Chapter 1

Introduction

1.1 Introduction

Increasing globalisation of the world by means of the exponential growth of modern technology has had negative effects on developing nations, in part due to the substantial increase in electronic imperialism. Today's news is overwhelmed with information on the latest breakthroughs in communications, the Internet, cyberwar, and information warfare (IW). These advancements in technology increase the imbalances in the world (IASIW n.d.).

Information technology is used in almost every sector of the business realm across the globe. An intrinsic element of the information age is that information carries more value than in previous periods of history. IW involves achieving and maintaining an information advantage over competitors or adversaries (Cramer 1996). IW thus adversely affects the information products in the developing world due to the developed world's technological advancement and superiority. The highly researched information products (inventions) of the developed world are urgently required by the developing nations for higher productivity and increased development, but they are only available at a price which most of the developing world cannot afford.

The origin of the concept of IW is briefly discussed under the subtopic of point of departure. Background information is also provided on the subject of IW.

1.2 Aim of the study

The aim of this study is to investigate the elements of IW concerning intellectual property rights (IPRs) and their effects on the developing world. A context-specific and appropriate solution will be formulated to address the circumstances that promote IW against the developing world.

1.3 Study objectives

The objectives of this study are to achieve the following:

- Determine what IW is
- Investigate the subject of IW within the field of Information Science
- Determine the relationship between IW and IK
- Understand the relationship between IPRs and IK
- Investigate how is IK currently protected
- Determine measures required to promote and protect digitised IK.

1.4 Research problem

The impact of the information exclusion aspect of IW against the developing world warrants a concern regarding the existing regimes for protection of IPRs. Indigenous knowledge (IK) is a form of intellectual property that the developing nations have at their disposal and mostly sought after by certain developed nations or, rather, their industries. For the aim of this research to be realised, a problem statement needs to be identified. The main problem statement to be investigated through this research is:

To critically investigate IW against IK in the developing world with specific reference to intellectual property rights.

It has become common knowledge that growth in cyberspace has reduced the distance between nations. This increases the exchange of information between the nations across the globe, which in turn allows IW to gain momentum. A brief background of IW is later discussed in this chapter under the point of departure. Relevant researches related to this one are analysed in this chapter.

This research will be based on the issues pertaining to the effects of information exclusion as a form of IW via the strict application of IPRs, with specific reference to the developing world in the information age and their status in the international IP arena.

The main research problem statement is supported by the research sub-problems that will be addressed as research sub-questions in this thesis. The following research sub-questions will be used to assist in answering the main research problem statement. The research sub-questions will be formulated and answered by the chapters as stated below:

What constitutes information warfare?

This question will be answered in chapter two, in which the background of IW will be outlined and the concept 'information warfare' defined within the context of the information age. An Information Science perspective of IW will thus be obtained. The IW approach to be adopted in this thesis will also be explored in chapter two.

What is IP and what role does it play in globalisation?

This sub-question will be answered in chapter three. This chapter will investigate what IP is and its global status. Supporting arguments will investigate how it has been implemented in various countries.

What constitutes IK and how is it treated in the global IP regimes?

This question will be addressed in chapter four. This chapter investigates different forms of IK that exist and how IK is influenced by the existing IP regimes.

What is the current state of IW against IP?

Chapter five addresses the above sub-question. It assesses several cases of IK appropriation and the validity of the Information Science perspective coined in chapter two. Some context specific case studies will also be used to elucidate the issues identified and discussed in chapter four.

Which measures are currently used to protect and promote IK?

This question is addressed in chapter six. Various measures that are currently used to promote and protect IK are investigated.

What information and communication technologies (ICT) solutions exist to promote and protect IK?

This question will be answered in chapter seven. Existing information and communication technologies (ICT) are employed to promote and protect IK as additional measures to those discussed in chapter seven.

1.5 Research methodology

This research covers a wide range of topics related to the theme of IW perpetrated against the developing world. This study includes a qualitative research design comprising an intensive literature study. It also entails some theoretical principles coupled with context-specific case studies. A critical analysis stance is taken in the analysis of various issues and cases identified. This research is descriptive in nature and uses professional and disciplinary literature. The literature researched consists mainly of multidisciplinary scholarly publications, which include, among others, scholarly empirical articles, dissertation, monographs and books, electronic articles, scientific publications and other types of material such as non-empirical scholarly articles. Certain nationally and internationally recognised magazines are also consulted (Berg 1998:257; Straus 1998:48-9).

The main reason for the choice of a qualitative methodology is that it ensures that the researcher explores the work of other researchers on the subject of IW, IP, IK and ICT. The idea is to cite relevant literature in the process of presenting the underlying theoretical and methodological rationale for this research. This means citing key studies and emphasising major findings rather than trying to report on every study done on the problem or providing unnecessary detail. It concentrates on whether the researchers' findings were consistent or whether they disagreed. It leads to the exploration of theories that address the topic. It can also determine whether there are flaws in the body of existing researches (Babbie 1998:112; Berg 1998:256-7; Singleton Jr, Straits & Straits 1993:505; Straus 1998:50).

This research investigates different aspects of IW perpetrated against IK of the developing world. The costly discoveries and inventions of developed nations are required by the developing nations mostly for survival. The economic conditions of the day disable developing nations to acquire such information legally or with consent. The developing nations contend that such information is required for development. The literature analysis does not only demonstrate scholarliness, but it also allows for extending, validating and refining the existing body of knowledge (Straus 1998:52).

IW within the Information Science milieu is determined by and leads to the establishment of an Information Science perspective of IW. A definition of IW is therefore also coined. This is possible by using the literature used as an analytic tool to allow for conceptualisation (Straus 1998:53).

This study also analyses the nature and evolution of IP in various areas of the world. Both the Western perspective (developed world) and those in other parts of the developing world are investigated. It is further ascertained that IK is a form of IP. Some IK resources are of economic value and are thus appropriated by multinational companies and researchers with interest in their properties. Research into IK is used to illustrate some cases, some of which were conducted in conjunction with indigenous researchers. IK researchers sometimes use various types of published and unpublished material to supplement their interviews and field observations (Straus 1998:53).

Through a critical examination of the literature, an analysis of the published studies, and a study of official documentation, IK appropriation as a form of IW against the developing world is studied. Particular attention is given to biodiversity, traditional names and tourism IW cases. In each case, an attempt is made to identify IW perpetrated against the developing world (Babbie 1998:A17).

Various measures, including IPRs, that are currently employed to promote and protect IK are identified. The impact and characteristics of these measures are investigated and their sustenance to promote and protect IK is assessed. Thereafter, the need for additional measures to protect and promote IK is investigated.

Finally, ICT is proposed as a tool that can be used to promote and protect IK. The implementation of technologies such as the deployment of repositories, cryptography, and digital watermarking are employed to protect IK. The organisation, promotion and retrieval of digitised IK will be done by means of DC Metadata Elements Set and OAI-PMH.

1.6 Point of departure

The origin of the concept of "information warfare" can be traced as far back as Sun-tzu in 400 BC, and as recently as the Gulf Wars of 1991 and 2003 (Cramer 1996; Devost, Houghton & Pollard, 1997; Harknet 1996; Janssen 1999:313; Luzwick 2000). Although IW has been used to describe the "war" on the Internet (Haeni 1997:4), it entails more than that. In chapter two, various perspectives of IW are identified and discussed. The infringement of copyright, trademarks, inventions, patents or designs, are not necessarily the only forms of known IW experienced by the world.

The real IW experienced by the developing world is exacerbated by the technological, economic and information exclusion caused by limited skills and technological know-how in these countries. This situation means that the developing world will continue to live on aid from the developed world without proper investment that could make these countries economically sustainable. Their information needs are not truly represented by the mass media, even the local media, which in most instances, are still funded by or act as subsidiaries of developed nations (Sodipo 1997:64).

