CANADIAN FORCES COLLEGE /COLLÈGE DES FORCES CANADIENNES

ADVANCED MILITARY STUDIES COURSE 2

NOVEMBER 1999

CANADIAN FORCES INFORMATION OPERATIONS:

A NEWBORN CONCEPT IN DANGER OF DISINTEGRATION

By/par **By Lieutenant-Colonel JAG Champagne**

This paper was written by a student attending the Canadian Forces College in fulfilment of one of the communication skills requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions which 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.

"CANADIAN FORCES INFORMATION OPERATIONS: A NEWBORN CONCEPT IN DANGER OF DISINTEGRATION"

> *"War is an act of force to compel our enemy to do our will"*
>
> *Clausewitz*
>
> *" For to win a hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill"*
>
> *Sun Tzus: the Art of War*

INFORMATION OPERATIONS EVOLUTION

The struggle to dominate the adversary on the battlefield in terms of information and knowledge can be traced as far back as Sun Tzus theories 25 centuries ago. The Gulf War dramatically increased, however, its relevance to warfighting in the 1990s. The introduction technology such as the US Airborne Warning and Control System (AWACs) and E-8 Joint Target attack Radar System (JSTAR) aircraft technologies, provided commanders with capabilities to improve the accuracy of the information, tighten the decision cycles and accelerate the operational tempo.[1]

In its attempt to benefit from their Gulf War, the United States Joint Chiefs of Staff, in March 1993, established the guidelines for command and control warfare (C2W)[2]. This concept was designed to integrate the three traditional elements of warfare, psychological warfare (PSYOPS), Operational Security (OPSEC) and deception, with electronic warfare (EW) and physical destruction of vital command and control nodes. Using C2W activities as a building block, the U.S. developed the Information Warfare (IW) concept,[3] in 1992, to exploit the expansion of the information

[1] Edward Mann. Col USAF. *Desert Storm: the First Information War ?*. http://www.airpower.maxwell.af.mil/airchronicles/apj/apj94/man1.html. Forecast International/DMS Special Project. *Conduct and Lessons of the Persian Gulf War*. Vol III, Part B. Forecast International/DMS Special Project. P. 37

[2] Command and Control Warfare (C2W) attacks adversary command and control targets while defending the friendly command and control target set.

[3] Information Warfare (IW) is defined as information operations conducting during time of crisis or conflict to achieve specific objectives over a specific adversary or adversaries.

environment for the purpose of military offensive and defensive actions. The aim of this new concept was the achievement of information dominance over its adversary. The emergence of~~ the~~ cyberspace[4] technology resulted in an overarching concept of strategic information operations[5] (IO), in December 1996. As indicated by Dr. Dan Kuehl, this latest concept recognises the span of the conflict spectrum from peace to war and the involvement of the national government.[6]

As one of its close allies, the Canadian Forces (CF) followed in its footstep the US IO evolution. In 1997, the CF had a core-staff to co-ordinate IO policy and operations, a battlelab, an expanded electronic warfare (EW) capabilities, and modernised signal intelligence (SIGINT) equipment and capabilities. Colonel Joe Stevens, then commander of the Supplementary Radio System, highlighted that the CF did not have the capacity nor the mandate to go beyond the defensive capabilities.

The emerging technology combined with the Revolution in Military Affairs (RMA) and the need to keep pace with Canada's allies contributed, in 1998, to a refocus on a more global concept including the integration of defensive and offensive information operations. In parallel, the senior leadership created the strategic framework to shape the CF future with the promulgation of its Strategy 2020 and the Defence Planning Guidance 2000 released in June 1999. These three documents should provide the strategic focus to face the challenges of the information environment in the 21st century.

This essay contends, however, that the new strategic environment, information revolution and the human dimension will necessitate a review of the latest doctrine and, specifically, its application

[4] ~~Dr.~~ Daniel T. Kuehl describes the cyberspace as that place where computers, communication systems, and other devices that operate via radiated energy in the electromagnetic spectrum meet and interact.

[5] DOD Directive 3600.1, dated 9 December 1996, defined the IO concept as military and governmental operations that protect and exploit the information environment to attain strategic objectives.

[6] Daniel T. Kuehl. *Defining Information Power*. National Defense University Strategic Forum. Institute for National Strategic Studies. Number 115. June 1997. http://www.ndu.edu/inss/strforum/forum115.html

on a single battlespace at the operational level. In particular, the new IO paradigm at the operational level across the spectrum of conflict will require an asymmetrical response.

The thesis of this essay proposes that the Canadian Forces is implementing too hastily the concept of IO with the possible consequence of depriving the~~his~~ operational commander from achieving information superiority on the battlespace of the 21st century. This lack of understanding of the complexity of IO may result in the disintegration of this newborn concept.

This discussion will start with the definition of concepts and terms to provide the operational framework for IO. The following portion will provide the symmetrical CF response to IO challenges by discussing the current doctrine and the CF evaluation of its strategic environment for 2020. It will then address the asymmetrical challenges of the future battlespace by addressing the information revolution and the human dimension factors.

CONCEPTS

To fully comprehend the complexity of IO, there must be an understanding of key concepts and terms related to IO. In particular, the concepts of information environment, battlespace and information superiority will be examined to provide the operational framework.

The information age globalized the information environment. The global information infrastructure (GII) comprises open and interconnected information systems and networks. In addition to the GII, the subordinate Canadian National Information Infrastructure (NII) and the Defence Information Infrastructure (DII) interdependence allow the full exploitation of this global flow of information.[7] For instance, ~~the ~~military communications rely at 95% on national information

ee

[7] Depart Nart

infrastructures[8]. This interconnectivity between each level of infrastructure permits information operations to evolve in an unlimited information environment, but it also increases our dependence and vulnerabilities.

This possibility to operate within a GII impacts on the operational commander's area of interest and influence. It implies the use of spatial and temporal aspects of operating environment. This fourth-dimensional notion has changed the battlefield to a battlespace. This battlespace allows commanders to operate on the physical and moral planes. At the operational level, the traditional linear battlefield no longer binds commanders. They should be capable to operate from a multidimensional perspective.[9] In short, operational commanders are limited only by their abilities~~y~~ to exploit the information environment to control the battlespace.

