Knowledge Operations: above and beyond Information Operations

Martin Burke
Joint Systems Branch
Defence Science and Technology Organisation
PO Box 1500
Salisbury
South Australia 5108
Australia
Tel: +61 8 8259 7004
Fax: +61 8 8259 5589
Email: Martin.Burke@dsto.defence.gov.au

Abstract

This paper defines Knowledge Operations as orchestrated activities in the knowledge and culture domains that have Defence objectives; Knowledge Operations are often, but not always, conducted in conjunction with Information Operations. It considers the nature of Knowledge Operations and their inter-relationship with Information Operations. Whereas the foci of Information Operations are information and information systems, the foci of Knowledge Operations are thoughts, thinking processes, and Thought Systems. Information Operations are concerned with the symbols to which meaning has been assigned and the ways and means by which such symbols are processed; Knowledge Operations are concerned with the ways and means by which meaning is assigned, derived and shared. The paper provides a variety of examples to illustrate these concepts.

1. Introduction

1.1 Background

US DOD Joint Publication 3-13, *Joint Doctrine for Information Operations*, (DOD 1998), explains that:

> *"Information Operations (IO) involve* ***actions taken to affect adversary information and information systems*** *while defending one's own information and information systems. They apply across all phases of an operation, the range of military operations, and at every level of war. They are a critical factor in the joint force commander's (JFC's) capability to achieve and sustain the level of information superiority required for decisive joint operations."*

It elaborates that:

> *"****Offensive Information Operations involve the integrated use of assigned and supporting capabilities and activities****, mutually supported by intelligence****, to affect adversary decision makers and achieve or promote specific objectives****. These assigned and supporting capabilities include, but are not limited to, operations security (OPSEC), military deception, psychological operations, electronic warfare (EW), physical attack/destruction, and special information operations, (SIO), and may include computer network attack.*

*Offensive Information Operations may be conducted in a variety of situations and circumstances across the range of military operations and may have their **greatest impact in peace and the initial stages of a crisis**. Beyond the threshold of crisis, offensive Information Operations can be a **critical force enabler** for the JFC. Offensive Information Operations may be conducted at **all levels of war** – strategic, operational and tactical – throughout the battlespace."*

It continues to explain that:

*"**Defensive Information Operations integrate and coordinate policies and procedures, operations, personnel, and technology to protect and defend information and information systems**. Defensive Information Operations are conducted through information assurance, OPSEC, physical security, counterdeception, counter-propaganda, counterintelligence, EW, and SIO. Defensive Information Operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes. **Offensive Information Operations can also support defensive Information Operations**.*

*Defensive Information Operations ensure the necessary **protection and defence of information and information systems** upon which joint forces depend to conduct operations and achieve objectives.*

***Four inter-related processes support defensive Information Operations**: information environment protection, attack detection, capability restoration, and attack response. Because they are so inter-related, **full integration of the offensive and defensive components of Information Operations is essential**. JFC's and their subordinate commanders should plan, exercise, and employ available Information Operations capabilities and activities to support integrated defensive Information Operations."*

1.2 Motivation

It is made clear in the above that the foci of Information Operations are:

- information, (ie symbols to which meaning has been assigned);
- information systems, (ie entities that process information).

However, there is a growing awareness in the Defence community[1] that there are other significant factors in modern warfare and anti-warfare[2], namely:

---

[1] See for example Toffler, A. and H. Toffler (1993), Baumard, P. (1996), Nicholson, A. P. (1998), Jarvis, M. W. (1999), Warren, L. (1999), Burke, M. M. (2000a), Burke, M. M. (2000b).

[2] Toffler and Toffler introduced the notion of War and Anti-War as a way of thinking about military conflict and its avoidance, Toffler, A. and H. Toffler (1993). They foresaw that advances in information and telecommunications technologies would lead to Knowledge Warfare and Anti-Warfare (KWAW) being the pre-eminent Defence issue in the twenty-first century. They introduced the idea of Thinking Systems as entities in which groups of people act as knowledge agents supported by networks of information and data systems. They discussed how KWAW concerns the interaction of allies' and adversaries' Thinking Systems.

Thinking Together, Burke, M. M. (2000b), addressed the same domain as Toffler and Toffler. However, by adopting an architectural perspective, it conceptualised the domain in a markedly different way; this afforded various significant new insights that are of potential Defence significance.

- the thought processes by which meaning is derived from information;
- the thought processes by which decisions are made;
- the cultural processes by which meaning is shared amongst groups of people.

Strong arguments have been made to suggest that our ways of thinking about future military conflict and its avoidance need to be extended to include not just the physical and information domains but the domains of knowledge and culture. This extension beyond the limits of Information Operations will be referred to in this work as Knowledge Operations[3].

