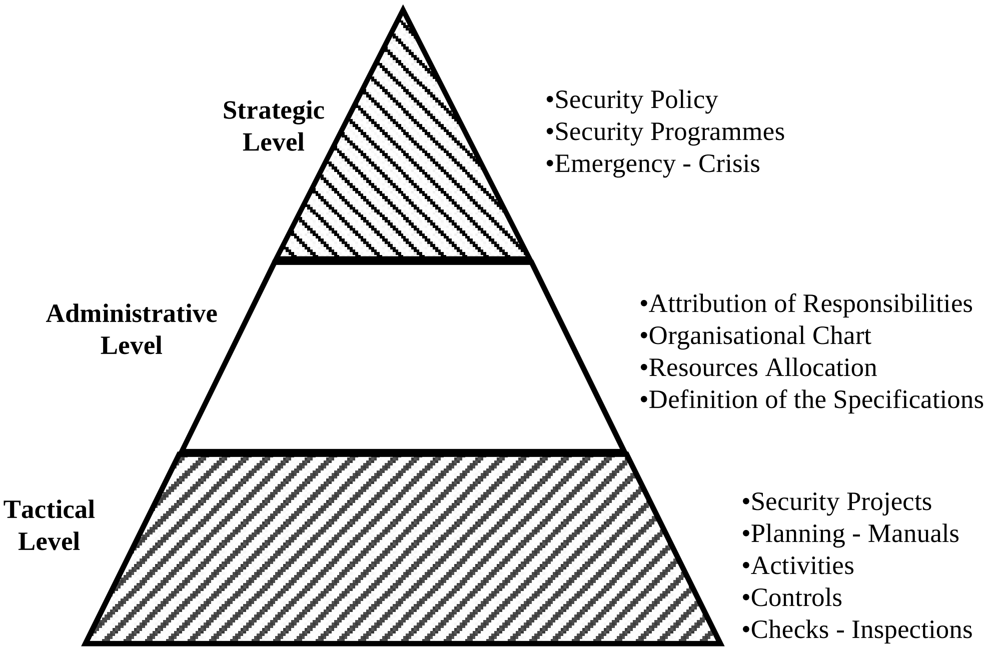

Figure 41 Different levels of decision in security. [328]

Other distinctions have been made between so-called programmable and non-programmable decisions, [329] and between routine and emergency decisions. [330] A programmable decision is one capable of being worked out by a computer. This presupposes that the variables are quantifiable and that the decision rules can be clearly stated. These criteria would certainly apply to numerous tactical and administrative decisions. By contrast, a non-programmable decision is one which can hardly be predicted or quantified, where human judgements have to be made, as, for example, strategic decisions. The difference between routine and emergency decisions lies in time space, surprise, intensity of the emotional involvement.

[328] Manunta,. (1993)

[329] Weeks & Whimster, 1985

[330] Lev, 1992

Routine decisions are largely programmable, emergency decisions are largely not. When the former allows the process for enough time, is based on a sufficient base of experience and has the support of a 'rational path of reasoning', the latter requires immediacy, may not be referred to a basis of previous knowledge, the reasoning is perturbed by emotional factors that may even 'freeze' the process. [331]

The second issue is about the final cause of decision, i.e., 'what is it for'? A different vision about different final causes was the premise to different areas of study, since

> *'Psychologists were interested in the motives underlying an individual's decision, and why some persons had greater difficulty than others in making decisions. Economists focused on the decisions of producers, consumers, investors, and others whose choices affected the economy. Business administration theorists sought to analyse and increase the efficiency of effective decision making...Decision making was a focal point for political scientists interested in analysing the decisional behaviour of voters, legislators, executive officials, politicians, leaders of interest groups, and other actors in the political arena'*
>
> (Dougherty & Pfaltzgraff, 1990:468*)*

Whatever the focuses, an agreement seems to converge on the idea that decision is for commitment to the chosen course of action. [332]. Therefore, it can be said, 'decision is for acting', but this answer would not hit the point, since action leads to effects and decision-makers want (a) to predict these effects; (b) to achieve the 'best possible' effects. Hence, the point is that - ideally - decision are taken for 'best acting', in order to achieve the 'best possible results'. This assertion raises the essential issues of justification and optimisation. What is the 'best possible' result? Who decides what is 'best'? How can we reach it? How can we say it has been reached? According to the economists (this position could also apply to security), the 'best' decision is the one which maximises the chooser's expected utility. Two problem areas have been identified in this definition. [333] First, the concept of expectation implies (a) the formulation of a set of desires and (b) some degree of belief that these desires

[331] Lev, 1992

[332] *'Both selection and commitment are important (Mintzberg, 1981). If there is only one course of action available, no selection can be made, and the concept of decision is hardly applicable. And if a purpose or plan is selected as the best, but the decision maker does not as yet feel committed to it, for all practical purposes no decision has been made.'* (Noorderhaven, 1995: 8).

[333] Garnham and Oakhill, 1994, Chapter 10

will be fulfilled in the future. Second, the concept of utility has different meanings and different values to different people, or to the same person in different circumstances. This raises questions about the choice of the decision-maker and the methodology.

If a decision maker wants to maximise his/her expected utility, s/he must firstly define a set of values and desires, then find a method of prediction (a way for reducing the uncertainty of the possible outcomes) and, finally, adopt a methodology for controlling the consistence of her/his decision not only with the fixed set of values, but with her/his desires. These requirements, which may, or not, be relevant in the realm of individual decisions, become inexorable in the realm of the organisation. Here, justification is unavoidable and the way this justification is produced has essential importance. The reasoning holds validity in security, because the concept of utility requires the costs and the effects of security measures to be reasonably predicted and respectively weighed against expected 'gains' and unwanted outcomes. This re-introduces the necessity of identifying first an acceptable criterion for measuring performances.

Assuming the first condition (notably, the setting of values and desires) is satisfied, the investigation on how to satisfy the second (belief) in order to justify/optimise the choice assumes relevance. Again, only when 'the best' is identified, 'the best' criterion of choice can be defined. This infers that the first and most important of all decisions is that about the criterion of decision and, ultimately, about the user of this criterion, i.e., the decision maker. This sort of circularity sounds like a 'dog chasing its tail': to decide for the best, one must firstly decide which criterion should s/he use; yet, to select a criterion, one must firstly decide what is best for him/her. In order to decipher this logical 'catch 22', an investigation upon the process of decision-making is inevitable.

This leads to the third issue: 'how a decision is made'?

The Penguin Dictionary of Psychology describes decision making as:

> *'a generic term used to cover 1 the process of choosing and 2 an array of theories and investigations into the question of how organisms make choices between alternatives'*[334].

This definition reflects two main positions, which have been the subject of systematic investigation within the area study of decision theory. [335] Decision theorists study how

[334] The Penguin Dictionary of Psychology, 1985:177

decisions *are* actually made and how they *ought to be* made, according to two different branches of decision theory, descriptive and normative. Both are relevant to this research. Descriptive theorists (mainly psychologists) describe and explain how people make their choice among actual options; as such, this branch of decision theory is an empirical subject that uses experimental and survey methods. Normative, or prescriptive, theorists are concerned about rational choices rather than actual choices. They essay to prescribe the course of action that should be selected in order to achieve a specified goal. As such, this branch of decision theory is considered a deductive discipline investigated by mathematicians, logicians, and statisticians, mainly under the paradigm 'problem-solving'. The concepts of description and prescription are closely linked. Only when the whole 'mechanism' of the process is clear and inspectable it becomes possible to check all the phases of the reasoning, learn from past errors, and correct them in order to optimise future processes. Description theorists see decision making as the functional area of reasoning which links (or interfaces) the areas of thinking and acting.

> *"The concept has to do with selection and commitment....Taking a decision is like turning a mental switch: before, various possibilities were considered, but once the decision is taken attention is focused on one option only."*
>
> (Noorderhaven, 1995: 7)

It is not easy to say how this link, or interface, works. Easton, reasoning on policy making, interpreted decision making as the process which transforms inputs into outputs. [336] In his model, the policy makers decide what to do according to the inputs they receive/perceive. Decisions are the outputs of a system (in his example, a political system), where inputs in form of information, support and expectations have previously been introduced. Easton realised that the process was circular, in that the output of a decision returns back into the system as input for a new cycle through a mechanism of feedback. What is relevant here, is that the 'decision box' can be seen not only as a processor, but as a filter. Presumably, not all the inputs received are passively accepted and automatically processed. Those which are accepted and processed, may have not been completely perceived, or 'correctly' interpreted (i.e., according to the intention of the source). Indeed, the decision making process is

[335] *'A label for any theory that seeks to describe and explain decision-making', whose approaches 'vary from the highly formal mathematical approaches based on game theory and probability theory to the more informal, intuitive theories which deal with beliefs, attitudes and other subjective factors'.*(The Penguin Dictionary of Psychology)

[336] Easton, 1965. His model has been presented in Section II

complicated by cognitive factors and by the interference of other similar processes, who overlap with different importance and in different temporal phases. [337] If inputs are seen in terms of information, then the conformity of decision and actions to external demands and support depends (a) on the quality and completeness of information, and (b) on the consistence, or in-consistence, of the system (notably, the decision maker) with the external requirements.

In order to understand the contents of the 'decision-making black box', a set of hypotheses has been provided. Burton introduced the ideas of perception, [338] interpretation, consideration and re-adjustment. [339] Inputs, in fact, are not isolated, but are received in a determinate environment, under certain particular conditions. [340] Since the decision maker cannot be assumed to have an empty mind, the perceived input is then compared to past experiences and analysed accordingly before even considering taking a decision. After the implementation, outputs become new inputs for re-adjustment.

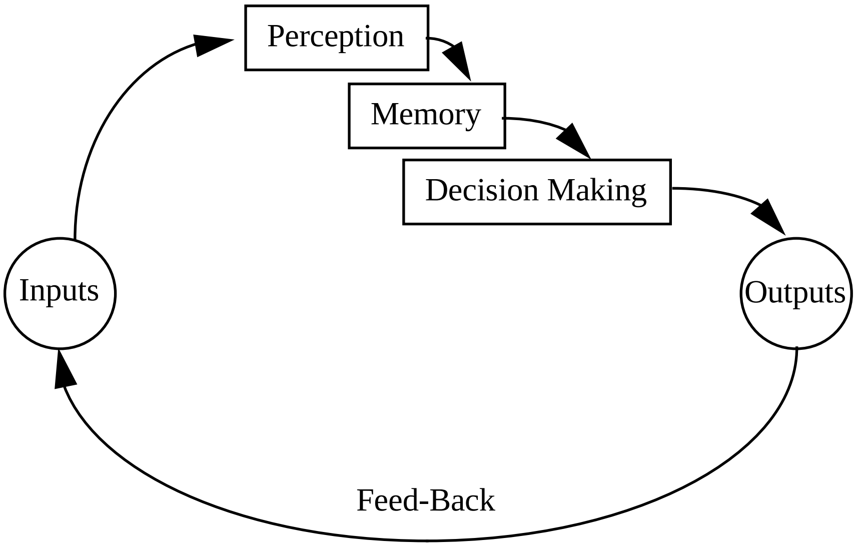

Figure 42 A Simplified version of Burton's Model of Decision Making

[337] Evidence has been offered in Section II

[338] *'Perception is assigned a central place in decision-making theory. When dealing with the "definition of the situation", most DM theorist regard the world as viewed by the decision makers to be more important than objective reality...Joseph Frankel...indeed argues that DM theorists must take the objective environment into account, for even though factors not present in the minds of policy makers cannot influence their choice, such factors may be important insofar as they set limits to the outcome of their decisions* (Penguin Dictionary of Psychology:470)

[339] Burton, 1968

[340] See: 'Mental set' and 'Functional fixedness' in Section II

Again, the quality of outputs depends on the quality of inputs, modified by perception and existing knowledge. Even assuming that the system accepts inputs and wants to implement them, cognitive processes exert substantial interference which must be taken into account when considering the 'rationality' of the process. [341] What is interesting here, is that, when repeated under the same circumstances, the circularity of the process causes a mechanism of adaptation through learning, which in ideal conditions tends to entropy. [342] This accounts for the previously mentioned factors of mental set and functional fixedness. [343]

Cognitive factors such as perception and memory are not considered the only source of interference.

> *"Common sense tells us that people's decisions depend both on their beliefs and desires. Some philosophers have been sceptical about common-sense psychological theories (e.g., Stich, 1983). Decision theorists, however, have, for the most part, accepted the common-sense analysis of decision making, and have, furthermore, assumed that beliefs and desires can be completely disentangled from one another (though see Shafer, 1986, for a dissenting view)."*
>
> (Graham and Oakhill, 1994:176),

Dixon, borrowing from communication theories [344], introduced the concept of 'noise'. His model on generalship provides a general frame of understanding with regards to whole process. [345]

[341] See: Section II: Dimensions of Security: Cognition

[342]In information theory, the measure of scarcity of information contained in a signal

[343] Section II, Dimensions of Security: Cognition

[344] Specific reference is made to Shannon and Weaver, 1949

[345] The choice of this model has been motivated by two considerations: the common origins of security and military methodology (see: Section I); and a partial similarity of the military with the security context is given by the existence of an antagonist.

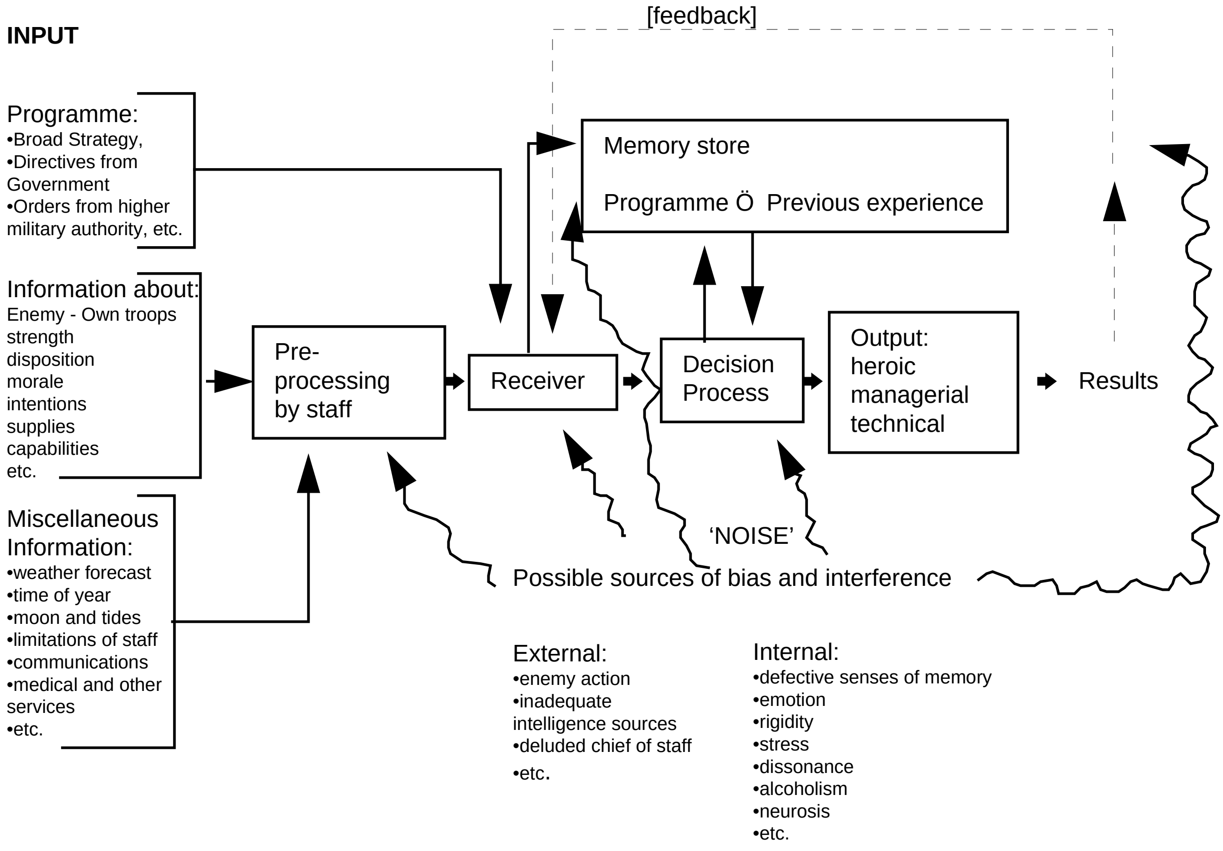

Figure 43: Dixon's Model

> *'The upper half of the above diagram provides a simplified view of the information processes before, during and after the making of military decisions. The very high information load, the great "uncertainties" that have to be reduced or tolerated, the many stages involved, the interaction between past experience and a "programme" of perhaps dubious validity, the dependence of decisions upon knowing the likely outcomes of possible alternatives and the necessity for possible revisions in the light of feedback of earlier outcomes constitute a large potential for error or breakdown in the smooth flow of information. The lower part of the diagram outlines typical sources of "noise" which could produce disturbance at one or other of the stages between Input and Output'.*
>
> (Dixon, 1976:29).

These 'sources of noise' have previously been identified as pertaining to the psychological, political and administrative dimensions of the security context. However, if a decision is made within this fairly subjective frame of reference, how can it be said that the 'best possible' decision has been made? This question re-directs to the prescriptive branch of decision theory, which identifies 'good' with 'rational' and tries to analyse how rational, not actual, decisions, should be made. With Noorderhaven, the logical conditions under which 'rational' decision making has meaning are: [346]

Complexity. If the situation is very simple, and the circumstances clearly dictate one particular course of action, then decision making is trivial, since is basically determined by its environment.

Uncertainty. A distinction is made between 'uncertainty' and 'risk'. In a situation of 'uncertainty', not all possible outcomes are known, and probabilistic information is incomplete, or incommensurable. A situation of 'risk' is that where the set of possible outcomes as well as their probability is known. If the outcomes are complex, but certain, even if it requires a long time for calculation, the process will eventually figure out one, and only one, 'best' course of action. In this case, we fall in the case of triviality of decision, as that previously outlined. This, according to Noorderhaven, reduces the degree of 'rationality' of the decision.

Rationality. It is assumed that decision is associated with commitment, and the process is started intentionally. Hence, it is also assumed that: the selection of choices and actions is made after the ability of reasoning has been fully exploited; some relations between means and ends exist, as well as between reality and cognition. Extensive analyses and calculations are not essential to rationality, nor is the ruling out of perceptions and emotions. Rationality is an individual, complicated concept, which cannot be expressed only in numbers. In order to obtain full confidence and commitment, a conscious appreciation of the existence of an objective is required, with the exact identification of the criteria and constraints which influence the choice.

Control. If no control is possible on the organisation where a given decision has to be actually implemented, then a decision has no utility, and is only a sterile exercise. Without control, the decision making perspective would be 'rather useless', since the outcomes would be the involuntary results of an interplay of casual forces, rather than the intentional results of deliberate actions of individuals.

[346] Noorderhaven, 1995: 9-11

Prescriptive theorists say that, in order to *rationalise* the process of making a choice between different options, three basic steps should always be followed, namely: a. Identify the options between which a decision is to be made; b. Define the criterion, or scale of values, against which these options are to be judged; c. Evaluate the options on this scale. In condition of uncertainty, criteria and values are arbitrarily set (e.g., via an expert's best estimate). Therefore, according to this position, the measure of its '*rationality*' seems to lay in the observance of the criterion -or scale of value- that has been stated as a premise to the reasoning.

The point is now: to which extent a 'rational' decision, such as that previously defined, is also 'reliable' and thus deserving 'commitment'? This is a very important point, since the degree of commitment appears -*ceteris paribus*- directly proportional to the degree of reliability. Assuming the decision maker possesses all the relevant information and accepting the prescriptive method of decision making, a common answer between prescriptive theorists is that the criterion of decision draws its reliability in the principle of 'confidence'. If a decision is taken via a method, then the 'commitment' of the decision maker should depend on the level of confidence on the method used. Since this particular breed of prescriptive theorists tends to have a background in mathematics and to be 'confident' in statistical methods of calculation, both reliability and confidence are frequently based on a 'justified true belief' typical of physical sciences. Mathematics and calculus should guarantee the minimum interference from and towards the solver: decision becomes an articulate 'weighing' of all the possible courses of action by which - no matter who decides - to draw the *logical* and *inevitable* conclusion. The concept of the 'inevitability' of a rational decision has its roots in the history. [347] Literary evidence of this process may be traced as far as twenty four centuries ago in Thucydides's *Peloponnesian War*, where the Greek historian

> ***"...examined the factors that led the leaders of city-states to decide the issues of war and peace, as well as alliance and empire, with as great precision as they did under the circumstances confronting them. He focused not only on the conscious reasons for statesmen's choices and their perception of the systemic environment -both of which are reflected in the speeches he attributes to them- but also on the deeper psychological forces of fear, honour, and interest that in varying combinations motivated them as***

[347] The term decision comes from the Latin *de-cidere*, which means to cut off, or prune, all the undesired branches of a tree. Hence, according this line of thought, a decision is not the act of choosing the preferred course of action, but the *inevitable* outcome of rejecting all the others, after a process of testing against information, constraints and a given set of criteria.

> *individuals and set the prevailing tone of their particular society. Thus, Thucydides was indeed an early student of decision-making"*
>
> (Dougherty and Pfaltzgraff, 1990: 469)

This position assumes that all the relevant information are known, or knowable, [348] and sets the criterion of rationality in applying a given criterion via calculus and measurement. However, research and experience shows this assumption to be fallacious in a number of aspects. Not all the relevant information are known, or knowable; life is not static but evolves and at the moment of decision data may be quite different from the moment were gathered; finally, each individual has different desires, beliefs and cognitive base. Besides, Easton and Dixon have shown that decision -making is not a self-contained, 'aseptic' exercise. It happens within an open system, subject to interference from the environment and circumstances, which are not perfectly, nor completely known. It is not a pure, single exercise either. The three basic steps of reasoning outlined by prescriptive theorists involve a number of different processes, frequently - with Ansoff - at different hierarchical levels.

> *"In the case of organizational decision making, the selection of an alternative by an organization member may have to be ratified by another organization member before organizational commitment can be said to exist."*
>
> (Noorderhaven, 1995: 8)

Any of these steps is a decision making exercise, including the definition of the criteria of choice,[349] the definition of the objective,[350] the intermediate goals,[351] and the criteria of performance.[352] There is no evidence that, once established, the criterion -or scale of value- will be always and absolutely respected. The decision maker may change during the process, or be a different person from the collector and analyst of data, or different decision makers

[348] It is assumed that information may be transformed into knowledge (Shannon and Weaver, 1948), and even that such a knowledge may be measured (Weiner, 1948).

[349] *'The area of choice that decision makers have must be determined...what alternatives exist is the first consideration...What is required is an analysis of the area of choice of decision making generally, in the light of which alternatives in particular situations can be examined...The more direct way is to examine areas of the environment or conditions that are alterable and unalterable by the deliberate decisions and policies of States'* (Burton, 1968, p.58-59)

[350] *'By objectives we mean a long term state towards which we hope the organisation is proceeding. Such objectives may be unobtainable but nevertheless they are there as the ultimate towards which one is proceeding and are yardsticks against which decisions can be tested'* (Rivett. 1980, p.22-23)

[351] *'Goals are measured states in which we want the organisation to be, at or during a specific period of time'*(Rivett. 1980, p.22-23)

[352] *'[criteria of performance] are those measures which we use as of now to check on the progress of the organisation towards its goal'.* (Rivett. 1980, p.22-23)

may be involved. Though may formally agree on the observance of the same criterion, different persons may not practically comply with it, because of their different sets of knowledge, values, beliefs and desires.

