CANADIAN FORCES COLLEGE / COLLÈGE DES FORCES CANADIENNES
CSC 28 / CCEM 28

EXERCISE/EXERCICE NEW HORIZONS

KNOWLEDGE WARFARE: VULNERABILITY OR OPPORTUNITY

"Thus, what is of supreme importance in war is to attack the enemy's strategy."[1]

- Sun Tzu

By/par Major RDL Knight

This paper was written by a student attending the Canadian Forces College in fulfilment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions that the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied except with the express permission of the Canadian Department of National Defence.

La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de diffuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale.

[1] Sun Tzu, The Art of War, (New York: Oxford University Press, 1971) p. 7.

Abstract

This paper focuses on the question of how well Canada is prepared for an attack by an enemy that has a Knowledge Warfare (KW) capability. The discussion uses current manoeuvre warfare theory and information operations concepts as framework to develop KW and then clarifies it as manoeuvrist concept of operations that focuses primarily on defeating the enemy's will by attacking the cognitive aspects of conflict. From this basis the three elements of KW of precision, tempo and perception are assessed against the Canadian Forces capability, where various gaps are exposed. The research for this paper used Canadian Forces Doctrine and a number of books on manoeuvre war; however because KW is a relatively new idea an extensive amount of information was found on Internet sources.

KNOWLEDGE WARFARE: VULNERABILITY OR OPPORTUNITY

The tragedy of September 11th 2002 and the worldwide military tempo of late are reminders to Canadians that we are indeed living in a dangerous world. Military operations have become progressively more complex where widely different operations such as combat engagements, humanitarian aid and counter-terrorist actions can be happening in the same area at the same time. The information age presents new challenges where one only has to call upon the Internet to access any number of theories about how future war will be fought through electrons and keystrokes. It is from these new ideas that the concept of information operations (IO) and information war has sprung. From this origin, a school of thought has been growing whereby it is possible to directly engage enemy decision-makers in what has been labelled knowledge warfare (KW). As early as 1993 the Tofflers spoke of KW as a state were "each side of the battle space will try to shape enemy actions by manipulating the flow of intelligence and information."[2] To date the Canadian doctrine on IO has been neglecting this avenue of attack on its national security. Although Canadian Forces IO doctrine includes a psychological and media element there has been a lack of any reasonable force structure, tactics or procedures to deal with it. Ideally, the first steps to correcting this should include the clear identification of the operational requirements, assignment of responsibility to develop the separate aspects, and finally methods of measuring effectiveness and risk must be developed.[3]

[2] Alvin and Heidi Toffler, War and Anti-War, (Little and Brown Co., Boston (USA), 1993) p.140.

[3] Paul K. Davis, David C. Gompert, Richard J. Hillestad, and Stuart Johnson, Transforming the Force, (Rand Corporation (USA), 1998) http://www.rand.org/publications/IP/IP179 p. 26.

This paper will show that Canada is vulnerable to the threat of an enemy capable of employing Knowledge Warfare attacks against it. To determine this it will be important to understand how Canada employs its current manoeuvre warfare concepts and interpret how IO functions within these. Once it has been established how IO links with current warfare practices it will then be possible to show that there is a subset of IO that targets the cognitive processes of the decision-maker vice his command and control mechanisms. This in turn provides the opportunity to describe this cognitive aspect of conflict as the domain of KW. Having narrowed the discussion to the KW aspects of battle, three specific elements of KW will be reviewed and, for each, an assessment will be made as to how Canada is vulnerable to attack. From this analysis it will then be possible demonstrate Canada's over all vulnerability to synchronised attacks using KW methods.

Canada's Manoeuvrist Approach to Warfare

The first step in determining whether or not Canada is vulnerable to such KW attacks is to understand the current theory of warfare adopted by the Canadian Forces. War by definition "is strife between nations conducted by force."[4] Warfare, is the art of campaigning within a state of war and is characterised by a violent physical struggle between combatants with the aim of defeating the opponent's armed forces to compel him to do the will of the other.[5] The dominant theory of war in Western military art is

[4] Edited by J.B. Sykes, The Concise Oxford Dictionary of Current English, (Oxford University Press (NY – USA), 1982) p. 1240.

[5] Carl von Clauswitz, On War, (New Jersey: Princeton University Press, 1989) p. 75.

manoeuvre warfare and this will be used as the base line in the subsequent discussion of how IO and then KW fits into warfare theory.

Canadian Forces manoeuvre warfare doctrine emphasises pre-emption, dislocation and disruption of an enemy using synchronised attacks on his weaknesses and avoiding his strengths, with the aim of destroying his ability and will to fight.[6] Classical manoeuvre warfare theory argues that manoeuvre through an enemy weakness toward a critical vulnerability or moral centre of gravity can bring about defeat when there is a sustained threat that works more on the mind then on mass.[7] Weakness, in this context, is a measure of combat strength, while vulnerability is a facet of the enemy's capability that, if lost, will neutralise some aspect of his forces.[8] This is of significance because critical vulnerabilities will usually represent military objectives and an experienced commander will defend his own vulnerabilities in strength. The manoeuvrist objective to dislocate strength and attack critical vulnerabilities is designed to isolate or destroy the source of his principle strength, this being the "centre of gravity".[9] This is important because "to weaken a centre of gravity is to imperil the enemy's ability to continue the conflict; to destroy the centre of gravity is to produce a cascading failure that leads to capitulation."[10] In the time of Clausewitz this was usually a pitched battle where

[6] Department of Army Doctrine B-GL-300-001/FP-000 Conduct of Land Operations-Operational Level Doctrine for the Canadian Army, (Government of Canada, 1998) p. 2-2 to 2-5.