As introduced earlier, military forces exploited the notions of information environment and battlespace with the evolution from C2W to information operations (IO). The United States defines IO as actions taken to affect adversary information and information systems while defending one's own information and information systems[10]. In order to limit the discussion on the definition of IO, this essay will use the official definition of the CF:

> "Actions taken in support of political and military objectives which influence decision makers by affecting adversary information while exploiting and protecting one's own information."[11]

[8] Douglas H. Dearth. *Imperatives of Information Operations and Information Warfare*. Ed. By Campen, A.D. and Dearth D.H Cyberwar 2.0: Myths, Mysteries and Reality. AFCEA International Press, Fairfax, Virginia. 1998~~.~~.p. 392

[9] Directorate Land Strategic Concepts (DLSC). *The Future Security Environment*. Report Number 99-2. Kingston, Ont., 1999.p. 59.

[10] United States, Department of Defense~~OD~~. *Joint Doctrine for Information Operations*. Joint Pub 3-13. Washington, DC: DOD, 1998. http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf. p. I-1

[11] This definition is also included in the Defence Administration Orders and Directives (DAOD 8010-0 and Deputy Chief of the Defence Staff (DCDS) Policy Directives). The stated definition was taken from Department of National Defence, B-GG-005-004/AF-033 *Canadian Forces Information Operations* (Ottawa: 1998-04-02). Chapter I p. 3 of 18.

In comparison to the US version, the Canadian definition is not limited to military objectives and targets the decision maker. This concept is important to understand the notion of information superiority. As the ultimate aim for IO, information superiority is defined in the US and Canadian doctrine as: "the capability to acquire, exploit, and disseminate an uninterrupted flow of information while denying an adversary's ability to do the same at a time and place of his own choosing".[12] This essay will address the feasibility of superiority throughout this following discussion.

DOCTRINE

These concepts are particularly important in reviewing the IO doctrine at the operational level. The CF adopted hastily the US doctrine for IO to reach rapidly an acceptable level of interoperability and operational readiness. This approach required a certain level of risks and the acceptance of the U.S. precepts for IO. While this hasty "canadianized" version reflects the right components, the implementation of it will be a bigger challenge than anticipated by the CF. Based solely on capabilities, this essay contends that the CF should not aim for the same level of U.S. involvement~~might not be able to keep apace with the US in every aspect, but we still need an interoperable doctrine~~. Canadian operational commanders must understand, however, this doctrine to fully exploit IO resources available in any theatre of operations. At this stage, this essay will review the evolution of the Canadian doctrine.

The CF approach to warfighting evolved in a number of areas. The new CF operational objectives are aimed at defeating the adversary by shattering his moral and physical cohesion, and its ability to coordinate his actions, rather than by destroying him physically through incremental attrition. More specifically, the actions can be directed to the adversary's moral components: willpower, ability to maneuver, morale, and command and control ability. Conflicts can be

[12] DND, B-GG-005-004/AF-033 *Canadian Forces Information Operations*. Chapter I, p. 10 of 18; and US, DOD. *Joint Doctrine for Information Operations*. Joint Pub 3-13. 1998. http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf. p. I-11.

conducted on a physical plane with maneuver and firepower, and/or the moral plane, which is psychological.[13]

This evolution of doctrine to exploit the information environment will favor the forces with a wide range of capabilities. The focus on information operations will enhance the combat power of operational commanders. As expressed by Dearth, commanders will have the ability to fight "the battle chosen" rather than fighting "the battle confronted". More importantly, it introduces the concept of effect-based attack where commanders will select between inflicting lethality and achieving effectiveness. The improved intelligence and situational awareness should make the battlespace more transparent and reducing, not eliminating, the uncertainty. We must engage in shaping and managing perceptions that effect the battlespace.[14] While IO can be easily related to the moral plane, it is also used on the physical plane. A quick review of the activities involved~~s~~ in IO will indicate the wide range of response or its asymmetry.

In order to maximize its chances to achieve information superiority, commanders should use an integrated approach consisting of offensive and defensive information operations[15]. The offensive capabilities include psychological operations (PSYOP), deception, electronic warfare (EW), intelligence, computer network attack (CNA), physical destruction, and special information operations (SIO). Defensive capabilities comprise intelligence, counter-deception, counter-psychological, public affairs (PA), counter-intelligence (CI), operation security (OPSEC) and offensive counter-IO.[16] Counter-propaganda could also be included in defensive IO. This essay will

[13] DND, B-GG-300-001/FP-*000 Conduct of Land Operations – Operational Level Doctrine for the Canadiaqn Army*. Ottawa. 1998.~~AF-033 *Conduct of Land Operations* (Ottawa:)~~ Chapters 1 and 2.

[14] Dearth D.H. *Imperatives of Information Operations and Information Warfare*. p. 396

[15] Offensive IO includes actions to influence actual or potential adversarial decision makers; while defensive IO are actions to ensure friendly decision makers have access to information and protected from adversary offensive IO efforts.

[16] DND, B-GG-005-004/AF-033 *Canadian Forces Information Operations*. Chapters 2 and 3.

provide current examples in the following paragraph. It is important to realize that this range of options can be applied throughout the spectrum of conflicts, which comprises peacetime, crisis and war operations.

The current doctrine clearly identifies different types of targets for IO. They include leadership target, civil infrastructure, military infrastructure and weapons systems. In particular, command and control infrastructure~~, which~~ could be military or commercial.[17] The selection of the targets will be discussed further in addressing the human dimension to IO.

STRATEGIC ENVIRONMENT

To support this doctrine, the CF needs to ensure that operational commanders have the required strategic support to benefit from IO. The primary responsibility of the senior leadership is to define the strategic environment. For the purpose of this essay, we will review the CF strategic environment as evaluated in the newly promulgated Defence Strategy 2020 and Defence Planning Guidance (DPG) 2000.

Those documents identify that the military responses to the information age challenges of the 21st century involve the Revolution in Military Affairs (RMA). The Canadian RMA concept[18] proposes that the premise for successful response to the challenges of the information age is a thorough review process to consider technology, doctrine and organization.[19] This essay contends that the same logic can be applied to information operations, but should also include specific mention of the human dimension.

[17] DND, B-GG-005-004/AF-033 *Canadian Forces Information Operations*. Chapter I, p. 14 to 15 of 18

[18] The National Defence RMA Concept Paper state: ***an RMA is a major change in the nature of warfare brought about by the innovative application of new technologies which, combined with dramatic changes in military doctrine and operational and organizational concepts, fundamentally alters the character and conduct of military operations***. NDHQ RMA Operational Working Group. *Canadian Defence Beyond 2010, the way ahead: An RMA Concept Paper*. NDHQ, Ottawa, 31 May 1999. P. 3/42. It should be remembered that this term was inspired by the Soviet " Military-Technical Revolution", which the U.S. found too restrictive.