> *"Decision making is, therefore, a more complex process than judging probabilities. Indeed, it typically requires a combination of the probability judgements associated with our beliefs and information about our preferences. Whether someone takes an umbrella when they go out depends both on whether they think it will rain, and whether they want to avoid getting wet. Indeed, probability theories was originally developed for analysing games of chance and for assessing insurance risks. In both cases, judgements of probabilities inform decisions with outcomes people really cares about -outcomes of financial gain and financial losses."*
>
> (Graham and Oakhill, 1994:176),

The above reasoning brings forward the question: How are choices made, in security? As for other contexts, the contents of the 'black box' in security are strongly influenced by emotional and other personal factors. Experience, research and literature show that, in security, decisions tend to be driven by emotions, political considerations, or sheer necessity, and the choice between different options are frequently based on costs. Moreover, decisions are not easy made, since many of them are to be made under uncertainty, and those most essential under conditions of danger and conflict, including fight. This research has also indicated security as being: egoistic in vision; risk adverse in behaviour and choices; conservative in strategy; self-utility prone in choice and scope, at the expense, if necessary and possible, of other people's interests. [353] Protector cannot - without contradicting her/his *raison d'être* and essence - *deliberately* accept the existence of risk. S/he attempts to reduce the decisional risks by means of intelligence, and the operational risks by means of information, education and training. Differently from other classes of conflicts, security favours flight to fight. Protector does not defend Asset to the last but only to a point, which is represented by her/his convenience, self interest and utility. No security-focused approach acts against them. Their influence drives and affects security decisions. Given the above features, it is only a consequence of our human nature that

> *'The decision making process can be faulty at many specific points'*

(Burton, 1968:58)

The ease with which a fault can be made and the gravity of their possible effects, require a method of evaluation and control to be set in advance, where coherence and consistency are the essential feature. With decision in any context being influenced by its peculiar priorities, focuses and constraints, the rationality of a decision making process requires their identification and evaluation as a preliminary step to the reasoning, and as a control of the outcomes. This is necessary for solving the knots of responsibility, blame and performance. Consequently, there is the need to analyse how a 'rational' decision can be made in security and, therefore, to which degree a security solution can be defended against others in contexts ranging from management to legal, so to ensure an adequate level of commitment and a correct judgement. This shifts the discussion to the issue of problem-solving.

3.2.3.1 Problem Solving

Problem solving has been defined in this research as 'the analytical tool within the decision-making process'. This tool is useful for assisting, by means of qualitative and quantitative methodologies, the choice among a set of alternative options, when none of them are immediately and obviously suitable.

Three basic components of problem-solving can be identified: a Solver; a Problem and a Process (the dynamics and activities which allow the solver to untangle the problem). They are discussed below.

3.2.3.1.1 The Solver

The discussion upon the solver is made via the analysis of three important factors: the links between the solver and the problem; the possible existence of different solvers; and the relationship between the solver and the process.

The first point is essential. Problems do not exist by their own capacity. They are seen and 'created' as such by a person who decides s/he has *'a question to be answered or solved'*.[354] The

[353]One of the most typical reasoning in security is aimed to relocate the threat, following a logic such: I only need to reinforce my defences to the point that the threat will find more convenient targets (i.e., less protected than mine)

[354] OALD: Problem.

interference of psychological, political and administrative factors to the process of reasoning has already been discussed. Therefore, the assumption is made that the existence and gravity of the problem, and the degree of commitment to its solution, are relative to the solver.

The second point (the possible existence of different solvers) has relevance in organisations. A significant number of decisions results from negotiation between departments. Most decisions are taken collectively, in meetings where participants defend different interests and viewpoints, hence different criteria and priorities, not all of them clearly identifiable. Different but connected problems may arise (e.g., a security problem within other organisation's problems), which require the interaction of different solvers. With security being rarely the core problem within an organisation, not all the solvers are plausibly concerned with security priorities.

There is one more aspect to be thought about. In solving a security problem, difficulties are added from the overlapping of antagonist processes. The existence of Threat as a solver must be considered. This issue has been researched by criminologists, [355] but is frequently neglected in managerial approaches applied to security. [356] In operational methodology, Threat is seen more as an 'attacker' than an additional problem-solver, whose influence on the solution of the security problem is substantial. Moreover, Threat is frequently composed of different and often unknown persons with different motivations, capabilities, priorities and criteria; hence, different antagonist solvers.

The final point (the relationship between the solver and the process) stems from research and decision theories, which show the solver to be 'irrational', in the sense that his/her processes are influenced not only by identified hindrances and constraints but also from the personal, unknown process, already defined as a 'black box'. The contents of the 'black box' are not completely known; it is generally accepted that its output depends on the person of the solver. In Section II, reference was made to Meltsner's three types of analysts in the American federal bureaucracy. [357] H.A. Simon (1965), considering decision-makers, distinguishes between 'economic man' and 'administrative man'. Economic man (in Meltner's words, the

[355] Wiersma, 1996

[356] E.g., OPSTAF Methodology (Placek, 1996). Threat is not considered in the methodology.

[357]'*the technician, interested in doing good quality -policy oriented- research and essentially an academic in bureaucratic residence; the politician, concerned to achieve advancement and personal influence and interested in analysis only in so far as it furthers these ends; and the entrepreneur, interested in using analysis to influence policy -and improve policy impact'.* (Ham and Hill, 1993:7)

'technician') tries to maximise utility, therefore operates within a clearly defined framework, where all non-economical considerations are excluded, all the elements have been identified and quantified (in terms of benefits, costs, and penalties), outcomes are listed and choices are made according to an economic scale of preference. Administrative man (in Meltner's words, something between the 'politician' and the 'entrepreneur') takes into account the influence of the environment. S/he understands that, ultimately, s/he will be part and subject to his/her decisions, and that these decisions will be applied within the environment, which may as well accept, support, or even reject their implementation.

Hearnden and Travers suggest that security managers tend to a behaviour which favours organised knowledge, detailed planning, organised life, and presents a major resistance to change. [358] It may be noted that 'resistance to change' is largely incoherent with the necessity of dealing with the dynamics of antagonism. This incoherence is but another factor of 'irrationality' of the solver to be considered in the process.

To conclude, evidence is that the solution of a problem is largely influenced by the solver, and that existing methodologies do not address the problem as a whole. When justification and rationality are required, this opens two issues: a) the choice of the solver and b) the choice of the methodology. The former point is not discussed, but left open to further study. The latter point is addressed in the following paragraphs.

3.2.3.1.2 The Problem

The concept of problem presents different facets in the dictionaries. Different ways of classifying problems can be found in literature, but the more appropriate to this research seems the classical distinction made by psychologists [359] between puzzles (non-adversary problems) and game playing (adversary problems). While not disregarding the first class of problems (which may, indeed, arise in security contexts), this research is more interested in discussing adversary problems. [360]

[358] Hearnden and Travers, 1995: 193

[359] Garnham and Oakhill, 1994:201

[360] Not all problems in security are pure adversary problems. For example, the administrative and managerials problems which belong to the routine area of security cannot be considered as such. However, in this research, the discussion is limited to the field of adversary problems.

According to Garnham and Oakhill, the essence of problem has been pinpointed by the Gestalt psychologist Duncker when he wrote:

> *'A problem arises when a living organism has a goal, but does not know how this goal is to be reached' In information processing terms, this idea implies that a problem has three crucial elements: 1. a starting state 2. a goal state 3. a set of processes (usually called operators) that can transform one state into another. The starting state is the state of the 'world' that poses the problem....The goal state is another state of the world in which the problem is solved...The processes are things that can be done to the world in an attempt to move from the starting state to a goal state..."*
>
> (Duncker, as quoted byGarnham and Oakhill, 1994:200)

This position fits well with Bellacicco's Model of Problem, where a problem is defined as

> *'the hiatus between the initial state of affairs (So), and the final one we want to reach (S1), characterised by different possible lines of action.'*
>
> (Bellacicco, 1987:1)

Consequently, problem solving (which Bellacicco identifies with decision making) is defined as the activity that allows the choice of the best possible alternative required to advance from an initial to a goal state of affairs. Decision is the conclusion of the process which -in this line of thought- is aimed to identify and evaluate the options which allow for bridging the gap within So and S1.

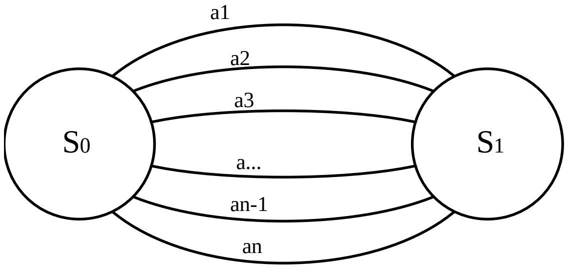

Figure 44 Bellacicco's Model of Problem

In this research, a security problem is analysed according to Duncker's and Bellacicco's model. Security is the goal condition that the Protector wants to achieve and maintain in antagonism with the Threat. Accordingly, in the above diagram S_0 represents the present, unwanted, condition of insecurity, and S_1 represents the desired condition of security; the problem space includes those dynamics and processes necessary to achieve the desired condition and is characterised by different possible lines of action. The solution (decision, in Bellacicco's terms) is the choice of 'the best' among all of the identified options. The next step is to analyse the process by which this choice can be made.

3.2.3.1.3 The Process

A typical problem-solving exercise involves the following 7 steps:

1. *Identify and define the problem.*
2. *Determine the set of alternative solutions.*
3. *Determine the criterion or criteria that will be used to evaluate the alternatives*
4. *Evaluate the alternatives.*
5. *Choose an alternative.*
6. *Implement the selected alternative.*
7. *Evaluate the results, and determine if a satisfactory solution has been obtained.*

(Anderson, Sweeney and Williams, 1994: 2)

Each step of the above process can be considered as a problem within the main problem. Analysis follows.

3.2.3.1.3.1 Identify and define the problem

The step of identification and definition of the problem is critical. The success or failure of the exercise depends upon the capability of transforming a general problem description into a well-structured problem that can be approached with the existing techniques. [361] This phase is normally assisted by a specialist, who develops a model that can be used to represent the problem. More is offered in the next sub-section.

A problem is frequently composed of different sub-problems, each referred to different context and priority. This means that different problem-solving processes must be combined.

[361] Anderson, Sweeney and Williams, 1994: 6

An example of this conjuncture (different problems requiring different criteria) can be found in the quote below, where the suggested methodology (referred to decisional process in the assessment of safety risks) consists of the following steps:

> *(a) Identify the inherent potential hazards.*
>
> *(b) Modify objectives so as to eliminate as many of the hazards as possible, and apply appropriate practice to reduce the risk of remaining hazards.*
>
> *(c) Quantify risks still inherent in the proposal.*
>
> *(d) If the risk and the consequential detriment are not acceptable, either find ways of reducing them to acceptable levels or abandon the project.*
>
> *(e) Monitor the actions that have been prescribed to reduce the risk and ensure that the actions continue to be performed.*
>
> *(f) Repeat stages (a) to (d) in appropriate depth before making any significant change in proposed equipment or procedure.*
>
> *(g) Inform and consult appropriate parties as circumstances require.*
>
> *(h) Be alert to developments that might permit further reductions in risk and detriment.*
>
> *(I) Act at all times with due regard to legal requirements and accepted good practice.*
>
> *The process must be gone through again for subsequent modifications to the plant and operating procedures.*
>
> (The Royal Society, 1983: 169,170).

The responsible for the above process is faced with a general problem (safety) composed of different sub-problems (identification, modification, quantification, acceptability, legal aspects, etc.) They proceed from different contexts and have different priorities. Questions arise: Which context (criterion) should be considered the most important? Are priorities in each problem issue listed in the same order? How can the relative influence of each criterion be demonstrated? These are essential questions to be answered, when its comes to considerations about responsibility and liability.

The impossibility of answering *a priori* which problem should be solved first stresses the need of identifying firstly the context, then each problem within this context, and solving each of these problems in an orderly way, according to 'its' priorities and constraints. The identification of the context (in this case, the security context) is vital because decisions made according to different priorities produce different effects, and rationality requires the identification and application of the criteria of choice, which may only be made after the context has been defined. It may be now easier to appreciate the priority given in this research to the identification of a clear, workable, criterion of demarcation of a security context, and to the analysis of both the requirements of management and the main issues within the decision-making process.

In order to avoid conflicts and confusion, a hierarchy of problems should be constructed, so that the output of the upper problem-solving exercise should be considered as a constraint, or a choice criterion, to the lower problem. This procedure, which may at first sight appear rigid, ensures the attribution of responsibilities and blame, because identifies the solver for each step of the decision-making process. What is also important, from the point of view of explanation, justification and control, the procedure offered allows the construction of models, thus the recourse to simulation and 'what if scenarios'.

Once the context has been defined (which implies the identification of the main criterion), Bellacicco's methodology requires the identification of the initial and goal state (definition of the problem), and the decomposition of the resulting problem space into minor, more manageable ones (determination of alternatives).

3.2.3.1.3.2 Determine the set of alternative solutions.

The identification of possible alternative solution is linked to the availability of information. Speaking of adversary problems, as most of those in security, this step is not one of simple collection of information, but a process of intelligence, including secret intelligence. The existence of an antagonist means that the most important information are protected or concealed; that those known to be known are changed, or used for deception and/or entrapping. Besides, the possible lines of action must be evaluated against the possible adversary's responses or activities, in order not to prejudice the goal-state of affairs, and to pursue utility, efficacy and efficiency.

3.2.3.1.3.3 Determine the criterion or criteria that will be used to evaluate the alternatives

This step derives from the precedents. If the problem has been well structured; if the possible alternatives have been identified, analysed and assessed, then the criteria to be used in the choice (time, availability, efficacy, user-friendliness, costs, etc.) become apparent from the reasoning.

3.2.3.1.3.4 Evaluate the alternatives.

In an ideal exercise, the evaluation of the alternatives would derive from the above steps, with it being the simple application of the selected criteria to each option. Evidence has been provided that this case is very rare in security. First, because different solvers will intervene at this stage of the process, each adding his/her own criteria, normally different from security. Second, because the security manager has no other means for defending the evaluation according to security criteria than asking an act of faith in his/her own experience. To-date, no agreed technique of evaluation has yet been offered by security scholars or professionals. Present attempts to evaluate security alternatives in terms of performance (eg, rates of deterrence, detection, charge, clear-up, number of intervention, etc.) do not cover the whole range of problems, and do not enjoy unanimous consensus. The available techniques come from general management. Having been conceived with different criteria and for different purposes, they have generally provided unsatisfactory responses to the task. Thus, frequently, a badly described evaluation in security terms of the alternatives is to be weighed against better structured - and frequently quantitative - evaluations, which, however, do not have security in mind.

3.2.3.1.3.5 Choose an alternative.

The above reasoning is likely to produce, at this stage, a situation where different solvers and/or different criteria intervene in the choice. An example is the following:

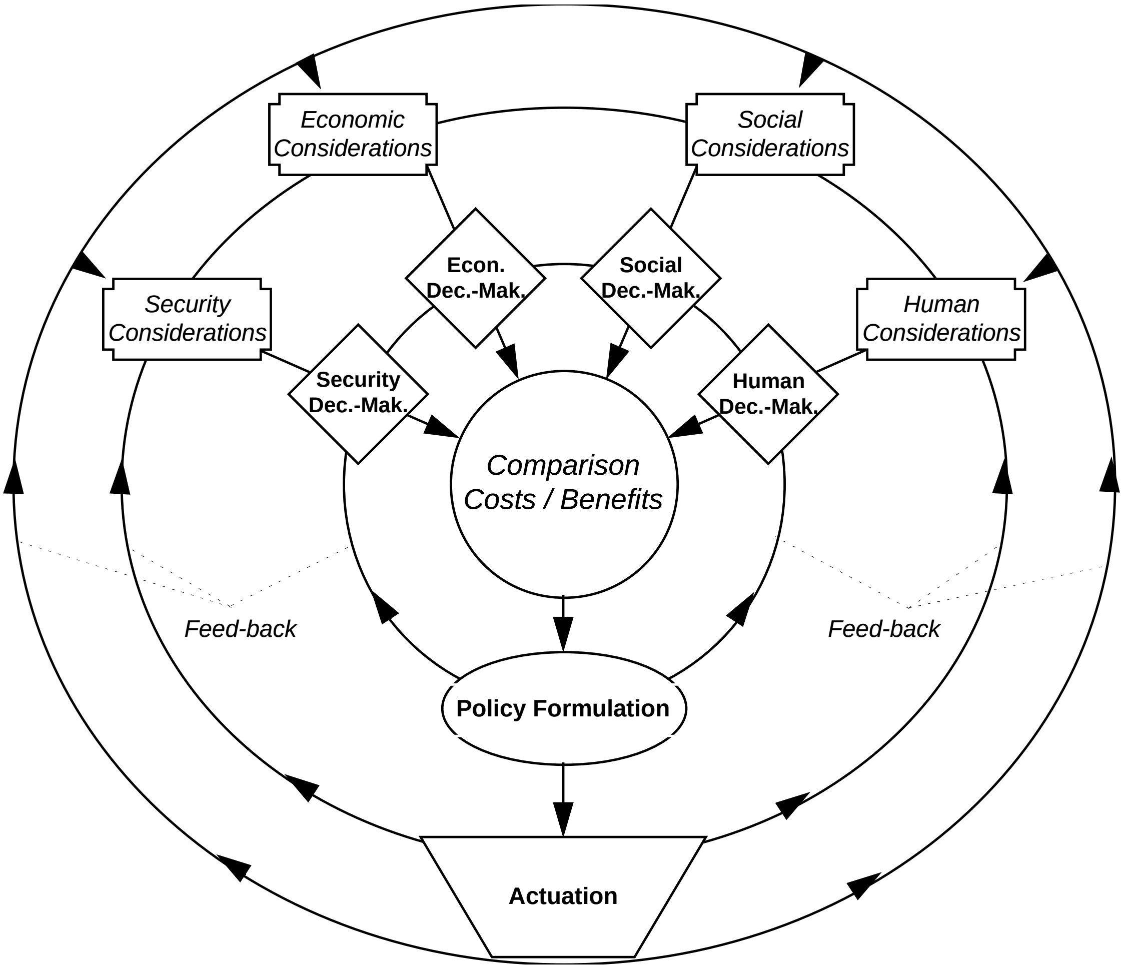

Figure 45: Interaction of different solvers at the same time

Here, a number of solvers of different aspects of a problem converge into a common process, where their reasons and criteria are taken into account. For simplicity, the process is represented at the same hierarchical and temporal level. That each solver has to deal with 'his' problem is obvious. What is not obvious, is how the phase of comparison (another Easton's 'black box'?) among different options coming from different criteria develops the final decision. In management theory, reference is made to the so-called 'multi-criteria' models of decision, where the decision maker prompts judgements about the relative weight of each criterion, and then specifies a preference for each alternative relative to each criterion. [362] This prompts questions: Who should be the decision maker? How relative weights are defined? How a 'best possible' choice is made? This calls in prescriptive theorists, who maintain that

[362] Anderson, Sweeney and Williams, 1994, Chapter 15

the analytical tool may only provide the correct solution to a given problem, where *correct* means 'in accord with the stated criteria and constraints'.

This raises two questions: How can we even say that a given solution is *'correct'*? Is a *correct* solution the one which also warrants better security?

In exact sciences, answers to these questions are not difficult. Straight and unbreakable rules exist; by applying them, one -and only one- correct solution is possible. If a wrong solution is found, the procedure (calculus) can be repeated and the error can be found and amended; thus, the correct solution can be recalculated. Section I indicates security as mainly connected with social sciences. In non-physical sciences, rules are not so straightforward and unbreakable to give one, and only one, solution. Hence, in security and outside technical problem, straight and unbreakable rules do not exist, and individual mental sets and reasoning are different. At the present, the only possible validation rule appears to be *'a posteriori'* from the outputs of its application. However, Section I has offered evidence that the same solution have different effects in different circumstances, and that its effects change after time. Thus, a correct solution (i.e., consistent with stated rules, criteria and constraints) may not necessarily offer better security. This raises problems whether a correct solution is also effective, and doubts about the reliability of 'a posteriori' validations in security. Here is where the statement of clear premises and the application of a scientific methodology according to an overall theory pay their dividends. They do not offer a perfect solution, but the possibility of explaining and improving the existing ones via a demonstrable procedure. They allow the problem-solver to *learn* from errors, modify the initial hypotheses and *converge* via correct solutions to the *best possible* solution, with *falsifying* the wrong ones and applying the necessary amendments to the faults of the reasoning, from premises to conclusions.

3.2.3.1.3.6 Implement the selected alternative.

The implementation phase does not present particular conceptual problems, apart from those arising from communication between the decision-maker, the planner and the executor. These can be reduced by using appropriate formats and models.

From a security point of view, problems arise at the moment of implementation in the presence of an antagonist. Any implementation of a security measure provokes a new problem: it changes the perception T has of the context, consequently T, and eventually P.

This requires the process to be re-started, according to new information. This is conceptually considered by the problem-solving process under discussion in the form of feed-back to the process.

3.2.3.1.3.7 Evaluate the results, and determine if a satisfactory solution has been obtained.

As for the alternatives, the evaluation of results is very difficult in security. Consistency requires the evaluation to be done according to the same criteria and techniques used for the alternatives. Again, the difficulty of measuring the effects of a security solution deputes the evaluation to general managerial techniques which do not provide a full account of what are the effects of a security measure.

Evidence has been provided that, with the partial exception of well structured cases of loss-prevention, results are hard to evaluate in security. First, because no value can be attributed to deterrence. Besides, a momentary suspension of T's activities in consequence of the implementation of new measures may prelude to an aggravation of the problem. Second, because the known indicators of performance (eg, rates of detection, charge, clear-up, number of intervention, etc.) while applicable - under not complete agreement - to some problems (deployment of resources for police forces and armed guards) do not cover the whole of security.

Again, a badly described evaluation in security terms is to be weighed against better structured - and frequently quantitative - evaluations, which, however, do not have security in mind, and take into consideration other aspects than security. Thus, in the absence of agreed criteria and methods of evaluation, comparison and assessment, the process of problem-solving cannot be satisfactorily applied to security.

It appears now that even a (hypothetical, in the absence of criteria for evaluation) 'perfect' solution to a security problem may be rejected by comparison with different solutions coming from different processes and criteria, which overweight the security criterion. [363] Examples are security decisions about terrorism in many countries, where security criteria are overweighed by the necessity of avoiding excessive interference with civil liberties and

[363] In the absence of agreed criteria of evaluation and for the purposes of this research, a security criterion is the one which applies the premises of the formal definition of security, i.e., the one whose aim is that of avoiding damages to the Asset

business. Managerial tools and criteria have been conceived for different contexts and problems than security. With security being not considered a hard-core activity within the majority of organisations, the possibility of its criterion being underestimated is not uncommon.