[7] Robert Leonhard, The Art of Maneuver, (Presidio Press (USA), 1991) p. 181-2.

[8] Leonhard, The Art of Maneuver, p. 167.

[9] Clauswitz, On War, p. 595-596.

[10] Jeffery A. Harley USN, Information Technology, and the Centre of Gravity, (Navy War College Review (USA),1997) http://www.nwc.navy.mil/press/Review/1997/winter/art4wi97.htm p. 7.

overwhelming strength or mass was required. Recent history, and current doctrine, suggests that a faster decision cycle, which allows for swift manoeuvre into the operational depth of an enemy can crush his will and capability to sustain a fight.

The ability to conduct such a manoeuvrist approach to warfare is based on the commander's ability to synchronise all of his capabilities in such a way as to create operational dilemma. This dilemma is created by threatening the enemy with a number of capabilities where the countermeasure for one makes him vulnerable to others. The operational aspect of this is to force the enemy to act predictably by creating the dilemma, not by winning individual tactical battles.[11] The development of air power provides a useful analogy to this phenomenon. Air power, although a powerful capability, by itself it cannot always be relied upon to complete the defeat of an enemy. It is through the delivery of air power within the context of a combined arms or operational manoeuvre that creates an insurmountable dilemma for the enemy. This dilemma denies the enemy movement using air power; however, if he defends himself against air attack, by static dispersion, he becomes vulnerable to land assault.

Another warfare concept that is important to this discussion is that of asymmetric warfare. Asymmetric warfare provides an alternative to engaging the enemy as he has equipped and trained himself. Although it is not necessary to be the underdog to employ such methods, asymmetric methods are usually used to level the playing field. The concept is simple; if you cannot beat the enemy by pitting yourself against his strength then you employ innovative methods to functionally dislocate his doctrine, system of

[11] Leonhard, The Art of Maneuver, p. 161.

fighting, in order to achieve a strategic aim.[12] In this way asymmetric warfare is a manoeuvrist approach to engaging an enemy that has an overwhelming superiority to your own. Like the Spanish guerrillas of Bonaparte's time, the French Resistance of WW2, or the Maoists insurrectionists, today's asymmetrical warfare, such as terrorism or computer network attack, is a departure from conventional doctrine and the customs of war.

Information Operations and Manoeuvre War

With these warfare concepts in place, it is possible to interpret the relationship between information operations to manoeuvre warfare. The increased use of high-speed communications, integrated networks and reliance on computer automation has created its own medium of opportunity and vulnerability. In the information age, the high-speed information system is the focus of much attention and is an established battle space environment. "Information as an environment may be difficult concept to grasp, but there is no arguing that there is a physical environment to which information is uniquely related: cyberspace. Cyberspace is that place where computers, communications system, and those devices that operate via radiated energy in the electromagnetic spectrum meet and interact."[13] There is nothing new about infiltrating or manipulating such command and control or intelligence systems, but the interconnectivity of information sources on a global scale provides new vulnerabilities to be exploited. It is also possible that this

[12] Steven Metz and Douglas V. Johnson II, Asymmetry and U.S. Military Strategy:Definition, Background, and Strategic Concepts, (Project on Defence Alternatives (USA), 2001) http://www.comw.org/rma/fulltext/asymmetric.html, p. 5.

[13] Dan Kuehl, Defining Information Power, (National Defence University Strategic Forum (USA), 1997) http://www.ndu.edu/inss/strforum/forum115.html p. 3.

information element of the battle space can prove to be a critical vulnerability or a centre of gravity because such manipulation of information affects leaders and it is only they who can negotiate or make concessions.[14]

As useful as this a capability is, information, in itself, cannot be relied upon to satisfy the requirement for defeat of an enemy, as it does not actually deal with the opponent's armed force. It may be possible to use information-focused attacks to render portions of the enemy's military capability ineffective but as for the previous example of air power; IO must be used together with other compatible military capabilities to achieve the manoeuvrist aims of pre-emption, dislocation and disruption of the enemy. The intent of IO engagements is to cause confusion and surprise, giving the friendly commander time to snatch the initiative. However, war is a contest of human wills not an engagement between machines, therefore, innovative applications of information technology may enhance the combined military capability but it cannot supplant it.[15] In the end, the human mind is the object of war and information provides a more direct and explicit avenue for attacking the will of the decision-maker than would blind firepower. It follows that IO can be used in manoeuvre warfare to attack the mind as well as shape the physical battle space. It is noteworthy that such methods can be considered asymmetrical where an appropriate military doctrine and training has is not developed to deal with it.