The following chapter explores the forms of IW that exist and determines the most appropriate approach to IW that can be adopted for this thesis. Chapter three investigates what IK is and determine various kinds of IK that exist. Several case studies are investigated in which IK is appropriated. This will be further investigated in chapter five. As the research progresses, problems relating to IW against IK are identified. Measures currently employed to protect and promote IK are investigated in chapter six. ICT-based solutions are identified in chapter seven to promote and protect IK.

1.7 Background

All forms of struggle over control and dominance of information are considered essentially a form of IW. The techniques of IW are seen as aspects of a single discipline because almost all forms of IW owe their origin to militaristic warfare (further elaborated on in chapter two). Those who are equipped and master the techniques of IW will find themselves at an advantage over those who are not (Libicki 2000).

One of the problems with IW, specific to this study, is that there is still as yet no specific, official definition for IW in the field of Information Science. An Information Science approach is therefore devised in chapter two of this thesis. The main reason for this lack of definition is that this kind of warfare is relatively new to the discipline. The military aspect of IW is very prominent and is also lately used to describe the "war" on the Internet (IASIW n.d.).

Libicki (2000) posits that the marriage of IW and economic warfare can take two forms: information blockade and information imperialism. The effectiveness of an information blockade presumes an era in which the well-being of societies will be as affected by information flow as they are today by the flow of material supplies. These issues contribute further to the exclusion of developing nations from the rest of the world by the developed nations. The developed nations tend to be knowledge intensive, they require and reinforce skills, which is detrimental to less developed nations particularly those with low-wage and low skilled workforces that cannot easily compete.

1.8 Related research

It is important to determine whether IW-related research has been conducted before. The aim of the exercise is to ensure that the current study does not duplicate previous research. Several research projects were studied and only two were identified as being particularly relevant to the subject of this namely, the studies conducted by Matthee and Ntsoane respectively. This section assesses the relevance of such studies to this thesis.

Researcher(s):	H Matthee
Title:	**Information warfare**
Language:	English
Purpose:	Non-qualification
Status:	Current
Year of commencement :	1999
Institution(s):	University of Stellenbosch_(US) Center for Military Studies (CEMIS)
Subject:	History South Africa - Military history
Intended publication:	Report; Articles; Databases; Papers

Aim:

The research investigates the interaction between new information technologies and forms of warfare. Similarities and differences regarding the use of such technologies in Africa and elsewhere are traced. Particular forms of IW, for example the use of the Internet in psychological warfare, are researched in depth, to establish whether or to what extent SA security may face such challenges in the region. A literature study and interviews form the mainstay of the research methodology (http://stardata.nrf.ac.za).

Researcher(s):	JM Ntsoane
Title:	The implications of **intellectual property** rights on IK systems in Southern Africa: a comparative study of selected rural communities in Botswana and South Africa
Language:	English
Purpose:	MSocSc
Status:	Completed
Year of completion:	2000
Institution(s):	University of the North-West (North-West) Dept of Sociology Subject Sociology Rural/Urban
Intended publication:	Dissertation

Aim:

The study investigated the implications of **intellectual property** rights and patents on veld product production and associated IK systems in Southern Africa with special reference to selected rural communities in Botswana and South Africa. The study was based on the argument that the exploitation of veld products and associated IK systems in South Africa should be viewed as part of the international capitalist exploitation of resources of developing countries including Botswana and South Africa through colonialism and other forms of imperialism such as globalisation. The study revealed that veld products and their related knowledge systems in the target communities were vulnerable to capitalist exploitation because there were no adequate structures for their protection from both local and private capitalist companies.

The research conducted by Matthee is founded on military history with a psychological perspective. This research investigates the different forms of IW and places less emphasis on its relationship with IK and IP. On the other hand, Ntsoane's research adopts a sociological perspective and does not consider the way IW influences IK. Neither study has a tightly coupled link between the IW, IK and IP.

These two research projects were selected because they are the only studies which seem to relate closely to this one. Most research solely emphasises IK, IP or IW.

The current study stands out from the above two and the others in the sense that it takes a holistic stance in assessing the influence of IW in the context of IK in the developing world. An ICT-based solution is devised to solve IW-related problems facing the developing world, with an emphasis on IK. An Information Science perspective of IW is used in conducting this research. This approach was selected because Information Science is a discipline that determines and assesses the information requirements and needs of the concerned target group and the satisfaction of such needs from authoritative sources. In this instance the focus is on the IK needs of developing communities. This study also reflects on issues pertaining to the protection and dissemination of such information. The uniqueness of this research is that it creates a relationship between the IPRs, IK, IW, and ICT-based solutions to solve IK appropriation and related problems (http://stardata.nrf.ac.za).

1.9 Concepts

The following concepts are covered in this thesis and some context specific definitions will be provided in the chapters as the concepts are discussed:

- Information warfare
- Information and communication technologies
- Indigenous knowledge
- Intellectual property
- Information Science
- National and international repositories
- Dublin Core Metadata Element Set
- Open Archive Initiative Protocol for Metadata Harvesting
- Digital watermarking
- Cryptography

1.10 Organisation

This thesis is divided into eight chapters containing the following content:

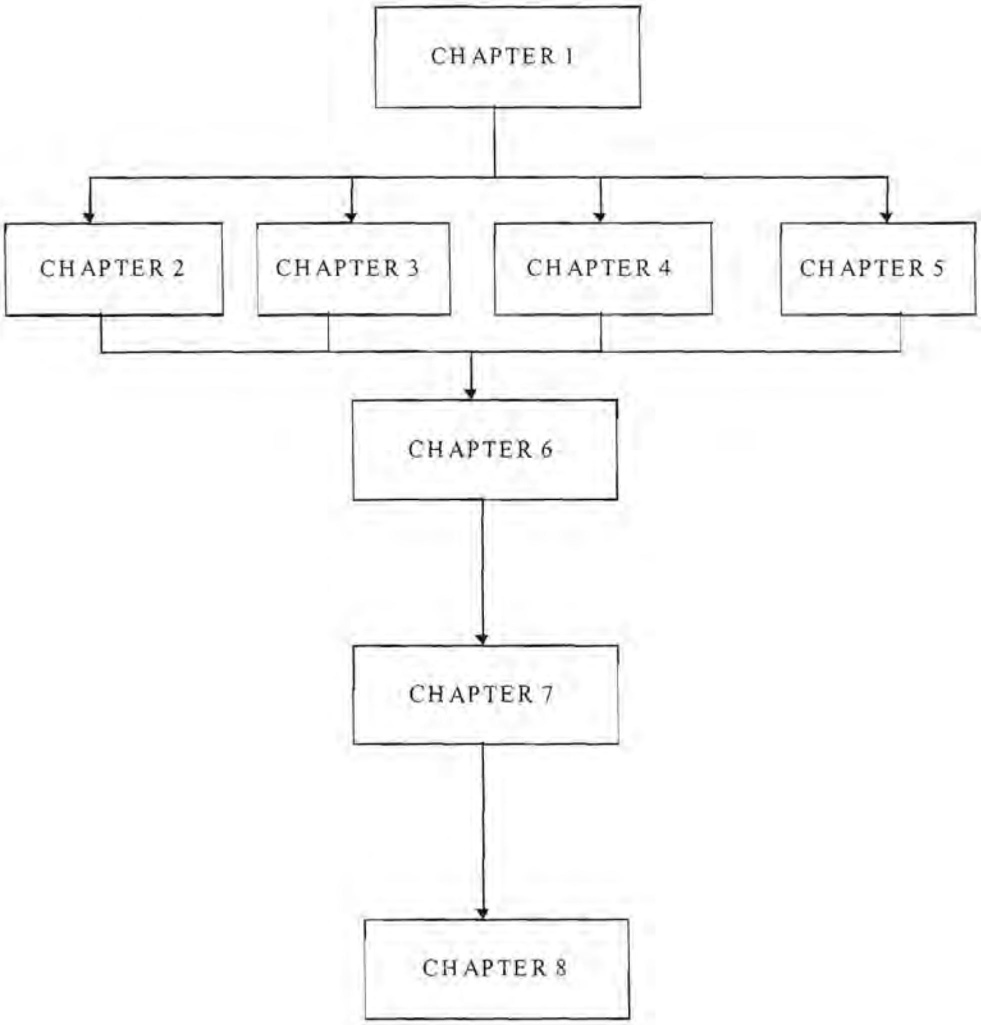
Table 1.1 Overview of the thesis

Chapter	Content
1. Introduction	Introduction, context, importance and statement of the problem. A 'road map' of the thesis is outlined.
2. Overview of IW	This chapter provides a background to IW and identifies various IW perspectives. A definition of IW within an Information Science context is composed.
3. Historical framework of IP in the global context	This chapter identifies various forms of intellectual property relevant to the context of this thesis.
4. IK within the global IPR context	This chapter investigates what IK is and its various types within the global IP context.
5. IW perpetrated against the developing world	This chapter investigates various case studies in determining whether IW is perpetrated against the developing world.
6. Current measures employed to protect IK	This chapter identifies various measures employed to protect and promote IK.
7. Using ICT to protect IK	ICT is used to protect and promote IK against IW.
8. Conclusions and recommendations	Conclusions are drawn from the strategy formulated and the implications of IW on societies are discussed. The contribution made by this thesis is discussed and evaluated. Future research directions are outlined.