1.3 Objective

Accordingly, the objective of the paper is to elaborate on the nature of Knowledge Operations and their relationship with Information Operations with the intention of stimulating discussion of the topic in the ICCRTS community.

1.4 Scope and Coverage

The document is based upon a discussion paper, (Burke 2000d) on the topic of Knowledge Operations prepared for the Australian Defence Organisation's Chief Knowledge Officer, Air Vice-Marshall Peter Nicholson. The scope and coverage of this original discussion paper is summarised in the MindMap[4] presented in Figure 1. For the sake of brevity, the scope and coverage of the current paper is limited to consideration of the Why? and What ? aspects, and, considerably fewer examples are included than in the original paper.

1.5 Disclaimer

It is strongly emphasised that the ideas and opinions expressed in both these papers are those of the author alone; they should not be taken to reflect the official position of the author's parent organisations, the Australian Defence Organisation, or its Chief Knowledge Officer.

1.6 Concepts and Terminology

As far as possible, this paper uses the concepts in the sense that they are defined in *Thinking Together: New Forms of Thought Systems for a Revolution in Military Affairs,* (Burke 2000b)[5]. Key concepts of direct relevance are:

- Knowledge is meaning derived from information and other knowledge. Knowing is the process by which meaning is derived from information and other knowledge. Knowing occurs by processing schemata relating to cultural, theoretical and practical matters.
- Information is a set of signs; it is a set of entities used to represent meaning.
- Personal knowledge is the knowledge of an individual knowledgeable entity; it is what is known by an individual.

---

[3] In this work, the term "Knowledge Operations" should be treated as being synonymous with the term "Thought Warfare and Anti-Warfare" defined and elaborated in *Thinking Together*, Burke, M. M. (2000b). The term "Knowledge Operations" is preferred in this context for political reasons. It is emphasised strongly that, in this work, the term "knowledge" should not be taken to relate only to cognitive thought processes but also to emotional and volitional thought processes.

[4] See Buzan, Buzan, T. (1993), for an exposition of the theory and practice of MindMaps.

[5] Appendix A of *Outwit to Win-Win*, Burke, M. M. (2000d), provides a Glossary of the key concepts. References to the sources of the definitions are provided. Appendix D of *Outwit to Win-Win* provides an architectural overview of the central concepts.

- Shared knowledge is knowledge that is common to a group of knowledgeable entities; it is what is known by the individuals in a group that they have in common with all other members of the group.