[14] Harley, Information Technology, and the Centre of Gravity, (Navy War College Review (USA), 1997) http://www.nwc.navy.mil/press/Review/1997/winter/art4wi97.htm

[15] Paul van Riper and Robert H. Scales Jr., Preparing for War in the 21st Century, (US Army War College Quarterly – Autumn, 1996) http://carlisle-www.army.mil/usawc/Parameters/97autumn/scales.htm, p. 7.

Information Operations and Knowledge Warfare

Western military definitions of IO have been slowly shifting from one that focuses on the information systems to one that focuses on the decision-maker.[16] This is significant because the later opens the concept up to far more than the former. When the decision-maker is the focus it implies that both the cyber domain and the cognitive mind are involved. Yet, both of the terms information and knowledge can be used to examine this phenomenon of influence on the cognitive process, therefore, it is necessary to determine the genuine difference between the concepts of information and knowledge. The Oxford Dictionary defines knowledge as "a familiarity gained by experience, a person's range of information, or a theoretical or practical understanding."[17] From this it is apparent that the concept of information is intertwined with that of knowledge. The relationship between these concepts is that information is something that is unknown at the intended destination until the moment of its reception, thus information must increase the amount of knowledge at the destination.[18] For these purposes knowledge refers to the understanding of information and the degree of comprehension of both the information held in a static structures, such as catalogues, as well as the dynamic behaviours or processes that act within an environment.[19] Information alone refers to the arrangement of data into order as to ascertain facts.

[16] Chief of the Defence Staff. B-GG-005-004/AF-010 - CF Information Operations. (Government of Canada, 1998) p. 1-6.

[17] Oxford Dictionary p. 556.

[18] Josip Pajk, Information or Knowledge Warfare?, 1997, http://members.tripod.com/~THREENITY/Infwar.htm p. 4.

[19] Edward Waltz, Information Warfare principles and operations, (Norwood USA, 1998) p.2 &50.

It is also important, in this context, to understand that knowledge is the means by which commanders make decisions and that this is done so based on trust. Modern commanders must believe that the symbols they see on their tactical displays are real. But what if the display had targets that do not really exist, or if a real threat was not displayed in time? In such a case the correct information would be thrown into doubt because of a failure of the dynamic system, meaning that there would be no knowledge gained from the information presented.[20] This is of great concern, especially where technology is rolled off of assembly lines and integrated into defined structures where vulnerabilities or flaws can be found and exploited by a worthy opponent.

A paper by Dr. Martin Burke from the Australian Defence Science and Technology Organization on "*Information Superiority, Network Centric Warfare and the Knowledge Edge"* explains that there is a linkage between IO and KW. He proposes that knowledge superiority is required for both information operations and for manoeuvre warfare. He goes on to explain that where knowledge superiority is required to make these warfare theories work, information superiority is only beneficial.[21] This is an interesting and astute distinction; he maintains that knowledge enables increased tempo and precision in operations or weapons because it gives an edge to the decision-maker. Information taken alone, on the other hand, enables the ability to derive knowledge but, if mishandled, it can also hinder it. This means that the concept of information dominance

[20] Pajk, Information or Knowledge Warfare? p. 9.

[21] Martin Burke, Information Superiority, Network Centric Warfare and the Knowledge Edge, (Australian Defense Science and Technology Organization Electronics and Surveillance Research Laboratory, July 2000) p.4.

is in reality something achieved by transforming knowledge into capability.[22] After all, the ability to identify the vulnerabilities and centres of gravity of an enemy, reshape organizations, or revise strategies is a decision process based on knowledge. The knowledge advantage enables the commander to better execute warfare.

The Elements of Knowledge Warfare

As we have seen KW is a manoeuvrist concept of operations that focuses primarily on defeating the enemy's will by attacking the cognitive aspects of conflict. This is achieved by synchronizing battle space effects, including the physical and cyber environments, with the ultimate aim of attacking the cognitive processes of planning or decision making. This said, it has been observed by many in the academic community that Western society has not fully recognised the potential of this concept. Dr. Philippe Baumard, Professor of Strategic Management at the University of Paris-XII in his paper *"From Info War to Knowledge Warfare"* has described one of the greatest set backs in Western development of this emerging concept. He points out that current thinking in the west views knowledge as a commodity.[23] From this professor's inspired work it is clear why modern warfare requires more then sensors and computer networks. It is because knowledge is not merely a static commodity, it is a dynamic notion centred on people and the human mind's ability to reason and understand its environment. Knowledge-based

[22] Lieutenant Colonel W.R. Fast, Knowledge Strategies: Balancing Ends, Ways, and Means in the Information Age, (Institute for National Strategic Studies (USA), 1998) http://www.ndu.edu/inss/siws/Ch1.html, p. 8.

[23] Philippe Baumard, PhD., From Info War to Knowledge Warfare: Preparing for the Paradigm Shift, (Intelligence online, 2002) http://gcc.uni-paderborn.de/www/WI/WI2/WI2_LIT.NSF/fb8fb1b65f7e25e3412568ce0052e511/6dee8c20b2de65004125692e00693585/$FILE/baumard.htm p. 3.

war is steeped in perception. "In the knowledge warfare paradigm, strategic advantage does not lie in the concentration of facts and figures, but in the complementarity and singularity of the brains who interpret them."[24] Indeed, there is more then information, processes and communications involved with this new world where it is possible to engage in KW it is also about a robust and innovative ability to make sense of the environment.