This RMA process is already underway with the principal allies of Canada. The U.S. intends to emerge from this review with a flatter structure, a more flexible command and control system; more precise and lethal power projection systems; and, progressive doctrine. Britain's way ahead will support capabilities to power projection with its Joint Rapid Reaction Force, and multinational operations in a joint environment. France focuses on interoperability among its allies and the creation of a Joint Command able to take command of French and Allied forces. A common trend is the focus on improving intelligence, surveillance and reconnaissance capabilities.[20]

Canada intends to create a high-quality, combat-capable, interoperable and rapidly deployable task-tailored force and to exploit leading-edge doctrine and technology. It ~~This revolution objectives also~~ involves bilateral and multilateral operations with Canada's allies; the assistance to other government department and levels; and the provision of support to broad federal government programs.[21] Pertinent to IO, DPG 2000 directs a refocus of research and development in the areas of space, remote sensing, telecommunication and information management. The CF will also stand up a permanent Joint Force Headquarters and a Computer Incident Response Team. Other initiatives not covered in DPG 2000 are research efforts on establishing battlespace damage assessments to provide the feedback mechanism to the operational commander on the effectiveness of IO. These strategic documents indicate concerns with decision-making processes, information management, and computer network attack (CNA) capacities. These capabilities are focused on technology and required the appropriate financial support.

[19] NDHQ RMA Operational Working Group. P. 3/42.

[20] Ibid.~~NDHQ RMA Operational Working Group.~~ P. 4-5/42

[21] The Strategy 2020 has the following vision statement: "The Defence Team will generate, employ and sustain high-quality, combat-capable, inter-operable and rapidly deployable task-tailored forces. We will exploit leading-edge doctrine and technologies to accomplish our domestic and international roles in the battlespace of the 21st century and be recognized, both at home and abroad, as an innovative, relevant knowledge-based institution. With transformational leadership and coherent management, we will build upon our proud heritage in pursuit of clear strategic objectives". DND. *From Strategy to Results*. Defence Strategy 2020, Ottawa. P. 1 of 5. http://www.vcds.dnd.ca/cds/strategy2K/s2k01_e.asp.

Canada is a wealthy country with the world's seventh largest Gross Domestic Product (GDP). It has, however, the second largest national debt (fifth largest per capita) and both levels of government's objectives include primarily its reduction. From the Defence perspective, Canada is 56th in Defence manpower, 133rd in Defence spending and 112th as a percentage of population in the military. Many of Canada's allies believe that Canadians can afford to assume a greater share in the burden of collective security.[22] The DPG 2000 outlines the adaptation process to respond to those challenges, and reminds us the importance to keep pace with our allies in technology and doctrine [23].

While we could argue with the anticipation of the required Defence budget, the Defence must continue to keep pace with new military concepts, doctrine and technological changes with innovative and progressive concepts.[24] This essay suggests that the harsh realities of the possible impact of IO has to be understood by all levels of the Canadian leadership, as a government-wide strategy and not only a Department of National Defence (DND) one. As indicated by the Canadian Security Intelligence Service (CSIS),[25] we just need to imagine if the 1998 ice storm in southern Ontario and Quebec had been caused by a major cyber attack on our power grid! The current budgetary planning indicates no increase in the CF budget. The CF response to the RMA challenges and new strategic environment should involve an asymmetrical response and not only rely on keeping pace with high-priced technology.

[22] DLSC Report 99-2. P. 18-22. These numbers were obtained from Statistic Canada.

[23] DND~~epartment of National Defence~~. *Defence Planning Guidance 2000*. Ottawa. http://www.vcds.dnd.ca/vcds/dgsp/dpg/intro_e.asp.

[24] DND. *Stakeholder Analysis*. Defence Strategy 2020, Ottawa. P. 1 of 1. http://www.vcds.dnd.ca/cds/strategy2K/s2k01_e.asp.

[25] Canadian Security Intelligence Service (CSIS) advises the Government on threats to Canadian national security.

THREATS

Before we expand on the question of technology, we need to look at the potential threat to Canada's national security and objectives. Due to the nature of IO, the threat will be evaluated from strategic and operational perspectives.

T~~he CF t~~o evaluate the possible threats over the next two decades, the CF sponsored a number of studies. In addition to the current ethnic unrest, religious extremism and resource disputes, the emerging threats involve threat to nation-state by globalization, non-state actors, non-governmental organizations and global corporations.[26]. The NATO LO2020 report indicates that the fundamental character of war will still include contest of wills involving death, terror, bloodshed, destruction and human suffering. This report identifies also the emergence of non-state center of power[27].

The advanced military technology now proliferates widely among states and non-state actors. The emerging technology will result in potential asymmetrical attacks[28], which will see opponents win against a physically stronger adversary by avoiding strength and exploiting vulnerabilities. Those threats will come from not only nation-state (global and regional), but rogue countries and non-state actors. The CSIS 1998 Public Report identified the increased Canadian dependence on technology and resulting vulnerabilities, and also the new trend with foreign governments, terrorists group and political motivated extremists, exploiting those vulnerabilities by engaging in IO to pursue traditional activities.

[26] DND. *Emerging Strategic Environment*. Defence Strategy 2020, Ottawa. P. 1 of 1. http://www.vcds.dnd.ca/cds/strategy2K/s2k01_e.asp.

[27] NATO LO2020 Report. *Nature of the Battlespace in 2020*. Document from~~part of the~~ DLSC Report 99-2 . P. 57-58.

[28] DPG 2000 defines asymmetrical threats as an attempt by an opposing party to avoid traditional strengths of our existing military force by employing unexpected or unusual techniques to gain an advantage. It includes the use of Weapon of Mass Destruction, cyber-warfare, or choosing to fight only in complex terrain. For the purpose of this essay, we will use asymmetrical threats in the context of cyber-warfare.

In this CSIS report~~As an example~~, Louis J. Freech, Director of the U.S. Federal Bureau of Investigation, characterized Canada as a "hacker haven" because of the sophisticated information technology system and open society. Groups involved in cyber-attack including a group that shut down a communications satellite operated by the People's Republic of China, are based in Canada using the highly sophisticated and international information technology systems to mount actions abroad.[29] While these examples from CSIS may seem as purely criminal acts, we could argue that this type of cyber-threat is a direct attack to our national security; hence, the need to realize that it is a government-wide problem including the CF. While the CF is not responsible to protect these infrastructures, the military needs to address those threats due to its convergence and interdependence on national information infrastructure.