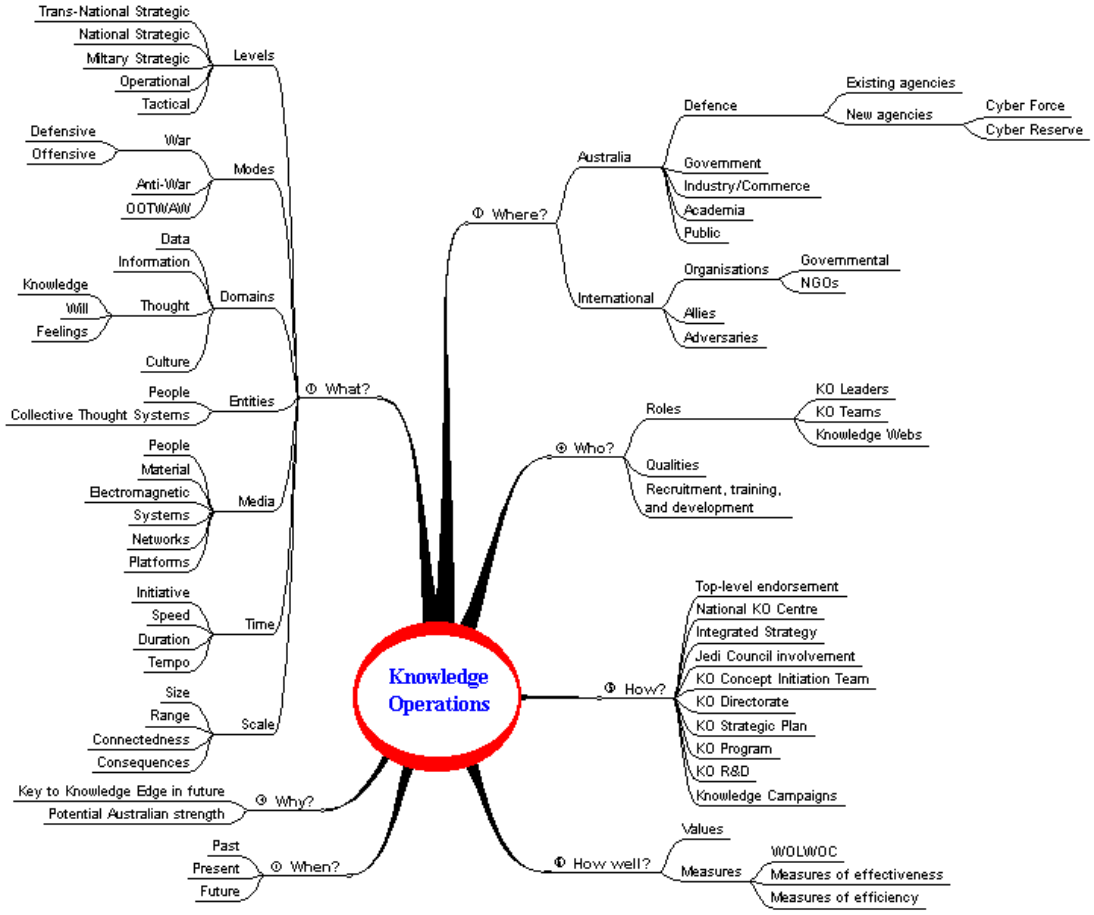

Figure 1. MindMap of the Knowledge Operations domain

- Collective knowledge is the totality of the knowledge of a group of knowledgeable entities; it is what is known by a collective.
- Explicit knowledge is knowledge that has been expressed; it is information.
- Implicit knowledge is knowledge that could be expressed but has not been.
- Tacit knowledge is knowledge that cannot be expressed.
- Knowledge Management is the ways and means by which the development of personal, collective, and shared knowledge is orchestrated within an enterprise. It is concerned with explicit, implicit, and tacit knowledge.
- Information Operations are actions taken to affect adversary information and information systems while defending one's own information and information systems.
- Knowledge Operations are orchestrated activities in the knowledge and culture domains that have Defence objectives.

- Knowledge Leadership is the instigation, direction, motivation, and coordination of cultural, structural, process, and technological initiatives to promote the development and use of personal, shared, and collective knowledge in an Enterprise. It is concerned with explicit, implicit, and tacit knowledge.

2. Knowledge Operations - Why?

The Australian Defence Enterprise faces challenges on a number of fronts in the twenty-first century. These include:

- National strategic. Defence must be prepared to respond to changes in the national strategic (and trans-national strategic) environment. Globalisation and multi-culturalism are anticipated to be significant issues in this respect. Environmental sustainability may also be an important factor.
- Military strategic. Defence must be prepared for changes in the military strategic environment. The Revolution in Military Affairs (RMA), (ORMA 1999) is expected to be a major factor in this regard. In particular, Dibb, (Dibb 1997), has argued that systems integration and cultural change are key issues concerning RMA in the Asian Security context.
- Operational. Defence must be prepared for changes in the nature of the operations that it may be called upon to conduct. For example, significant changes in the nature of warfighting and Operations Other Than War that can be expected as a consequence of the Information Revolution, (Burke 2000b; Burke 2000d). Significant developments in both Information and Knowledge Operations can be anticipated, especially in respect of peacekeeping.
- Inter-operability. Defence can expect to need to be able to operate effectively and efficiently in various roles as members of joint, coalition and multi-national forces. Knowledge and cultural inter-operability may become key issues in this respect. The need for knowledge and cultural inter-operability with (potential) adversaries may also become a key issue in maintaining and/or restoring peace.
- Business. Defence can expect to be called upon to achieve the highest levels of performance and accountability by government and the voting public. Defence will need to be able to perform as a highly effective, efficient and ethical business enterprise at all times.
- Partnerships. Defence may need to establish non-traditional types of relationships with industry, academia, other government departments, etc. Knowledge and culture will be important factors in the success of such collaborative partnerships.

It is plausible that in the future Australia's likely adversaries will have superior numbers and similar technology. Furthermore, they may have access to the same information (ie information security cannot be assured). If this is the case, then it is contended that the most likely source of competitive advantage for Defence will be in making best use of knowledge and cultural resources.

This strongly suggests that Knowledge Management and Knowledge Operations will be increasingly important issues in the Defence's future. Enlightened Knowledge Leadership will be needed if Defence is to adapt appropriately to meet these challenges.

3. Knowledge Operations - What?

3.1 Levels

Knowledge Operations can be categorised broadly in terms of a Knowledge Operations Hierarchy with five indicative levels:

- Trans-National Strategic;
- National Strategic;
- Military Strategic;
- Operational;
- Tactical.