Complementary to Dr Baumard's assessment, a paper from the US Foreign Military Studies Office, by Timothy L. Thomas, called "*Like Adding Wings to the Tiger*", gives a similar assessment from the Chinese perspective. In this paper the author points out that Chinese IO theory is more diverse then the West because it is strongly influenced by Chinese military art and stratagems.[25] These stratagems emphasize deception, disruption, physical and functional dislocation, as well as economy of force. This sounds very much like our own manoeuvrist doctrine; however, the Chinese attitude toward IO has a clearer focus on knowledge. Since 1996 Chinese military thinkers have been proposing definitions of IW and currently this intellectual process has provided that, in addition to a technological battle, "the main tasks of IO are disrupting the enemy's cognitive system and trust system."[26] In their framework KW refers to a battle of competing brains that must process seemingly endless streams of information and then assemble this into an intelligible, useable form that gives one side an advantage. The

[24] Baumard, From Info War to Knowledge Warfare: Preparing for the Paradigm Shift p.8.

[25] Timothy L. Thomas, Like Adding Wings to the Tiger: Chinese Information War Theory and Practice, (Foreign Military Office (USA), 12 June 2000) http://call.army.mil/call/fmso/fmso/fmsopubs/issues/chinaiw.htm.

[26] Thomas, Like Adding Wings to the Tiger, http://call.army.mil/call/fmso/fmso/fmsopubs/issues/chinaiw.htm

speed of processing and the ability to innovate quickly determines combat power where the likely losers are those who lack command thinking rather than advanced technology.[27]

Dr Baumard and Mr. Thomas make the point that in Western practice of IO, the cognitive aspects, or the knowledge aspects, are not receiving the attention they deserve. To explore these knowledge aspects this paper will use a three-tiered operational model for IO described by Edward Waltz in his book, *Information Warfare Principles and Operations*. This model, depicted at Figure 1, includes the perceptual tier, as the highest order, supported by an information infrastructure tier and finally the physical tier, at the foundation.[28] The significance of this model is that it provides a theoretical structure to

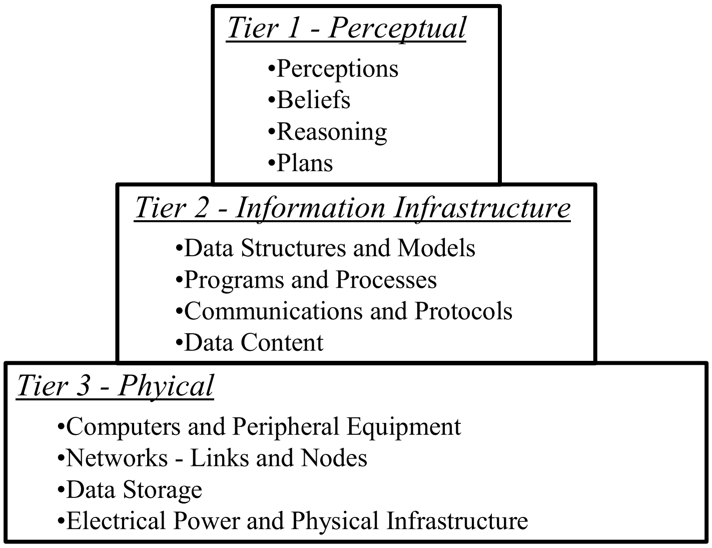
Tier 1 - Perceptual
•Perceptions
•Beliefs
•Reasoning
•Plans
Tier 2 - Information Infrastructure
•Data Structures and Models
•Programs and Processes
•Communications and Protocols
•Data Content
Tier 3 - Phyical
•Computers and Peripheral Equipment
•Networks - Links and Nodes
•Data Storage
•Electrical Power and Physical Infrastructure

Figure 1. An Operational Model of Information Operations

[27] Thomas, Like Adding Wings to the Tiger, http://call.army.mil/call/fmso/fmso/fmsopubs/issues/chinaiw.htm.

[28] Waltz, Information Warfare principles and operations, p.148-152 & 239-243.

debate how information aspects of conflict can be affected. The two lower tiers describe cyberspace and are more in line with conventional theories of IO that focus their effects on command, control and information systems. At this level it is possible to see the impact on the physical battle space through such battlefield systems as electronic attack and physical destruction of infrastructure. However, the highest tier addresses the aspect of understanding of the battle space through perception, reasoning and belief systems. It is this highest tier that is the true concern of KW. Within the KW paradigm, actions taken at the lower tiers of the model are only important with respect to the impact they have on the perceptual tier. The desired effect of these actions is to influence cognitive functions such as decision-making and planning but more importantly the decision-makers understanding of the situation which in turn affects everything else. Using the model it is possible to distinguish those effects that have an impact on understanding and classify them into three broad areas: precision, the ability to understand detail; tempo, the ability to understand quickly; and perception, the act of understanding in itself. This discussion will use these three broad areas of effect to discuss the KW requirement and the capability gap that Canada finds itself in.