1.11 Road map of this thesis

Figure 1.1 is derived from table 1.1. It shows the logical flow of this thesis. Chapter one provides the background to this research. Chapters two, three, four and five contain components that should be understood before chapters six and seven can be studied.

Figure 1.1 Road map of the thesis



Chapter 2

Overview of information warfare

2.1 Introduction

In the previous chapter, a 'road map' of this thesis was outlined. In this chapter various forms of information warfare (IW) are investigated. IW as a concept has been used in various contexts. As such, various forms of IW will be explored. This is done to facilitate the development of an IW definition based on an Information Science perspective. In the attempt to address the main research problem statement, this chapter will answer the following research sub-question posed in the previous chapter:

What constitutes information warfare?

In answering this research sub-question, this chapter will be structured as follows. The background of IW will be outlined and various popular forms of IW will be investigated. An Information Science-based definition of IW will be investigated for use in the remainder of this thesis.

The aims of this chapter can be summarised as follows:

- to identify the origin of the concept IW
- to identify prominent forms of IW
- to revisit the fundamentals of Information Science as a discipline
- to define IW within an Information Science context

2.2 Background

The terminology of IW has its roots in military operations and many of its elements have been part of military doctrine for many centuries. Although IW owes its origin to the military, the modern concepts have evolved more recently, born from the changes that have been driven by the new technologies (Cramer 1996).

In their book *War and anti war*, Alvin and Heidi Toffler approach the history of warfare using a model of three waves. The agricultural revolution started the first great wave of change in our history. Agriculture enabled communities to produce economic products in that age and was also the cause of many wars. '*War*' is usually defined as a state of "open, armed conflict", and *'warfare'* as a "conflict, struggle or strife" (Barrett n.d.).

Barrett (n.d.) posits that in the information era, IW is simply understood as the process of waging war within the domain of information processing resources. It involves the exploitation of computers, databases and network connections. It also involves the strategic application of computer viruses, network 'snoopers', electrical emission detectors and a host of sophisticated, technological tools.

IW is thus a consequence of the changes brought about by the information revolution. It is forced by nations that are highly technologised. IW on the battlefield will therefore be used mostly by the highly technologised nations. Unfortunately, today, most potential enemies of the developed world do not have the technological capability to respond to such attacks and thus IW can successfully be used against them (Cramer 1996; Haeni 1997:14).

The industrial revolution (the second wave according to Toffler & Toffler (1993)) changed the way wars were fought. The element of mass production introduced weapons of mass destruction (nuclear and chemical). In the late 1970s and early 1980s, third wave technologies and ideas began to change industrial wave societies. Further development of technologies bolstered the amount of information available to these societies. The mass society thus slowly became a communication society. With this development the military doctrine began to change (Cramer 1996; Devost et al. 1997; Haeni 1997:3; IASIWA). Among the three waves only the third wave forms the core part of this thesis, and will be given particular attention in chapter seven.

The late 20th and early 21st centuries have come to be known as the 'information age'. The growing sophistication of digital technology and data processing capabilities has enabled organisations to work even more effectively. This unfortunately has also enabled their competition to work more effectively. Organisations must then increasingly depend upon information processing technology, not simply to operate efficiently, but also to perform their basic work. Due to this, organisations of the same nature become steadily more vulnerable to the theft, destruction or subversion of their technological resources (Barrett n.d.).

Various forms of IW are discussed in this chapter, and one approach adopted for further use in the current research. The logic of the adopted approach will be further expanded on in subsequent chapters.

2.3 Forms of information warfare

It is important to identify and discuss various kinds of IW. Libicki, the US defence analyst, identified several forms of IW (Libicki 2000). Such forms include militaristic (command-and-control) warfare, intelligence-based warfare, electronic warfare, psychological warfare, hacker warfare, economic warfare and cyber warfare. Each of these forms of IW is discussed in this chapter.

The 1991 Gulf War inspired widespread realisation of the immense importance of information superiority in a modern conflict. It is not surprising that the Gulf War also saw the emergence of an alternative image of information vulnerability, the flip side of the information dominance coin (Eriksson 1999).

Harknett (1996) presumes that what is potentially revolutionary and distinctive about the information age is the emergence of the network organisational form and the increasing importance of connectivity among existing computer networks. Arquilla & Ronfeldt (1993) place netwar in the context of a competition over ideas. As they present it, the target is information itself, or more specifically, knowledge. To consider societal connectivity (networks) as a useful target, a society must be dependent enough on these networks to make their loss important. Thus, nomadic, feudal, or even moderately industrialised societies that show few signs of network characteristics are not likely targets for offensive netwar operation. However, should they make their indigenous resources available through the Internet, the possibility of them being violated on the network increases (Harknett 1996).

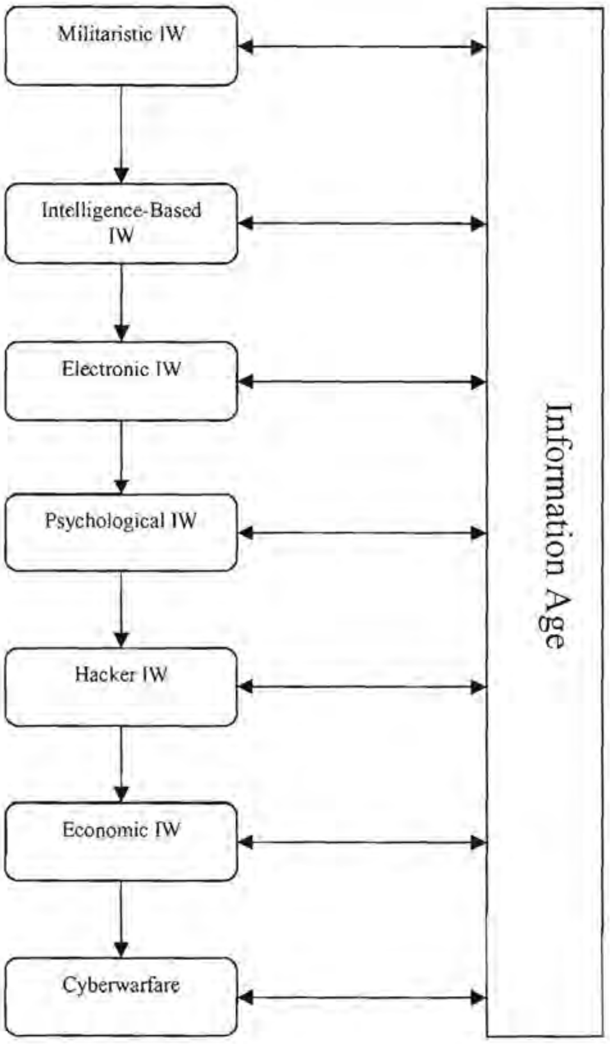


Figure 2.1: Forms of IW

Figure 2.1 shows how the information age determines the nature of various forms of IW. Militaristic warfare is the forerunner of other types of IW as most of them evolved from it.