The levels in the hierarchy are distinguished on the basis of the nature, purpose, desired outcomes, and timescales of Knowledge Operations. (Levels do not depend on the scale of the operation[6], or the level of command involved.) In practice, specific Knowledge Operations may not fall neatly into any one of the levels but may "span" the boundaries between levels. For example, specific tactical Knowledge Operations can also have strategic implications at both the national and trans-national level. Furthermore, classes of Knowledge Operations, for example Psychological Operations[7], can be conducted at all levels in the Knowledge Operations Hierarchy; in some circumstances this can happen concurrently.

This paper is primarily concerned with Knowledge Operations at the Strategic levels.

3.2 Modes

Three modes of Knowledge Operations are distinguished:

- War
- Anti-War
- Operations Other Than War and Anti-War (OOTWAW)

In addition, some important examples of orchestrated activities in the knowledge and culture domains that have objectives that are not specifically Defence related are identified. Bringing these examples to the reader's attention is considered worthwhile since if the changes augured above (in the Why ? Section) occur, the boundaries between Defence and non-Defence related matters are anticipated to become increasingly blurred.

3.2.1 War

War is a state of open hostility between two or more adversaries in which the opposing parties[8] attempt to exert their will on each other using means that are outside the laws, agreements, or

---

[6] See below for a definition and explanation of the concept of the "scale" of a Knowledge Operation.

[7] Appendix F of *Outwit to Win-Win*, Burke, M. M. (2000d), contends that within the conceptual framework and terminology used in this work, Psychological Operations are Knowledge Operations mediated through the information domain.

[8] Note that although it is common that the adversarial parties are nation states, this is not necessarily the case. Consider, for example, "the troubles" in Northern Ireland in which the IRA considers that it is at war with the British government. Interestingly, the British government does not share this view.

treaties that would otherwise govern their inter-relationship. War often involves the violent clash of military forces but this is not necessarily the case.

In war, the key success factor is the ability of the dominant force, working as a coordinated entity of heterogenous parts, to outwit its adversaries and to act to realise it's will over that of its adversaries. Although it is normally advantageous to be better informed than an adversary, this is not sufficient in itself to ensure victory[9]. Working as a distributed entity capable of sensing, thinking, communicating, and acting, the dominant force will have superior coordinated approaches to acquiring information, deriving meaning from information, making apt and timely decisions that make appropriate use of information and other resources, sharing meaning including communicating intent, and taking commensurate action. Irrespective of the actions, structures, processes, and technologies involved, such approaches are always knowledge and culture intensive but not always information rich[10].

Aspects of war that are prosecuted in the knowledge and culture domains are referred to as "Knowledge Operations in the war mode". There are both offensive and defensive aspects of Knowledge Operations in the war mode.

Offensive Knowledge Operations aim to achieve or promote objectives by affecting adversaries' thoughts, thinking processes, and Thought Systems including those involved in deriving meaning from information, making decisions, sharing meaning, and communicating intent. Examples include:

- Cognitive Mapping for Knowledge Attack. In Air Power Studies Centre Paper No. 65, (Nicholson 1998), AVM Nicholson argues that:

  > *"to fight in the knowledge domain we must attack and defend both situation awareness and the decision making process. … The revolutionary aspect is knowledge attack aimed at the decision process. … Success in this arena will require a much better understanding of not just how humans make decisions but the decision making process of particular individuals, especially the opposing commander. This 'cognitive mapping' of the opposition may well provide the ultimate knowledge edge."*

  This is an example of an Offensive Knowledge Operation at the Operational/Tactical level.

- Edward VIII. An example of a Offensive Knowledge Operation at the Military Strategic level is provided by the attempt by Nazi officials to encourage the pro-German and pro-Hitler sympathies of (abdicated) King Edward VIII in order to enlist his support for their invasion plans in Europe. It was also their intention to reinstate Edward as King if/when Britain was occupied. If it had become well known that such an important cultural figure as the former

[9] A competitive advantage does not necessarily require "a superior information" position if a protagonist can "outwit" an adversary without being better informed than it. Burke, (Burke, M. M. (2000a), Appendix B), provides a lighted-hearted "quasi-case-study" that, by analogy, affords useful insight into this relationship.

[10] *Thinking Together*, Burke, M. M. (2000b), argues that the collaboration of groups of people on thought-based tasks is currently extremely information intensive and is usually both ineffective and inefficient. It argues that reliance on information sharing is the cause of the most significant deficiencies of current Thought Systems.

British monarch held such views, then the impact on the thinking of both the British leadership and the British people would have been extremely significant.

Defensive Knowledge Operations aim to protect and defend thoughts, thinking processes, and Thought Systems including those involved in deriving meaning from information, making decisions, sharing meaning, and communicating intent. Examples include:

- McCarthyism. In the early days of the Cold War, the Senator JR McCarthy led a team in the USA that attempted to identify and remove people with communist sympathies from the government, educational and media establishments in order to prevent them influencing policies and public opinion. This is an example of a Defensive Knowledge Operation at the National Strategic level.