Precision

> "Information Warfare – if it is to be meaningful at all – must ultimately impact upon other aspects of warfare. Information Warfare is not just about destroying enemy information; it is about making the friendly force move faster, shoot better and protect itself more economically. It is about slowing the enemy, disrupting his operations and demoralising him. It is about political penetration of a theatre of war."[29]

[29] Robert Leonhard, The New Principles of War for the Information Age, (Presidio Press (USA), 1998) p. 232-3.

As this quote from Robert Leonhard's book The New Principles of War for the Information Age indicates IO is more than attacking the enemy's information, it is about increasing the precision of our own force. Precision results from the ability to understand the detail of the environment, the first element of KW. In the time of Clausewitz, detail was very elusive and this elusiveness he expressed as "the fog of war".[30] However, modern sensor and communications technologies combined with the ability to fuse data in real-time has given the modern commander a much improved capability. The results from this level of mastery of information and information processes are the capabilities observed today where modern armed forces have extraordinary battle space awareness, information dissemination and precision weapons. Together, these technology applications offer the ability to know what is happening, what is important, where the points of maximum leverage are, and can connect all of this to an appropriate and accurate means to apply force, all on a vastly compressed time scale.[31] Such a KW enhancement clearly increases the ability to wage war; however it would be a mistake to believe it does anything more then reduce chance and uncertainty.[32] No system is perfect. The lesson to be taken is that "as relative ignorance which prevailed in warfare, especially since the 19th Century, begins to give place to knowledge, information and truth; the commander should and must replace mass warfare with precision warfare: the accurate allocation of combat power to achieve a specific purpose."[33] Precision

[30] Clausewitz, On War, p.84

[31] Ryan Henry and Edward Peartree, Military Theory and Information Warfare

permeates everything in a modern battlefield from sensing the enemy to delivering the weapon, from assembling the force structure to just-in-time sustainment.

Situational awareness is one of the key aspects of precision. Canada has placed a great deal of money, time and effort into projects to enhance battlefield awareness for naval, ground and air forces; however, there is almost no true cyber awareness beyond some firewalls and a regrettably undermanned Computer Incident Response Team that focuses more upon technology issues then it does on content.[34] An influence attack on our politicians, people or forces, conducted through cyber space may emanate from anywhere, have no national boundaries and causes confusion as to the identity of the originator. Furthermore, cyber space in general lacks appropriate intelligence and battlefield damage assessment (BDA) because of the rapidly changing nature of threats and the vulnerabilities arising from a complex and often chaotic information infrastructure.[35] Without an understanding, or awareness, of the approaches and cyber environment there is the distinct possibility of belligerent states or organizations delivering different information to allies or deliberately deceiving and dividing countries and coalitions by causing a schism between populations and decision-makers.

Another important feature of the cognitive aspects of precision is that of analysis and development. "Processes such as analysing national security issues, developing new technologies or equipment, and fielding the results of research that once took months or

[34] The author has 5 years recent experience in Canadian Forces Information Operations where CF and DND Information System Security was of central focus.

[35] Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, Strategic Information Warfare: A New Face of War, (US Army War College Quarterly, Autumn 1996) Http://carlisle-www.army.mil/usawc/Parameters/96autumn/molander.htm, p. 4-7.

years now can be completed literally in seconds."[36] With such precision capabilities and increasing open source information at the finger tips of an enemy, it is possible for him to close the technological and knowledge gap with the first world nations very quickly. If information age nations are to stay ahead of potential adversaries, they must be capable of analysing information quickly and provide solutions just as quickly; whether the requirement is for individual equipment, force structures, intelligence assessments or integrated logistics. The value of knowledge systems is the provision of customized solutions through fast prototyping and integrating research and development into procurement. In this way requirements can be filled quickly and more accurately because we would longer be forced to accept the mass-produced norm.[37]

Tempo

The second element, tempo, deals with the agility of mind not the precision with which one executes a manoeuvre or the velocity of a machine. This applies to the process by which a "superior information position is turned into a competitive advantage and is characterized by decisively altering initial conditions, developing of high rates of change, and locking in friendly success while locking out alternatives enemy strategies."[38] The key to this element of KW is understanding the situation faster than the enemy and then having the means to impact the battle space at a time, place and pace of

[36] Timothy L. Thomas, Deterring Information Warfare: A New Strategic Challenge, (US Army War College Quarterly, Winter 1996-7) Http://carlisle-www.army.mil/usawc/Parameters/96winter/thomas.htm, p. 7.

[37] Fast, Knowledge Strategies, p. 2.

[38] Vice Admiral Aurther K Ceborwski and John J. Garstka, Network-Centric Warfare: Its Origin and Future, (U.S. Naval Institute, 1997) http://www.usni.org?Proceedings/Articles98/PROcebrowski.htm, p.13.

the commander's choice.[39] This supposes that there is some agile manoeuvre force capable of reacting to such a superior understanding; therefore, this is an enhancement to battle space manoeuvre, not a replacement. In modern warfare, the speed at which information is collected, analysed, and more importantly understood drives the tempo of operations.