3.2.3.2 Summary

To proceed in the discussion from clear premises, a summary of the findings is essential. Evidence has been offered that security is frequently a problem within a larger one, for instance those at strategic or tactical levels typical of the organisation to which the security department belongs. It is also likely that the security problem contains other problems, as the obligations to respect laws and established rules, to protect image and to remain within a fixed budget, or to negotiate with the reluctance of a living Asset to carry out planned lines of actions.

It has been said before that prescriptive models of decision-making require that three basic steps should always be followed; namely: (a). Enumerate the alternatives between which a decision is to be made; (b). define the criterion, or scale of values, against which these alternatives are to be judged; (c). evaluate the alternatives on this scale. The task has been entrusted to problem-solving and its analytical tools, and Bellacicco's model has been chosen to provide the framework.

Experience indicates that, when applying Bellacicco's model to reality, (1) more than one possible solution remain; (2) constraints exist which, once taken into account, may oblige the solver to prefer not the 'best', but the 'most feasible' solution. Further steps are then to be added to the basic process, so as to prioritise the remaining options, verify the application of the existing constraints, and evaluate the results. As the process does not guarantee an exact solution and it happens in a changing environment, a feed-back mechanism of control must also be added, to modify the inputs where necessary, according to the necessity of optimisation and the basic Easton's reasoning in terms of cycles.

The process of identifying and evaluating the possible options, and making a choice, has prompted questions: Which criterion should be considered the most important? Are priorities in each possible context listed in the same order? How can responsibility and liability be attributed? The solution offered has been that of identifying firstly the context, then each problem within this context, and solving each of these problems in an orderly way. This is allowed by the framework of theory offered in Section II and assisted by scientific methodology. Descartes has taught how to conduct an orderly reasoning, through the proceeding of rejection, analysis, synthesis and control (the 4 golden rules). Popper has shown that a theory or hypothesis cannot be absolutely *verified*, but that it can *falsified* by evidence. Operational research offers operational methods and models. The security problem can be structured in accord with Bellacicco's model; having defined the initial and the goal states, the space problem can be divided into as many parts as necessary and possible, proceeding from the easiest to the most complex. Once the possible solutions (lines of action) are identified, the wrong ones can be '*falsified*' by data, information and evidence and the evaluation of the surviving ones can be done by means of OR qualitative and quantitative techniques, provided proper criteria of choice and performance have been defined. By this procedure, a solution (decision) can be defined as 'correct' when survives this logical ordeal, and is made according to precise rules of judgement (criteria and constraints). 'Correctness' is then translated into 'effectiveness' via feed-back processes of control and improvement, assisted by a theory and a methodology, based on empirical 'trial and error' process, simulation and analysis of 'what if scenarios'.

This reasoning leaves out areas for further study. Subject issues to be addressed are related to the choice of both the solver and the decision-maker, to the definition of criteria and techniques for evaluation, and to the comparative weighing of various non homogeneous criteria coming from general management, environment and security.

Having re-stated the premises, a framework of methodology follows.

3.2.4 Methodology

3.2.4.1 The identification of the context

All security decision processes start from the identification of the context. This is done by the verification of the presence and interaction of A, P, T. The verification of the existence of a security context allows for the priority of security criteria over the others. Once the existence of a security context has been confirmed, its main features must be defined, in order to draw a frame of reference which includes goals, priorities, criteria and constraints.

3.2.4.2 The Initial State

The definition of the initial State is based on an assessment. As considered in the previous Section, this assessment is based on 4 mental processes: perception, cognition, reasoning, and decision. It is relevant to appreciate that, without the perception of a Threat and a decision to protect, there is no security context, and that the assessment of a state of affairs in condition of antagonism is not a mechanical exercise of measurement, but an 'adversary' problem to be solved.

Surveys, interviews and data provide the relevant information for the analysis, which must be held initially on the basis of the general formula S = f (A, P, T) Si. Once all As have been identified, each possible S (A) = f (P, T) Si should be analysed.

The vital knot in this class of assessment lies in understanding the processes of perception and cognition, which provide the information and data to the reasoning, and therefore have a vital influence on the decision. The comprehension of the main hindrances to these processes, identified in Section II, (e.g., mental set, functional fixedness, interference, trial and error learning and insight) should convince the professional of the need of reducing to the maximum degree the subjectivity of this exercise, without losing in creativity, or flexibility. This result can partially be obtained through the use of pre-arranged standards, channels and procedures. Stimuli are filtered through a pre-selected standard; the accepted stimulus is communicated through the pertinent channel and processed via the appropriate procedure. The limits of this method are given by the existence of an antagonist, who can alter an existing stimulus, create a new, non categorised one, and provoke different stimuli at the same time. Hence, and provided it is known where it is applied, an input of subjectivity (human judgement) must be accepted.

The balance between the subjectivity of judgement and the objectivity provided by pre-arranged schemes depends on a 'quid' in the 'black box' of the solver, that is, 'something' based on his/her particular criteria of choice. It has previously been argued that even the choice of a standard, or method procedure, is an arbitrary act. These findings pinpoint to the core of each solution: the choice of the solver.

3.2.4.3 The Final State

The definition of the goal state may be based on a prediction (evolution of the present), or an arbitrary statement such as, for example, a desire, an attitude, an expectation, or an 'expert's best estimate'. In the first case, this statement may be formally justified via a mathematical calculus of the elements of the formula based on statistics, or by the explanation of the reasons behind the choice of a credible scenario (what has been defined: 'an educated guess'). In the second cases, the principle of justification lies in the authority of the decision-maker. Choosing one approach or the other is not relevant for a methodology to be rational, provided the final state is feasible and compatible with the problem space (or vice-versa). Feasibility depends on constraints (legal, financial, social, structural, etc.). Compatibility is sometimes difficult to ensure within organisations, where the overlapping of different solvers, problems and criteria may lead to the definition of a final State which is inconsistent, or even incoherent, with the problem space. All in all, in order to be rational, the stating of the goal state implies the identification of all the parameters of choice (including criteria, constraints and possibilities) to be adopted in the decision about the possible options, and the standards to be achieved for each element of the formula (A, P, T, Si). In the absence of such a procedure, the problem of defining, or limiting, the extent of the 'black box' will remain unaltered, and only 'aesthetically manipulated' by some sort of formal justification.

3.2.4.4 The Problem Space

Assuming So and S1 are defined, the problem consists in elucidating the space between them (problem space, or distance). Two ways are known in which a given problem space can be reduced.

One, is to use an algorithm, which may be thought of as a repetitive *'method or procedure for solving a particular problem that is guaranteed to lead eventually to a solution'* .[364] However, even in the simplest security cases the problem space may be quite wide, and the exploration of all possibilities may be beyond the capabilities of solution through algorithms.

[364] Penguin Dictionary of Psychology: Algorithm

> *'In many cases, they* [algorithms] *either do not exist (e.g. proving most mathematical theorems) or are so inefficient as to be of no practical value (e.g. finding the optimum move in a chess game)'.*
>
> (The Penguin Dictionary of Psychology: Algorithm)

An algorithm is more related to computerised than to human processes, as research shows that human beings, when solving problems, do not try to analyse all of the possibilities. On the contrary, they tend to stick to those possibilities which appear more likely to produce good results, or, when known, the desired results. How this first selection occurs is uncertain, but criteria of choice appear to be conditioned by learning, motivation, existing knowledge and perception more than by logic.

The second method, is to use an heuristic approach:

> *'Essentially, a heuristic is any sophisticated, directed procedure that functions by reducing the range of possible solutions to a problem or the number of possible answers to a question...they are provisional characterisations that allow for testing, evaluation and refinement of ideas and theories... Compared with algorithm, which is a procedure that guarantees the finding of a solution, in heuristic the search for solution is directed and not guaranteed'.*
>
> (The Penguin Dictionary of Psychology: Heuristics)

The heuristic strategy of decision is more congenial to human reasoning, and, in fact, this strategy was identified by Descartes (Discourse sur le Methode) a long time before the appearance of computers. [365] Essentially, it aims to break down the unknown area into different sub-areas, that are easier to define and analyse because of their inferior complexity. To reduce gradually the problem space, a series of sub-problems is identified, and then solved one at a time. After each step, an evaluation (or assessment) is made about the new situation.

Considering that even the simplest security problem is composed by a large number of variables and is subject to the dynamics of antagonism; and that most of problems must be solved 'in the field' by a 'human computer', frequently in a very short space of time, and

[365] This issue was analysed by Renè Descartes (Discourse on Method: discourse 2) and 'four golden rules' of an orderly reasoning were identified: (1) Never accept anything as true if it is not known to be evidently so. (2) Divide each of the difficulties under examination into as many parts as possible and necessary in order to solve it. (3) Conduct thoughts in an orderly way, beginning with the simplest objects and the easiest to know, in order to climb gradually, as by degrees, as far as the knowledge of the most complex. (4) Make such complete enumerations and such general reviews so as to be sure of omitting nothing.

sometimes in a situation of real fight with a reacting antagonist, security reasoning is best based on an heuristic approach.

One of such approaches uses the so-called 'Means-End Analysis'. This technique was developed by Newell and Simon in 1972, as a process of computer simulation, the GPS (General Problem Solver). It consists of comparing the initial with the goal states of affairs. The general problem solver's task is to reduce the problem space, that is to reduce the area of uncertainty between the two given states of affairs. By using a strategy of approximation based on a means-end analysis, it is possible to identify intermediate sub-goals which can lead to the final goal. Once each sub-goal is attained, then the problem space from the next sub-goal is evaluated, and the steps (or the strategy) necessary to achieve it are identified. Again, a Cartesian approach to the solution of a problem!

A caveat is appropriate. Research suggests that the development of a 'mental set' may distract the solver from considering fully all the available options. Experience shows that heuristics cannot guarantee a solution and, whilst they can be very useful as short-cuts to solving problems, nevertheless, as short-cuts often do, they sometimes impede the identification and exploitation of possible alternatives. A useful technique to circumvent this difficulty is 'Protocol Analysis'. Protocol are the steps taken in solving a problem, and are generally represented in security with event trees and flow-chart diagrams.

The identification of the protocol used in solving a given problem can help the solver to understand why a certain decision was taken, and to identify possible faults. In the first case, protocol analysis of similar cases may even provide evidence for a pattern, such as: 'when conditions are like this, s/he does that'. This evidence may be very helpful in making some hypotheses (for example, in the realm of the so-called physical security'), and in preparing procedures. In the second case, the protocol analysis may be the only possible way of controlling each step of the reasoning process.

This reasoning is repeated with increasing degree of resolution through the planning phases of policy, strategy, programme and project. It is assisted by qualitative and quantitative methods provided by Operational Research. [366] Qualitative techniques are best used in the

[366] The term was coined during W.W.II to describe the increasingly scientific approach being adopted in the planning of military operations. As scientists went back to their peacetime jobs, this approach spread, first to the nationalised industries and then to other industrial concerns.

beginning of the process, in order to clarify the general dynamics and to identify the areas where quantitative techniques are possible and useful.

The problem-solving process is a cycle. It is complete by adding the relevant controls in each step of the reasoning and by feeding back the relative outputs at the appropriate stage, in order to obtain approval and/or modify the inputs to be provided at the lower stage. Each modified stage restarts the process. The overall process of problem-solving in security is represented as follows:

Different Problems at Different Levels

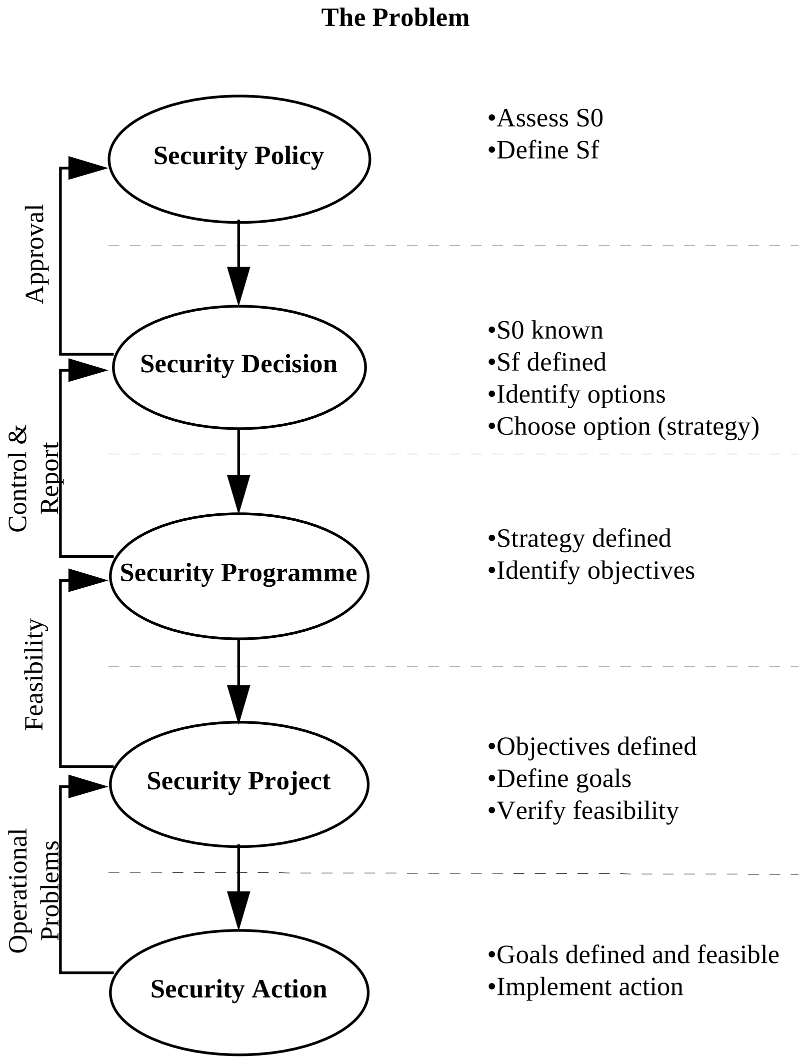

Figure 46 The Problem

3.2.4.5 The role of Operational Research.

It has been submitted that a set of useful techniques for assisting security problem-solving derives from Operational Research (OR). This discipline covers a wide range of approaches to the analysis of a complex system, in order to determine its overall mode of operation and to maximise its effectiveness.

> *'Operational Research is the application of the methods of science to complex problems arising in the direction and management of large systems of men, machines, materials, and money in industry, business, government and defence. The distinctive approach is to develop a scientific model of the system incorporating measurements of factors such as chance and risk, with which to predict and compare the outcomes of alternative decisions, strategies and controls. The purpose is to help management determine its policy and actions scientifically'*
>
> (in front of every issue of the Journal of the Operational Research Society)

OR quantitative and qualitative mathematical methods assist 'rational' decisions according to a succession of steps aimed to: the assessment of both the Protector and Threat's capabilities; the evaluation and prioritisation of goals and objectives; the evaluation and prioritisation of the options; the comparison of goals and options with the existing and predictable constraints; the identification of trends, 'what if' scenarios, and future problems.

It is not in the scope of this research to provide detail of these techniques (they have already been confined to the level of 'tools'), but to indicate those considered most interesting in solving security problems. Among the many techniques used in operational research, combining classical statistics with recent non probabilistic techniques, are: Soft System Methodology, Dynamic Programming and Control Theory; Optimisation Theory and Simulation. These methodologies usually involve the production of both a mathematical model of a system and a program that may be run on a computer. Because of the dynamics of the antagonism and of the psychological and political hindrances to the reasoning, no technique can guarantee a perfect result, therefore a caveat is appropriate.

Various considerations can be made, starting with the definition of OR. Firstly, it stresses the fact that OR is the application of scientific methods. Secondly, it implies that a earlier step had been taken, that is, the decision to direct and manage the various resources. Thirdly, it incorporates 'measurements of factors such as chance and risk' in its study, in order to compare the various possible alternative strategies, with 'the purpose is to help management determine its policy and actions scientifically'. Yet, difficulties present themselves in giving quantitative values to chance and risk, and the interference of the analyst cannot be avoided. This is an area of controversy and tension between the operational research analyst and the decision maker, and as such, should be carefully considered. To conclude, no claim is made to make scientific decisions, rather, to help structuring them as scientifically as possible. This, eventually, means understanding which parts of the decision are more exact than others, why, and according to which assumptions.

This understanding should be provided by models, whose main role consists in the identification of the limits of the study undergone. According to previous reasoning, this identification is essential for the clear statement of criteria and constraints, and particularly for the co-ordination between different actors in the decision-making process. OR scientists admit that the application of the OA approach to the study of a decision problem may require the use of the recognised techniques of any of the sciences, including the social sciences.

> *'...Given this it was natural that a separation of duties grew up between the operational research scientist and the manager'*
>
> (French, 1989, p.17).

3.2.4.6 The choice of the 'best' option

Once elucidated the problem space, and identified the possible options apt to bridge it, the question is how the choice (decision) is made.

Prescriptive theorists maintain that the choice must come from a comparison between different options weighted by a set of known criteria. This brings in the issue about how much can be known about, for example, the possible outcomes.

Different decisional environments have been identified, according to the degree of knowledge or predictability of the outcomes, i.e. decision under certainty, risk, or uncertainty.

Decision making under certainty means that the outcomes of each option are exactly known. The major problem in the process of making a decision under certainty is the determination of the trade-offs among conflicting objectives with direct relationship, such as, for example, quality versus price, or demand versus offer. Cost-benefit analysis was one of the models developed for decision under certainty. If outcomes are not certain, but their probability of occurrence can be statistically predicted, then decision are made under risk. Decision making under uncertainty means that neither the outcome nor the probability of occurrence of each option is known. The analysis of decision making under risk and uncertainty describes a problem in two ways: or in term of a decision tree, whose branches and knots represent alternative courses of action, decisions, and states of nature, [367] or in terms of a payoff matrix, a rectangular array whose rows represent alternative courses of action and whose columns represent so-called states of nature. A particular class of decisions under uncertainty is represented by 'games'. [368]

No '*perfect'* process exists that guarantees a '*perfect'* decision, or solution. Those identified issues which affect both thinking and problem solving come from subjective and objective factors, which have been identified in psychological, political and administrative, and generalised in Section II within the 'Situation'.

Situation (as the whole of factors which configure the 'here and now' of the reasoning) interferes with choices both at the beginning and end of the process. At the beginning, Situation should be seen as the main hindrance, in that its assessment is affected by both perceptive and cognitive factors. Indeed, it has been said that the same situation is seen differently by each individual. At the end of the process (notably, the moment of choice), Situation as the *ensemble* of physical and non-physical factors, gives the 'green light' to the decision, in that allows for, or forbids, feasibility of options. Factors such as legal and normative considerations, availability, funds, ease of installation, user-friendliness and maintenance of the systems, applicability of the procedures, are the ultimate obstacles to a 'rational' security decision.

[367] In decision theory this term refers to conditions that determine the consequences of a chosen action and that are assumed to be mutually exclusive and exhaustive.

[368] Games represent a problem under uncertainty in which the relevant states of nature are determined by other players, for example, on a wartime battlefield. Games in decision theory are distinct from those in Game theory, in which games are played against intelligent opponents -as in a game of chess- and not states of nature.

When making a 'rational' decision, it is then essential to identify what are the reasons behind the choice; that is, to know what the goals, desires, criteria, and constraints are, why and where should they be applied, in order to understand their influence. This reasoning is represented in the following model:

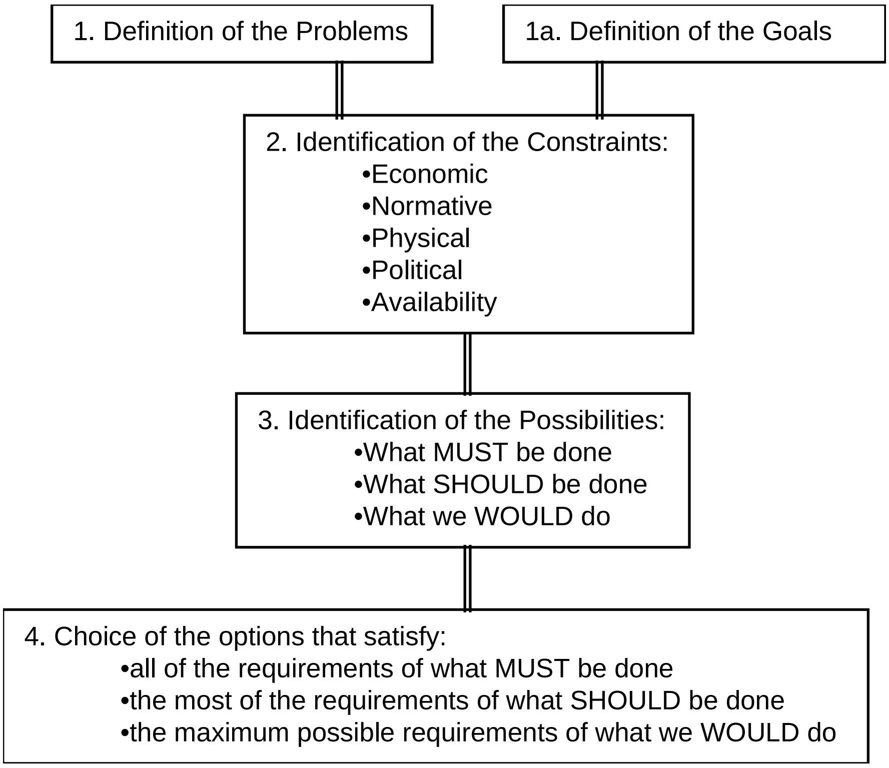
1. Definition of the Problems
1a. Definition of the Goals
2. Identification of the Constraints:
•Economic
•Normative
•Physical
•Political
•Availability
3. Identification of the Possibilities:
•What MUST be done
•What SHOULD be done
•What we WOULD do
4. Choice of the options that satisfy:
•all of the requirements of what MUST be done
•the most of the requirements of what SHOULD be done
•the maximum possible requirements of what we WOULD do

Figure 47: A modified version of the decision making process
proposed by The National Audio-Visual Association

The setting of decisional criteria may be considered as a postulational premise, thus a constraint to the solver. Yet, an important difference between choice criterion and constraint should be highlighted. Criterion, from the Greek κριτεριον (kriterion: 'sieve'), is a *'standard by which something is judged',* [369] in order to pass it, or pass not. On the contrary, constraint is *'something which limits, or restricts'.* [370] The analogy with the sieve is evident, when criterion is thought of as the mesh, and constraint as the rim. While the former is the *'sine qua non'* of admitted quality, hence non-negotiable, the latter is negotiable and acts as a 'limitation, or

[369] OALD

[370] OALD

restriction' of admitted quantities. To avoid confusion between criteria and constraints, their different relevance to the process should be well defined in advance.