- The Inquisition. In an attempt to "protect the faith", The Inquisition was active for centuries in identifying, persecuting, torturing, and executing "heretics", ie those who did not subscribe to the doctrine of the Roman Catholic Church. This is an example of a Defensive Knowledge Operation at the Trans-National Strategic level.

Examples of mixed offensive and defensive Knowledge Operations include:

- Military deception. US DOD Joint Publication 3-13, *Joint Doctrine for Information Operations*, (DOD 1998), defines military deception as:

  > *"Actions executed to deliberately mislead adversary military decision-makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission."*

  Military deception can occur at all levels in the Knowledge Operations Hierarchy and can be either offensive or defensive or both.

- *Fatwah*. An example of a mixed offensive and defensive Knowledge Operation is provided by the *fatwah* declared by the leaders of the Islamic orthodoxy on the author Salman Rushdie after his publication of the novel *The Satanic Verses*. By calling for the death of this thinker and writer whose work was considered offensive and threatening, an attempt was being made to prevent further heretical thinking by Rushdie and to deter others from daring to think in unorthodox ways. The *fatwah* is therefore an offensive Knowledge Operation at the Tactical level and a defensive Knowledge Operation at the Trans-National level. In banning the novel to the Islamic faithful, an associated defensive Information Operation was also being conducted.

- Hitler Youth. The Hitler Youth was an organisation set up to educate and train all male "Aryan" German youths in Nazi principles. It involved a regime of dedication, fellowship, and Nazi conformity, generally without parental guidance. Its intention, in which it was highly successful, was to prepare a generation of men mentally and physically conditioned for service

in a nation at war. It was an example of a Knowledge Operation at the Military Stategic/National Strategic Level.

3.2.2 Anti-War

Anti-War is the state in which one or more protagonists act in attempts to avoid war or to regain peace after war has broken out. Anti-War usually complies with the laws, agreements, and treaties that govern the inter-relationships of the belligerent parties in peacetime but this is not necessarily the case. Examples include:

- Diplomacy.
- Peacekeeping.
- Counter-terrorism.
- Awareness campaigns.
- Education and training.

An example of Knowledge Operations in the Anti-War mode is:

- Social netwar. Ronfeldt et al, (Ronfeldt, Arquilla et al. 1998), describe a social netwar as a mode of conflict (or crime) at societal levels, involving measures short of traditional war, in which the protagonists use network forms of organisation and related doctrines, strategies, and technologies attuned to the information age. These protagonists are likely to consist of dispersed groups who communicate, coordinate, and conduct their campaigns in an internetted manner, without a precise central command. Appendix C of *Outwit to Win-Win*, (Burke 2000d), summarises the first example of a social netwar: the Mexican Zapatista social netwar. It is a noteworthy example of a Knowledge Operation at the National/Trans-National Strategic level.

3.2.3 Operations Other Than War and Anti-War

Operations Other Than War and Anti-War (OOTWAW) are operations that Defence may be called upon to conduct or be involved in that do not fall under the categories of War or Anti-War. Typically, they involve considerable interaction with other government and non-government agencies. They can occur before, during or after acts of War or Anti-War. Examples of OOTWAW include:

- Sanctions enforcement;
- Humanitarian operations;
- Defence aid to the civil community, eg controlling civil unrest;
- Emergency relief.

An example of Knowledge Operations in the OOTWAW mode is:

- ADF Recruitment campaign. The Australian Defence Force recruitment campaign currently being conducted in the popular media is intended to attract appropriate new recruits to the services. The messages that the campaign conveys are intended to have an immediate impact on the thinking of the people that respond to them. Furthermore, if appropriately

reinforced, they can be expected to have an ongoing impact on the thinking of those people who are successfully recruited in subsequent stages of their careers. Additionally, the positive images projected in the campaign can also be anticipated to influence the general public's attitude to the military and the morale of current members of the armed services. It is an example of a combined Information and Knowledge Operation at the National/Military Strategic level.

3.2.4 Non-Defence Knowledge Operations

Examples of Non-Defence Knowledge Operations, ie orchestrated activities in the knowledge and culture domains that do not have Defence objectives, include:

- "Stolen Generation" The practice instituted by the Australian government of removing Aboriginal children from their families and traditional cultural environments in order to bring them up in European (mainly British) environments was intended to educate and enculturate the children to align them with the prevailing social and cultural norms of the time. This is an example of a non-Defence Knowledge Operation at the National Strategic level.