From the KW perspective, tempo relates to the speed at which one can deliver believable problems to the adversary while limiting the number being received. Where it is not possible to limit the adversary's attempts to deliver a problem the emphasis must be to limit his ability to make false ones believable.[40] To this end, the Canadian Armed Forces has begun investments into a number of intelligence, surveillance and reconnaissance (ISR) projects. Essentially, the purpose of these assets is to limit the enemy's ability to deceive and to provide the commander with warning of any real event. But how is this accomplished in the cyberspace or in the media? "Warning may be almost impossible to achieve since no one entity controls the whole of the information infrastructure and attacks can be made to look like normal system failures or problems."[41] In addition to the lack of indigenous indications and warning (I&W) there is no staff to devise contingency plans for a propaganda or psychological attack on the Canadian population or its soldiers.[42] It is quite possible that an attack on the communication

[39] Lawrence E. Casper, Irving L. Halter, Earl W. Powers, Paul j. Selva, Thomas W. Steffens and T. Lamar Willis, Knowledge-based Warfare: a Security Strategy for the Nest Century, (Joint Forces Quarterly (USA), Autumn 1996) p. 84.

[40] Pajk, Information or Knowledge Warfare? p. 9.

[41] Molander, Strategic Information Warfare, p. 4-7.

[42] The author has 5 years recent experience in Canadian Forces Information Operations where this was one of the major concerns and observations.

infrastructure combined with a powerful propaganda message could paralyse the Canadian government and her forces long enough to influence the outcome of any number of strategic, coalition, decisions. There is a need for some method of indication and warning of cyberspace and propaganda attack, combined with a contingency planning staff.

<u>Perception</u>

> "Knowledge, once absorbed into the mind almost ceases to exist separate from the individual; it is this total assimilation into the mind and life of a commander that yields genuine capability."[43]

Perception is the most elusive, and often forgotten, effect of KW because it is the most difficult to measure. The act of understanding encompasses the intellect, experience and state of mind of the decision-maker. The lesson to be taken from Clausewitz's quotation above is that if it is possible to intentionally influence the perceptions and, knowledge of a decision-maker, then it may be possible to get him to act predictably or to directly attack his orders and plans. There are three major factors that influence a combatant's actions in a conflict situation: the capacity to act, meaning the forces in relation to the opponents; the will to act, meaning the measure of resolve of the combatant; and finally the perception of the combatant, meaning the understanding of the situation or his ability to measure the first two factors accurately or timely.[44] The observation here is that by attacking the third factor it is possible to have an effect on the other two.

[43] Clauswitz, <u>On War,</u> p.147.

[44] Waltz, <u>Information Warfare: principles and operations</u>, p. 4-5.

Ideally, one would want to have clear intelligence on the decision maker's psychological profile and those of his trusted advisors and allies. With this in place, it would then be necessary to have a clear understanding of the information paths to the targeted decision-maker and which paths are trusted. However, even in less then ideal conditions, clear messages that are presented using a trusted means, which are consistent with reasonable explanations, can serve to influence or at least delay understanding. In this way it is possible to use the commander himself as a vulnerability. Furthermore, it has been shown that the presence of heightened threat, short timeframes and surprise causes stress on human beings that has the effect of reducing the span of attention, increasing cognitive rigidity and a fixation on short-term outcomes.[45] This is recognized by the military as shock or the fear that is generated from the sudden realization that the plan is falling apart, or that there is mortal danger nearby.[46] When such stress is placed on a targeted decision-maker and where there is a clear picture of how he assembles situational awareness it becomes possible to force the opponent into programmed behaviours and thus make him predictable. At this point the target will begin to initiate sub-optimal solutions to the problems that are presented to him. This is the essence of creating the operational dilemma as discussed earlier regarding combined and joint operations. The application of precision and increased tempo within the KW concept serves to inflict exactly the stresses required to affect the enemy cognitive state. The target has little choice but react to these stresses, yet, as he does he becomes more vulnerable to well-planned and co-ordinated attacks on his perceptions. Then, if it is

[45] Betty Glad ed., Psychological Dimensions of War, (Sage Publications, London (UK), 1990) p. 122-128.

[46] Leonhard, The Principles of War for the Information Age, p. 102-3.

possible to manage an opponent's perceptions through the media, direct manipulation of information, information blockade, deception, or synchronization of precision attacks then it is also possible to strip him of his will to fight before the actual military capacity is substantially eroded.[47] Such attacks can have the effect of moral dislocation where by the enemy strength is offset by through the defeat of his will.[48]

> "In the socio-political field, technology, in the forum of media communications and distribution, has had enormous impact upon open democracies such as Canada. War can now be projected into the living rooms of people thousands of miles away from the conflict and thus public opinion has far more influence on government will and its decision-making process within a democracy then in the past."[49]

Whether this propaganda is projected through the television, the internet or other forms of media, the Canadian population and its government are open to foreign influence where perception management will become a daunting task.[50] The possibility of such psychological attacks being ur can 25ign

Canada must come to the realization that “the media no longer simply reports military activity, but rather participates in it. Strategy, operational art, and tactics must now accommodate the presence and effects – both positive and deleterious – of media operations.”[52]

The cultural awareness programs and pre-deployment training that the Canadian Forces has put into place has been of great aid in defending our leaders and soldiers from such perception attacks. Yet, the impact of increased tempo and shock through psychological means such as terror attacks is another matter. The Canadian Army has had little in the way of collective training in high tempo operations over the past ten years and therefore an expanding vulnerability is emerging.[53] As tempo increases and rogue nations catch up to the information age methods of waging war, our combat troops will require effective collective training so that they become used to new tactics and their own situational awareness tools. Future leaders must train to deliver optimal decisions in high stress and highly complex situations.