2.3.1 Militaristic warfare

Military warfare is the forerunner of the other forms of IW. Throughout history, military doctrine, organization and strategy have continually undergone profound, technology-driven changes. Industrialisation led to attrition warfare by massive armies in World War I. Mechanisation led to manoeuvre predominated by tanks in World War II. The information revolution implies the rise of a mode of warfare in which neither mass nor mobility will decide outcomes; instead, the side that knows more will enjoy decisive advantages (Arquilla & Ronfeldt 1993). This is the form of IW explained in the previous chapter that is experienced by the developing world.

The following definition of information warfare provided by the US Department of Defense (DoD) covers only the military perspective:

IW comprises "actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems while leveraging and defending our information and systems" (Devost et al. 1997; IASIWA).

IW was introduced as a major basis of US military strategy by the then Chairman of the Joint Chiefs of Staff, General Colin Powell in 1993. Emmet Paige, the Department of Defense's Director of IW, has an interesting definition of IW. He maintains that:

> "Information Warfare consists of actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems while leveraging and protecting our information and information systems ... Information Warfare addresses the opportunities and vulnerabilities inherent in increasing dependency on information and the use of information throughout the conflict spectrum ... Information Warfare has offensive and defensive elements ..." (Barrett n.d.).

The important elements of this definition are the requirement that military warfare activities are performed in support of "national military strategy", that it involves both "offensive and defensive elements", and that it is important throughout the conflict spectrum. IW will become as central to battles of the future as 'firepower', 'air superiority' and 'mobility' have proved to be in the battles of the 20th century (Cramer 1996; Harknett 1996).

Bey (n.d.) contends that the information age is characterised by misinformation, missiles and propaganda bombs of outright IW. Traditionally, war has been fought for territory or economic gain. Information wars are fought for the acquisition of territory indigenous to the information age, namely, the human mind itself. In particular, it is the faculty of the imagination that is under the direct threat of extinction from the onslaughts of multimedia overload. According to Bey (n.d.), as a culture becomes more sophisticated, it deepens its reliance on its images, icons and symbols as a way of defining itself and communicating with other cultures.

In the past, to perform sabotage, a person had to be physically present at a key point as a trespasser, an insider, or a combination of the two. Technological development benefits the cyber attacker because methods and resources of attack can be freely moved to and launched from anywhere to any target (Anderson & Hundley 1994; Eriksson 1999).

The elements of IW are closely allied to the equivalent elements of 'normal' warfare. Barrett (n.d.) and Cramer (1996) identify five activities of interest which are discussed in the paragraphs that follow:

- the gathering of 'intelligence' and of information relevant to an enemy's use of computer resources
- the introduction of 'disinformation' or propaganda into an enemy's computer resources
- the act of 'denying' an opponent access to information resources upon which they rely
- the 'destruction' of those resources - an act of permanent denial
- the 'protection' of one's own resources from similar activity or responses from one's enemy

Figure 2.2 represents various military IW activities that demonstrate that most, if not all, other types of IW emanated from military IW because such activities are evident in almost every form of IW. The following subtopics on military IW activities will be based on figure 2.2.

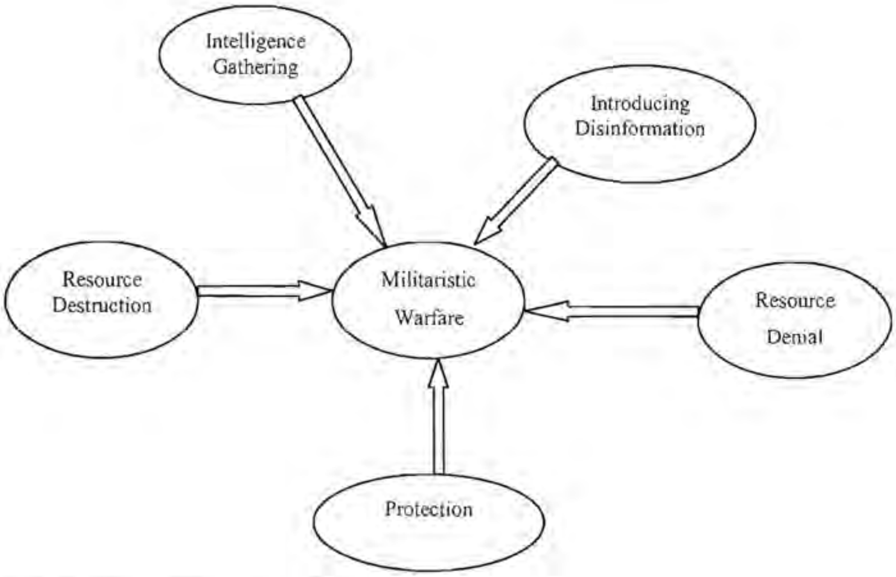


Figure 2.2: Military IW activities

2.3.1.1 Intelligence gathering

In military terms, intelligence is not equated with formal, academic degrees and a high IQ; military intelligence is concerned with learning about one's enemies, their position, strength, information sources and intentions; in the crudest sense, it is about *spying*. In the context of IW, such spying relies on discovering the contents of an enemy's data transmission and computer systems. It involves the application of hacking techniques, but with a crucial difference.

An important difference between general hacking and hacking with military intelligence in mind is that the latter must leave no traces of the penetration, and is directed with specific objectives in mind. Even without actual penetration of a computer system, a great deal of intelligence can be easily gathered in the information age. For example, electronic intelligence techniques that detect and locate radio transmissions can allow an enemy's headquarters to be discovered (Barrett n.d.).

2.3.1.2 Introducing disinformation

Intelligence gathering simply requires information to be abstracted from an enemy's computer system. Disinformation, on the other hand, requires that false or misleading information be *introduced* into the system (Barrett n.d.).

This is an efficient way to corrupt an adversary's databases. It relies on providing false information to the targeted competitor's collection systems to induce this organisation to make bad decisions based upon faulty information. For example, a software developer, Company A, gets information about a new product being developed by a competitor, Company B. Although it has no comparable product in development itself, Company A issues a press release describing its own superior (but fictional) product.

In response to Company A's press announcement, Company B thinks that it has lost its market lead and puts its development efforts elsewhere. Even after Company B brings the real product to market, its lead can be effectively lost when potential customers postpone their purchases waiting for the fictitious product from Company A. This example has unfortunately become commonplace in today's software market. The military versions of this type of denial operation include tactical deception and psychological operations (Cramer 1996).

Information can therefore be introduced through channels that seem to be valid, and so fool the enemy's own data gathering activities. Alternatively, the data already within the system can be manipulated by changing the contents of databases. By introducing such polluted data, news articles can be modified; threat databases of operating anti-aircraft missiles can be subverted; key financial information can be ignored; even traffic control systems can be undermined. Because many modern processes rely on first capturing, then operating with, and finally acting upon database-held information, modifying it can have very wide impact (Barrett n.d.).

2.3.1.3 Resource denial

A clearly hostile act is to 'deny' the enemy access to its own information resources. This seldom involves permanent or even temporary damage to the resources themselves; instead, the means by which the enemy gains access is subverted.

In computer systems, for example, a series of failed login attempts usually then results in the user being barred from the system, and it is then is necessary for a system manager to explicitly re-admit them. Denial of service can therefore be achieved by a series of quite deliberate failed login attempts, targeted at a known user. Alternatively, large quantities of electronic mail can be generated, swamping system resources; or computer viruses can be introduced that seize all process and file space on the system (Barrett n.d.; Cramer 1999).

2.3.1.4 Resource destruction

Through standard Internet protocols such as the file transfer protocol (FTP), the entire contents of a computer can be copied or replaced within minutes. Integrity attacks include the introduction of corruption into data or software so that the targeted competitor will not be using the information or processes it expects (Cramer 1996).

The permanent denial of information resources usually occurs through their destruction. It is far easier to destroy a database or other computer resource than it is simply to subvert it. Introducing false information in a way that is undetectable and convincing is very difficult; deleting the database is simplicity itself. Both data and systems can be destroyed through a logical, hacking attack that can delete not only data files, but also programmes, or even the whole operating system (Cramer 1999).