> *"For example, an individual buying a car may, on the basis of a rational evaluation of all alternatives, come to the conclusion that one particular model is objectively preferable, but still lack the inner conviction that this is the best choice. This lack of commitment may be caused by a subconscious criterion (does the car confer sufficient status?) that conflicts with the criteria used consciously".*
>
> Noorderhaven, 1995: 8)

Decisional criteria in organisations are essentially driven by interest, while constraints are essentially imposed by contingency needs and obligations. Different types of interest, needs and obligations may be identified, but for the purposes of this research they have been reduced to three: political, social and economic. In the majority of the cases, the first tend to be a criterion, the last two tend to act more as constraints. At the political level of interest, the existence of a 'black box' (see: Easton's model) shows all of its evidence. The main point is that nobody knows what happens inside this box, except that a process of 'personalisation', which is probably based on 'expected utility' intervenes to modify any going-through decision. [371] Unfortunately, evidence exists that expected utility theory is not adequately supported by facts. A common position holds that, if we want the belief on which to base our decision to be 'rational', i.e., a 'justified true belief' it should be supported by statistic calculus. [372] However, the measure of preference is very hard to define, with the most 'objective' -money- having different values to different peoples, or to the same person in different circumstances. [373] This explains why the concept of 'expected value' was shifted to that, less specific, of 'expected utility'. Besides, the preferred outcomes coincide rarely with the most probable ones, and the expectation principle is often violated by overweighing outcomes obtained with certainty in comparison to outcomes that are merely probable. People actually appear to make different choices under seemingly identical conditions, and the need to

[371] *'[t]he essence of ultimate decision remains impenetrable to the observer -often, indeed, to the decider himself...There will always be the dark and tangled stretches in the decision-making process -mysterious even to those who may be most intimately involved'* (John F. Kennedy, former president of the United States, as quoted by De Smit, 1982: 45)

[372] Expectation is *'in statistics, the weighted arithmetic mean of the values taken in a distribution, the weights being the probabilities attached to the values'.* The Fontana Dictionary of Modern Thought.

[373] Daniel Bernoulli and other 18th-century researchers replaced the objective notion of monetary value with the subjective notion of expected utility, which takes into account the relative desirability of avoiding risk.

simplify complex decision problems leads them to adopt rules in which not all options are evaluated.

Social considerations play an important role in the decision, whose resulting activities must be placed to work into a social matrix, accepted and applied by people, within a social environment.

Ultimately, any decision involves economic gains and costs; while the possibility of a gain may be seen as a driving force, hence cost acts, at least in terms of feasibility, as a constraint.

Once the goals have been clearly stated, so to determine exactly what the criteria and constraints are, these features should not be considered once-for-all, but used as the 'touchstone' of every step of the process. A graphical representation of this concept follows:

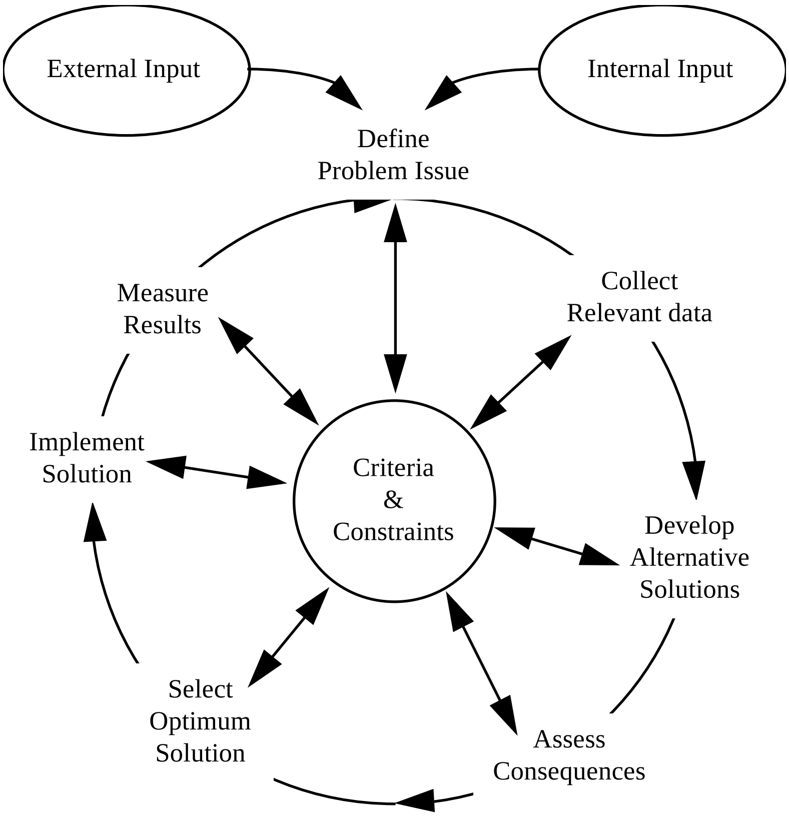

Figure 48 The Role of Criteria and Constraints

From the previous reasoning, it seems that arbitrariness and 'irrationality' can hardly be avoided in the 'definitional' process leading to the statement of criteria and constraints. This is not a major impediment to a 'rational' decision, assuming it is clear where they are applied.

Both arbitrariness and irrationality have a definite value, since creativity, leadership, and insight could not find place in the process, which would become automatic and deterministic, hence predictable (the worst possible outcome in antagonism). The issue is then: how can we control arbitrariness and 'irrationality', in order to obtain only positive results? Against which criterion of measurement, appreciation, or judgement? These questions lead the reasoning to a sort of inevitable circularity, whose only escape route has been identified in placing the criterion of arbitrariness in the choice of the solver and then constraining him within a fixed frame of reference, criteria, and rules.

The problem now becomes that of defining this frame of reference, criteria, and rules. Experience shows that arbitrariness tends to settle at the strategic level of decision. Some criteria tend to be arbitrarily settled, such as, for example: a philosophy, a policy and a set of constraints to the policy. Some goals are arbitrarily set, in terms of preservation and in terms of expectations. Even rules tend to be arbitrarily set: a hierarchy; line and staff communications; a methodology; a set of standards and procedures.

If a rational decision must be made on a given security problem, if some of the building blocks of the problem may not have an objective value, if the decisional criteria are affected by non measurable and hardly definable factors, then, how can it be stated that a rational decision is even possible?

It has been submitted that the reasons behind the dedication of efforts, time and resources to a decision making process are those of explanation and optimisation. Justification may be ensured by the application of the theory offered in Section II. As per the premises, in order to ensure rationality, security is to be the decisional criterion (the '*sine qua non*') within a security context, and all the other considerations must be seen as mere constraints (*sources of attrition*). The knot is: in a security context, the criterion of security must be absolutely respected; a strong influence of the constraints may be accepted (depending on the gravity of the problem), but not to the point of altering the priorities. When the criterion is social, political, or economical and security is only seen as a constraint, then that should not be considered a security context. This appear to be a very strong condition, which may leave out some areas traditionally belonging to security, such as, for example, the one known as 'loss prevention', where other criteria (for example, the monetary) have the priority over straight security consideration. Yet, it seems the only reliable condition for attributing security blames and responsibilities.

Assuming the condition of justification has been fulfilled, optimisation may only come from the application of a methodology, where all the intervening factors may be identified and weighted according to some model of qualitative and quantitative analysis, such as those coming from Operational Research. The interest is in evaluating and predicting the capabilities of a security system in terms of flexibility and reaction versus the settled goals and priorities; and the effects a new security measure has on the context as a whole (mainly, on Threat and Situation).

It has also been said that the key for rationality resides in the capability of perceiving changes and monitoring effects, so to allow for timely and consistent modification of the system in progress. Assuming, as this research does, the process as circular, these dynamics are ensured by appropriate feed-backs. Two of the relevant feed-back mechanisms depend on the 7th step of the problem-solving exercise (evaluation of the effects, and determination if a satisfactory solution has been obtained).

3.2.5 Conclusions

Security activities within an organisation are subject to management principles, and are evaluated according to managerial criteria of performance. This can open the way to problems, because of their possible incompatibility with pure security criteria, who are not definable in the same rigorous way. In order to understand these problems, a discussion has been made about the general decision-making process, and -more specifically- about the problem-solving process. The possible areas of conflict between the general manager and the security manager have been identified and discussed.

With present security lacking an overall theory and clear criteria of demarcation and performance, a confusion of roles and processes may emerge. There is evidence that managerial models are frequently adopted without any critical attempt of reinterpretation towards security concepts. [374] Doubts are expressed about this approach, [375] with a concern about the hybridisation of managerial and security processes, which (as hybrids are) has demonstrated a tendency to sterility in providing sound 'security' solutions. The answers to

[374] Broder ,1984; A.I.PRO.S., 1984; The Royal Society, 1984 and 1992; Walsh, T.J., and Healy, R. J.,1996

[375] Juliano, 1996

these problems are linked to the choice of the methodology, since justification and optimisation depend upon it. One has been offered.

Previous discussion on science has shown that methodology alone is not enough. To ensure both justification and optimisation, uncertainty must be reduced to a set of 'justified true beliefs'. To add to general knowledge, methodology must be supported by a theory. The offered theory shows here its value: it allows for the formulation of hypotheses which, assumed as constraints, reduce the uncertainty into a frame of reference, thus allowing - via the offered methodology - for the use of known methods of analysis, modelling and calculation. If this theory is valid, or imperfect, it is not the point. What matters, is the fact that it allows for falsification and, eventually, progress.

The procedure outlined in this sub-section delineates a logical path applicable to possible problems and reasoning. In order to apply it to a given context, it is important to know not only *how*, but also *why*, *where* and *when* to apply it. This knowledge is necessary, because any decision provokes a change of the existing state of affairs, and consequently, a knowledge of the general dynamics of the context is essential to identify, understand, and possibly evaluate, the resulting outcome. Outputs will provoke new inputs, and there is a need to predict and influence the subsequent next process. This procedure can be carried out if a model has firstly been set up, where these outcomes are normally seen in terms of outputs, which provoke a new cycle of decisions. This is discussed in the next sub-section.

3.3 THE PROPOSED APPROACH

The theory and the methodology previously delineated offers a frame of reference on which to attempt the development of a model. This frame of reference has been formalised in the logic formula:

$$S\ (A) = f\ (P, T)\ Si$$

and in the procedure for solving a security problem. Security activities are seen as a part of the conflict between P and T, where A is the stake, in a given Situation. The condition of security is then the result of the activities of opposite counterparts, aimed to achieve and maintain a competitive advantage, in a context characterised by A and Si. On the one hand P, according to her/his interest on A and striving to maintain the control of the context, reacts to new perceptions of T or to a change of A by modifying Si. On the other hand, T reacts to changes of Si, P, A, by modifying her/his choices and capabilities, and trying to adapt, or use, Si according to her/his own intentions. Since every action is initiated by, and provokes, a decision, a security process is marked by a series of decision-making exercises. Each decision is followed by the implementation of appropriate measures, and the whole process is subject to careful evaluation and control, in order to adapt it timely to any relevant change. With any context being, by its own nature, a unique and open system, all the actors are modified by, or react to, any perceived change of the Situation and the Environment. It follows that the basic components and relations of a particular security context may be assessed only after the Situation and the Environment.

Once this process of definition is made, the possible resulting dynamics and effects can be evaluated, in the limits of the existing knowledge, thus allowing for a reasoned statement of goals. Once goals are stated, rationality requires policies, strategies, programmes and projects to be formulated in cascade, so that the outputs of each process constitute the input to the successive. The consistency and coherence of these different steps may be achieved and controlled through the application of a defined methodology, possibly encapsulated in a suitable model. After verifying that the model does indeed reflect the intended methodology, comparison of its results and experience drawn from the real world, will allow to validate it and, with it, the methodology at its origin.

Once the rationality of the general process is ensured, optimisation can be taken into consideration. This is aimed to the reduction of time, costs and risks associated to any particular security decision, and may be performed in two main ways, as a trial-and-error process , or as a structured analysis, supported by calculus, linear programming, simulation and so on. The latter seems a more profitable and less risky way of attaining the desired results. Here, the recourse to modelling pays further dividends. The questions are: can such a model be built, in security? And, if possible, to which extent a model built on these premises can be considered as reliable?

3.3.1 The Model

A model may be defined as a subjective and simplified representation of the system object of analysis. It cannot represent the whole of the system, but it is forced to focus on certain particular aspects. Subjectivity depends on the choice of these aspects based on the assumption of their relevance. Wilson emphasises the subjectivity of models, their subsequent variety, and identifies the key to model evaluation in usefulness:

> *'A model is the explicit interpretation of one's understanding of a situation, or merely of one's ideas about that situation. It can be expressed in mathematics, symbols or words, but it is essentially a description of entities, processes or attributes and the relationships between them. It may be prescriptive or illustrative, but above all, it must be useful'*
>
> (Wilson, 1990, p.11)

This usefulness is reflected in the possibility of organising the knowledge on the system under study available to the model builder. This can be done in a number of ways. According to Mc Quail and Windahl (1993), Deutsch made a distinction between 'structural' models, which were mainly focused on the pure structure of the system, and 'functional' models, aimed to reflect the actual interrelationship between the elements within the structure of the system. He identified the main advantages of models in their capability of providing organisation (description), prescription and prediction[376].

[376] *'Deutsch (1966) notes the following main advantages of models in the social sciences. Firstly, they have an organising function by ordering and relating systems to each other and by providing us with images of wholes that we might not otherwise perceive...Secondly, it helps in explaining, by providing in a simplified way information which would otherwise be complicated or ambiguous. This gives the model a heuristic function, since it can guide the student or researcher to key points of a process or system. Thirdly, the model may make it possible to predict outcomes or the course of events. It can at least be a basis for assigning probabilities to various alternative outcomes, and hence for formulating hypotheses in research. Some models claim only to describe the structure of a phenomenon. In this sense, a diagram of the components of a radio set could be described as*

For the purposes of this explanation, descriptive and organising models may be equated, since the description has to derive from some organised knowledge base. Prescription differs from description in that it aims to identify possible solutions and courses of action, rather than just offering a convenient layout of the system under study. Descriptive models are used in many different disciplines, from logic to linguistic analysis, from management to training and planning. By identifying the key elements of the system, a model shows how such elements interact causing the system to behave the way it does[377]. The same model may then be used to prescribe how the system should work, by, for example, adding values (the difference between a event tree and a decision tree), adding a time factor (the passage form model to simulation).

A typical example of a descriptive-functional model in security may be found in the Kluwer's Handbook of Security (5.8-09):

"structural". Other models, which we call "functional", describe systems in terms of energy, forces and their direction, the relations between parts and the influence of one part on another' (McQuail & Windahl, 1993 p.2-3)

[377] *'A model seeks to show the main elements of any structure or process and the relationships between these elements'* (McQuail & Windahl, 1993 p.2)

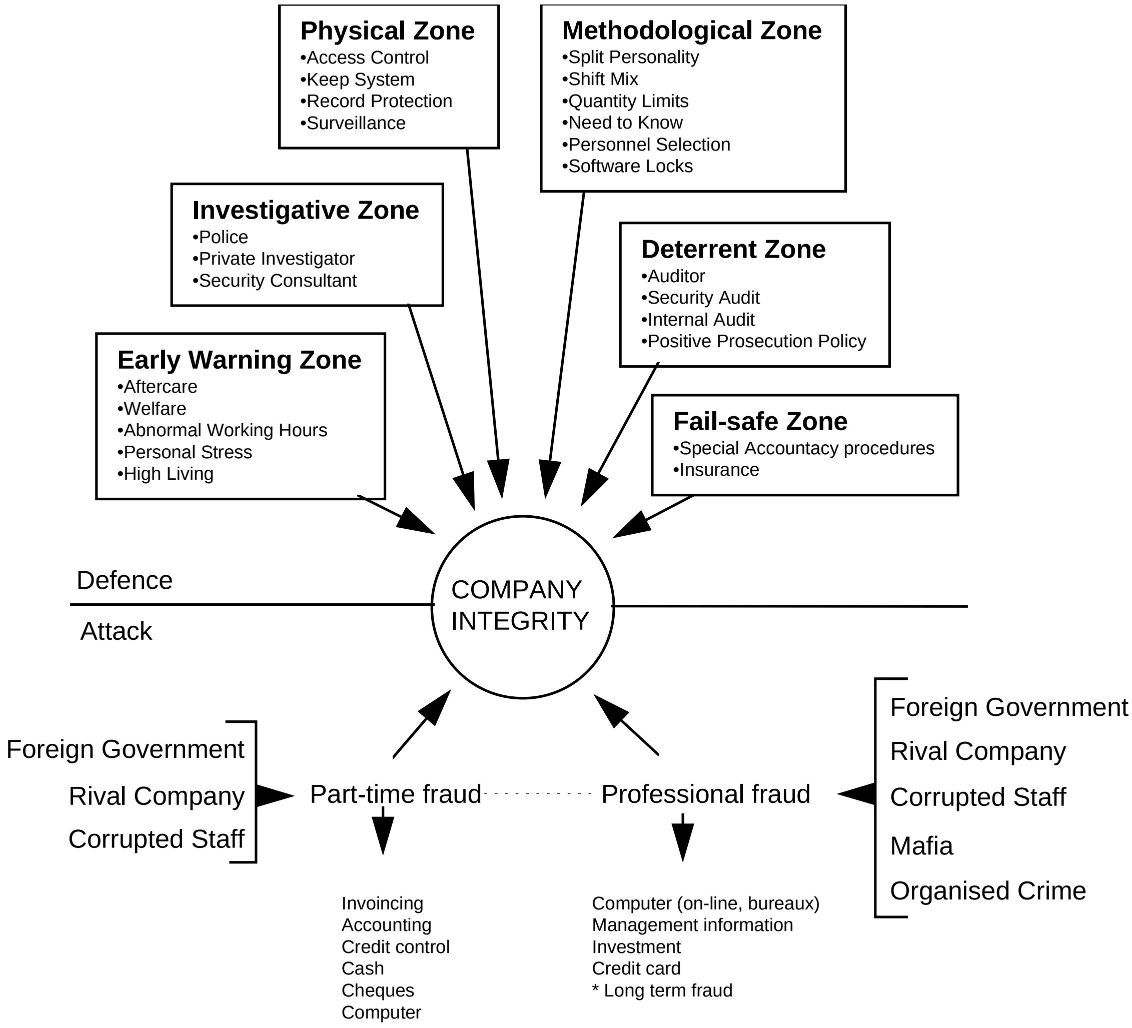

Figure 49 Security against fraud

No information in this model is aimed to indicate what actions may be taken to reduce fraud, the model is not, therefore, prescriptive. A time factor is not included, which makes it impossible to carry out some form of prediction on the problem. Nevertheless, by identifying the key functions and elements present in a fraud security context, it allows for more specific models and/or simulations to be developed, if prescription, prediction and optimisation need be performed.

Many predictive models are drawn by simply translating a descriptive model into mathematical formulas. Once components and special patterns or relationships have become clear, they may give an insight into the future behaviour of the system[378], in a similar way of a

[378] *'A model is first of all a convenient way of representing the total experience which we possess, of then deducing from that experience whether we are in the presence of pattern and law and, if so, of showing how such patterns and laws can be used to predict the future'* (Rivett, 1980, p.1)

mathematical formula, where the building blocks and their relations are defined. Finally, and similarly, a predictive model may provide a powerful tool for creating 'what-if-scenarios'[379], by changing the input value of the determined variables, and allowing, therefore, for sensitivity analysis on the elements of the system, and optimisation to be carried out.

Game theory, flow-charts, event and decision trees, influence diagrams and system dynamics, and so on, are all techniques allowing for descriptive-prescriptive-predictive models to be developed. All models are, by their own nature, imperfect and limited. They are built on the ground of assumptions and use input data which are often only estimated. Outputs from the model can only be interpreted properly with a knowledge of the assumptions and the reliability and credibility of the data, and must be treated with caution, particularly when attempting some form of prediction. In order for the models to be serviceable, of course, a certain amount of 'faith' upon the analyst is implicit; no harm may come, however, if 'faith' is tempered by scepticism on the supposed 'objective value' of the results.

> *'The measure of success in modelling is not that you can produce a model that is bigger and more sophisticated than anyone else's but that it adequate answers the original questions for which it was developed'*
>
> (Wilson, 1990, p.10)

The opinion that models should have strong quantitative characteristics, allowing, therefore, as in the case of a mathematical formula, for some kind of exact solution, is not unusual. Wilson, on the contrary, stresses the fact that this need is not always imperative, and a more qualitative approach may be pursued, leading to a softer analysis, but not necessarily less precise outputs. Models are built to assist the decision making process, which, in organisations, is made of different sub processes, at different levels (strategic, administrative, operational or tactical). Models should then be built to represent the different needs, characteristics and aims of this different stages. This Babel of models is not, per se, confusing, if the decision making process, and its different sub-processes or stages, are well understood. Only by preparing a meta-model representing the meta-knowledge according to which decisions have to be taken, may 'rationality' be ensured, and these models developed, verified, validated and applied consistently and coherently. This requires reciprocal understanding and

[379] *'...it allows extrapolations to be made from known to unknown conditions and often provides an indication of the manner in which the real life system can best be controlled and decision about it taken'* (AMOR: OA 003 OCT '95)

close co-operation between the analyst and the decision maker. Waters (1989) sees the process as follows:

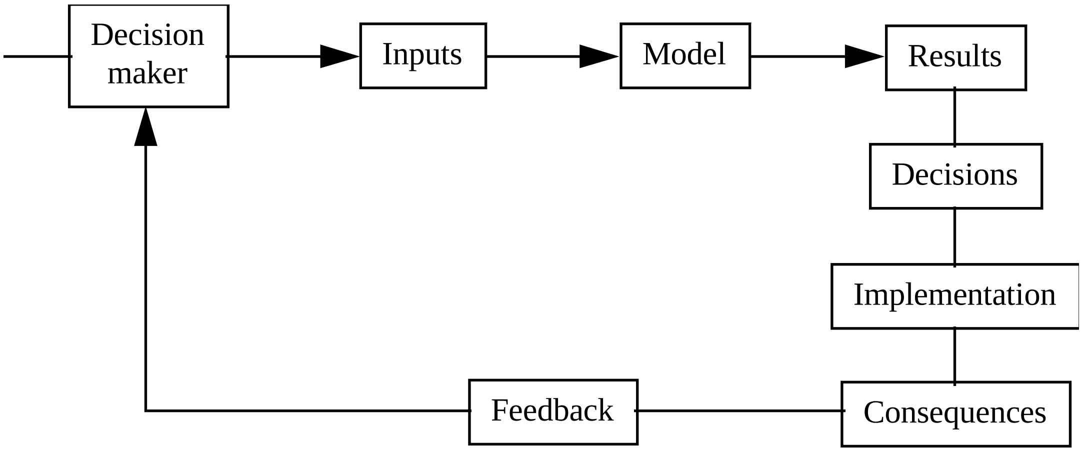

Figure 50 Waters's Feedback in Decision Making

The decision maker gives certain inputs to the analyst so as to create the most convenient model. This part of the process may be seen as the model requirements phase, where the decision maker assesses in which part of her/his decision making process s/he is in (study of the initial state of affairs, identification of the alternatives, and so on). This leads to further consider the importance of co-operation between the analyst and the decision maker, in the attempt to understand their reciprocal needs, and the ways these needs can be satisfied. If the decision maker is not able to realise at which stage of the process s/he is in, or cannot explain this to the model-builder, the latter might provide the wrong type of model (e.g., predictive instead of descriptive) and jeopardise the outcome of the process.

For instance, if the decision maker asks for a description of a situation, the analyst has two choices: either to gather all possible data on the situation and build a descriptive structural model, or to identify the main actors in the systems and their general relationships and, in so doing, formulate a functional model. Whether to follow the first or the second approach, depends very much on the way the decision maker poses the nature of the problem. What is essential, is that both decision maker and analyst agree on what they are doing, on the role of the study commissioned, and, therefore, on the role of the model to be built.

This procedure can be carried out if a 'general' decisional meta-model has firstly been set up, where -according to Easton- outputs provoke a new cycle of decisions. The following attempt to describe the co-operation between the security decision maker and the analyst will start from a general model of a security decision-making process. The identification of the different decision-making processes inside the security function will guide the choices behind the building of coherent operational models.