By examining these three elements of the KW milieu it is evident that Canada has a number of troubling vulnerabilities. The predominant deficiencies are in awareness of both propaganda attacks and of their cyber delivery systems. The fact that the information medium is unconstrained by national boundaries, has extensive penetration into Canadian society, and has little in the way of regulatory constraints represents an alarming vulnerability. This is further exacerbated by the lack of appropriate intelligence, including I&W and BDA, and the lack of contingency planning staffs or

[52] Leonhard, The Principles of War for the Information Age, p. 24.

[53] BGen Kennedy and Col Appleton (briefing to CFC) 18 April 2002.

force structure to deal with psychological based attacks. As tempo increases and rogue nations catch up to the information age methods of waging war it will be necessary to invest in collective training that exercises new tactics and procedures. Combat leaders will have to become experts in their situational awareness tools be prepared to deliver optimal decisions in high stress and highly complex situations. Although Canadian doctrine includes the framework for dealing with such a threat it appears that the Canadian Forces has yet to fully realize that the perceptual tier of our operational model on KW is truly an operational military activity.

Summary

In the paper *Information War and the Air Force; Wave of the Future? Current Fad?* produced by the Rand Corporation the author states: "Information dominance is likely to be hard to define or measure, particularly in the complex military-political situations that seem to typify the post-Cold War era, and could well be very difficult to achieve in any meaningful way in many classes of conflict."[54] Although this is fundamentally true, and echoed in this paper, such statements must not be interpreted that because it is difficult to measure or war-game that it can be ignored. In truth we must reflect upon the theories of war discussed earlier in this paper and seize upon the idea that it is neither the information edge nor blind military power that is essential but it is the knowledge edge. This knowledge edge provides the basis for KW, which we have shown to be an extension to manoeuvre warfare theory and a subset of IO where focus is on

[54] Glen Buchan, Information War and the Air Force: Wave of the Future? Current Fad?, (Rand Corporation, 1996) http://www.rand.org/publications/IP/IP149, p. 4.

influencing the mind of the target decision-maker or perhaps a population. It has is also been suggested that KW can also be considered an asymmetrical attack, not because of some physical linearity issue, but because such an attack would be outside of what is expected by current training and practices.

KW or even dominance in the knowledge realm does not mean overwhelming superiority in fibre optics or bit counts, it means that we have access to the target's knowledge mechanism or we can at least disrupt or dislocate its functioning. Whether the targeted commander is a warlord, a head of state, or the leader of a global terrorist network they all have a tailored system designed to enhance their knowledge. The object of KW is to use the manoeuvrist methods of penetration, dislocation and disruption against the opponent's knowledge system and cause him to lose trust in it.

> "To be fully effective, appropriate offensive information warfare weapons, for example, should be added to the repertoires of all elements of forces concerned with the whole spectrum of offensive application of force, from psychological operations to tactical deception to the whole range of ground attack operations. Not only would such integration make using the weapons effectively much more likely, but also it would help place information warfare techniques and technologies in a more useful operational context. Similarly, the defensive side of information warfare needs to be infused into all the organizations responsible for developing, procuring, and operating information systems."[55]

Although the author of the above quote refers to Information Warfare and specifies information systems he has also hit upon the essence of KW. The lesson offered, and emphasized in this paper, is to have a wide range of military mutually supporting capabilities including those that can engage and protect within the command cognitive and trust system. From the examples sighted in this paper it is apparent that

[55] Buchan, Information War and the Air Force: Wave of the Future? Current Fad?, p.12.

Canada is indeed vulnerable to a number of KW affects, the most alarming being cyber situational awareness, intelligence and force structure. While it is possible to point to a number of issues within the Canadian Forces context, the real challenge will be to bring about timely change. Yet, the difficulty with transformation in the military is that to get prompt action it usually requires an over riding impetus whether this be a budget issue, recent debacle or a looming threat.[56]

[56] Paul K. Davis, David C. Gompert, Richard J. Hillestad, and Stuart Johnson, Transforming the Force, (Rand Corporation (USA), 1998) http://www.rand.org/publications/IP/IP179, p. 5.

Bibliography

Baumard, Philippe, PhD. From Info War to Knowledge Warfare: Preparing for the Paradigm Shift. Intelligence online, 2002, http://gcc.uni-paderborn.de/www/WI/WI2/WI2_LIT.NSF/fb8fb1b65f7e25e3412568ce0052e511/6dee8c20b2de65004125692e00693585/$FILE/baumard.htm.