Another perspective on the future threats is the different perceptions, values and motivation about the Laws of Armed Conflict and humanity of the potential adversary. The reports indicate that they will not hesitate to exploit the fears and beliefs of our population and undermine the political support for our government or its actions. These objectives can be achieved by the exploitation of our sensitivities to casualties, disrupting our complex economies and threatening~~ of~~ our desire for legitimacy.[30]

It could be proposed that these types of threats are shared in the western hemisphere. A quick review of the Russian perspective on IO indicates similar concerns of potential asymmetrical threats. In their view, IO must lie at the heart of any nation's military reform and modernization effort for the 21st century. In particular, Russian believes that IO assets require the same level of protection as for nuclear weapons. They are also concerned with the elimination of global power parity and the difficulty to identify the initial period of war. Due to the lack of physical damage or loss of life, they

[29] CSIS~~anadian Security Intelligence Service~~. *Information Operations (The Cyber Threat)*. CSIS 1998 Public Report. 1999. http://www.csis-scrs.gc.ca/eng/publicrp/pub1998e.html.

[30] DLSC Report 99-2 *The Future Security Environment*. Kingston, Canada. 1999. P. 13.

also propose that IO may become more acceptable. Russians theorists call for the creation of an information deterrence concept, similar to the nuclear one, to alleviate the risks among nations of attacks on C4I systems, the use of computer viruses, and ability to affect the psyche of another nation through information technology.[31]

This review of the threats reveals a number of issues. First, the nature of the threat will more than likely be asymmetrical. Second, the adversary will vary from nation-state to non-state actors. Finally, the threat could include high technology and exploitation of traditional activities such as PSYOPS. The possible lethal response to offensive IO also forces leaders to consider the desired effect, the acceptable risk level and the perception of the intent.

TECHNOLOGY

In response to those potential asymmetrical threats and the future operational requirements, the CF studied a number of technological options. A DND study on the challenges and opportunities posed by emerging technology, concluded that the information revolution would be characterized by fast pace development, global impact, society-wide, no limit on pace and direction of the revolution.[32] A US Department of Defense study indicated that technology would see the current battlefield evolve to nonlinear and simultaneous operations; rapid decisive operations to disintegrate adversary; and joint forces capable of precision operations and information dominance[33]. DPG 2000 priorities include the improvement of our command and control systems, the development systems to facilitate decision-making process, and the improvements to EW and computer attack networks assets.

[31] Thimothy L. Thomas~~ T.L~~. *The Threat of Information Operations: A Russian Perspective*. Ed. By Pfaltzgraff R. Jr, and Shultz, R.H. Jr. War in the Information Age: New Challenges for U.S. Security Policy.International security Studies Program. The Fletcher School of Law and Diplomacy, Tufts University. 1997. P. 70 to 75.

[32] John Leggat and Moen Ingar. Challenges and opportunities posed by emerging technology : a Defence Management Committee discussion paper. Ottawa : Defence Management Committee, Dept. of National Defence, 1999. P. 5-7/9.

[33] US DOD. *Knowledge and Speed: The Annual Report on the Army After Next Project*. Jul 1997. Extract of document from DLSC Report Number 99-2. P. 24

While we focus on technologies to support the decision making process, new technologies are on the horizon, which will focus on the defense of friendly and targeting adversary data-processing capabilities of the body or *psychotronic* weapons. These weapons aim to control or alter the psyche, or to attack the various sensory and data processing systems of the human organism. According to Russian Dr. Victor Solntsev, behavior modification could be one objective while another could be to upset the individual mental capacity. Russian Major I. Chernishev indicated a number of categories of psychotronic weapons such as nervous system generator to paralyze the central nervous system; ultrasound emanations capable of carrying out bloodless internal operations; noiseless cassettes to affect the subconscious; and psychotropics to induce a trance, euphoria or depression. As stated by Timothy Thomas, psychtropics weapons may bring home the fact that our current efforts to focus on the data-processing elements of systems and computers lead us to forget about the human factor, but we need to protect the human in our data management structure.[34]

Ryan Henry and Edward Peartree remind us that artillery was supposed to supplant all other tools of wart, but five hundred years later, artillery still plays a subordinate role in combat operations[35]. As history has shown, we must be cautious with our expectations from the capacities of future technology. We must be cognizant of the measure/counter-measure cycle, the effectiveness of asymmetric response to high-technology and the achievement of the technology[36]. Dr. Charles Dunlap provides another aspect by advancing that the rapidly declining costs of emerging technologies might empower the less developed countries and level the battlespace. It may prevent the achievement of superiority, much less dominance, by current global power. We may be forced to

[34] Thomas~~, Timothy L~~. "The mind has no firewall."~~ Parameters. 28 no. 1 (Spring 1998): 84-92.~~ http://carlisle-www.army.mil/usawc/Parameters/98spring/thomas.html.

[35] Ryan Henry and Edward Peartree. *Military Theory and Information Warfare*. Parameters Journal of the US Army War College. Carlisle. Autumn 1998. Vol 28 Issue 3.

[36] DLSC Report 99-2. P. 25.

operate with information transparency or information parity.[37] Commanders claim that IFOR and SFOR achieved information dominance in Bosnia. The lessons learned are not completed yet on the Kosovo campaign, one could wonder if NATO forces will claim information dominance or superiority. Certain nation-state and non-state actors with this new or old information technology could challenge the concept of superiority. As we have witnessed in Somalia, Haiti and Bosnia, some opponents are adept of deception and psychological campaigns designed to hamstring the political and military effectiveness. It reinforces the point that the impact of technology can be reduced by an asymmetrical response. It is feasible at this time to entertain that a response to this asymmetrical threat would be an asymmetrical response including the exploitation of technology and the human dimension.

IO COMPONENTS

The review of the threat, strategic environment and technology reveal that we must look at an asymmetrical response to the asymmetrical threat and technological challenges. I wish to use some recent examples to support the IO components designed to shape the environments at the operational level.

One misconception that requires clarification in our doctrine is the difference between deception and psychological warfare (PSYOP). Deception is defined as the measures to mislead the adversary by manipulation, distortion or falsification of evidence to induce him to react in a manner prejudicial to his interests. PSYOP as actions to convey selected information and indicators to foreign audiences. The Canadian doctrine must indicate that PSYOP projects the truth and may support the deception plan. Colonel Joe Steven mentioned in 1997 that the Canadian Forces could not mention the use of PSYOP eventhough Major-General Dallaire requested for its operations in Rwanda in 1994. The success story of IFOR and SFOR should alleviate some of those fears by the senior

[37] Charles J. Dunlap. *21st century land warfare: Four Dangerous Myths*. Parameters: Journal of the US Army War College. Carlisle. 1997. P. 27-37

leadership in Canada and the population. PSYOP was used successfully as force protection. It was also instrumental in the achieving of the information campaign and the establishment of the force credibility[38]. Recent discussions on Operation Abacus indicates the same concerns due to nation's political sensitivities, cultural differences and lack of support for this type of activities. The Canadian Forces needs to promote the importance of this capability and develop it.