- AIS. The Australian Institute of Sport (AIS) identifies potential future elite sportspeople on the basis of their performance in physiological and psychological tests conducted at very early ages. Indeed, talented athletes can be identified before they have shown any particular flair for the events for which they are considered well suited. Having been identified and enlisted into appropriate programs, the athletes are committed to intensive physical and mental training schemes designed to exploit their natural sporting capabilities to best advantage. Australia has been markedly more successful in the world sporting arena since the AIS was established. A most significant point in the context of this work is that this success is grossly disproportionate to the size of the Australian population and the levels of funding and technology involved. Interestingly, other centres of sporting excellence both in Australia and in other parts of the world, have been established subsequently in attempts to emulate the success of the AIS's initiatives. This is an example of a non-Defence Knowledge Operation at the National Strategic level.

- Indian Independence. The non-violent, non-cooperation policy (*Satyagraha*) of the Independence Movement in India led by MK Gandhi (known in India as *Mahatma*) was an inspired Knowledge Operation ideally suited to the cultural environment in which it was conducted. It is noteworthy that the Information Operation associated with this Knowledge Operation, although directed to an enormous target population – principally the population of India but also the world at large - was largely conducted without the organised use of high-technology communication media. This is an example of a non-Defence Knowledge Operation at the National Strategic level with Trans-National Implications, see below.

- British Public Schools. In the United Kingdom, public schools are fee-paying, secondary-level, educational establishments that operate independently of the state system. Traditionally, the public schools were male-only, run on a boarding basis, and the exclusive reserve of the upper social classes; their role was to prepare students for further education in the ancient universities of Oxford and Cambridge and/or for public service. The impact of the public

school system has been immense, particularly in building and administering the British Empire. It produced a continuous stream of men inculcated in a common ethos who went on to play most of the important roles in running Britain both nationally and internationally. The ethos was a class-conscious code of behaviour, speech and appearance, but was not particularly academically based. It set the standard for conduct in the life in British officialdom from the early 19th century to the mid-20th. Although only a relatively tiny proportion of the British population, those with a public school education held most of the positions of power and influence in the British Empire. The ethos was further reinforced by practices such as:

- successive generations from the same family attending the same public school;
- expatriate Britons, and those serving abroad, sending their children back to Britain to be educated at public school;
- children from socially elite families in the British colonies sending their children to be educated at British public schools.

This is an example of a non-Defence Knowledge Operation at the National Strategic level with Trans-National Strategic implications.

3.3 Domains

The nature of the domain of Knowledge Operations and its relationship with that of Information Operations has been outlined above. Whereas Knowledge Operations are concerned with the ways and means by which meaning is assigned, derived and shared, Information Operations are concerned with the symbols to which meaning has been assigned and the ways and means by which such symbols are processed. A key consideration in gaining a more thorough understanding is to appreciate the role that "meaning" has in distinguishing between the following concepts.

- Data;
- Information;
- Thought;
- Knowledge;
- Will;
- Feelings;
- Culture.

The conceptualisation of Thought Systems presented in *Thinking Together*, (Burke 2000b) attempts to facilitate gaining such an understanding by defining and explaining the concepts and their inter-relationships.

3.4 Entities

Thoughts, thinking processes, and Thought Systems are the primary foci of Knowledge Operations. *Thinking Together*, (Burke 2000b), defines these concepts as follows.

- Thought is meaning derived from knowledge, will, feelings and other thoughts; it is a state of mind[11].
- Thinking is the process by which meaning is derived from knowledge, will, feelings and other thoughts.
- A Thought System is an entity capable of thinking; it deals with data, information, knowledge, will and feelings.

Thought exists only in Thought Systems; it is what a Thought System thinks[12].

Thought Systems, therefore, are the entities that are the "targets" of Knowledge Operations. There are two classes of Thought System that are anticipated to be the major concern of Knowledge Operations in the foreseeable future:

- People. Notwithstanding any advances that may be made in Artificial Thought Systems[13], it is expected that the majority of important cognitive thinking in Defence affairs, and all emotional and volitional thinking, will be conducted by human minds. Even if some cognitive activities become the exclusive realm of Artificial Thought Systems, the most adaptive element in the overall Defence Thought System of which they are components will remain the human mind.
- Collective Thought Systems. Collective Thought Systems are an important class of Hybrid Thought System[14], in which, typically, large groups of people interact via networks of information and data systems to create emergent properties[15]. The dominant architectural characteristics of Collective Thought Systems include:
  - Extremely large group sizes
  - Extremely high levels of data and information usage
  - Poor levels of coordination
  - Widespread distribution
  - Extremely high levels of diversity
  - The emergent property of Collective Intelligence[16]

3.5 Media

There are various media that can be used in the conduct of Knowledge Operations. These include:

- People. Traditionally, people have been the most important medium in the conduct of Knowledge Operations. They can be involved in the creation, destruction, manipulation, influence, etc of most categories of Thought Systems, particularly other those involving other people.