Barnett, Thomas PM. The Seven deadly sins of Network-Centric Warfare. US Naval Institute Proceedings, 1999, http://www.nwc.navy.mil/dsd/7deadl~1.htm.

Bourque, Col JDR. Information Operations for Canada. CFC Papers and Publications: AMSC 1, 1998, http://wps.cfc.dnd.ca/papers/amsc1/003.html.

Buchan Glen. Information War and the Air Force: Wave of the Future? Current Fad?. Rand Corporation (USA), 1996, http://www.rand.org/publications/IP/IP149.

Burke, Martin. Information Superiority, Network Centric Warfare and the Knowledge Edge. Australian Defense Science and Technology Organization Electronics and Surveillance Research Laboratory, 2000.

Canadian Department of Army Doctrine, B-GL-300-001/FP-000 Conduct of Land Operations- Operational Level Doctrine for the Canadian Army. Government of Canada, 1998.

Canadian Department of Army Doctrine, B-GL-300-003/FP-000 Command. Government of Canada, 1996.

Casper, Lawrence E, Irving L. Halter, Earl W. Powers, Paul J. Selva, Thomas W. Steffens and T. Lamar Willis. Knowledge-based Warfare: a Security Strategy for the Nest Century. Joint Forces Quarterly (US), Autumn 1996.

Ceborwski, Vice Admiral Aurther K and John J. Garstka. Network-Centric Wa.826A12 0 0 12 221.56 2341 253.6203 Tm(4.33T/T 0 0 12 221.59.8Its Origin19

Davis, Paul K, David C. Gompert, Richard J. Hillestad, and Stuart Johnson. Transforming the Force. Rand Corporation (USA), 1998, http://www.rand.org/publications/IP/IP179.

Fast, Lieutenant Colonel WR. Knowledge Strategies: Balancing Ends, Ways, and Means in the Information Age. Institute for National Strategic Studies (USA), 1998, http://www.ndu.edu/inss/siws/Ch1.html.

Glad, Betty, ed. Psychological Dimensions of War. Sage Publications, London (UK), 1990.

Harley, Jeffery A. Information Technology, and the Centre of Gravity. Navy War College Review (USA), 1997, http://www.nwc.navy.mil/press/Review/1997/winter/art4wi97.htm.

Henry, Ryan and Edward Peartree. Military Theory and Information Warfare. US Army War College Quarterly, Autumn 1998, http://carlisle-www.army.mil/usawc/Parameters/98autumn/henfy.htm.

Kuehl, Dan. Defining Information Power. National Defence University Strategic Forum (USA), 1997, http://www.ndu.edu/inss/strforum/forum115.html.

Kuehl, Dan. Defining Information Power. National Defence University Strategic Forum (USA), 1997, http://www.ndu.edu/inss/strforum/forum105.html

Leonhard, Robert. The Art of Maneuver. Presidio Press, USA, 1991.

Leonhard, Robert. The Principles of War for the Information Age. Presidio Press (USA), 1998.

Mains, Major SJ. Adapting Doctrine to Knowledge-Based Warfare. Military Review (USA), March-April 1997, http://www-cgsc.army.mil/milrev/English/marapr97/mains.htm.

Metz, Steven and Douglas V. Johnson II. Asymmetry and U.S. Military Strategy: Definition, Background, and Strategic Concepts. Project on Defence Alternatives (USA), 2001, http://www.comw.org/rma/fulltext/asymmetric.html.

Molander, Roger C, Andrew S. Riddile, and Peter A. Wilson. Strategic Information Warfare: A New Face of War. US Army War

College Quarterly (USA), Autumn 1996, Http://carlisle-www.army.mil/usawc/Parameters/96autumn/molander.htm

Oxford English Dictionary Second Edition Volume 3, Oxford (UK): Clarendon Press, 1989.

Pajk, Josip. Information or Knowledge Warfare?. 1997, http://members.tripod.com/~THREENITY/Infwar.htm

Reith,BGen JG. An Alternative Approach to Defence. Canadian Forces College Press: Toronto, LFS/LFO/523/LD-3, 2002.

Sun Tzu. The Art of War. Trans. Samuel B. Griffith. New York, USA: Oxford University Press, 1971.

Thomas, Timothy L. Deterring Information Warfare: A New Strategic Challenge. US Army War College Quarterly – Winter 1996-7, Http://carlisle-www.army.mil/usawc/Parameters/96winter/thomas.htm .

Thomas, Timothy L. Like Adding Wings to the Tiger: Chinese Information War Theory and Practice. Foreign Military Office (USA), 12 June 2000, http://call.army.mil/call/fmso/fmso/fmsopubs/issues/chinaiw.htm.

Toffler, Alvin and Heidi. War and Anti-War. Little and Brown Co., Boston (USA), 1993.

Waltz, Edward. Information Warfare: principles and operations. Artech House, Norwood (USA), 1998.

Van Riper, Paul and Robert H. Scales Jr. Preparing for War in the 21st Century. US Army War College Quarterly (USA), Autumn 1996, http://carlisle-www.army.mil/usawc/Parameters/97autumn/scales.htm.