During the Gulf WAR, the coalition operation security (OPSEC) and deception campaigns were aimed at convincing Saddam Hussein of a coalition main offensive using ground and amphibious attacks into central Kuwait. The deception activities would create false indicators and OPSEC would alter or hide the real indicators.[39] We know today that this defensive information operation was successful.

Our recent experiences with the media certainly support the decision to include PA officers at every level of command to advise our commanders. This capacity of IO is certainly the most important one in this information age. One of the lessons learned by IFOR/SFOR in Bosnia is the critical role of PA in determining the success or failure of a mission[40]. IO are about perceptions and, on those missions, perceptions are as important as reality. An excellent PA plan will enhance an operational commander's objectives.

Another important aspect to consider in the CF doctrine is the application of IO in a coalition environment. The difference in technological advances among partner requires us to consider the

[38] Combelles-Siegel P. *Target Bosnia: Integrating Information Activities in Peace Operations*. Washington, DC: National Defence University Press, 1998. P. 82 and 159.

[39] US, DOD. *Joint Doctrine for Information Operations*. Joint Pub 3-13. Washington, DC: DOD, 1998. http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf. p. II-3.

[40] Combelles-Siegel P. P. 159.

technological asymmetries within a coalition such as different degree of reliance, utilization in different forms or for different purposes.[41]

Numerous examples exist to demonstrate the difficulty to conduct IO within a coalition. During the operations by IFOR/SFOR in Bosnia, PSYOP forces were not welcomed by every contingent. Due to previous experiences with their own PSYOP forces on previous deployment, the French forces were reluctant to employ U.S. PSYOP units and use them for liaison. The UK, however, recognized early the importance of the PSYOP teams.[42] During the recent Kosovo campaign, the U.S did not share all of the intelligence and targeting information with its allies, which included its closest one, the U.K.[43].

Operational commanders need to understand the complexity of IO within a coalition. Not all contingents will employ those resources the same way or understand the capability at their disposal. We need to develop this expertise to employ efficiently every aspect of IO and better coordinate the efforts within a coalition. We also need to increase our credibility with our allies to be able to use more extensively the IO resources of all members of the coalition. In other words, we need to reach the level of equal partner in the field of IO.

ORGANIZATION

The Canadian Forces need to deal with the restructure caused by the flow of information, which may pose potentially powerful inter-hierarchy conflicts over defining turf. Michael Vlahos proposes that commanders are not assured of ~~the~~ control with the complexity of the interacting forces

[41] S. Metz~~S~~. *The Effect of Technological Asymmetric on Coalition Operations*. Ed. By Marshall T., Kaiser P., Kessmeir. Problems and Solutions in Future Coalition Operations. Strategic Studies Institute, Carlisle. 1997. P. 51 and 56.

[42] S. Collins~~S~~. *Army PSYOP in Bosnia: Capabilities and Constraints*. Parameters. 29 no. 2 (Summer 1999): 57-73 http://carlisle-www.army.mil/usawc/Parameters/99summer/collins.htm. ~~, and~~ Combelles-Siegel. ~~P.~~ p. 82.

[43] Michael Inatieff. *The Virtual Commander: How NATO invented a new kind of war*. Annals of diplomacy CORBIS/SYGMA. P. 34

and the evolving target-set. He recommends the de-layering of command hierarchies, the leveling of authorities and the distilling and thinning of decision-elements.[44] These factors affect both the overall requirements to restructure the CF and the complexity of command and control with IO. Any restructure to support IO will require jointness and integrated approaches. Military leaders will need to forego parochialism and integrate air-sea-land-space-special operations assets to supportt a common IO plan.

At the strategic level, the CF participates to the Interdepartmental IO Working Group (IIOWG) under the chairmanship of the Communications Security Establishment (CSE) and the Royal Canadian Mounted Police (RCMP). The IIOWG share information related to threats to networks.[45] DPG has now directed the creation of a computer incident response team. It would be important to note that there are no common bodies to coordinate the national efforts to deal with the complexity of information operations at the strategic level.

In addition to the creation of the IO Group (IOG) as part of the joint staff at our National headquarters, this essay proposes that there is also a requirement to create, at the national level, an operation cell responsible specifically to further develop IO strategies. This organization would be responsible to raise the awareness of IO, increase our involvement with other government agencies and continue the development of IO doctrine. Operation Abacus, the year 2000 domestic operation, might the required catalyst to force major changes and initiatives in the field of IO.

From the conduct of information operations perspective, we need to exploit the capability offered in such discipline as PSYOP and SIO. While the reluctance is understood to invest in those traditional fields, we can not afford to rely only on the technology. We should not ~~either~~ expect that

[44] Michael Vlahos. *The Emergence of the Infosphere and its impact on Military Operations*. Ed. By Campen, A.D. and Dearth D.H Cyberwar 2.0: Myths, Mysteries and Reality. AFCEA International Press, Fairfax, Virginia. 1998. P. 83-87.

[45] CSIS 1998 Public Report. 1999. http://www.csis-scrs.gc.ca/eng/publicrp/pub1998e.html.

ad hoc PSYOP element~~unit~~s used in recent missions, will fulfill this need. The CF should create an embryo of experts in those specialized fields to deploy on current and future missions to support our operational commanders. Units such as the Joint Task Force II could certainly help with most components used in IO, but they have limited resources.

In this information age, military forces could reorganize with the reduction of the traditional pyramid with small units reporting up to progressively smaller numbers of larger organizations. Cohen suggests, however, that the structure change will be the last manifestation of RMA and will be the most difficult one to implement.[46]

HUMAN DIMENSION

Up to this point, this essay described the efforts by DND and the CF to set the conditions for successful IO in a single integrated battlespace of the 21st century at the operational level. The execution of IO is, however, subject to other factors, which must be taken in consideration by operational commanders. Commanders should recognize that the human dimension affects greatly information operations.