In practice, of course, this is not achievable remotely. It is necessary to be physically quite close to the machine to destroy it in this way; nonetheless, such units have been developed and used by the US military to destroy missile control systems, for example.

Cramer (1996) notes that direct attacks on an adversary's computer networks are a highly risky and usually illegal activity; nevertheless, the current state of the Internet makes attacks difficult to trace and international intrusions difficult to prosecute. According to this author, direct attacks are an element of IW that an adversary may choose to employ as part of its strategy, they must be considered in formulating strategy and in planning protection.

2.3.1.5 Protection

The obverse of destroying, subverting or illicitly accessing machines is the parallel requirement to ensure that such attacks are not possible against one's own resources. Protection is a key part of any military strategy, but it is even more important in the case of IW. It is vitally important to understand that the security and protection of any computer system is as much a question of people as it is a question of technology. Barrett (n.d.) and Cramer (1999) state that most security breaches are found to have been caused by a system's legitimate users; indeed, the majority of breaches are entirely accidental. In an IW context, any target that is vulnerable is a potential victim. Even without the storage of sensitive data, or a requirement to handle particularly crucial parts of the country's infrastructure, a system can still be a potential target (Barrett n.d.; Cramer 1999).

Once information is collected by an organisation, the next logical consideration is how to protect it. Cramer (1996) states that an organisation's information includes items that may have a high value to a competitor. Examples include future plans, product technical data, customer lists, personnel files, and financial records. This type of data needs to be protected from disclosure to competitors by controlling how, where, by whom, and when it is generated, stored, or accessed. Cramer (1996) goes on to note that the specific data being protected in these ways are often identified in some distinguishing manner and labelled as proprietary, confidential, sensitive, or classified.

Protection is therefore required to an equal extent within the civilian infrastructure. A computer system that is connected to the global Internet is an open door to the rest of the world; it can be used or abused by a hacker or cyberwarrior. These systems may unwittingly be sheltered by a poorly secured computer system or by an ignorant commercial or government organisation (Anderson & Hundley 1994; Cramer 1999; Vatis & Gallagher 1998).

2.3.2 Intelligence-based warfare

Intelligence-based warfare (IBW) occurs when intelligence is fed directly into operations, notably, targeting and battle damage assessment, rather than using it as an input for overall Command and Control (C2) (Libicki 2000). C2 warfare focuses on trying to maintain control over the enemy's military C2 information systems assets. The problem is that C2 warfare in itself lacks completeness since it does not integrate the broader strategic cultural, social, economic and political constraints into relevant action in support of the crisis management (Libicki 2000).

Despite differences in cognitive methods and purpose, systems that collect and disseminate information acquired from inanimate systems can be attacked and confused by methods that are effective on C2 systems. The evolution of IBW may be understood as a shift in what intelligence is useful for. Traditionally, the commander uses intelligence to gauge the disposition, location, and general intentions of the other side. The object of intelligence is to prevent surprise, a known component of IW, and to permit the commander to shape battle plans. Good intelligence allows for the coordination of operations; great intelligence allows for coherence.

Information technology can be viewed as a valuable contributor to the art of finding targets; it can also be viewed as merely a second-best system to use when the primary target detection devices are too scarce, expensive, and vulnerable to be used this way. Whether high-tech finders will necessarily always emerge triumphant over low-tech hiders, remains unclear.

2.3.3 Electronic warfare

Electronic warfare (EW) or operational techniques entails radioelectronic and cryptographic communications. EW attempts to degrade the physical basis for transferring information (Libicki 2000).

Libicki (2000) explains that a large portion of the EW community deals with radars (both search and target) and worries about jamming and counterjamming. Offense and defense keep coming up with new techniques. Traditional radars generate a signal at one frequency; knowing the frequency makes it easy to jam a return signal. More modern radars hop from one outgoing frequency band to the next. To counter radars, today's jammers must be able to acquire the incoming signal, determine its frequency, tune the outgoing jamming signal accordingly, and send a blur back quickly enough to minimise the length and strength of the reflected signal. Jamming aircrafts that are riding with attack aircraft often wipe out return signals by overpowering them, but doing so makes jammers very visible so they must protect themselves (Libicki 2000).

Harknett (1996) and Libicki (2000) believe that digital technologies will make spoofing (substituting deceptive messages for valid ones) nearly impossible. Digital signature technologies permit recipients to know both who (or what) sent the message and whether the message was tampered with. Unless the spoofer can get inside the message-generation system or the recipient cannot access a list of universal digital keys, the odds of a successful spoof are becoming quite low (Harknett 1996; Libicki 2000).

Electronic warfare is limited to radioelectronic and cryptographic communications. The context of the radioelectronic communication does not fall within the scope and parameters of this thesis.

2.3.4 IW as a form of psychological warfare

The use of psychological warfare against the national will, through either the velvet glove ("accept us as friendly") or the iron fist ("or else") approach, is a long and respected periphery to military operations (Libicki 2000). IW can also be used in a non-military attack against individuals and whole societies (IASIWA).

When using direct broadcast satellite, a nation does not need permission from overseas counterparts to speak directly to people in other countries. This capability is now available to anyone at a low cost. Techniques such as video morphing and communications spoofing make it possible for a country to manipulate the perceptions of its adversary's leaders and populace. According to Haeni (1997), a country may spread confusion or disaffection by covertly altering official announcements or news broadcasts, or it may confuse or frighten leaders by spoofing intelligence or other government communications.

The Somali clan leader, Mohammed Aideed, appears to have been a master of the uses of psychological warfare. In a confrontation that cost the lives of nineteen U.S. Rangers, Aideed's side reportedly lost fifteen times that number, roughly a third of his strength. Photographs of jeering Somalis dragging corpses of U.S. soldiers through the streets of Mogadisho, transmitted by CNN to the United States turned US TV audiences against staying in Somalia. U.S. forces left, and Aideed, in essence, won the information war using psychological tactics (Libicki 2000).

The use of psychological methods against the other side's forces offers variations on two traditional themes, namely, fear of death, or other loss, and potential resentment between the trench and the castle (or home front). In the Gulf War, coalition forces convinced many Iraqis that if they abandoned their vulnerable vehicles they would live longer. The coalition's persuasiveness was fortified by weapons that had just destroyed such vehicles during the fighting.

Psychological warfare can also be applied to the everyday task of deceiving opposing bureaucracies, diplomats and spies about one's intentions and capabilities. Weapons can be said to be more or less efficient or speedy than they actually are. This type of warfare is used to make the victims of IW accept their circumstances and not question the status quo.

2.3.5 Hacker warfare

The term hacker warfare is used to refer almost exclusively to attacks on computer networks (Libicki 2000). In contrast to physical combat, these attacks are specific to properties of the particular system because the attacks exploit knowable holes in the system's security structure.

Hacker warfare varies considerably. Attackers can be onsite, although the popular imagination can place them anywhere. The intent of an attack can range from total paralysis to intermittent shutdown, random data errors, wholesale theft of information, theft of services (e.g., unpaid-for telephone calls), illicit systems monitoring (and intelligence collection), the injection of false message traffic, and access to data for the purpose of blackmail. Among the most popular devices are viruses, worms, logic bombs, trojan horses, and sniffers (Haeni 1997:11-13; Libicki 2000; Vatis & Gallagher 1998).

Although attacks on civilian and military targets share some characteristics of offense and defense, military systems tend to be more secure than civilian systems, because they are not designed for public access. Critical systems are often disconnected from all others by a physical separation between those system and all others (Harrett n.d.).

Hacker warfare can be further differentiated into defensive and offensive operations. The debate on defensive hacker warfare concerns the appropriate role for the Department of Defence in safeguarding non-military computers. The debate on offensive hacker warfare concerns whether it should take place at all. In contrast to proponents of tank or submarine warfare, only a few hackers argue that the best defense against a hacker attack is a hacker attack (Libicki 2000; Vatis & Gallagher 1998).