---

[11] In this work, the term "mind" is used in the following sense: "Mind is the seat of cognition, emotion, volition and consciousness, it is that which knows, feels, wills and thinks."

[12] Appendix E of *Outwit to Win-Win*, Burke, M. M. (2000d) , provides a categorisation scheme for Thought Systems.

[13] See Appendix E of *Outwit to Win-Win*, Burke, M. M. (2000d) for a definition of this concept.

[14] See Appendix E of *Outwit to Win-Win*, Burke, M. M. (2000d) for a definition of this concept.

[15] See Levy, Levy, P. (1997) and *Thinking Together*, Burke, M. M. (2000b), for a discussion of these ideas.

[16] See Levy, Levy, P. (1997) and *Thinking Together*, Burke, M. M. (2000b), for a discussion of this concept.

- Material. Physical material items, eg explosives, bullets, shells, etc, may be used in Knowledge Operations that involve physical attack or destruction of Thought Systems.
- Electromagnetic. Electromagnetic and directed energy may be used as the medium to conduct Knowledge Operations.[17]
- Systems. Various types of engineered systems, in particular information systems, may be used as the medium to conduct Knowledge Operations.
- Networks.
- Platforms.

3.6 Time

3.6.1 Initiative

Knowledge Operations usually involve the dynamic interaction of two or more Thought Systems[18]. The Thought System that starts such an interaction is said to have taken the initiative in the Knowledge Operation. If, however, another Thought System succeeds in taking over control of the dynamics of the interaction, then it is said to have gained the initiative in the Knowledge Operation. As in other forms of military operations, taking (or gaining) the initiative can be a critical factor in the outcome of a Knowledge Operation. In Knowledge Operations boldness and imagination are especially important factors in taking (or gaining) the initiative. The AIS initiative outlined above provides an excellent example of this.

3.6.2 Speed

The rate of development of a Knowledge Operation is referred to as its speed. The speed of Knowledge Operations can vary enormously. Scrutiny of the examples outlined above suggests that the dominant factor affecting the speed of a Knowledge Operation may be the medium that is used in its conduct. For example, the use of modern information systems in the Zapatista Social Netwar meant that it proceeded very much more rapidly than the Indian Independence movement which was conducted to a large extent by word of mouth.

3.6.3 Duration

The period of time over which a Knowledge Operation is conducted is referred to as its duration. The duration of Knowledge Operations can vary enormously ranging from split seconds to decades or more. Typically, but not always, Knowledge Operations at lower levels in the Knowledge Operations Hierarchy will be of shorter duration than those at higher levels. For instance, scrutiny of the examples outlined above suggests that the duration of Knowledge Operations at the National and Trans-National Strategic levels is typically of the order of a human generation.

3.6.4 Tempo

The tempo of a Knowledge Operation is the rate of development of the Operation relative to that of another party, usually an adversary. Again, the tempo of Knowledge Operations can vary

---

[17] Note that US DOD Joint Publication 3-13, Joint Doctrine for Information Operations, DOD, U. (1998), explains that Electronic Warfare (EW) is "any military action involving the use of the electromagnetic or directed energy to control the electromagnetic spectrum or attack the enemy".

[18] In some cases, one or more of the Thought Systems involved can be a Culture System, ie a System of Thought Systems. See *Thinking Together*, Burke, M. M. (2000b), for a more detailed discussion of Culture Systems.

enormously. A critical success factor in Knowledge Operations is dominating or controlling its tempo. An example of this is the established need, "to get inside the enemy's decision cycle". Tempo is expected to be of utmost importance in Knowledge Operations at the Tactical and Operational level such as "knowledge attack aimed at the decision process", (Nicholson 1998).

3.7 Scale

3.7.1 Size

The number of Thought System components in a Knowledge Operation is referred to as its size. The size of Knowledge Operations can vary enormously ranging from just two to billions. The typical scale of the Knowledge Operations in which Australia will be involved in the future is anticipated to become increasingly large as a consequence of developments in information and telecommunications technologies, and the changing demographics of the populations of Australia, its allies, and adversaries. The Zapatista Social Netwar again provides useful insight in this respect.

3.7.2 Range

The physical distance over which a Knowledge Operation is conducted is referred to as its range. As can be seen from the examples outlined above, the range of Knowledge Operations can vary enormously ranging from the immediately local to global.