DEMOGRAPHY

The Canadian demography should be a concern at the strategic level, but the nature of IO makes it an issue also at the operational level. This is particularly true with domestic operations such as operation Abacus. Canada continues to evolve as a multi-racial and multi-cultural society. Diversity will have an increasing effect on our domestic outlook and foreign policy. We need to consider the people's intentions, motivations and aspirations in a variety of fields such as military, diplomatic, financial, corporate and academic.[47] For instance, immigrants may focus national

[46] Eliot A. Cohen . *A Revolution in Warfare*. Foreign Affairs New York, Mar/Apr 1996. P. 6 of 10

[47] Dearth. p. 397-398

attention on regional conflicts, including ethnic clashes and international human rights abuses.[48] The recent deployments made Canadian leaders notice the importance of such support. We continuously face protest for actions taken overseas. The coordinated representation by the Serb community, during the national televised debate on the participation of Canadian troops to Kosovo, provided a good insight on Canadian demography. The government reacted to a certain degree to the results of this debate. One could imagine the results if a similar debate had developed in concert with coordinated deception and psychological activities designed to hamstring the political and military effectiveness.

Opponents with different moral, political and cultural values, will not hesitate to manipulate the media. For example, we witnessed the effects on the international community when Somalis dragged the body of a US serviceman through the streets of Mogadishu, the civilian hostages at a Russian hospital taken by Chechens or the Serbs who chained UN personnel to potential targets. The media could become the poor man's intelligence service. Future adversaries could wage horrific actions to offset and divert high-tech forces. The quote by James F. Dunnigan summarizes this concern: " If the opponents are bloody-minded enough, they will always exploit the humanitarian attitudes of their adversaries".[49] We need to put in place the mechanisms to gain and maintain the Canadian society support and political will. These examples bring forward the challenges for operational commanders in developing IO plans abroad and at home.

LEGAL

In today's environment, operational commanders must consider continuously the legal aspects of warfighting. IO also requires a close look at the law and its relevancy in today's

[48] Whitehorn A. *Canada's Domestic Scene and the Canadian Army Towards 2020, in the Arena-The Army and the Future Environment*. DLSC. p. 18-19.

[49] ~~Charles J. ~~Dunlap. *21st century land warfare: Four Dangerous Myths*. ~~Parameters: Journal of the US Army War College. Carlisle. 1997.~~ p~~P~~. 27-37

technological environment. Because it was developed long before information operations, Laws o~~O~~f Armed Conflict (LOAC) and other international laws regarding the conduct of military campaigns are silent as to which information attacks are legal. We must consider for example other related laws such as the special protection for international civil aviation, international banking, International Liability for Damage Caused by Space Objects. We must also look at the violation of a nation neutrality by an attack launched from a neutral country (Hague Convention V), and PSYOP broadcasts from the sea which may constitute unauthorized broadcasting (UN Convention on Law of the Sea).[50]

Charles Dunlap argues that article 51 of the UN charter might be interpreted for application of the international law against offensive IO. Specifically, he proposes that if economic damage caused by electronic attacks is of sufficient scale and scope, then the coercion equates to an armed attack justifying an article 51 response. IO can also be under article 41 under measures not involving the use of armed forces.

There are a number of legal aspects that must be reviewed under international law and national law. We need to identify the status of cyberwarriors, their act and the target. For instance, the law of war forbids attacks on civilian targets, but dual installations (civilian/military) are permissible as long as the law of proportionality is met. For example, Lt Gen Micheal C. Short, NATO's Joint Force Air Component Commander in the Balkans, had no doubt that Milosevic had no compunction at all about putting internal displaced persons inside valid military targets [51]. During the Kosovo campaign, a military lawyer from the Judge Advocate General's office assessed the targets in

[50] US, DOD. *Joint Doctrine for Information Operations*. Joint Pub 3-13. http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf. p. I-12 to 13. It should be noted that the Canadian version of this publication does not cover the legal aspect of IO offensive actions.

[51] John A. Tirpak. *Short's View of the Air Campaign*. Air Force Magazine. September 1999. P. 43

terms of the Geneva conventions governing the laws of war. He would look at the factors of justifiability, proportionality, and collateral damage.[52]

Captain Hanseman provides excellent insights on the legitimacy of offensive IO. He suggests that the basic principles of Law of Armed Conflict (LOAC) in the context of Hague Law, which include military necessity, proportionality and chivalry, addresses how new weapons should be used. He does, however, reflect on the dilemmas faced by this type of operations. How can we make sure the military results of our attacks are proportionate to the casualties and destruction they cause? How will the prohibition against perfidy (false surrender) apply to psychological operations, or electronic deception? As he suggests, the ultimate question, then, is, "When would an IW attack constitute a use of `armed force?". He states that, at this point, the concepts are too new and the technical possibilities are evolving too quickly to definitively categorise all information warfare attacks and to determine whether they constitute an armed attack. Another dilemma is the connectivity between military and civilian systems, which renders difficult the separation of the systems. Currently, he submits that IW would allow opponents to completely ignore the presence of military assets when contemplating an attack on the civilian sector. Military use of civilian networks makes them legitimate targets under the rules of LOAC.[53]

I would like to reiterate the proposed Russian theorists initiative for the creation of an information deterrence concept, similar to the nuclear one, to alleviate the risks among nations of attacks on C4I systems, the use of computer viruses, and ability to affect the psyche of another nation through information technology. Hanseman also supports this initiative because he also believes that the U.S. might not necessarily maintain its information superiority.

[52] Inatieff. P. 33

[53] R.G. Hanseman~~ R.G~~. *The realities and legalities of information warfare*. The Air Force Law Review; Maxwell AFB; 1997. Vol: 42 p. 173-200

The political and military leadership must understand the implications of a lack of focus with the legal aspects of IO. As stated by Russian military analysts, the lack of legislation may result in a wide range of responses. In addition, military planners need to assess the principle of LOAC and the acceptable level of risk of retaliation. The legal challenges introduced by Dunlap and Hanseman highlight the requirements for the Canadian judge advocate personnel to address these issues in the most urgent manner.

ETHICS

Dr John Arquilla examined the ethical aspects of conducting information operations using the Just War theory.[54] In particular, he reviews the criteria of *right purpose*, *duly constituted authority*, *last resort*, *noncombatant immunity*, *proportionality* and *more good than harm*.

Information operation is a new field, which will require a high degree of ethical interpretation. The possibility of preemptive strike challenges the principle of right purpose. Operational commanders' ethical dilemmas could reside in the exploitation of the difficulty in detection of IO and the identification of the start of hostilities of offensive operations. From the concept of duly constituted authority perspective, nation-state could use non-state actors to conduct their offensive IO without running the risk of retaliation[55].