The Internet provides facilities for extremely secure communication. It also provides a means of collecting or disseminating information about potential victims. Finally, it can be used as a source of information about hacking and virus writing. With the availability of such facilities, the potential 'cyber-terrorist' needs only one thing: the motivation to attack. Fortunately at present, the more extreme terrorist organisations are unlikely to resort to the use of hacking tactics, most obviously because the leaders of those groups are not sufficiently familiar with the prospects and capabilities of the new technology. They can be expected, however, to learn quickly. Because of this, it is becoming increasingly important for organisations which use computers and the Internet to ensure that their security is as tight as possible (Anderson & Hundley 1994). Hacker warfare is primarily based on the attacks on the Internet.

2.3.6 Economic information warfare

As outlined in the previous chapter, the marriage of IW and economic warfare can take two forms: information blockade and information imperialism. The effectiveness of an information blockade presumes an era in which the well-being of societies will be as affected by information flows as they are today by flows of material supplies. Nations would struggle for access to external data and, to some extent, would find it difficult to maintain their ability to earn currency by exporting data services. Cutting off access to information would cripple the economies of those nations, bringing them to their knees (Libicki 2000).

Information blockades can be understood as a variant on economic blockades. Cutting off trade in goods can affect the well-being of a country by disrupting production flows and, in the long run, eliminating the benefits of foreign trade. An information blockade works similarly by forcing the target country to work in the dark, eventually removing the benefits of information exchange. It also limits the ability of the blockaded country to engage in psychological warfare (Harknett 1996; Vatis & Gallagher 1998).

An information blockade would interrupt real-time interactions and restrict access to very large information flows. It would be both easier and harder than blocking the country's supply of goods. With less opportunity for physical confrontation, the odds of violence are less. For the most part, information conduits are vulnerable. Physical linkages, such as copper or wire, can be cut off at the border, in the waters, or at the nearest switch. During World War I, England severed Germany's cable links to the United States (Harknett 1996).

Terrestrial radioelectronic connections can be silenced either by silencing the nearest transmitter (e.g., microwave towers) or by selective jamming. Space-based communications pose a bigger problem. Even if all sources uploading to geosynchronous satellites ceased transmissions, some services such as direct broadcast satellite would be nearly impossible to block (Libicki 2000).

For an information blockade to have power similar to that of an economic blockade, the target nation would need to be dependent on external information flows, although information exchange is only one component of trade. A nation that loses access to electronic information exchange could be hindered although not prevented from conducting trade. Iraq, for instance, could still sell oil. Without real-time access to commodity exchanges or the ability to tap databases on usage patterns, a targeted nation might find it more difficult to write the most advantageous contract for itself (Harknett 1996).

Conversely, dependence could arise more from importing information than from exporting it. The growth of computers, communications, and simulation suggests the growing attractiveness of offering services, especially expert services, over the Internet. If the threat of an information war is present, few countries might allow themselves to become so vulnerable. Yet, under peaceful conditions, the prospect of a blockade may seem remote. Dependence on global information links will increase, and even leaders with hostile intent may not perceive that such dependence leaves them vulnerable to retribution if and when the leadership carries out hostile acts (Harknett 1996; Libicki 2000).

To believe in information imperialism means believing in modern day economic imperialism. Thus, trade is war. Nations struggle with one another to dominate strategic economic industries. Nations specialise in certain industries; some industries are better than others. The good industries command high wages and usually feature high growth rates. They tend to be knowledge-intensive; they require and reinforce skills against other nations, particularly those with low-wage workforces that cannot easily compete. Acquiring and maintaining a position in these industries is a reinforcing process. National policies may reinforce virtuous cycles (Libicki 2000).

Intellectual property products such as patents, trademarks, copyright and trade secrets produced by the developed nations from their innovative research are not readily available to the developing world due to the high prices they fetch. Some indigenous knowledge (IK) artefacts that are indigenous to the developing world are being patented by the developed world. This may be seen to constitute IW against the indigenous communities because they cannot afford the patented products and it therefore becomes illegal for the original communities to use their traditional resources. Thus information warfare also results in economic warfare against the developing nations.

The main cause for IW as discussed in the background to the previous chapter can be translated into economic ambitions. The information possessed by the powerful has some economic value. Poor communities can seldom afford to pay for this. This therefore constitutes a form of economic warfare.

2.3.7 Cyber warfare

Cyberwar refers to the execution of military operations according to information-related principles. It means disrupting or destroying information and communications systems; and trying to know everything about an adversary while keeping the adversary from knowing much about oneself. It means turning the balance of information and knowledge in one's favour, especially if the balance of forces is against one. It means using knowledge to prevent the expenditure of capital and labour (Arquilla & Ronfeldt 1993).

The main difference between cyber warfare and hacking is that hacker warfare concentrates on infiltrating computer networks and system security structure (or rather spying) whereas cyber warfare concentrates on corrupting data and impairing communication networks and even rendering the victim's system totally dysfunctional. This form of warfare may involve diverse technologies, notably for command-and-control, for intelligence collection, processing and distribution, for tactical communications, positioning, identifying friend or foe, and for smart weapons systems. It may also involve electronically blinding, jamming, deceiving, overloading and intruding into an adversary's information and communications circuits. Today, on personal level for example, files cover health, education, purchases, governmental interactions (e.g., court appearances), and other data. Some are kept manually or are computerised but inaccessible from the outside, yet in time most will reside on networks. Many people, for instance, might be embarrassed if the information in their collected datasphere was opened to public view; even though that does not necessarily make them good objects for blackmail (Arquilla & Ronfeldt 1993; Libicki 2000; Vatis & Gallagher 1998).

Cyberwar may also imply developing new doctrines about the kinds of forces needed, where and how to deploy them, and how to strike the enemy. How and where to position certain kinds of computers, sensors, networks and databases may become as important as the question of how to deploy bombers and their support functions. The problem in conducting cyberwar is knowing what to do with the information collected (Anderson & Hundley 1994; Bey n.d; Devost et al. 1997; Libicki 2000).

As an innovation in warfare, cyberwar may be to the 21st century what blitzkrieg was to the 20th century. At the very least, cyberwar represents an extension of the traditional importance of obtaining information in war, namely, having superior command, control, communication and intelligence and trying to locate, read, surprise and deceive the enemy before they do the same to you (Arquilla & Ronfeldt 1993).

States that acquire dominance in cyber warfare could make the whole prospect of challenging them seem prohibitively costly. The problem, of course, is that such dominance can be contested, both before and after war begins. Command, control, communications, computer, and intelligence (C4I) assets are susceptible to disruption and failure. The employment of computer viruses, electronic disinformation, or direct destruction of sensing equipment could therefore become increasingly prevalent as the importance of connectivity increases (Libicki 2000).

Interconnected systems are vulnerable to increased connectivity. Haeni (1997:15) notes that systems are mainly vulnerable to the following reasons:

- High-tech equipment is available all over the world (for both friend and enemy).
- The awareness of the danger of IW is mostly absent at the executive level.
- Many computer systems are poorly managed and poorly equipped to prevent intruders.
- Attackers use sophisticated tools to break into systems or to obtain desired information.
- Attacks over the Internet can originate from places that are physically located on the other side of the globe.
- It is impossible to make a system absolutely secure.

2.4 Summary

In this chapter, the various popular forms of IW were identified. In its wider sense, IW is used daily amongst individuals and nations. Almost all other types of IW identified in this chapter, namely, intelligence-based warfare, electronic warfare, psychological warfare, hacker warfare, economic IW and cyber warfare, owe their origin to militaristic warfare. An understanding of IW is therefore limited without an understanding of military tactics, namely, attack and protection.

It can thus be concluded that all forms of IW entail an attempt by a stronger party to subvert a weaker party. This prominent characteristic of IW will be used as a basis for determining whether the problems faced by the developing world in the appropriation of their IK are really a form of IW.

The scope of IW can be expanded to concentrate on controlling minds, knowledge and information. IW as discussed in the above section does not seem to address these issues. It is very important to determine and understand what an Information Science perspective of IW entails before a perspective can be adopted for this thesis on IW. Therefore, the following section aims at achieving an understanding of IW within an Information Science perspective to facilitate an informed choice on the IW perspective to be adopted for this thesis.