3.7.3 Connectedness

The extent and manner in which the Thought System components in a Knowledge Operation are accessible or linked with one another is referred to as its connectedness. The connectedness of Knowledge Operations can vary enormously from disconnected – no Thought System components are linked to one another - to completely connected – all Thought System components are linked to one another. Although the medium used to conduct a Knowledge Operation can be a strong factor, the connectedness of a Knowledge Operation is ultimately an architectural issue. Comparison of the Hitler Youth and the "Stolen Generation" schemes outlined above provides interesting insights in this respect. The Hitler Youth scheme created a hierarchically connected corpus with a high degree of cultural conformity whereas the "Stolen Generation" scheme destroyed the connectedness and cultural identity of the targeted group.

3.8 Consequences

The impact of the outcomes of a Knowledge Operation is referred to as its consequences. Consideration of the examples outlined above shows that consequences may be beneficial or undesirable and can vary from the almost inconsequential to profoundly significant.

4. Concluding Remarks

There is growing awareness in the Defence community that our ways of thinking about future military conflict and its avoidance need to be extended to include not just the physical and information domains but the domains of knowledge and culture; the perception is that there is a need to go beyond the limits of Information Operations to consider Knowledge Operations. Accordingly, this paper has speculated on the nature of Knowledge Operations and their relationship with Information Operations with the intention of stimulating discussion of this topic in the ICCRTS community.

Furthermore, there is a burgeoning school of thought within Australia that believes that Knowledge Operations will be an increasingly important issue in the nation's long-term Defence strategy – particularly as emphasis continues to shift from warfighting to maintaining and/or restoring peace. The diversity of Australia's multi-cultural population is anticipated be a sustainable source of strength in such an epoch, see (Burke 2000b; Burke 2000d).

It has been argued elsewhere, (Burke 2000d), that realising this potential is most unlikely to happen by accident; bold and imaginative initiatives will be needed to orchestrate the nation's knowledge and cultural resources to these ends. In particular, it is contended that enlightened Knowledge Leadership[19] will be needed if Defence is to adapt appropriately to meet these challenges. Fortunately, such initiatives are not expected necessarily to require huge investments of money and technology. Furthermore, it is anticipated that significant results could be achieved within the timescale of a typical major Defence procurement.

The Australian Defence Organisation's Chief Knowledge Officer, Air Vice-Marshall Peter Nicholson, intends to explore the viability of this thinking more thoroughly. As a first step in this process, he has directed that a Concept Initiation Team be established to consolidate and extend the provisional thinking that has been outlined above, which will then be probed through War-gaming activities. The results of such work will be reported in due course.

5. References

Baumard, P. (1996). From InfoWar to Knowledge Warfare: Preparing for the Paradigm Shift. Intelligence Newsletter.

Burke, M. M. (2000a). Information Superiority, Network Centric Warfare and the Knowledge Edge, DSTO Research Report DSTO-TR-0997.

Burke, M. M. (2000b). Thinking Together: New Forms of Thought System for a Revolution in Military Affairs, DSTO-RR-0173.

Burke, M. M. (2000c). Web Spinning and Weaving: Knowledge Leadership for the Defence Enterprise. Available from the author on request.

Burke, M. M. (2000d). Outwit to Win-Win: Knowledge Operations for the Defence Enterprise. Available from the author on request.

Buzan, T. (1993). The Mind Map Book, BBC Books.

Dibb, P. (1997). The Revolution in Military Affairs and Asian Security. IISS Annual Conference on Security Challenges in the Rising Asia-Pacific, Singapore.

DOD, U. (1998). Joint Doctrine for Information Operations, Joint Pub 3-13.

Jarvis, M. W. (1999). Organisation, Knowledge and Change: Defence as a Learning, Adaptive, Innovative Organisation, Capability Analysis Staff, ADHQ.

Levy, P. (1997). Collective Intelligence: Mankind's Emerging World in Cyberspace. New York, USA, Plenum Press.

Nicholson, A. P. (1998). Controlling Australia's Information Environment or Decision Superiority and Warfighting, Air Power Studies Centre.

[19] See *Web Spinning and Weaving*, Burke, M. M. (2000c), for a discussion of Knowledge Leadership.

ORMA (1999). The 'Revolution in Military Affairs' and the Australian Defence Force: A Public Discussion Paper, Office of the Revolution in Military Affairs.

Ronfeldt, D., J. Arquilla, et al. (1998). The Zapatista Social Netwar in Mexico, RAND, Arroyo Center.

Toffler, A. and H. Toffler (1993). War and Anti-War: Survival at the Dawn of the 21st Century, Little, Brown and Company.

Warren, L. (1999). Towards an Understanding of Knowledge Operations.