The idea of striking at an adversary's transportation, power, communication, and financial infrastructures could be interpreted as targeting noncombatants in a deliberate manner[56]. The concept of proportionality (avoidance of excessive force) is probably the most difficult one because it relies on the level of acceptable retaliation – including lethal force - in response to IO attacks, and the potential escalation.

[54] John Arquilla . *Ethics and Information Warfare*. Ed by. Khalilzad Z.M. and White J.P. Strategic Appraisal: The Changing Role of Information in Warfare. RAND Project AIR FORCE. Washington. 1999. Pp. 379 - 399

Arquilla proposes that IO fall~~s~~ between airpower and economic sanctions on the spectrum of tools of suasion. He concludes with the statement that information warfare attenuates the ethics of going to war; while, just warfighting retains its currency and value.[57]

On May 24th, NATO bombers destroyed the Yugoslav power grid. Everything from banking system to military assets depended on the grid. The political elite and the civilian population knew that NATO had secured control of the regime's nervous system. This successful military action was underscored, however, by the moral problematic of hitting the grid supplying power for hospitals, babies incubator and water-pumping stations.[58] The principles of last resort, non-combatant immunity, proportionality and more good than harm probably impacted on the operational commanders decision to delay this attack late in the air campaign.

CONCLUSION

In conclusion, the CF went a long way from the purely defnsive nature of its information operations in 1997. The refocus of IO to include both offensive and defensive operations will certainly set the conditions to face the challenge of the 21st century battlespace. The Defence Strategy 2020 and DPG 2000 provide the vision to address most of our deficiencies in the application of IO at the operational level. While these efforts are commendable, this essay demonstrated a number of key areas~~,~~ where the CF did not understand the impact of such a concept. The political and military leadership must understand the complexity and necessity of IO, and the requirement for an asymmetrical response.

Operational commanders will need to develop their skills to exploit this fourth dimension of the battlespace by operating on the moral and physical planes. We possess a sound doctrinal base, but

[56] Ibid. p. 388

[57] Ibid~~Arquilla~~. p. 394-398

[58] Inatieff. p. 35

should not expect the same level of technological support as the US commander. Operational commanders must, therefore, have access to the full spectrum of capabilities cited in the CF doctrine to compensate for any technological deficiencies.

The technological focus for the next 20 years should span from low to high technology. The review of the evolution of technology indicates the complexity of this endeavor. While the focus is on decision-making processes, improved intelligence, surveillance and reconnaissance abilities, it seems obvious that new technology such as psychotronic weapons and the low cost of emerging technology favor an asymmetrical response to the IO threat. For this reason, this essay supports any initiatives to form units and develop the appropriate doctrine to implement all components used in IO such as PSYOP and special information operation.

The examination of the CF strategic environment revealed that we may not have the funding or capacities to keep acquire the same technology as our allies. The threat evaluation indicates the emergence of asymmetrical threats from the full spectrum of potential adversary.

The human dimension of IO should also be studied to provide commanders with possible alternative during operations. The legal and ethical issues should be subject to extensive studies to allow operational commanders to operate with all components of information operations.

This discussion raised a number of issues from the strategic environment, doctrinal, organizational and human dimension perspective. The Canadian Forces have made major strides to support their operational commanders in the achievement of information superiority throughout the spectrum of conflict. Without an integrated technological-doctrinal-organisational-human approach, we run the risk of preventing our operational commander to achieve information superiority on the single integrated battlespace of the 21st century.

This essay attempted to highlight the major areas of concern in the application of information operations on a single battlespace of the 21st century. The CF must provide the right strategic conditions for our operational commanders to operate across the spectrum of conflict. The lack of progress in these areas will potentially result in the disintegration of this concept or the impossibility to ever achieve information superiority.

BIBLIOGRAPHY

Allard, Kenneth. "Information operations in Bosnia : a preliminary assessment." American Intelligence Journal. 17 no. 3&4 (1997): 55-58

Arquilla J. *Ethics and Information Warfare*. Edited by Khalilzad Z.M. and White J.P. Strategic Appraaisal: The Changing Role of Information Warfare. RAND Project Air Force. Washington 1999.

Baker J.B. Brigadier General. *IO Commanders Brief*. Defense Colloquium on Information Operations. Foundation Forum 1999. http://www.aef.org/baker.html.

Bourque, Col J.D.R. Information operations for Canada. Toronto : Advanced Military Studies Course, Canadian Forces College, 1998. http://www.wps.cfc.dnd.ca/irc/amsc/amsc1/003.html.

Campen, Alan D., and Dearth Douglas H. *Cyberwar 2.0: Myths, Mysteries and Reality*. AFCEA International Press, Fairfax, Virginia. 1998

Canada. Department of National Defence. *Shaping the Future of the Canadian Forces: A Strategy for 2020*. Ottawa, 1999. http://www.vcds.dnd.ca/cds/strategy2k/s2k01_e.asp.

Canada. Department of National Defense. *Defence Planning Guidance 2000*. Ottawa 1999. http://www.vcds.dnd.ca/vcds/dgsp/dpg/intro_e.asp.

Canada. Directorate – Land Strategic Concepts. *The Future Security Environment*. Report 99-2. Kingston 1999.

Canada. National Defence. *1994 Defence White Paper*. Minister of Supply and Services Canada, 1994.

Canada. Department of National Defence. B-GG-005-004/AF-000 *Canadian Forces Operations* Ottawa. 1997.

Canada. Department of National Defence. B-GG-005-004/AF-033 *Canadian Forces Information Operations* .Ottawa. 1998.

Canada. Department of National Defence. B-GG-005-004/AF-004 *Force Employment*. Ottawa. 1998.

Canada. Department of National Defence. B-GG-300-001-FP-000~~AF-033.~~ *Conduct of Land Operations-Operational Level Doctrine for the Canadian Army*. Ottawa. 1998

Canada. NDHQ RMA Operational Working Group. *Canadian Defence Beyond 2010, The Way Ahead: an RMA Concept Paper*. NDHQ Ottawa. 1999

Canadian Security Intelligence Service. *Information Operations: The Cyber Threat*. CSIS 1998 Public Report. 1999. http://www.csis-scrs.gc.ca/eng/publicrp/pub1998e_html.

Cohen E.A. *A Revolution in Warfare*. Foreign Affairs. New York. Mar/Apr 1996.

Collins, Steven. "*Army PSYOP in Bosnia : Capabilities and Constraints.*" Parameters. 29 no. 2 (Summer 1999): 57-73. http://carlisle-www.army.mil/usawc/Parameters/99summer/collins.html.