2.5 Information Science perspective on information warfare

2.5.1 Background

IW seems to be mostly defined from a military perspective. This leaves some restrictions in the definition and application of what happens in the information world today – specifically regarding IK and intellectual property rights (IPRs) around the globe.

This necessitates a new look and perspective on IW. The new approach that will followed in this thesis will be explained in this section. It will be an Information Science perspective. The reasons for this choice are as follows:

- Such an approach puts the flow of information into perspective.
- It identifies main role players in the access to, use and control of information.
- It allows a discussion on ownership of information with regards to power and dependency.

Before elaborating further on the Information Science perspective of IW, it is important to provide some theoretical background to this field. This will not only permit an understanding of an Information Science perspective but will also promote an understanding of the relationship between power (possessors of information) and dependency (those who need information). All these factors are important in understanding IW within the Information Science perspective.

Figure 2.3 illustrates that all human beings have needs. In order for these needs to be satisfied, resources are required. Information is an example of such a resource. Information or access to information is instrumental in satisfying people's needs. It is essential that users have relevant information about a particular resource that is required to satisfy needs, as well as the information on where to find such a resource.

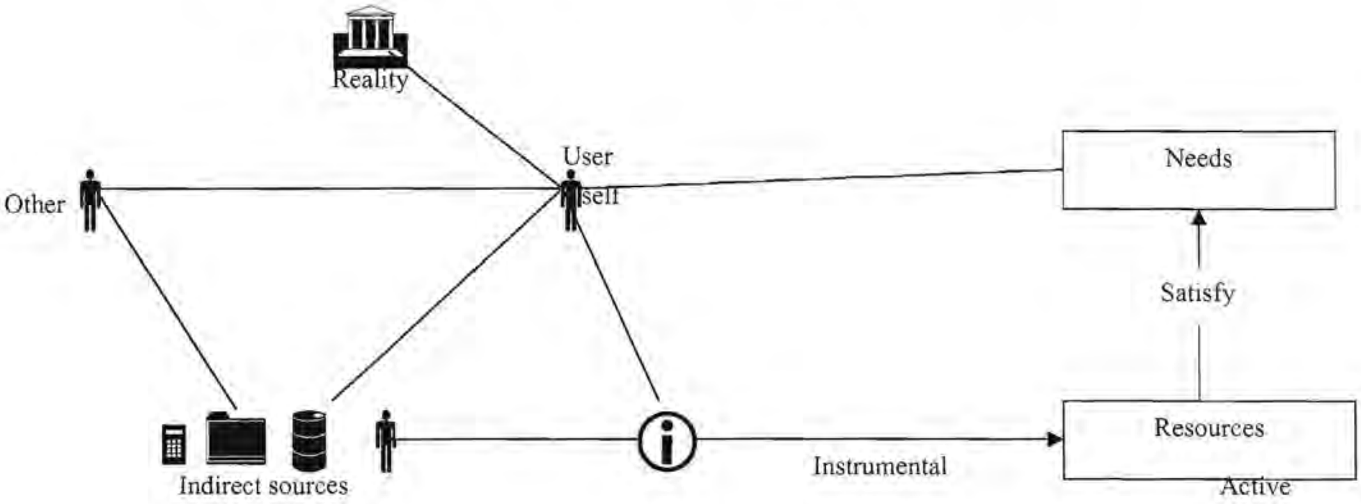


Figure 2.3 **Information sources diagram**

Access to essential information to activate resources to satisfy a need is a basic human right. The main question regarding the satisfaction of needs is where to find relevant information. Figure 2.3 depicts that most information originates from four main sources, namely:

- oneself
- other people
- reality
- indirect sources

Before we define the relationship between IW and Information Science, it is important to take a brief look at the origin of Information Science as a discipline. The next section therefore examines how Information Science is defined as a discipline.

2.5.2 Information Science as a discipline

Information Science has its origin in the successful scientific and technical collaborations of the Second World War. Information Science developed historically, not because of a special phenomenon which has always existed and has now becomes an object of study, but because of a new need to study a problem which has completely changed its relevance for society. For professionals in the field of information, transmitting information to those who need it is a social responsibility (Paisley 1990:4; Saracevic 1990:2; Vickery & Vickery 1992:1).

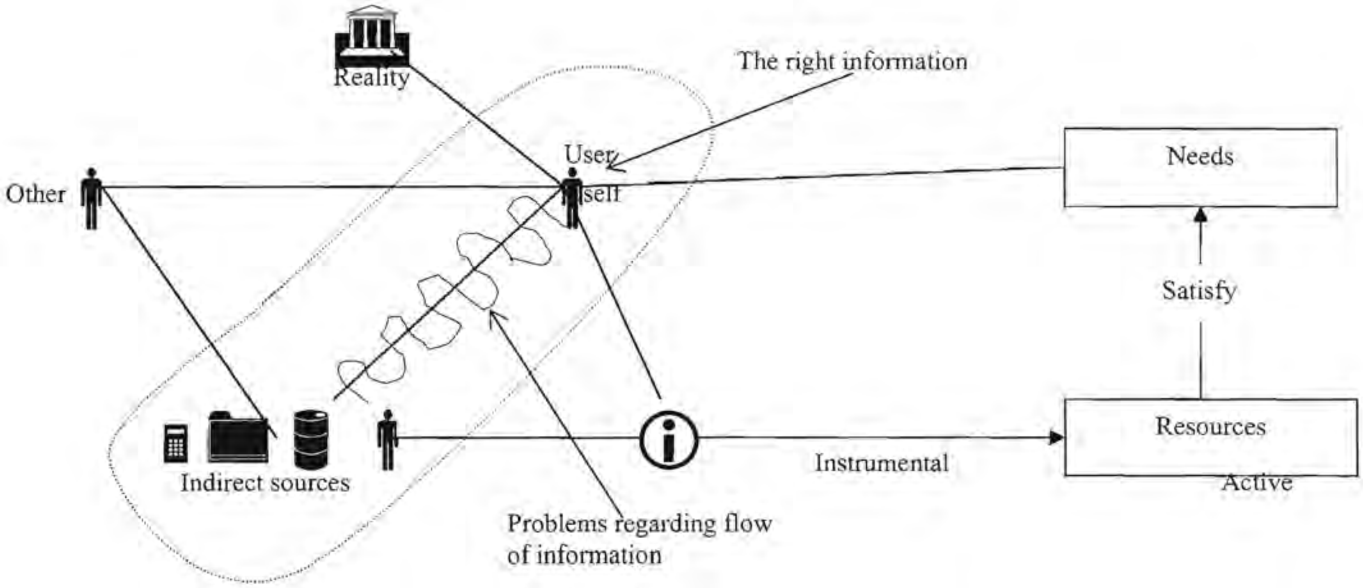


Figure 2.4 Problems with information flow diagram

Based on figure 2.4, the main objective of Information Science is to study the problems pertaining to the flow of information between indirect sources and end-users.

There are several main problems associated with indirect sources (Barker 1992:139):

- They are not always easy to update.
- They are usually expensive to disseminate.
- They can be reproduced.
- Information is more expensive.
- It is difficult to access unorganised information.
- Unknown language is a serious barrier.
- There may be too much information.
- A single copy cannot easily be shared.
- Such sources are easily damaged and vandalised.
- They are sometimes bulky to transport.
- Information is usually scattered among various sources.
- Embedded material is unreactive and static in some sources.
- Some resources cannot utilise sound.
- Some cannot utilise animation or moving pictures.
- It is not always possible to monitor readers' activity.
- Readers' understanding not always possible to assess.
- Some material cannot be dynamically adapted.