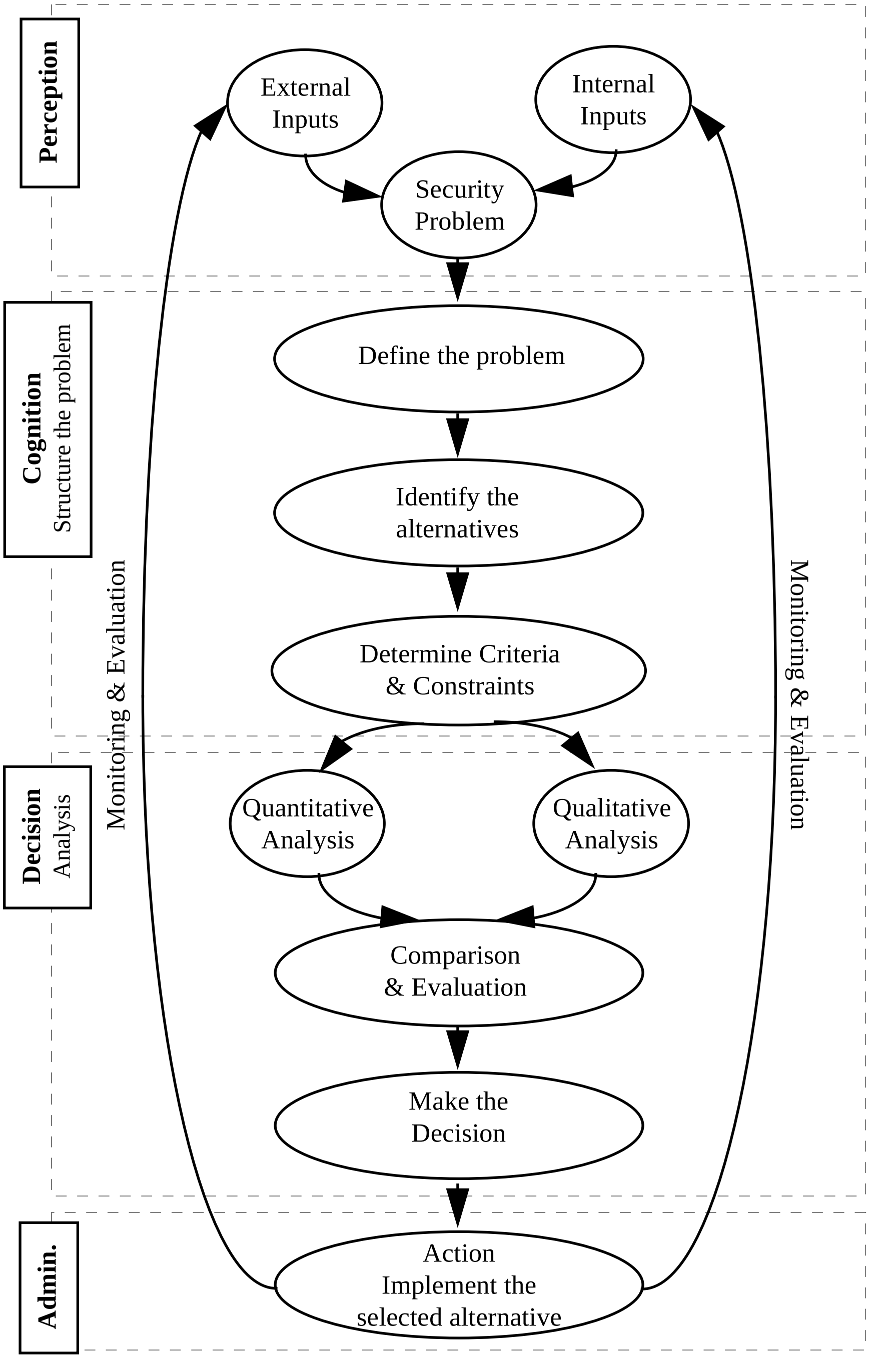

Figure 51 A Security Decision Making Process

The model above depicts a complete process, and identifies the main decisional levels. These, previously identified as: perception, cognition, decision, and action, will be now analysed according to the previous findings and my overall position.

3.3.1.1 Building a Security Model

The first phase to consider is that of Perception. Perception in security needs timing and precision. A stimulus may only be noticed in time and precisely, if the appropriate steps of training are taken to stretch the perceptive outreach and improve the perceptive range through an appropriate process of cognition. In security, the necessity of perceiving a threat timely and precisely calls for an initial decision making process, so as to define what is essential to perceive, through which channel it has to be communicated, and within which framework it has to be processed. This initial process will follow the model depicted above at a very general level of definition. What is essential at this phase is not that outputs are absolutely correct, but that the absolutely wrong inputs are rejected. The resulting decisions must be implemented through planning, and actions (e.g., installing an alarm system, providing intelligence, training for awareness...), which, in a pro-active approach, are introductory to the main process of dealing with, or 'managing' the threat.

Assuming the above process to have been accomplished as the initial and essential groundwork for establishing a security function, the model will only consider pre-defined classes of stimuli to be accepted as input in the general process. Once the existence of a problem has been perceived, the verification of the problem context constitutes the preliminary step to the main exercise. This step aims to verify whether the frame of reference of the reasoning is, or not, one in which security is the main criterion of decision. In this research, the presence and interaction of an Asset, a Protector and a Threat are considered the necessary and sufficient condition to configure a security context.

Assuming this preliminary condition has been satisfied, the process of modelling in security may continue from clear premises.

The second phase of the model is that of Cognition. This starts from the so-called 'definition of the problem', an essential step, since on it depends the structure of the model to be used for its solution. Understanding and co-operation between the decision maker and the analyst will help obtain the desired results with the minimum of interference and without overlooking vital areas while concentrating efforts in the wrong direction.

According to the approach offered in this research, and making reference to Ansoff's and Bellacicco's models, security problems fit into three levels of definition (strategic, administrative and operating or tactical) and can be classified into four types of circumstances:

1. that of knowing (assessing) the present (or initial) state of affairs;

2. that of deciding which final state of affair is best suited to the organisation's needs, beliefs, and desires;

3. that of identifying which final state of affairs we will reach using well identified lines of action. In this case only the initial state of affairs is known, and different final states of affairs are possible, so that the intermediate space is unknown, and the final one is undefined (i.e., Protector -being in a dynamic, changing condition- has not yet identified all her/his possible options and cannot even make a choice of her/his preferred state of affairs).

4. that of clarifying the intermediate space between known states of affairs (i.e., Protector wants to obtain a specific result, such as the exclusion of the possibility of intrusion, a diminution in losses, an improvement in control, and the possible options must be identified and weighted).

At a first look, only the fourth type of problem seems to fit well with the classical (e.g., Bellacicco's) definition of problem. However, some more thought is dedicated to the matter, all categories listed above are problems to be solved.

It has been said before that these problem-solving exercises have different level of resolution and are aimed to the definition of policies, strategies, programmes, and projects. Since the choice of the model depends on the goal to be achieved, it is important to define at which level is needed. The whole security problem is represented in the following diagram:

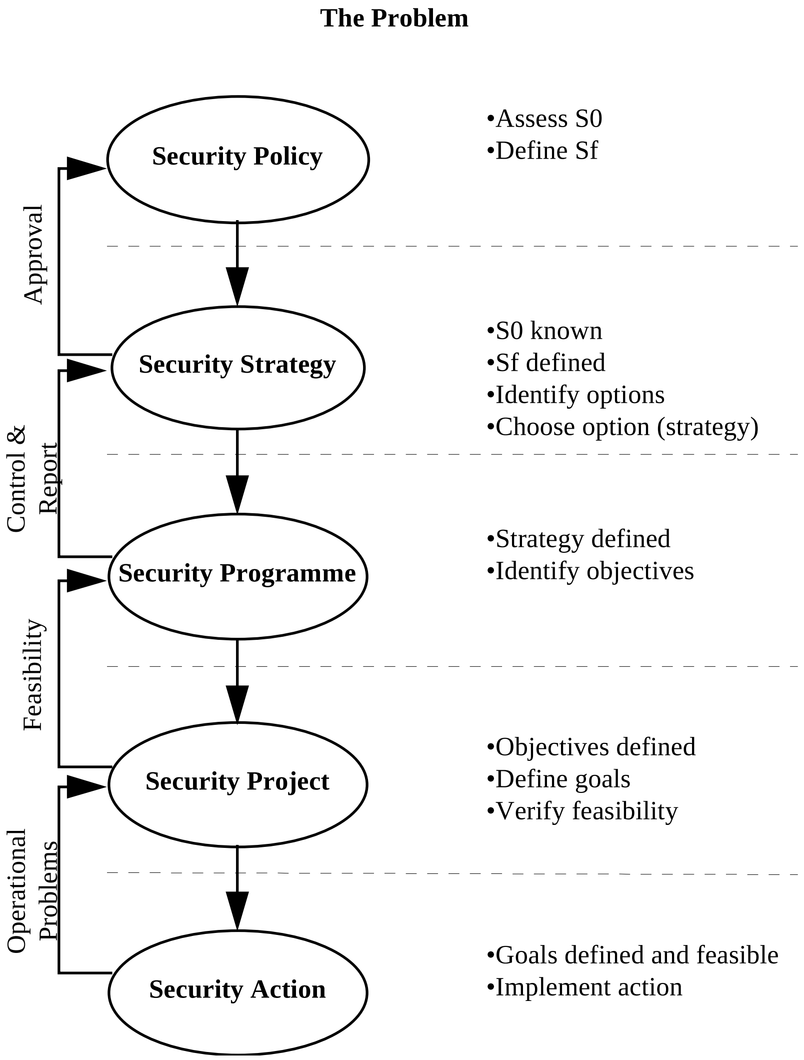

Figure 52 The Security Problem

Having defined both the problem and the level at which it has to be solved, the choice of the model technique (i.e., qualitative or quantitative, descriptive or prescriptive...) follows as a consequence of the reasoning. This makes a dispute between the decision maker and the analyst very unlikely and, anyway, easily solvable, because of the clarity of the premises.

Having chosen the technique considered useful for the problem , and according to its level, it becomes now possible to proceed to 'structure the problem', which -according to methodology- requires the unequivocal definition of the following premises:

1. the identification of the options,

2. the analysis of the criteria of choice,

3. the assessment of the constraints,

4. the proper setting of the subsequent priorities.

At this stage, the identification of the relevant features of the Situation, and the Environment, helps to identify their interactions with the basic components (A, P, T), hence to define the secondary criteria, and the main constraints.

The phase of the identification of the options is peculiar to each exercise, and as such will not be dealt with at this stage of the reasoning, which is only aimed to identify the general guidelines for the decision maker and the analyst. A general idea of the process will be provided in the discussion about the applicability of the model.

The settlement of criteria and constraints need to be made at each convenient decisional level, where they should be ordered according to the preferred priorities. It is plain that, in order the process to be 'rational' and to reduce arbitrariness, all the rules must be clearly stated as a premise to the exercise, together with a clear methodology of control. Rationality will then consist in the observance of stated criteria and constraints (rules) in each phase of the process, and not only at the moment of the decision. To prepare this set of rules, a series of question must be answered, of which those here considered as the most essential are:

Are priorities the same at each level?

Certainly not. Their determination depends on the typology and culture of the organisation. For example, in the context of business and industry, it may be found:

Table 4 The priorities at different decision levels

At the Strategic level	*Brand*
	Image
At the Board level	*Image*
	Secrecy
	Credibility
	Profit
At the Area level	*Profit*
	Business continuity
	Market share
	Research
	Credibility
	Public Relations
At the Sub/area, local, level	*Internal relations*
	Production
	Storage
	Communication
	Distribution
	Sale

Experience shows that a very common priority of the decisional criteria to be used in organisation after the principal (i.e., that of security) is the following:

Table 5 Decisional criteria at different levels

Strategic level:	Utility
Administrative level:	Cost-effectiveness
Operational (Tactical) level:	Efficacy

How do we control if the stated priorities are true, in a given organisation?

- In terms of results

- In terms of expectations

How do we measure achieved and expected performance? Since security is an auxiliary function within the organisation, to abandon the definition of the criteria of measurement to security people (the same whose performance should be 'measured') would be a naiveté and an organisational absurdity, and, consequently unacceptable to any serious manager. Of course, this does not mean that the Security Responsible must be a passive receptor of decisions, but that her/his point of view, though relevant, should not be the essential. The position in this research is that of delineating a methodology where responsibilities, scopes, goals, blame, and performances can be precisely identified, attributed, and measured when and where necessary and convenient. In this view, no decision at any level can be made in any organisation until the following areas of doubt are made absolutely clear:

- How do we measure expected utility?
- How do we measure utility?
- How do we measure expected effectiveness?
- How do we measure effectiveness?
- How do we measure expected cost-effectiveness?
- How do we measure cost-effectiveness?
- How do we measure expected efficacy?
- How do we measure efficacy?
- How do we measure expected costs/losses?
- How do we measure costs/losses?

The third phase of modelling is that of Decision Analysis. Once the problem has been structured according to the previous step, decision comes from the choice among different options, which can now be carefully weighed via a process of analysis of their relevant features. Many different techniques exist for such a process, from qualitative to quantitative.

It is not relevant to this research to analyse all of them. The extreme difference in the nature and characteristics of the actors (in term of Motivation, Capability, Mental Processes...etc.), of the Situation (such as Vulnerability, Opportunity, Constraints and Possibilities...etc.), and of their resulting dynamics and processes, strongly suggests to go no further in this direction, at this level of argumentation. Since their analysis has little or no influence on this level of reasoning, they are seen in this research as 'tools', and, as such, to be chosen and employed according to specific needs and peculiar interests which discussion is considered irrelevant for the purposes of this research. There is not such thing as 'a single most useful tool'; any of them may be important, even essential, in some level and phase of a security activity, but it is not possible to anticipate which, in a general methodological approach. It is important, though, that the chosen technique allows for a comparison and evaluation of the options and constraints as identified and defined in the previous stages.

It is now the moment of making a decision, i.e., making a choice between all the identified and weighed options. To say that this choice will always be the *inevitable* outcome of the above methodology would, according to the findings, be 'unnatural', since the influence of the human factors inside the 'black box' would be denied. Besides, it would consider as definitive the response of a methodological process which may only have the ambition of assisting decisions, but certainly not making them.

The fragility of the human support of rationality in security decisions should not discourage from a quest for a methodology. This is needed to provide a framework against which the contents of 'rationality' of security decisions can be measured and assessed, and to identify the areas where this rigour is not achievable.

The principle of 'rationality' has been ensured in the application of a given criterion, or 'scale of value'. It has also been said that the different levels of decision making (which in this approach range from policy to project) are made within different frames of reference in the organisation, each one having, probably, different criteria and priorities. Since not all criteria and constraints are equally important (or equally compelling) for every organisation, it seems reasonable to list them in an explicit scale of precedence, so that only those options who pass a previous, and more important, criterion, will be admitted to the test of the following, less important ones. An example of such reasoning may be found in the following diagram, where all the options which have passed the criterion of security are subject to sequential tests, according to a priority of criteria here identified as possibility, budget, constraints, and effectiveness:

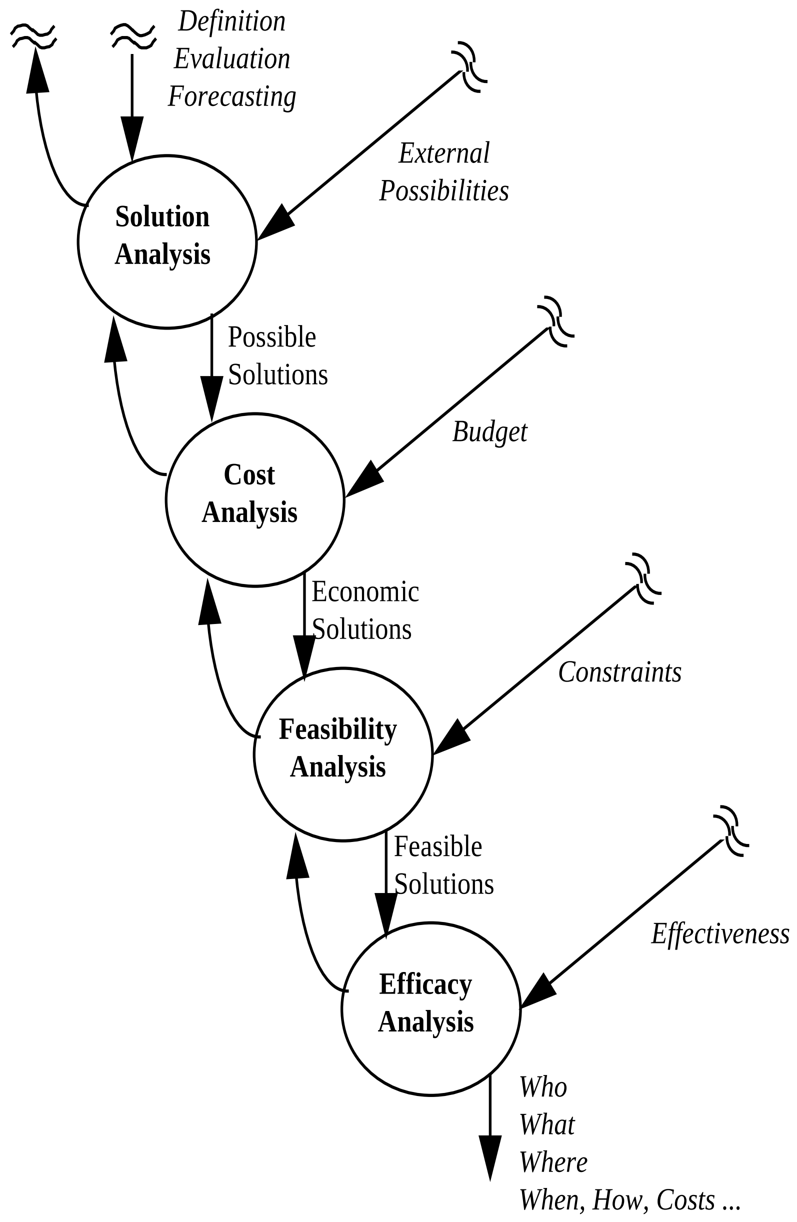

Figure 53 The cascade application of criteria

Of course, a model of (simultaneous) multi-criteria choice may also be applied but, because of the different belief-systems in security and business, this would probably be at the expense of clarity. In a multi-criteria model of choice, it seems highly probable that the justification of the rules (priorities and principles) followed in a particular choice could be less evident to, or even lost by, the non-specialists.

The last phase of the security decision making modelling is the Administrative. Here the decisions taken have to be implemented and closely monitored, so that their effects can be immediately re-evaluated in a further incrementalist decision making process.

To conclude, it seems important to repeat that the definition and structuring of a security problem is not a once-for-all exercise, as it happens within the dynamics of conflict. The need for decision in security is continuous and lasts until a Protector is present and active, and has previously been represented as a never ending spiral of problem-solving exercises adjusting the system to changing circumstances, and stimulated by a new perception of Threat.

3.3.1.2 A Security Model

In the previous paragraphs, all the relevant aspects of a security process have been identified and a decisional model has been defined. Consequently, the different stages where a security decision can be necessary and the different typologies of problems which need to be solved have been identified. Different typologies of problems are dealt with different techniques of analysis, whose choice may lead to ineffective results if the co-operation between the decision maker and the model builder is not based on a ground of mutual understanding. Coherently, a procedure has been discussed for assisting the security decision maker in guiding the analyst through the building of a model consistent with her/his problems and needs.

3.3.1.2.1 Premises

Before proceeding to prepare a general model of a security process, to be coherent the methodology and findings, it is necessary to state the premises on which this part of the research is based. These are the following. The solution of a security problem starts from the verification of being in a security context, and from the assessment of the secondary criteria and the constraints coming from the situation (general and specific). This allows the reasoning to start from clear premises. Once criteria and constraints have been fixed, the security process passes through a series of problem-solving exercises, which are characterised by a top-down approach (assisted by opportune feed-backs) and by an increasing degree of resolution. Each exercise conforms to the general methodology, which requires the following steps: (1) the assessment of the present state of affairs; (2) the exact identification of the goal(s); (3) the setting of a scale of values; (4) the identification of the possible options; (5)

their analysis and weighing; (6) the choice of the preferred option; (7) its implementation; (8) the control of its output; and (9) the input of the relevant feed-backs into the pertinent phases of the process. The solution of each exercise provides the general framework (premises, criteria and constraints) to the following. The idea is that a security problem must be re-analysed repeating the whole decision-making methodology from the political to the tactical level with increasing degrees of resolution. This allows consistency, rationality and control.

3.3.1.2.2 The Fundamental Problems

Having stated the premises and the general methodology, this attempt starts from the consideration that, in security, six basic questions are to be answered at all levels of the process:

- What is to be protected?
- From Whom?
- Why to protect?
- Where to protect?
- When to protect?
- How to protect?

These answers (decisions) are repeated with increasing levels of resolution according to the previously described top-down approach, which starts from the general Policy of the Organisation and aims to:

- state a Security Policy;
- decide a Security Strategy;
- formulate a Security Programme;
- prepare a Security Project.

The process produces a series of plans which, in order to be accepted and effective, are to be prepared consistently with the organisation's planning.

3.3.1.2.3 Stating a Security Policy

The first exercise aims to the statement of a Security Policy. Because of its relevance on the Organisation's assets and image, this policy derives from, and is consistent with, the Overall Policy. Ideally, the exercise should be conducted at Board Level, with the addition of the Security Manager and, eventually, external consultants.

A Security policy is intended to indicate to those concerned what the organisation will, and will not, do in pursuit of its overall purpose. Such statement expresses the organisation's culture and belief-system, which is certainly affected by a major factor (the attitude of the organisation's owners and rulers), but is also influenced by the environment, and particularly by the so-called 'social responsibility' factor. Moreover, a Security Policy must obey to constraints coming from the external environment (laws, regulations, codes of conduct, image, etc.) and from the internal (trade and labour unions, pressure groups, etc..). All the constraints and influences are evaluated in terms of the organisation's interests, all the threats to the organisation are identified and the relevant problems which solution pertains to the security function are delineated. Until these general interests and needs are not clarified, the formulation of a security policy and the choice of a responsible for its implementation is premature.

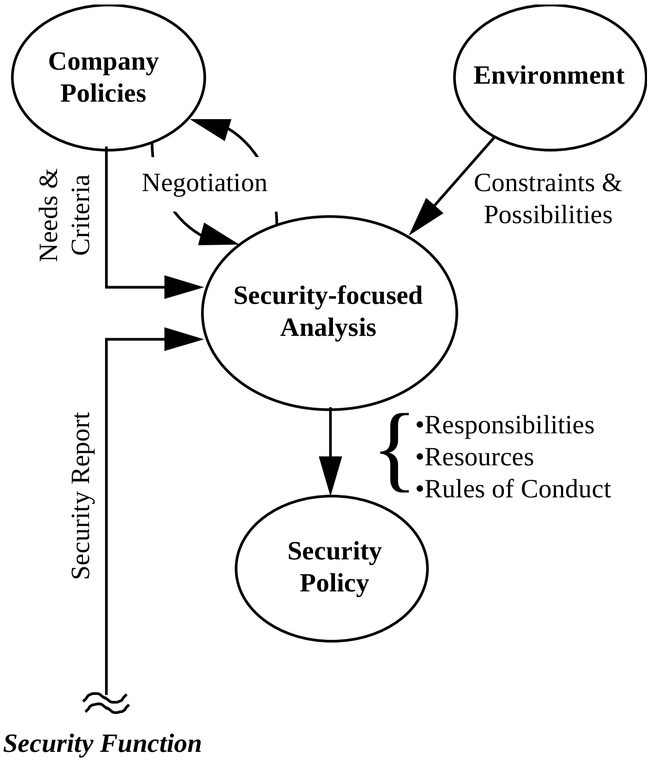

Figure 54 The Formulation of a Security Policy

In this diagram, all the organisation's resources are represented, and applied to the formulation of a Security Policy, which is also affected by the environment. In the researcher's experience the policy process is essentially based on a negotiation among the interested parts, where the weight of the security representatives only partly depends on their professional credibility. In fact, it depends on their capability of justifying their positions with instruments homogeneous with the organisation's culture and belief system.