Combelles-Siegel, P. *Target Bosnia: Integrating Information Activities in Peace Operations.* Washington, DC: National Defence University Press, 1998

Dearth D.H. *Imperatives of Information Operations and Information Warfare*. Ed. By Campen, A.D. and Dearth D.H. Cyberwar 2.0: Myths, Mysteries and Reality. AFCEA International Press, Fairfax, Virginia. 1998.

~~Denning, Dorothy E. *Information Warfare and Security*. ACM Press Book, New York.1999.~~

Dunlap C.J. *21st Century Land Warfare: Four Dangerous Myths*. Parameters. Journal of the US Army War College. Carlisle. 1997.

Dunlap C.J. Jr. *The Law of Cyberwar: A Case Study from the Future*. Edited by Campen A.D. and Dearth D.H. Cyberwar 2.0: Myths, Mysteries and Reality. AFCEA International Press, Fairfax, Virginia. 1998.

Fredericks, Col Brian E. "Information warfare at the crossroads ." Joint Force Quarterly. No. 16 (Summer 1997): 97-103

Gentry, LCol John A. "Knowledge-Based 'Warfare' : lessons from Bosnia."American Intelligence Journal. 18 no. 1&2 (1998): 73-80

Hanseman R.G. *The Realities and Legalities of Information Warfare*. The Air Force Law Review. Vol 42. Maxwell AFB. 1997.

Hobson S. *Canada's Information Operations in Defensive Role*. Jane's Defence Weekly. Oct 1, 1997.

Inatieff M. *The Virtual Commander: How NATO Invented a New Kind of War*. Annals of Diplomacy CORBIS/SYGMA.

Kelley, Jay W. Lt Gen. *2025 Executive Summary*. Alabama, Air University Maxwell Air Force Base, Air University Press, 1996

~~Khalilzad, Zalmay M., and White John P. *The Changing Role of Information Warfare*. RAND Project AIR FORCE, 1999~~

Kuehl D. *Defining Information Power*. National Defense University Strategic Forum. Institute for National Strategic Studies. Number 115. June 1997. http://www.ndu.edu/inss/strforum/forum115.html.

Kuehl D. *Strategic Information Warfare: A Concept*. Strategic and Defence Studies Centre Working Papers. The Australian National University. Canberra, 1999.

Leggat, John and Ingar Moen. Challenges and opportunities posed by emerging technology : a Defence Management Committee discussion paper. Ottawa : Defence Management Committee, Dept. of National Defence, 1999.

Mann, Col Edward. "Desert Storm : The First Information War?" Air Power Journal. 8 no. 4 (Winter 1994): 4-14. http://www.airpower.maxwell.af.mil/airchronicles/apj/apj94/man1.html.

Marshall, Thomas J.; Kaiser, Phillip; and Kessmeire, Jon. *Problems and Solutions in Future Coalition Operations*. Strategic Studies Institute, U.S. Army War College. December 1997.

Metz S. *The Effect of Technological Asymmetric on Coalition Operations*. Edited by Marshall T., Kaiser P., Keismer. Problems and Solutions in Future Coalition Operations. Strategic Studies Institute, Carlisle. 1997.

Minihan K.A. LtGen USAF (Ret.) *Conflict in the Information Age*. Defence Colloquium on Information Operations. March 1999. http://www.aef.org/minihan.html.

National Defence, *1994 Defence White Paper*. Minister of supply and Services Canada, 1994

~~NDHQ RMA Operational Working Group. *Canadian Defence Beyond 2010, the way ahead: An RMA Concept Paper*. NDHQ, Ottawa, 31 May 1999.~~

Pigeau, Ross, and McCann, Carol. *Clarifying the Concepts of Control and Command*. Defence and Civil Institute of Environmental Medicine, Toronto, 1999.

Ryan H. and Peartree E.C. *Military Theory and Information Warfare*. Parameters: Journal of the US Army College. Vol 28 Issue 3. Carlisle. Autumn 1998.

~~Schneider, James J. "Black lights : chaos, complexity, and the promise of information warfare." Joint Force Quarterly. No. 15 (Spring 1997): 21-28~~

Thomas, Timothy L. "The mind has no firewall." Parameters. 28 no. 1 (Spring 1998): 84-92. http://carlisle-www.army.mil/usawc/Parameters/98spring/thomas.html.

Thomas T.L. *The Threat of Information Operations: A Russian Perspective*. Edited by Pfaltzgraff R. Jr. and Shultz R.H. Jr. War in the Information Age: New Challenges for U.S. Security Policy. International Security Studies Program. The Fletcher School of Law and Diplomacy, Tufts University. 1997.

Tirpak J.A. *Short's View of the Air Campaign*. Air Force Magazine. September 1999.

~~United States. Department of Defense. "Information Superiority." Concept for future joint operations: expanding Joint Vision 2010. Washington, DC: DOD, 1997. 35-45.~~

United States. Department of Defense. *Joint Warfare of the Armed Forces of the United States*. Joint Pub 1. Washington, DC. 1995. http://www.dtic.mil/doctrine/jel/new_pubs/jpl.pdf.

United States, DOD. *Joint Doctrine for Information Operations*. Joint Pub 3-13. Washington, DC: DOD, 1998. http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf

United States. *Conduct and Lessons of the Persian Gulf War*. Vol III, Part B. Forecast International/DMS Special Project.

United States Department of Defense. *Knowledge and Speed: The Annual Report on the Army After Next Project*. 1997. From Directorate-Land Strategic Concepts Report Number 99-2.

Vlahos M. *The Emergence of the Infosphere and its Impact on Military Operations*. Edited by Campen A.D. and Dearth D.H. Cyberwar 2.0: Myths, Mysteries and Reality. AFCEA International Press, Fairfax, Virginia. 1998.

~~Whitehead, Maj YuLin. "Information as a weapon." Air Power Journal. 11 no. 3 (Fall 1997): 40-54.~~

Whitehorn A. *Canada's Domestic Scene and the Canadian Army Towards 2020, in the arena-The Army and the Future Environment*. Directorate-Land Strategic Concepts Report 99-2. 1999.

~~Wilde, LCdr Andy. "Update : information operations." A Common Perspective: USACOM Joint Warfighting Center's Newsletter. 6 no. 2 (October 1998): 7-10.~~

Williamson C.A. *Psychological Operations in the Information Age*. Edited by Campen A.D. and Dearth D.H. Cyberwar 2.0: Myths, Mysteries and Reality. AFCEA International Press, Fairfax, Virginia. 1998.

~~Wright, MGen Bruce A. "Information operations, operational level support to the JFC." Defense Colloquium on Information Operations. Arlington,VA: Aerospace Education Foundation, 1999.~~