The problems listed above may present serious limitations in making information accessible to both the public and the information professional. These problems are prominent in information contained in indirect sources such as published information. As happens in other fields, a number of definitions of Information Science have been offered. The classic definition derived in the early 1960s and formally synthesised by Borko (1968:3) is a good starting point:

> Information Science is that discipline that investigates the properties and behaviour of information, the forces governing the flow of information, and the means of processing information for optimum accessibility and usability. It is concerned with that body of knowledge relating to the origination, collection, organization, storage, retrieval, interpretation, transmission, transformation, and utilization of information...

It has a pure scientific component, which inquires into the subject without regard to its application, and an applied science component, which develops services and products (Saracevic 1990:4).

Machlup (in Saracevic 1990:6) expresses the belief that Information Science is a part of a constellation of disciplines and interdisciplinary research areas that have information and communication as a common focus. He chooses to call this constellation the 'discipline of information'. In order to avoid confusion he suggests that these disciplines be assembled under the banner of Information Science (Saracevic 1990:6; Paisley 1990:5; Vickery & Vickery 1992:11).

The economic realities of the day make it compulsory for those who have generated information contained in indirect sources to be adequately remunerated for their efforts. The laws and IPR regulations accord these generators rights of ownership to the information they generated. Access to the information contained in indirect sources is priced and this accords the generators a measure of power and control over such information. Information and communication technologies are used to protect proprietary information to better control it. One characteristic of the information age is that all communities are more dependent on information than before. All communities, including the poorer communities of the developing world, can only access this information at a cost. This makes access to information for poorer communities very limited because their resources are already over-stretched by other factors.

2.5.3 IW defined within Information Science

The Information Science perspective on IW allows us to address three important topics that have a direct bearing on IW against developing nations. These topics are:

- The commoditisation of information
- Barriers of access to information
- Current trends in IPR regimes

2.5.3.1 Commoditisation of Information

Information professionals are faced with the task of making information available to end users in the right format, at the right time, and in the right context. The problems listed in the previous section sometimes prevent them from effectively performing this function. On the other hand, information users need information to satisfy their needs. Laws in a country, economic conditions of the day, IPRs and censorship are barriers faced by information professionals in their job of disseminating information and by people who wish to access information. These barriers lead to the exclusion of those who desperately require such information. The control over information by its owners accords them the power to restrict, deny or allow access to information. This power may then be used as a form of IW against developing nations.

Schiller (1984:103), and later Lyotard (1993:136), pointed out that this control over information has resulted in commoditisation of information that poses a serious threat to the information commons and the public sphere in general, where information is shared freely between people.

When information is recognised as a commodity, its management becomes paramount. The meaning of the expression "knowledge [information] is power" becomes obvious. If an individual or organisation has sole possession of a particular body of information, that information may enable whoever holds it to achieve objectives. As more information becomes commoditised, the economic value of such information becomes more important to the owners. This is likely to prompt them to lobby for the strengthening of the countries' laws, especially those related to IPRs. This power and control over access to information would further curtail access to protected information. Protection of this information is further enhanced by information and communication technologies available in the information age (Debon et al. 1988:2).

Herbert Schiller (Schiller 1984:81), a neo-Marxist thinker, acknowledges the importance of information in the current era, but also stresses its centrality to ongoing developments. He argues that information and communications are foundational elements of established capitalist endeavour. Webster (1995:74) summarises Schiller's studies of other scholars such as Peter Golding, Graham Murdock and Nicolas Garnham in Britain, and Vincent Mosco and Steward Ewen in the United States, who offer a systematic and coherent analysis of advanced capitalism's reliance on and promotion of information and information technologies.

Schiller draws attention to the pertinence of market criteria in information developments. In his view, it is essential to recognise that information and communications are decisively influenced by the market pressures of buying, selling and trading in order to make a profit. To Schiller, the centrality of market principles is a powerful impulse toward commoditising information, which means that it is being increasingly made available only on condition that it is sellable. He further posits that private firms and institutions are making information a merchandisable good, a commodity produced for profit and sale. Information is something which is increasingly being bought and sold (Schiller 1984:102; Webster 1995:75).

The second argument insists that class inequalities are a major factor in the distribution of, access to and capacity to generate information. Bluntly, class shapes who gets what information and what kind of information they may get. Thereby, depending on one's location in the stratification hierarchy, one may be a beneficiary or a loser in IW.

Schiller further argues that one society that is undergoing momentous changes in the information and communications areas is corporate capitalism. Contemporary capitalism is dominated by corporate institutions, which are concentrated, chiefly oligopolistic organisations that command a national and generally an international reach (Schiller 1984:120; Webster 1995:75).

The pivotal role of the market in the information realm means that information and information technologies are created for and made available to those who are able to pay for them. This does not necessarily mean that they are totally exclusive. In other words, class inequalities exercise a central pull in the information age. Schiller (Webster 1995:91) mentions Vincent Mosco who describes 'pay per society' as the ability to pay as a determining force in the generation of and access to information. The higher one is in the class system, the richer and more versatile the information to which one has access. This creates a class of the 'know' who are the rich and powerful. The quality of information they have enriches their knowledge and status. As one descends the social scale, one gets information of an inferior kind. Those who are at the lower level of the scale are disadvantaged and remain being the 'know-nots' because they are too economically poor to afford or access quality information (Schiller 1984:103).

Based on the above discussion, it is concluded that IW entails a situation whereby people do not have access to information to enable them to exercise their basic human rights. IW from an Information Science perspective can therefore be defined as *a deliberate or non-deliberate attempt to restrict and control access to information.*

2.5.3.2 Barriers of access to information

Coinciding with the commoditisation of information are the various barriers of access to information. It is important to briefly identify these barriers because they will form part of the IW argument later in this thesis. These barriers are:

- Patent protection of products derived from IK resources
- Unauthorised use of tribal names
- Tourism as a means to commercialise indigenous people
- Restricted access to healthcare and healthcare information

2.5.3.3 Current trends in IPR regimes

Multilateral institutions such as the World Trade Organisation, the World Bank, and the International Monetary Fund create global economic policies, including those related to IP, with input mainly from multinational corporations and very little input from the grassroots citizenry. Currently, IP accounts for more than 20 per cent of world trade (Ganguli 2000:167).

Meanwhile, the introduction of the IP system in industrialised economies coincided with the growth of industry, publishing and commerce. On the other hand, the introduction of the IP system does not seem to have made much impact to technological progress in many developing economies (Hoekman & Kostecki 1996:149; Stiglitz 2003:11).

Maskus and Lahouel (2000:595, 598) posit that competition law has emerged as an issue for the WTO because exporting firms in the high income, developed countries argue that anti-competition practices in foreign markets hinder their ability to penetrate those markets. Some observers in developing countries argue that competition law conflicts with the fundamental goal of industrialisation, because open competition favours efficient and established foreign enterprises over inefficient domestic firms.

Multinational firms operate their foreign subsidiaries either as a loose federation or nearly autonomously in order to be able to respond to local needs and national opportunities. In some instances they apply strict controls in order to coordinate worldwide activities and gains from standardised products, manufacturing processes and operations. These firms usually own and control information necessary to produce these products and processes. This valuable information is not readily available to the developing communities and this may ultimately remove their industries from the market (Avgerou 1998:22). The effects of the certain international organisations and conventions are included in this thesis to depict current trends in IPRs internationally. These include the World Intellectual Property Organisation, the General Agreement on Trade and Tariffs, the Trade Related Aspects of Intellectual Property and the Convention on Biodiversity.

2.6 Summary

In attempting to answer the main research problem statement, this chapter addressed the research sub-question:

What constitutes Information Warfare?

A definition of IW from an Information Science perspective was coined. This definition considers IW to be a deliberate or non-deliberate attempt to restrict and control access to information. People's dependency on information has resulted in stringent control over commoditised information being administered by its 'legal' owners by means of IPRs. This has accorded them power and control over information, and subsequently over those who require such information. As a result of the adoption of the Information Science perspective, the IW perspectives touched on in this chapter, namely hacker, cyber, psychological and economic information warfare, will not be examined in further detail.

The next chapter (chapter 3) will investigate the historical context of various types of IPRs and will examine how they are adopted and administered by various countries. This is important because, according to the Information Science approach, IPRs are used to control access to information and protect both societal and economic benefits.