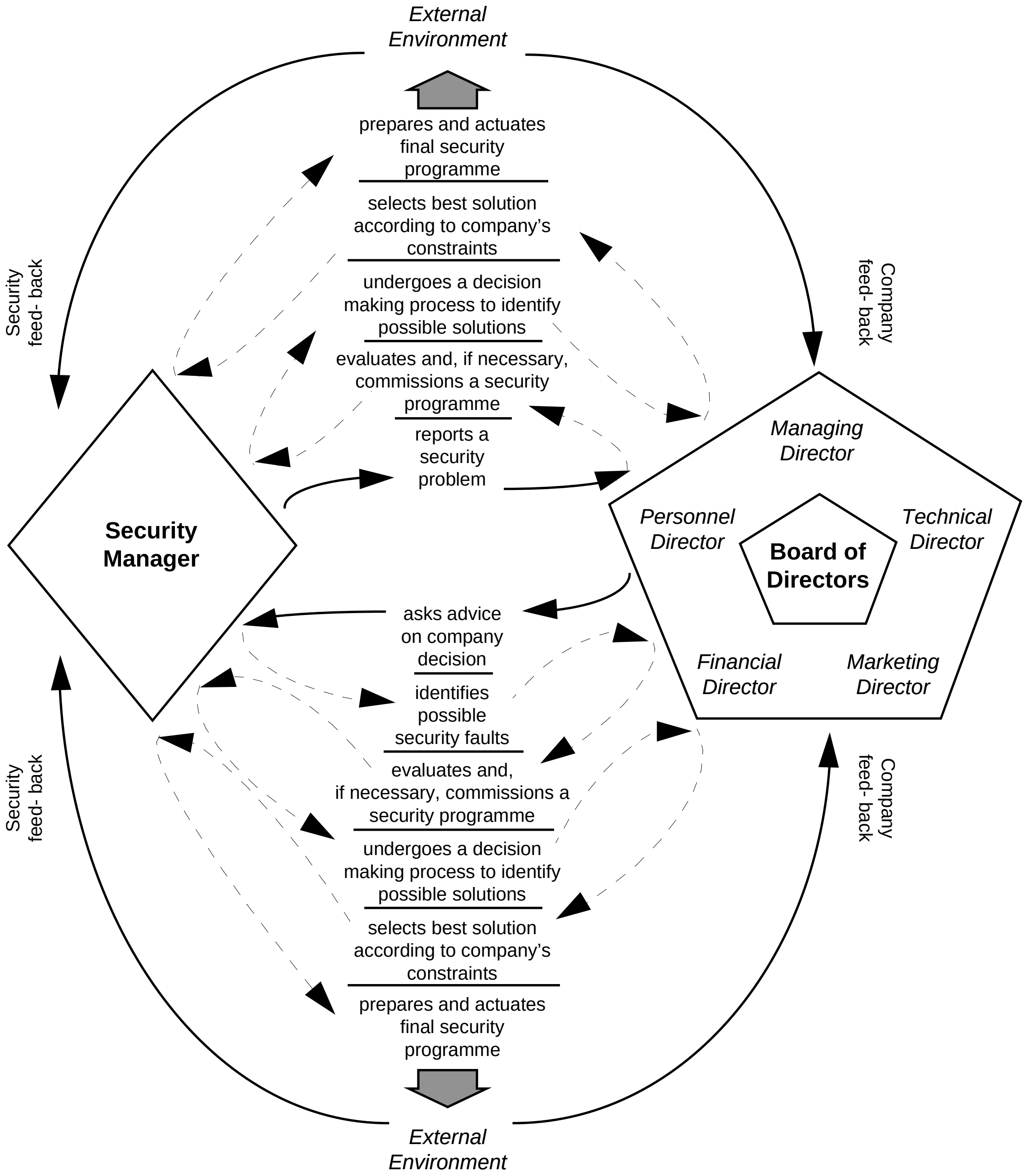
External Environment
prepares and actuates final security programme
selects best solution according to company's constraints
undergoes a decision making process to identify possible solutions
evaluates and, if necessary, commissions a security programme
reports a security problem
Security feed- back
Company feed- back
Security Manager
Managing Director
Personnel Director
Technical Director
Board of Directors
Financial Director
Marketing Director
asks advice on company decision
identifies possible security faults
evaluates and, if necessary, commissions a security programme
undergoes a decision making process to identify possible solutions
selects best solution according to company's constraints
prepares and actuates final security programme
Security feed- back
Company feed- back
External Environment

Figure 55 The relationship between the Security Manager and the Board of Directors

The model above describe two of the possible situations in which the Security Manager and the Board of Directors have to negotiate a security decision. The top part of the diagram refers to the case where the negotiation is initiated by the Security Manager, who perceives the existence of a problem and reports it to the Board. The lower part of the diagram refers, instead, to the case where it is the Board who, while deciding on other matters, realise the need for a security input.

Solving these types of problems, requires the formulation a priori of a Security Policy (which in this approach is not just a declaration of principles, but a preliminary step to a Strategy), which may be achieved via an overall understanding of the organisation as a system, the knowledge of its goal, and involves deciding on:

- Who will be responsible for the 'enforcement' of the policy?
- Which resources are necessary?
- Where, when, and how these resources should be directed?

These choices overlap, and are connected by a network of feed-backs and inputs between them. This area of overlapping is represented by the necessary, operational connections between policy and strategy. Only policy may give strategy a goal and a statement of conduct, but only after strategy has defined the dimensions of the need to be met it will become possible to decide on how to implement the mission:

- Who will pay for it?
- How much?
- Who will be responsible for it?
- Who will evaluate, assess and control it?

This problem area should define responsibility and resources; until these areas are not clarified, no exercise of dimensioning the problem in view of its modelisation is possible. Previous analysis indicates that the process of assignment of responsibility of a Security Policy is essentially directed to the choice of the solver. It is not primarily important to decide or list which responsibilities should be charged upon a particular person, but to decide which qualities the solver should possess for carrying out her/his mission, according to what are seen as the general interests and needs of the organisation.

Resources must allow the responsible to undertake her/his task. They can be grossly figured in terms of a budget, people, structures and systems. In their simplest form, this means an office, an assistant, a telephone/modem, a computer and funds for expenses and external consultancy. The allocation of a dedicated room is required by the confidentiality of the task.

The definition of a Security Policy is, basically, the definition of Bellacicco's final state. To be useful for directing the formulation of a Strategy, a Security policy should give an indication of a goal, i.e., where resources and efforts should be directed. According with the theoretical approach, this assumes that absolute security (as the certainty that a given feared event will not happen) does not exist in nature. However, it exists, and it is theoretically possible to attain, a 'practicable' security, in the sense of 'the justified true belief' that a given feared event will not happen in the immediate future. This condition, in conformity with the theory, is represented by the formula [380]:

$$\mathbf{S_1\ (A) = f\ (P_x,\ T_x)\ Si_x}$$

P, T, Si have not yet been defined. Their definition will derive from the necessary steps to achieve **S_1 (A)**. As the existing level **So (A)** does not ensure this 'justified true belief', and there is will to protect, it becomes necessary to achieve the level **S_1 (A)** > **So (A)** judged necessary and consistent. This is equivalent, according to the general formula, to state the desired level **S_1 (A)**. The important questions to be answered are:

- Is the present state of affairs satisfactory? According to which criterion?
- If not, what state of affairs will do? What is the level **S_1 (A)**?
- How such an ideal state of affairs may be attained?

More often than not, the initial condition is not perfectly known, and, before proceeding, the preliminary problem of assessing the existing level of security **So (A)** has to be solved. In that case, the assessment of **So (A)** requires the identification, evaluation, and assessment of all the building blocks of the formula, notably, **A, P, T, Si,** and of their possible dynamics and effects, such as those identified in Section II. This requires a preliminary analysis of the

[380] Every Asset has its peculiarity, attracts different Threats, has different vulnerabilities, and may suffer different damages. In order to be precise, the reasoning has to be made for any identified A, and it is not possible to generalise it to a whole set of A, so to give an 'average' measurement of security in relation to the entire set.

fundamental six questions (see above). Since a Security policy is a statement of conduct and goal, the answer to the these questions will be on very general terms (valid for any decisional or functional level). The adequate tools for this kind of resolution are qualitative in nature, such as soft systems methodology, influence diagrams and system analysis. It is clear that the formulation of a policy must be consistent with the possibility and the goals of the organisation. It is not uncommon to find security policies whose implementation is beyond the reach of the organisation. The general dimensions of the problem must be defined, if the implementation of the policy must be feasible. Qualitative techniques as those cited before are also valid - assisted by basic calculation - for analysing the initial problem of defining quality and quantity of resources necessary to implement the task, and to ensure that responsibilities are achievable. In many cases, the analysis of existing data, budgets and past experience is useful to provide general figures at the required level of definition.

In conformity to the dimension of the organisation, problems of allocation may arise between different:

Table 6: Possible Sub-Policies

geographic areas	*continents, subcontinents*
	countries
	regions
	areas
	places
	plants
	buildings, volumes, spaces, routes, points...
initiatives	*brands*
	businesses
	strategies
states of affairs	*short-term*
	medium-term
	long-term

This may introduce the necessity of sub-policies at each level where goals, priorities and criteria change by reason of different environment and situation.

Once policies are defined at each necessary level, it becomes mandatory at Board Level, to

- appoint a Responsible of the implementation,
- nominate a Sponsor/Controller
- assign resources (not only a budget, but people, structures, and systems).

This allows the responsible to formulate a Strategy.

3.3.1.2.4 The Formulation of a Strategy

The formulation of a Strategy requires more detailed answers to the basic six questions, since strategy is the stage of formulating general directives to the preparation of a Security Programme.

The strategic level lies within the competence of the Security Responsible, and/or Consultant, under the control of the Sponsor. S/he receives from the Board level a security policy (which, ideally, s/he has contributed to formulate), the aim, the mission, and the means to fulfil it. S/he knows what the existing state of affairs is, and is the receptor/processor of all the relevant security matters. S/he receives problems from the organisation, and perceives threats from both the external and internal environment. On the basis of these general directives, and of the perceived needs, the problem-solving exercise aims to the formulation of a 'Security Strategy', i.e., the 'determination of the basic long-term goals and objectives, the adoption of courses of action, and the allocation of the resources necessary for carrying out these goals'. [381] At this stage, tools such as system analysis may give an important contribution, together with more quantitative techniques intended to solve problems of resource allocation.

If the organisation and the security function are well managed, there is no point in being directed by contingency in formulating goals or directing security resources. On the contrary, means and activities should be directed in accord to the overall organisation's strategic plan. For example, the resources of intelligence are better employed in producing area and profile studies for problems of expansion, negotiation and competition, rather than being limited to investigate on suffered damages and losses.

[381] Cole, 1993: 102

Since the final state of affairs has been identified, the responsible for the Strategy must elucidate the remaining part of the formula **(P, T, Si)** which equals the desired **S1 (A)**.

This condition, in conformity with the theory, is represented by the formula:

$$\mathbf{S_1 (A) = f (P_x, T_x) Si_x}$$

The problem is that of defining those levels of P, T, Si judged necessary and consistent, so to have:

$$\mathbf{S_1 (A) = f (P_y, T_y) Si_y}$$

The fulfilment of this necessity presumes the solution of a problem (the security problem):

'How can we attain **S_1 (A)** starting from the existing **So (A)**?'

It is now assumed that **So (A)** is known, **S_1 (A)** has been defined and that **Py** is potentially there, since it has had the perception of a new Threat, and has consequently changed her/his level of commitment, in order to solve the new problem. In agreement with the approach, it is also assumed that all the elements of the formula should be taken into consideration, thus also A can be modified into Ay. This is explained below. The solution of the problem, in agreement with the theory, depends then on the solution of the equation **S_1 (Ay) = f (Py, Ty) Si_y**, and the problem may then be reformulated as:

'How can be possible to modify **A**, **P**, **T**, **Si**, to attain the desired state **S_1 (Ay)**?'

The solution of this problem depends on the identification of that combination of A. P, T, Si, which results in **S_1 (A)**. This opens four sub-problems:

1. How to modify Ax to Ay
2. How to modify Px to Py
3. How to modify Tx to Ty;
4. How to modify Six to Siy.

Each problem, in accord with Bellacicco's model, can be defined as single problems where both the initial and the final state of affairs are known. Actually, the final state of affairs is yet to be defined. The sequence of solution depends on the feasibility, and may be changed, but is conceptually simultaneous. It is also evident that not all elements are necessarily to be changed, since the equation may be solved through:

a) the elimination of A;

b) the elimination of T;

c) a substantial modification of P, to improve defences beyond the reach of T;

d) a substantial modification of Si;

e) a mix of a, b, c and d.

The option of eliminating A is one which eliminates the need for security. Having described security as risk-adverse, it is also one of the favourite, particularly when the Asset is not considered very important, or its protection may jeopardise other and more essential Assets. Examples are transferring a potential loss via insurance, or relinquishing the purse to a robber to protect life and health. More sophisticated examples consist in the *apparent* elimination of the Asset, e.g. removing it to a secret location, or where a Threat does not exist. This is frequently done for protecting potential victims of kidnap or assassination, but the reasoning holds for all those Assets whose presence or activity in a particular location is not essential. 'Elimination' is not the only option relative to the Asset, and does not need to be total: useful attempts can be done to modify its visibility, accessibility, desirability and vulnerability, or that aspect of the Asset which may motivate a Threat. For example, a person blackmailed because of her/his personal habits may decide to reveal them openly, or a civil servant threatened by a spy to reveal some secret of her/his office may ask to be moved to a less sensitive area.

The option of eliminating T may seem excessive, or unrealistic, to those who only think in terms of 'physical' elimination. This extreme measure has been exploited by different subjects in different occasions both at government and private level; in some country, and in some situation of extreme danger it still seen as the only 'rational' solution of an overwhelming security problem. However, other possibilities of 'elimination' can be exploited, such as the use of avoidance, deception, persuasion, bargaining, pressures and even threats, when appropriate and feasible. [382] This option is always worth to be considered, since it may prove effective, economical, and decisive. However, it assumes that T is known and approachable, and requires time, patience, information, ingenuity and a deep knowledge of the human being. Deplorably, this level of sophistication seems rather scarce (at least in private security) and the idea of this option seems far beyond the average security people.

The actual approach in democratic countries tends towards the other options, those of confronting T by reinforcing P and Si. Conceptual examples are 'opportunity reduction', 'social prevention', 'legislative prevention' and 'deterrence'. Practical examples are the reinforcement of physical defences by means of barbed wire, spikes, fences delivering electric shock, mines, high-security access controls, bulletproof towers and the use of armed guards and dogs. Most of these approach are certainly inspired, or limited, by legal, moral and ethical considerations, but are mainly grounded on the idea of reinforcing P beyond the capabilities of T, in the logic of increasing confrontation between the gun and the shield. These cultural biases probably come from the military and political doctrines of power within human relationships, be they government or personal-related. Operational literature and daily evidence reveals security as being still influenced by the Vigilante and Fortress syndromes. With security being egoistic in vision, the modification of P with these means endeavours to deter T to the point of obliging him to desist, or to 'convince' him to change is target (dislocation) to another A outside of the responsibility of P. However, and perhaps, this position does not dedicate enough thought to the special feature of security of being risk-adverse.

The above approach, which is mainly based on confrontation, can also be seen in a Lewinian vision as an attempt of 'bargaining' with T through P and Si, tends to have tactical advantages, but strategical limits. The history of security shows that T tends to adequate its level of capability to P and Si, and the Lewinian field theories prove that 'the ambience is a teacher'. For example, the reinforcement of physical defences around an Asset may suggest T to increment violence, to use more powerful technologies and weapons, to direct her/his ingenuity to less direct and obvious, but more effective approaches, such as bribery, deceptive tactics, and corruption. The impenetrability of the defences may even create new threats, such as, for example, an internal source of information, a traitor, or a new opponent. Sun Tzu *docet.*

[382] According to the general position, the discussion is about the *theoretical* possible options in solving a security problem, and not on their *legal*, *moral* and *ethic* aspects. In this approach, these aspects are considered under the issue of 'constraints'.

In this logic, the change from **So(A)** to **S1(Ay)** has only shifted the level of the problem, but not its substance, because, after the necessary time or re-adaptment, **S_1(A) ≤ So(A)**. Besides being ineffective after a first impact, an approach centred on the modification of P and Si is expensive, rigid (it takes time, and, once modified, is difficult to adapt to new exigencies) and follows a one-way logic: that of increasing the level of conflict. Moreover, it does not solve the essence of the problem: the existence of a Threat, and the impossibility of avoiding or deterring all Threats.[383]

In order to maintain their effectiveness, a security strategy should direct solutions at all components (A, P, T Si), keeping concern with maintaining the desired resulting state of affairs, which must be and remain **S_1 (Ay) > So (A)**. The concept of security requires a distribution of efforts between A, P, T, Si in the 'best' possible way (depending on the preferred criteria) and in the direction of diminishing, not improving, the future level of conflict. The problem, then, consists in understanding the dynamics of antagonism and in the definition of the goal (policy) and of the strategy (means and objectives) to achieve this result. The solution (definition of policy and strategy) should be based on 'political' insight and overall considerations of a more general interest, rather than on short term advantages, and oriented to improve or, at least, not exacerbate, the security quality of the future condition.

3.3.1.2.5 The Security Programme

Once the final state **S_1 (A)** has been defined in all the components of the formula, the practical problem of attaining it in the 'best' way must be solved: How can **S_1 (A)** be attained starting from the existing **So (A)**? This is essentially a problem of management. A policy, a strategy, a responsible and the necessary resources are already available. Priorities, criteria and constraints have been identified and stated. Plans for the attainment of the stated objectives must be now provided. The process for solving this sub-problem leads to the formulation of a Security Programme. This requires a series of different problem-solving exercises, aimed to the identification, evaluation, and choice of the possible options which may respect the policy and actuate the strategy.

A first series of problems is now about how the final states Ay, Py, Ty, Siy can be reached according to the preferred options. The Security Responsible, or Consultant, must decide

[383] McCrary, 1997.

how to implement each option and solve a problem of allocation of resource between the components of a Security System (Intelligence, People, Structures, Systems, Procedures and Controls). S/he receives from the internal environment all the necessary information in terms of feasibility of the proposed measures, and can assess the effectiveness of the existing ones. When necessary, s/he reports needs and problems (as well as possible solutions) to the superior level.

The formulation of a Security Programme is the third problem-solving exercise, and the first where quantitative techniques of analysis may appear in their full strength. As a matter of fact, following the offered methodology, a Security Programme is essentially a scheme of allotment of means and activities into the six basic components of a Security System:

- Intelligence
- People
- Structures
- Systems
- Plans and Procedures
- Controls

Therefore, this exercise should essentially be seen as a problem of resource allocation within a changing and conflicting environment. A detailed answer to the first five of six basic questions (What, from Whom, Why, Where, and When) is the necessary and sufficient condition to answer the final: HOW TO, which is basically the Programme. This process is usually done in two steps: the initial is qualitative and the second (where possible and convenient) quantitative.

The initial answer to each question results from the relative appreciation of the main element (the one at the moment object of consideration) against the others. For example, the first question: What to protect? requires the identification, evaluation and assessment of the Asset. This has already be done in the previous phases, but now more detail is required. In this approach, this step is based on the understanding that a) A is the stake in a game, or conflict, of mutually incompatible interests, which opposes P to T; b) this stake is perceived in different ways from P and T, according to their cognitional, cultural, social, and political differences; c) A presents different vulnerabilities to different T in different temporal phases. Consequently, the problem solving exercise lays in the identification of the relative weight of all of these factors, and in the evaluation of their relative outcomes. It is a fact that a rational answer can only be given by parallel and contemporary processes aimed to answer the remaining W's (Why, from Who, Where, and When). This phase is based on Intelligence, and assisted by qualitative and quantitative analysis wherever possible and convenient..

As for the techniques of analysis, it has to be considered that - in the presence of antagonism - this exercise is frequently conducted in an environment of uncertainty (unknown probability of outcomes), at least at the general level. This leaves out, until the appropriate level of resolution is reached, quantitative risk assessment techniques, which require the knowledge of the probability of the outcomes, and the estimate of their probable dimension. At the initial stage, qualitative techniques are generally more appropriate.

3.3.1.2.6 Security Projects

The operational (tactical) level is that of the Security Executive, or Technical Consultant. S/he receives from the Security Responsible, or Consultant, the Security Programme (the desired levels of **Ay, Py, Ty, Siy**), and must plan the necessary actions to achieve these levels, through specific Security Projects directed to modify **A, P, T, Si** in the desired direction. S/he must solve a problem of allocation of resource between each component of the Security Programme (e.g. the resources received for the component People must be allocated between recruiting, vetting, education, training and control). S/he collects the necessary information in terms of technical feasibility of the proposed measures, and evaluates the effectiveness of the existing ones. When necessary, s/he reports needs and problems (in addition to possible solutions) to the superior level.

The preparation of a Security Project is a consequence of the development of any single module of the overall Programme (notably, People, Intelligence, Structures, Systems, Procedures and Control). It is a problem of allocation of technical resources, which is made in a given, well defined environment, where all the measurable variables have been dealt with at the Programme level, and the non measurable, arbitrarily defined and assumed as constraints in the previous exercises. The project can therefore be designed with proper quantitative techniques. At this level, the answer to the five W's questions is known, but not to the detail of single accesses, rooms, spaces, volumes, sensors, etc., and has to be worked out. The answer to HOW is the key to the reasoning at the Project stage. In a limited space or volume, each relevant detail of any component of the security system (see above) is known, or can be measured, and the technical and tactical capabilities of any given T in the given Si towards any given A can be measured or, at least, reasonably appreciated in a quantitative form. Hence, the choice of a particular component of the security system (people, structure, etc.) will dictate the definite answer to all six basic questions.

3.3.1.2.7 Conclusion

The procedure outlined is didactic, and is aimed to explain how the offered approach can be applied, proceeding from the general to the particular, without losing in precision and ensuring control. The exercise is mostly a circular reasoning, where the feedback can be identified, estimated and converted in inputs, converging via a series of more definite steps to the optimal solution of the problem. It has to be acknowledged that this optimal solution is not the best in absolute, but the heuristic, according to the fixed constraints, which fall from the overall processes of Policy, Strategy, Programme to Project. The whole process may now be described via a diagram, which shows all the relevant dynamics within the management of security previously identified and discussed:

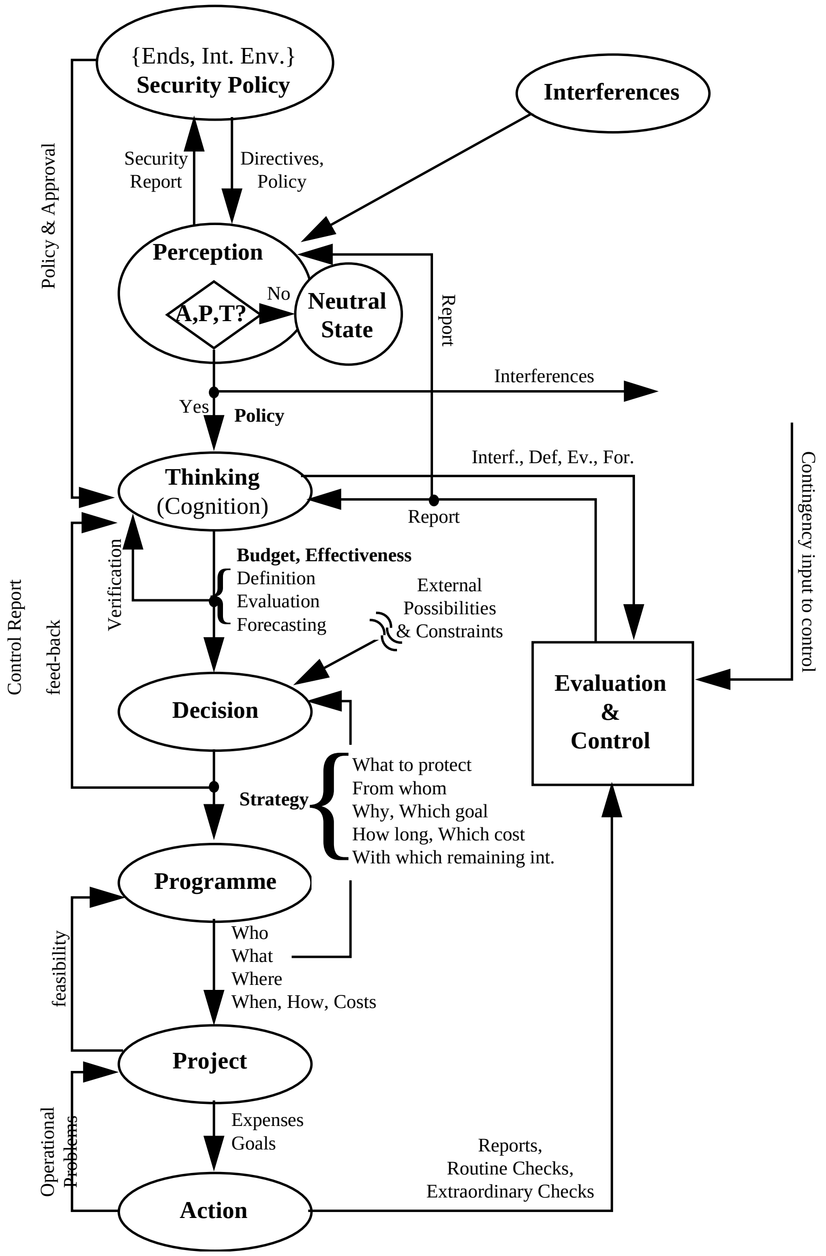

Figure 56 The Security Process from Policy to Implementation

It is submitted that, at this stage, it is possible to explain, justify, find the eventual faults of decisions and actions, and correct them by taking into account their relative feed-backs at the convenient level of reasoning. Each level of decision can be made with the necessary rationality and precision, in accord with the theoretical approach.

Having prepared a general working model, it is possible to make analyses, to assist research and to attempt predictions. [384] In short, this approach offers the possibility of analysing security decisions and activities via a methodology capable of assisting explanation, justification and, to some extent, prediction.

[384] Different models can be used. One of the preferred by the researcher is Powell's Powergraph (Powell, preprint 1997?)

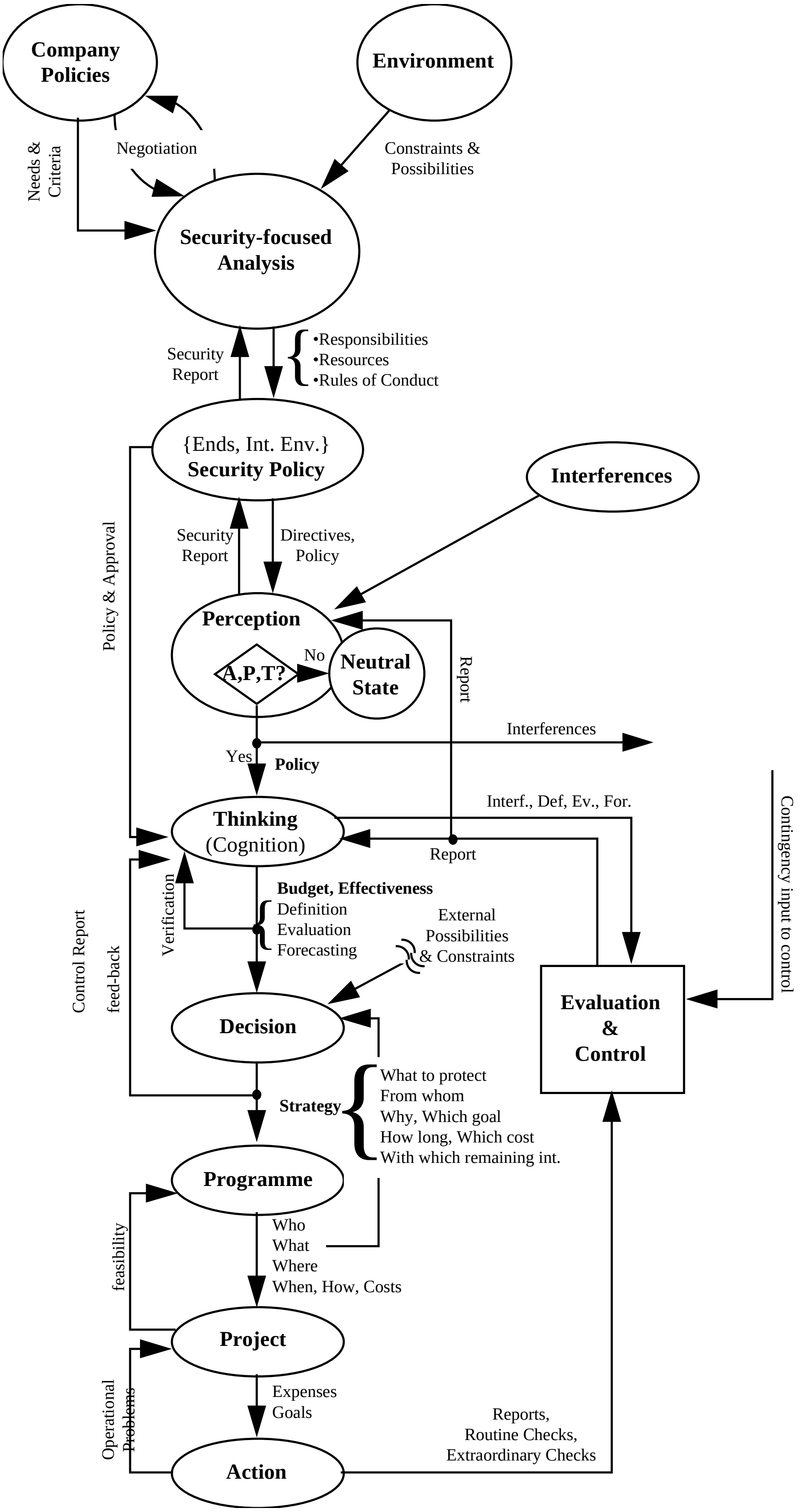

Figure 57 The complete security process

Conclusions

The initial purpose of this research was to examine the existing body of knowledge of security and to reorganise it into a disciplined structure. This task, which at first seemed to be one of taxonomy, has required the analysis of a miscellany of material and a fundamental reappraisal of the concepts.

The concept of security ranges from philosophical to technological and common-sense. On the one side, the term security is interpreted as the response to practically all negative facts of life (particularly, when it comes to attribute blame and responsibility elsewhere). On the other side, ready-made solutions are offered to security problems without any attempt to address the wider issue. The current, philosophical, interpretation of security as an all-embracing concept has rendered security an impossible task to be accomplished. Conversely, too limited a focus impedes both understanding and communication between different subjects. This makes the explanation, the attribution of responsibilities and the measurement of performances unrealisable, or disputable. The attempt of addressing these issues has prompted questions and doubts. The most important are described.

Problems

As the analysis proceeded, a great many problems came to light. The most pressing, and hardest to address, is the multitude of disciplines with interest in security. Security relates to all aspects of life; consequently, security concepts are included in a multitude of approaches, from politics and international relations to loss prevention and common sense. These, in turn, contribute their ideas and paradigms to the concept and practice of security. The multi-disciplinariety of security brings in issues of scope, methodology and goal, all of which require a definition of security. The ambiguity of the concept has necessitated the drawing of arbitrary limits, in order to distinguish philosophical from practical security. One which is consistent with the current practice of security has been offered and stated as a premise to further reasoning.

A second problem, and that which prompted the research, is the serious gap between expectations and practical possibilities. The limitless utopian expectations are not accompanied by a matching cornucopia of knowledge and resources. Thus security is frequently deemed negligent or inadequate, with negative consequences on the attribution of blame. The solution of this problem has been facilitated by the previous steps of definition. It has required the demarcation of the security context from others apparently similar but substantially different, then the outlining of a decision-making process where the interference of social, political, economic and managerial constraints can be identified and assessed. This makes the proper attribution of responsibilities possible at each step of decision.

A third problem is the influence of prejudice, accumulating over time, and frequently in defence of specific interests or ideologies. A set of cultural, moral and political biases have been identified, which influence the whole process of security, from perception to judgement and decision. This issue has been addressed by holding security to be a neutral concept, and by assessing these influences not at the general, but at the operational level.

The fourth, and final, problem is that of providing a framework of understanding which accommodates all the existing concepts and techniques. Such a framework is necessary for two reasons: one is to benefit from the existing knowledge by better understanding of its possibilities and limits; the other reason is to assist explanation, justification and control of present security decisions and activities. A solution has been offered in the form of an operational model of security. This also constitutes the suggested means of testing the validity of the proposals.

THE ITER

This research started from two basic assumptions: the need of a more disciplined approach to security, and the validity of such an approach. The demonstration of the need has been relatively easy.

In the absence of scholarly attention, security remains an empirical subject with disputed boundaries. A multitude of actors operating in a multitude of fields have produced a plethora of approaches. Starting from different premises and characterised by narrow interests, different approaches have followed different paths of specialisation and have arrived at different positions and definitions. These differences cause cognitive, communicational and decisional interference, which produce conceptual and operational faults. In the absence of a theory, these faults can be corrected only by means of a trial-and-error process. Being it based on personal experience and outside experimental set-up, this process adds little to the general knowledge. The conclusion has been that a fundamental reappraisal of the security concept is needed.

Demonstration of the validity of an organised approach to security started from two postulates: that the existing body of knowledge of security had a structure sufficiently organised for the exercise, and that the task could be governed by scientific methodology. The former postulate rests on two bases: the first is derived *'per existentiam'* and the second '*per absurdum*'. There is a body of knowledge related to security, taught at academic level and applied at the operational. Security activities are ruled by laws and regulations, enforced at different levels (government, public, private), and carried out according to settled and accepted principles and methodologies, most of which are derived from existing sciences. Thus these existing activities, regulations, people, methods, systems, accord to principles and are organised according to rational tenets. Turning to the second postulate, scholarly evidence of the possibility of a scientific explanation, with criteria of testability and falsification, has been offered. An examination of the concepts and principles of science justifies the choice of the methodology for the research. The possibility of identifying '*general truths'* in the existing body of knowledge about security and of identifying the '*fundamental laws that operate or rule them'* according to a scientific methodology is thus validated.

Having satisfied these basic assumptions, the theme of the research has been identified in answering the following questions: 'What is security?' 'How can we analyse a security problem? What value can be attributed to a security decision?

The research strategy was to start the analysis *ab ovo*. No answer was judged possible without a *tabula rasa* of the existing definitions and approaches, because different interests, assumptions and goals lead to different, at times incompatible, solutions. The goal of the proposed approach was to offer a solution to the problems of definition, explanation, justification and control. This goal has been pursued via the following objectives: 1) Security must be clearly demarcated from other contiguous fields of activity as, for example, safety. 2) A verifiable decision-making process must be outlined, where all the intervening factors can be identified, evaluated and prioritised, in order to establish which decision was taken by whom, and according to what criteria. 3) A model of the security process must be formulated to provide an instrument for control and experiment. That was the strategy of the research.

Thus the theme and strategy of the research constrained the discussion to a logical path of reasoning. A series of steps was then planned, with increasing degree of resolution. The attainment of the first objective (demarcation) has been achieved via three steps: a) the identification of the set of defining properties of security; b) the formalisation of a definition of security which, in accord with the scientific methodology, was then assumed as the 'postulational set of premises' to c) the definition of the security context, i.e., one in which security is the main concern and goal. The attainment of this first objective has allowed the analysis of the process of security, firstly at its basic level (the 'laboratory' model composed of Asset, Protector and Threat), then at its operational level, with the addition of more specific factors defined as 'Situation'.

The second objective was to define the process of decision-making in security. Three steps have been planned in the analysis: a) comprehension that the security function operates within an organisation and an environment, which add their own criteria and constraints; b) analysis of the management of security; c) examination of general decision-making process and problem-solving and of their application to security. These three steps have allowed the analysis of the planning process of security. They make it clear that the decision is the product of a series of intervening decisions, each governed by its own criteria, not only those of security. Thus, the priorisation of the intervening decision-makers, criteria and constraints is the necessary premise to a rational decision (i.e., consistent with its context). The attribution of blame and responsibilities must follow the same path.

The third objective was to synthesise the analysis into a model of a security process. Three phases have been involved: a) the preparation of a model, and the problems behind it; b) the model itself; c) the utilisation of the model in an analysis of an complete security process. This last objective allows the testability of the security process, including explanation and control, and permits a degree of prediction by means of the preparation of different scenarios.

It is suggested that three steps of the scientific methodology are thus satisfied: the formulation of a *set of premises* (definition of security), the deduction of *general laws* (the security context and its processes), and the *explanation in clear, falsifiable steps* (the whole exposition of the approach, and the model of a security process).

The final step required these conclusions to be tested *via observation and experimentation*, in order to investigate their actual and potential value. Part of this test was against existing theories. Analysis of the most debatable concepts of the proposed approach (those referring to the psychological, political and managerial -administrative - aspects of a security context) has supported, or at least not falsified, them. The final test of its scientific value is the verification of the model's capacity of assisting explanation. This was done by applying it to the analysis of a general process. A scientifically acceptable test requires the application of the model to a significant number of different security situations. Given the limits of this research, it is possible only to propose an instrument for the purpose.

FINDINGS

The theoretical approach of this research can be summarised in the following: the state of affairs where security activities have both sense and utility is that where security and non-security coexist. The concept of security is initiated by worry, based on antagonism, driven by self-interest and inspired by conservatism. Security is a condition created and maintained by a protector through antagonism to reacting threats. It aims to avoid, or protect from, the occurrence of an event feared capable of causing damage, loss or injury to an asset. The will to avoid an undesired event originates by the perception of a possible source of 'worry and danger', and opens a security context. Every security context is established by three components (Asset, Protector and Threat), whose mutual relationships give origin to a number of effects (prevention, protection, damage…). The verification of the existence of a security context constitutes the criterion of demarcation between security and other states. Each security context is different, and peculiar to its particular Situation. If the parameters of the Situation are known, then the resulting effects can be identified and evaluated. It is therefore possible to analyse a security context according to general laws and principles. A model can be prepared by means of which a security process can be analysed, explained and, where necessary, corrected. This model can constitute an experimental set-up for research and experiment. These are the main conclusions of the research.

One further point is now worthy of discussion. In this research the framework offered has been deliberately limited to security in the context of business and industry, for which it is used as a criterion of demarcation. However, these deliberate limitations do not alter the applicability of the framework to other contexts where a degree of antagonism exists. This approach has been applied by the researcher - *mutatis mutandis* - to safety, business and political problems, and to the planning of special forces operations. Results are satisfactory, and the verification of the applicability of the model within the widest interpretation of antagonism, from business to combat, supports the researcher's belief that the approach has wide application.

This research has identified fields where existing theories and disciplines provide (or may provide) contributions. These fields have been related to the temporal and functional phases of a security process and identified as: psychological, political, managerial (administrative), and technical. Evidence has been offered that all the activities within a security context are multidimensional. They are primarily produced by 'people' via specific 'principles', 'procedures' and 'functions', supported by physical and non-physical factors, such as 'intelligence', 'structures', 'systems', 'procedures' and 'controls'. Being dependent on, and directed by, basic human factors, all physical and technical factors have been considered to be auxiliary factors, or tools. Support for this assumption has been cited in existing literature, where 'software' factors such as motivation, survey, analysis, assessments, decisions, planning and behaviours are clearly stressed as primary and essential over the 'hardware' factors such as structures and systems. Accordingly, the former areas (the psychological and political, defined as the 'basics') have been placed at the general level, and the latter (the managerial and technical, the 'tools'), at the operational.

The analysis of the existing body of knowledge of security has identified a number of issues, some of which merit further research.

The first issue relates to the apparent incompleteness of current approaches. This research has confirmed that security needs, and benefits from, a multi-disciplinary approach. This appears to involve only physical and non-physical sciences. The absence of direct links to natural sciences is judged by the researcher to be a gap in the current thinking about security, which needs to be filled by research.

The second issue relates to perception. It has been submitted that a security context is initiated by, and depends upon, a perception. With the notable exception of studies of the paradigm 'risk perception', this area is under-researched. Areas meriting research are the differences in perceiving a threat, an hazard and a risk, and the cognitive factors leading to different assessments of the same state of affairs.

This leads to the third issue, that of the influence of the situation on the whole security process, from perception to action and assessment of the results. Scholarly attention to situational problems has been found in criminology. Some of the studies, notably those of Balloni, Bisi and Abrahamsen, are directly linked to, or closely influenced by, Lewin's field theories. This area is under-researched in security. There is no scarcity of operational evidence and post-facto inquiries, where the influence of situational factors on security processes appears to have been neglected in the planning of security measures.

The fourth issue refers to considerations of self-interest and utility. These features make security unique and cast doubts over some of the accepted paradigms. For instance, crime prevention theories are often considered to be one of the cultural postulates to security. Frequently, the two areas are confused and the premises behind crime prevention theories are taken to be similar to security. However, this assumption is far from proved. For example, one of the favourite theories in crime prevention, opportunity reduction, is inspired by utilitarian theories. This research has shown that there is no apparent reason why security should be so interpreted.

This leads to a fifth issue, the management of security. This issue is important, as current security study is greatly influenced by management theories. However, the literature on security management does not cover all the spectrum of management studies. It is generally limited to simple considerations of organisation. Much of it is dedicated to the economic justification of the security function within an organisation. The contribution of management concepts to security is one-way. Security contributions to management are overlooked, or under-emphasised (apart from considerations of loss-reduction). No evidence of security concepts is to be found in management works, but many of them are explicitly inspired by the principles of war. Yet, while war in management is perhaps only an hyperbole in the minds of some desk-bound strategists, the media offer daily evidence of the strong security implications of most management activities. Examples are the contribution of security concepts to the formulation of the organisation's policies and strategies, and to the ensuring of its freedom of action. Therefore, on the basis of self-interest and utility, it is evident that the contribution of security cannot be measured in purely financial terms. Security does not exhaust its function with loss reduction.

This leads to the last issue, which is related to Aristotle's final cause, 'what security is for'. One of the assumptions of the research is that the focus of security is the avoidance, by the protector, of damages to an asset. Questions arise from the understanding of how this damage can be caused, and consequently of how this interest and utility can be measured. Damage of reputation, credibility, loss of control, confidentiality, peace of mind are all possibilities. This is central to the 'final cause', as the justification of the security function and its costs, particularly within an organisation, is still disputed. What is clear is that the security criterion of utility cannot always be restricted to the monetary dimension. This research has offered a point of view, that different possible criteria underlie decisions on security. This area deserves further study. The investigation of the issues of interest and utility in security could make contribution to the understanding of the wider concept.

CONSIDERATIONS

The final question is whether the assigned goals of the research have been reached. It is submitted that the goal of outlining a solution to the problems of definition, explanation, justification and control has been met, within the limits of this research. This is a first attempt at theorisation. Difficulties have arisen from the absence of primary scholarly sources, the confusion of the concept, a plethora of biases and prejudices, difference of approaches and interests and, particularly, the complexity of the subject. Some of the findings merit further scholarly attention, for example:

- the differences in perceiving a threat, an hazard and a risk;
- the cognitive assessment against different frames of reference derived by different approaches;
- the influence of different situations upon the same problem;
- the influence of managerial criteria in decision-making;
- the multiplicity of actors and approaches within the same process;
- the problems in balancing different decision makers, criteria and constraints;

- the strong legal, political and economic implications of every security decision;
- the difficulty of identifying a reason for security, with its motivation varying from survival to peace of mind;
- the difficulty in measuring utility, effectiveness and performance of the security function;
- the possibility that in emergency conditions such a process must be accomplished in very short periods of time and under exceptional pressure.

All of these issues have been briefly addressed in this research. The analysis has been focused on identifying and prioritising the different problem areas, to allow justification, performance, blame and responsibility, and determine the rationale of the conceptual and practical activities of security. It is submitted that scholarly research could contribute to the clarification of these specific areas, and add decisively to the knowledge of security. Therefore, the researcher submits that the scientific value of this work lies not in its accuracy, but in its testability. Each step of the analysis has been made clear, from premises to conclusion, to facilitate its eventual falsification.

The road toward the formalisation of the existing body of knowledge of security into a discipline is long, and goes beyond security management. There is a cultural gap within this body of knowledge, represented by the lack of operational experience within the academics, and of tertiary education within the operatives. A degree of mutual distrust sometimes occurs in their relations, and does not facilitate communications. The hope of this work is to prepare a bridge between the two worlds, by furnishing the former with suggestions for study and experiment, the latter with the comfort of a necessary, albeit small and modest, cultural background.

To conclude,

> *'There are more things in heaven and earth, Horatio*
>
> *Than are dreamt of in our philosophy.'*
>
> *(Shakespeare, Hamlet, Act 1 Scene 5: 1671-1681)*

BIBLIOGRAPHY

A

A Companion to Epistemology, (1993) Blackwell

A Dictionary of Philosophy, (1983, 2nd ed. Rev.) PAN Books

Abrahamsen, D. (1967) The Psychology of Crime, NY: Columbia University Press.

Adams, J. (1995) Risk, London: UCL Press Limited

AIPROS (1984) La Moderna Gestione dei Rischi Aziendali, Quaderni AIPROS

Allison, T.G. (1971) Essence of Decision, Harper Collins.

Amerio, P. (1982) Teoria in Psicologia Sociale, Bologna: Il Mulino.

AMOR OA 003 (Oct 1995) Cranfield RMCS Shrivenham (not available)

Anderson, D.R., Sweeney, D.J., Williams, T.A. (1994, 7th ed.) An Introduction to Management Science, West Publishing Company

Andrews, E.A. (1875) Latin-English Lexicon London, 2nd ed., Sampson, Low, Marston, Low and Searle,

Ansoff, H.I. (1969) Corporate Strategy, Penguin

Antifurto, 1990-1994.

Aquinas (c 1225-64) Summa Theologiae

Argyris, C. (1960) Understanding Organisational Behaviour, Tavistock

Aristotle (c. 384-322 BC) Metaphysics, Politics

Associazione Nazionale Imprese Assicuratrici (1992) Manuale di Prevenzione Contro il Furto, Milano: ANIA.

Ayer, A.J. (1956) The Problem of Knowledge, London: Penguin

B

Balloni, A. & Bisi, R. (1993) Criminologia e Security, Bologna University.

Balloni, A. & Bisi, R. (1993) Grande Distribuzione. Furto, Sicurezza e Controllo: Analisi Criminologica, Bologna: CLUEB.

Balloni, A. (1983) Criminologia in Prospettiva, Bologna: CLUEB

Balloni, Viano IV CONGRESSO MONDIALE DI VITTIMOLOGIA, 1989 Bologna QUEB

Baratte, E. Marion A.P.: A Method of Improving Computer Security: Two Years of Experience. A. Grissonnanche (ed), IFIP/SEC '86 (Preprints)

Barefoot, & Maxwell, (1987) Corporate Security Administration And Management, Boston: Butterworths.

Barnard, C.I. (1938) The Functions of the Executives Cambridge, MA: Harvard University Press.

Beaudry, M.H., Can we keep up with the changing times? in Security Management, May 1992

Beck, A. & Willis, (1991) A. Selling and Security: Addressing the Balance, Centre for the Study of Public Order, Leicester University.

Beck, A. (1993) A Profile Of Shoplifting, Centre for the Study of Public Order, Leicester University.

Bellacicco, A. (1987) Elementi introduttivi ai metodi della statistica e della ricerca operativa. Civitavecchia: Scuola di Guerra. (n.a.)

Bennet, T. & Wright, R. (1984) Burglars on Burglary: Prevention And The Offender, Aldershot: Gower.

Biasiotti, A. (1991) I Sistemi di Sicurezza in Azienda., Milano: Pirola.

Borodzicz, E.P., Security and Risk: a Theoretical Approach to Managing Loss Prevention, in International Journal of Risk, Security and Crime Prevention, (1996) Vol. I n.2

Borrelli, G. & Pacilio, N. Use and Abuse of Mathematical Culture on Risk Analysis (n.a.), CRE Casaccia: ENEA,

Bottom, N. & Gallati, R. J. (1984) Industrial Espionage, Butterworths.

Bottom, N. & Kostanosky, (1990) Introduction to Security and Loss Control, Prentice-Hall.

Bound W.A.J., & Ruth D.R. (1983) 'Making Risk Analysis a Useful Management Tool with Microcomputer Worksheet Packages', Computer & Security, vol. 2.

British Security Industry Association (1988-1990) Code of Practice for the Planning, Installation and Mantainance of Closed Circuit Television Systems, London: BSIA.

Broder J. (1984) Risk Analysis and the Security Survey, Butterworth.

Burrell, I & Leppard, D.: Fall in Crime. A Myth as Police Chiefs Massage Figures, in Sunday Times, 16 October 1994

Burton, J.W. (1968) Systems, States, Diplomacy and Rules, Cambridge: Cambridge University Press

C

Carcopino, J. (1995) La vita quotidiana a Roma, Roma: Laterza.

Chisnall, P.M. (1995) Consumer Behaviour (3rd ed.), London: McGraw-Hill.

Chovanes, M.H. Corporate Liability: Security's emerging role in Security Management, February 1994

Clark, P. and Mayhew, P. (1980) Designing Out Crime, London: HMSO.

Clarke, M (1993) New Perspectives on Security, London: Brassey's.

Clausewitz, C. von (1832) Vom Kriege.

Clutterbuck, R. (1975) Living with Terrorism, London: Faber and Faber.

Cole, G.A. (1993) Management Theory and Practice (4th ed.), DP Publications Ltd.

Cooper, J. (1972) The Principles of Personal Defense, Boulder (Colorado): Paladin Press.

Cornish, D. and Clarke, R. (1986) The Reasoning Criminal: Rational Choice Perspectives On Offending, NY: Springer-Verlag.

Courtney, R. Security Risk Assessment in Electronic Data Processing Systems, AFIPS Conference Proceedings, n.46, 1977

Cunningham, J. E. (1987) Understanding Security Electronics, Howard W Sams & Co Inc.

D

D'Addario F.J. (1989) Loss Prevention through Crime Analysis, Butterworth

Davies, J. (1990) Protect Yourself! A Woman's Handbook, Piatkus.

De Smit, J. (1982) Planning Rituals: the Development of the Planning Process for the Dutch University System, Delft University Press

Derrer, D.S. (1992) We Are All the Target, Annapolis, United States Naval Institute

Descartes, R. (1968) Discourse on Method and the Meditation, Penguin.

Deutsch, K. (1966) The Nerves of Government, New York: Free Press.

Dillon, M. (1996) Politics of Security, London: Routledge.

Dixon, N. (1976) On the Psychology of Military Incompetence, Pilmico.

Dobson, T. & Miller V. (1993) Aikido in Everyday Life, North Atlantic Books.

Dougherty, J.E. & Pfaltzgraff, R.L.Jr: (1990) Contending Theories of International Relations. (3rd Ed.), Harper Collins Publishers.

Drummond, H. (1993) Effective Decision Making, Kogan Page Ltd.

E

Easton,D. (1965) A System Analysis of Political Life, New York: Wiley.

Encyclopaedia Britannica, (1986)

Erickson, R.J and Stenseth, A. Crimes of Convenience, in Security Management, October 1996

Essecome, 1990-1994.

F

Fayol, H. (1954) General and industrial Management, London: Pitman & Sons.

Fennelly, L.J. Stoneham (1989) Handbook of Loss Prevention and Crime Prevention, Butterworth,

Fisher, P. A. What Can We Add to the Bottom Line? in Security Management, June 1992

Flynn, Joe B. (1979) Executive Protection Systems, Springfield: Thomas Pubbl.

Force Sicurezza, 1990-1994.

French, S. (1989) Readings in Decision Analysis, Chapman and Hall.

G

Garnham, A. & Oakhill, J. (1994) Thinking and Reasoning, Blackwell.

George, B. and Button, M. (1996) 'The Case for Regulation', International Journal of Risk, Security and Crime Prevention, Vol. 1 No 1.

Gettier, K.J. (1963) Is Justified Belief True Knowledge? Analysis 23

Gigliotti & Jason 1984 Security design for maximum protection, Butterworths.

Gill M (Ed) (1994) Crime at work: Studies in security & crime prevention, Leicester: Perpetuity Press.

Gladstone, F.J. (April 1980) Co-ordinating crime prevention efforts, Home Office Research Studies.

Golsby, M. Four Steps to Success, in Security Management, August 1992

Goodin, R.E. (1995) Utilitarianism as a Public Philosophy, Cambridge University Press.

Gottfredson, M. (1984) The Dimensions Of Risk, Home Office Research Study 81, HMSO

Green, Gion, rev.by Fisher (1992) Introduction to security, Butterworth.

Groebel, J & Hinde, R. (Eds) (1989) Aggression and War, Cambridge University Press.

Group 4, (1992) Training Services Manual, Group 4.

Guarro, S.B. (1987) 'Principles and Procedures of the LRAM Approach to Information Systems Risk Analysis and Management', in Computer & Security, vol.6.

H

Handy, C.B. (1987) Understanding Organisations, Penguin.

Hawthorne, W.A. Should Security Reach Out to the Legal Community? in Security Management, August 1996

Hayes, N. (1994) Foundations of Psychology, London: Routledge.

Hayes, R. (1991) Retail Security and Loss Prevention, Butterworth-Heinemann.

Hearnden, K. & Travers C. Managing change: the implications for security managers -based on a psychometric profile of UK security managers, in Security Journal 6 (1995)

Hemming, M. Is Security Enough?, in International Journal of Risk, Security and Crime Prevention, 1996, Vol.1, n.1

Hempel, C. and Oppenheim, B. (1988) Studies in the Logic of Explanation in Theories of Explanation, New York: Oxford University Press.

Hitchins, D.K. (1992) Putting Systems to Work, John Wiley & Sons

Hobson, R. Keeping an Eye on Security, in The Times, 16 Feb 1994

Hodges, W. (1977) Logic, Penguin Books

Hollis, M. (1994) The Philosophy of Social Science, Cambridge Univ. Press

Holmes, Richard (1985) Firing Line, London: Pimlico

Home Office Research Study. British Crime Surveys, HMSO.

Home Office. Crime Prevention Unit Papers.

Hume, D. (1748) Enquiry Concerning Human Understanding.

Hume, D: A (1739) Treatise of Human Nature.

I

ICPO-INTERPOL Guide for Combating International Terrorism (not available)

Indico Scrl. Securicom '92. Convegno Nazionale Bologna.

Indico Scrl. Securilocks '93. Convegno Nazionale Roma.

Indico Scrl. Securindustria '92. Convegno Nazionale Bologna.

Ingberg, C.J. A duty to protect, in Security Management, December 1993.

International Security Review, 1990-1996.

J

Jenkins, B. (Ed) (1985) Terrorism and Personal Protection, Butterwoths

Jenkins, S. Home Office Crime, in Sunday Times, 16 October 1994

Johnson, L. (1992) The Rebirth of Private Policing, London: Routledge

Jomini, A.H. Baron de (1992) The Art of War, Greenhill Books, Lionel Leventhal Ltd

Jones, P. (1996) 'Hume' in The Blackwell Companion to Philosophy, Blackwell

Juliano, R. Has Security Lost its Perspective? in Security Management, September 1996

K

Kagan, D. (1995) On the Origins of War, London: Pimlico.

Kahn, J.R. The premise behind premises liability, in Security Management, February 1994

Kant, E. (1781) Critique of Pure Reason.

Keegan, J. (1994) A History of Warfare, First Vintage Book Edition

Kellet, A. (1982) Combat Motivation: The Behaviour of Soldiers in Battle, Boston: Kluwer-Nijhoff Publishing

King, M. and Brearley, N. (1996) Public Order Policing: Comparative Perspectives on Strategy and Tactics, Perpetuity Press

Kingsbury A. (1973) Introduction to security and crime prevention surveys, Thomas

Kluwer's Handbook of Security. Kluwer-Harrap ed. London, 1991

Knight, Richardson (1963) The Scope and Limitation of Industrial Security, Thomas

Kobetz, R.W. and Cooper, H.H.A. (1978) Target Terrorism, IACP

Koertge, N. (1994) Curs De Filosofia De La Ciencia, Barcelona: L'Esparver Legir

Kunze, D.A. How can Fuzzy-metrics Help Sell Security? In Security Management, February 1997.

L

Langley, P., Simon, H.D., and Zytkow, J.M. (1987) Scientific Discovery, Cambridge (MA): MIT Press

Laqueur, W. (1987) The Age of Terrorism, London: Weidenfield and Nicholson

Leivesley, S.: Controlling Human Factor Risks in 12th INTERNATIONAL SYMPOSIUM ON TERRORISTS DEVICES AND METHODS. RMCS Shrivenham, 1995a (n.a.)

Leivesley, S: SECURITY INTO THE 21st CENTURY. The Risk and Security Management Forum, Police Staff College, Bramshill, 1995b (n.a.)

Lemmon, E.J. (1965) Beginning Logic, Thomas Nelson and Sons Ltd

Leppard, D. Police Ignore Victims to Cook Crime Books, in Sunday Times, 23 October 1994

Lev, S.: Human Behavior in Emergency Situations in SECURINDUSTRIA '92. Bologna

Lewin, K. (1935) A Dynamic Theory of Personality, McGraw Hill

Lewin, K. (1936) Principles of Topological Psychology, McGraw Hill

Lewin, K. (1973) Resolving Social Conflicts, London: Souvenir Press Ltd.

Liddel Hart, B.H. (1967) Strategy (2nd ed.), London: Faber & Faber

Livingstone, K. (1996) Managing the Policing Business, Scarman Centre Crime, Order and Policing Series, Paper n.6

Locke, J. (1690) Essay Concerning Human Understanding.

M

Machiavelli, N. (1512) Il Principe

Maggioni, Angelo e Renato: Una breve storia di chiavi e serrature. In SECURILOCKS, Roma, 1993

Maguire, M., Morgan, R. & Reiner R. (Eds.) (1994) The Oxford Handbook of Criminology, Clarendon Press.

Makila, R.: The Relative Impact Measure of Vulnerability, J.B. Grimson & H.J. Kugler (eds) , IFIP /SEC '85, North-Holland, 1985

Malik, O. The Future of Information and Technology Requirements for Aviation Security in 12th International Symposium on Terrorists Devices and Methods. RMCS Shrivenham, 1995 (n.a.)

Manunta G. (1996a) Teoria e metodologie di sicurezza in Criminologia Applicata per l'Investigazione e la Sicurezza, Milano: Franco Angeli

Manunta, G. (1990) Autodifesa, Milano: Arnoldo Mondadori.

Manunta, G. (1991) Note di Security Management, Biella: L&M Partners, (n.a.)

Manunta, G. (1996c) La Sicurezza Aziendale, in Balloni, A. and Bisi, R. Dalla Criminologia alla Security, Bologna: CLUEB

Manunta, G. I Convegno Nazionale: La Sicurezza Industriale e delle Infrastrutture a Rischio, Torino, 1988

Manunta, G. II Convegno Nazionale: La Sicurezza Industriale e delle Infrastrutture a Rischio, Torino, 1989

Manunta, G. Per una corretta politica aziendale in materia di sicurezza, in Sicurezza, Giugno 1993

Manunta, G. The Case Against: Private Security is not a Profession, in International Journal of Risk, Security and Crime Prevention, (1996b) Vol.I n.3

Marcello, A. La Valutazione del Rischio Informatico della Realta' Aziendale, in Convegno :'La sicurezza nei sistemi informativi, Torino, May 1989

Mc Inness, C (Ed.) (1992) Security Strategy in the New Europe, London: Routledge

McCrary, G.O. Deterrable Crimes? In Security Management, February 1997

McInerney, R.X. Who's Wielding the Weapons of Security Surveys? In Security Management, January 1997.

McKay, T. Does CPTED need to be revised? in Security Management, December 1996

McQuail, D. & Windahl, S. (1993) Communications Models, 2nd ed., Longman.

Miguel, J. (1984) A Composite Cost/Benefit Analysis Methodology, J.H.Finch & E.G. Dougall Eds, IFIP/SEC '84, North Holland

Mill, J.S. (1843) A System of Logic, 1961 London: Longworth

Musashi, M. (c. 1643) Gorin-no-sho

N

n.a. Mobile Army Against Crime, in The Star, 25 January 1996

Narayan, S. The West European Market for Security Products and Services, in International Security Review, Spring 1994

Nichter, D. A. Training on Trial, in Security Management, September 1996

Nielsen, R., et al. (1978) Computer Security Integrity: a Relative Impact Measure of Vulnerability, SRI International.

Noorderhaven, N. (1995) Strategic Decision Making, Addison Wesley Publishing Company

Nuclear Regolatory Commission. (1979) Generic Adversary Characteristics. Summary Report. NUREG-0459, The Commission, Washington DC

O

Oliver, W. (1972) Practical Security in Commerce and Industry, London: Gower

Orlandi, E. (1989) Ingegneria del rischio, Milano: Franco Angeli

Ortmeier, P.J. Adding Class to Security, in Security Management, July 1996

Oxford Advanced Learners' Dictionary, (1989)

P

Paine, D. (1972) Basic Principles of Industrial Security, Oak Security Publications

Papineau, D. (1996) Philosophy of Science, in The Blackwell Companion To Philosophy, Blackwell

Pasquinelli, A., (1970) Nuovi Principi di Epistemologia., 4 ed., Bologna: CLUEB

Pinnelli, L. Il Personale della Sicurezza Aziendale, in I Convegno Nazionale 'La Sicurezza Industriale e delle Infrastrutture a Rischio, Torino, (1988)

Pitt, J.C. (1988) Theories of Explanation, Oxford University Press

Placek, S. Smithsonian displays new security model, in Security Management, August 1996

Plato (c. 427-346 BC) Cratylus, Meno, Theaetetus.

Popper, K. (1990, 14th impression) The Logic of Scientific Discovery, Unwin Hyman Ltd

Popper, K., The Propensity Interpretation of Probability, in British Journal For the Philosophy of Science, 1959, 10, 25-42

Post, R. S, and Kingsbury, A.A. (1991) Security Administration, Butterworth Heinemann

Powell, J. (preprints 1997?) An Application of a Network-based Futures Method for Strategic Business Planning, Journal of the Operational Research Society

Pugh, D. (1971) Writers on Organisation, Penguin

Purpura, P.M.: Too Secure to be True? In Security Management, July 1991

Q

Quine, W.V. (1986) Philosophy of Logic, Harvard University Press

Quine, W.V. (1993, Revised edition) Pursuit of Truth, Harvard University Press

R

Riddell, P. Crime and Jobs Top Voters' Concern, in The Times, 30 June 1995

Rivett, P. (1980) Model Building for Decision Analysis, John Wiley & Sons.

Robinson, O.F. (1994) Ancient Rome. City Planning and Administration, Routledge

Roget's International Thesaurus (1992, 5th Ed.) Harper Collins

Royal Society (1983) Risk Assessment, London: The Royal Society

Royal Society (1992) Risk: Analysis, Perception and Management, London: The Royal Society

Russell, B. (1980, 9th impression) The Problems of Philosophy, Oxford University Press.

S

S.M.E. (Italian Army) (1987) Il metodo per la risoluzione dei problemi operativi, Civitavecchia: Scuola di Guerra.

Sandia Labs. (1977) Barrier technology Handbook, Sandia Labs, Albuquerque (n.a.)

Sandia Labs. (1978) Intrusion Detection Systems Handbook, Sandia Labs, Albuquerque (n.a.).

Scarman Centre for the Study of Public Order (1996) Course Material for MSc in the Study of Security Management, University of Leicester

Scarman Centre for the Study of Public Order (1992) Course Material for MSc in the Study of Security Management, University of Leicester

Scarr, H. A. (1973) Patterns Of Burglary, U.S. Gvnt. Printing Office.

Schweitzer, J.A. (1990) Managing Information Security, Butterworths.

Scuola di Guerra (1987) Elementi Introduttivi ai Metodi della Statistica e della Ricerca Operativa, Civitavecchia: Scuola di Guerra.

Searle, J.R. (1996) Contemporary Philosophy in the United States, in The Blackwell Companion to Philosophy, Blackwell

Security Management, 1990-February 1997

Shalit, Ben (1988) The Psychology of Conflict and Combat. New York, Praeger Pubblishers

Shannon, C.E. and Weaver, W. (1949) A Mathematical Theory of Communication, Urbana: University of Illinois Press

Sharrat, T. Security Cameras Raise Hopes for Big Cut in City Crime, in The Guardian, 6 July 1994

Shaw, E. (1993) Crimesafe Guide, London: Constable.

Sicurezza e Prevenzione, 1990-1994.

Siljander, R. P. (1980) Terrorist Attacks, Springfield: Charles. C. Thomas Publisher

Simon, H.A. (1960) The New Science of Management Decision, New York: Harper & Row

Smith, M. R. (1989) Common Sense Computer Security, London: McGraw - Hill Intl.

Sorensen, C.E. The Case For: Security Management is a Profession, in International Journal of Risk, Security and Crime Prevention, (1996) Vol.I n.3

Starr, C.G. (1974) Political Intelligence in Classical Greece, Leyden, E.G. Bryll

Stoessinger, J.C. (1993) The Might of Nations, New York: McGraw-Hill

Sun Tzu (400-320 BC) On The Art Of War.

Surette, K. J. The Budget Paradox, in Security Management, November 1993

Sutherland, G.E. Answering the question: What is security? in Security Management, June 1992,

T

Tapia-Valdes, J.A. A Typology of National Security Policies, in YALE Journal of World Public Order, 1982, 9 (10)

The Blackwell Companion to Philosophy, (1996)

The Fontana Dictionary of Modern Thought, (1988, 2nd Ed)

The Penguin Dictionary of Psychology, (1985)

Thucydides (c. 460-400 BC) History of the Peloponnesian War

Tuchman, B.W. (1991) Sand Against the Wind. London, Papermac: Macmillan Publishers Ltd

U

Università di Bari. I Convegno Nazionale Criminologia e Criminalistica. Atti, 1987.

Università di Bologna. I Convegno Universitario in Tema di Sicurezza: Dalla Criminologia alla Security, Atti, 1993.

W

Walsh, D. (1986) Heavy Business, London: Routledge & Kegan-Paul.

Walsh, T.J. and Healy, R. J. (1996) Protection of Assets Manual, Merrit Co. Pubblication

Waters, C.D.J. (1989) A Practical Introduction to Management Science, Addison-Wesley Publishing Company

Webtster's Third New International Dictionary, (1986) Weeks, D. & Whimster, S. (1985) Contexted Decision Making. in Wright ed. Behavioral Decision Making, New York: Plenum

Weiner, N. (1948) Cybernetics, New York: John Wiley

Whidden, G.H. (1994) A Guidebook for the Beginning Sweeper, Washington: TSA

White, D.J. Eds. (1975) The Role and Effectiveness of Decision Theories in Practice, Hodder & Stoughton.

Wiersma, E. Commercial burglars in Netherland: Reasoning Decision-Makers? in International Journal of Risk, Security and Crime Prevention, (1996) Vol.I n.3

Wilkinson, P. & Stewart, A.M. (Eds.) (1987) Contemporary Research on Terrorism, Aberdeen University Press

Wilkinson, P. (Ed) (1993) Technology and Terrorism, London: Frank Cass & Co.Ltd

Wilkinson, P. (1986) Terrorism & The Liberal State, 2nd ed, London: MacMillan Education Ltd

Wilkinson, P. (Ed) (1981) British Perspectives on Terrorism, London: George Allen & Unwin, Ltd

Wilkinson, P. Town Seeks Protection from one Boy Crime Wave in The Times, 23 November 1994

Williams, K. S. (1994) Textbook On Criminology (2nd Ed.), Blackstone Press Ltd.

Wilson, B. (1990) Systems: Concepts, Methodologies, and Applications, 2nd ed. John Wiley & Sons.

Wolpert, L. (1992) The Unnatural Nature of Science, London: Faber and Faber

Wright, K.G. (1972) Cost Effective Security London, Mc-Graw - Hill

Y

Yoder, D. and Honeman, H. (1979) ASPA Handbook of Personnel and Industrial Relations, Washington: BNA Books

Young, J. & Matthews, R. (1992) Rethinking Criminology: The Realist Debate, London: Sage.

Young, J. (1988) Risk of Crime and Fear of Crime: Realist Critique of Survey-Based Assumptions, in Maguire, M. & Pointing, J. (Eds.). Victims of Crime: A New Deal, Milton Keynes: Open Univers Press.

Young, J. (1994) Incessant Chatter: Recent Paradigms in Criminology, in McGuire et al (1994) The Oxford Handbook of Criminology, New York: Oxford University Press.