CANADIAN FORCES COLLEGE / COLLÈGE DES FORCES CANADIENNES
JCSP 34 / PCEMI 34

MASTER OF DEFENCE STUDIES
RESEARCH PROJECT

THE SHARPEST KNIFE IN A GUNFIGHT: ADAPTING TO THE UNCONVENTIONAL THREAT

By/par Maj Ted Middleton

ABSTRACT

THE SHARPEST KNIFE IN A GUNFIGHT: ADAPTING TO THE UNCONVENTIONAL THREAT, by Major Ted Middleton, Canadian Command and Staff Program 34, 103 pages.

The rise of the unconventional has dramatically changed the security environment as nations are confronted by highly adaptive, technologically enabled, media savvy foes bent less on defeating armed forces than eroding a nation's will to fight. Threats to vital national interests are no longer posed exclusively – or explicitly – by near-peer competitors in the conventional arena. Guerrilla militias, criminals and terrorists typical of today's insurgencies have increased the complexity of warfare so much so that it is difficult to discern the Davids from the Goliaths.

This research project frames the problem posed by evolved forms of insurgency and highlights the challenges of adapting organizational, doctrinal, and strategic frameworks to beat insurgents at their own game.

It concludes that to extrapolate the ideas, strategies, doctrine, and operational concepts from several decades ago and apply them to the complex insurgencies of the 21st century is a recipe for ineffectiveness. The challenges that confront the transformation of these frameworks are shown to be less technological than they are cultural and institutional. Key to successfully overcoming these challenges will be overcoming the bureaucratic, cultural, doctrinal and organizational inertia that inhibits interoperability, information sharing, and mission effectiveness.

CONTENTS

LIST OF FIGURES

INTRODUCTION

> In 1989, some American military experts predicted a fundamental change in the future form of warfare . . . They predicted that the wars of the 21st century would be dominated by a kind of warfare they called "the fourth generation of wars." Others called it asymmetric warfare . . . .
>
> This new type of war presents significant difficulties for the Western war machine and it can be expected that [Western] armies will change fundamentally.[1]

The above quotation appeared in a February 2002 edition of *al-Ansar*, an al-Qaeda sponsored online magazine, and to some it marked the validation of a theorized shift in the traditional conflict paradigm from armies attacking armies on the battlefield to a "de-statization" of warfare that blends the civil-military distinction into complex, violent, and unconventional struggles that cannot be decided militarily.

The rise of the unconventional has dramatically changed the security environment as nations are confronted by highly adaptive, technologically enabled, media savvy foes bent less on defeating armed forces than eroding a nation's will to fight.[2] Threats to vital national interests are no longer posed exclusively – or explicitly – by near-peer competitors in the conventional arena. The guerrilla militias, criminals and terrorists typical of today's insurgencies have increased the complexity of warfare so much so that it is difficult to discern the Davids from the Goliaths.

While insurgency has a long history that pre-dates Westphalia, its strategic salience cannot be taken in stride – its protracted and complex nature increasingly frustrates

---

[1] Ubeid al-Qurashi quoted in "Bin Laden Lieutenant Admits to September 11 and Explains Al-Qa'ida's Combat Doctrine," *The Middle East Media Research Institute Special Dispatch Series,* no. 344 (10 February 2002) [journal on-line]; available from http://www.memri.org/bin/articles.cgi?Page=archives&Area=sd&ID=SP34402; Internet; accessed 9 April 2008.

[2] Department of National Defence, B-GL-310-001/AG-001 *Land Operations 2021: Adaptive Dispersed Operations, The Force Employment Concept for Canada's Army of Tomorrow* (Ottawa: DND Canada, 2007), 4.

conventional military capabilities and the instruments of national power today. Insurgency is mutating from what it was understood to be during its "golden age" in the latter half of the 20th century to more unique, complex, and volatile campaigns that concentrate more on the political and psychological domains, subsequently making the military battlespace less and less decisive. "To simply extrapolate the ideas, strategies, doctrine, and operational concepts from several decades ago and apply them to 21st century insurgency is a recipe for ineffectiveness."[3] Western nations need to re-evaluate their grand strategies for counterinsurgency and reconceptualise military and other components of government ". . . to confront the new variants of this old challenge and to distinguish insurgency's enduring characteristics from those undergoing change."[4]

The Complexity of the Threat, Simply Described

For the most part, it would be convenient to draw a line differentiating insurgency from conventional warfare. However, the security environment has become far too complex to permit such a distinction. Unfortunately, insurgency – in both its classic and more evolved forms – and conventional warfare are not mutually exclusive concepts. Their elements are often intertwined, complementing one another occasionally, but mostly creating a complex, adaptive, non-contiguous, asymmetric threat environment that cannot be easily reduced to constituent parts for conventional military forces to either defeat piecemeal or to focus a strategically decisive blow on some centre of gravity.

However, efforts to understand the nature of insurgencies have resulted in two broad forms. The first form is that of a "national" insurgency where the primary antagonists are the

---

[3] Steven Metz and Rayond Millen, *Insurgency and Counterinsurgency in the 21st Century: Reconceptualizing Threat and Response*, Report Prepared for the U.S. Army War College Strategic Studies Institute (Carlisle PA: Strategic Studies Institute Publishing, November 2004), 1.

[4] *Ibid*., 1.

insurgents and national government. The government regime, which is assumed to have at least some degree of legitimacy and support, can be distinguished from the insurgents based on a variety of factors including economic class, ideology, ethnicity, race, religion, or political belief. While the conflict is clearly between the insurgents and an endogenous regime, national insurgencies may involve a host of actors who can influence the struggle by shifting their support between the antagonists. The most important of these actors is typically national or sub-national – i.e. the populace of the country or region within the country – but the significance of entities such as external states, international organizations, or trans-national groups should not be underestimated as these actors contribute significantly to the complexity of the conflict. Generally speaking, national insurgencies reflect the struggle between the antagonists to weaken one another while simultaneously attempting to win over the neutrals or those not committed to either side.[5]

The second form is that of the "liberation" insurgency where the insurgents are pitted against a ruling group that is seen as foreign occupiers by virtue of race, religion, ethnicity, or culture. The goal of the insurgents is to liberate their territory from alien occupation. Examples of insurgencies of liberation include the Afghan resistance to Soviet occupation, the current Taliban resistance against NATO and the Canadian Forces, and the quagmire that continues to unfold in Iraq.

What makes liberation insurgencies particularly difficult to counter is the motivation of the insurgent. Unlike national insurgencies, where a government can attempt to address the root causes through reform, liberation insurgencies are driven by resentment of occupation and the perception of oppression by foreigners. Unfortunately the leopard cannot

---

[5] *Ibid*., 2.

change its spots – the foreign regime will always remain foreign to the insurgents. This presents quite the conundrum for the counterinsurgent who is affronted by a movement, or various factions of movements, that can exploit an "organic" mobilizing factor of alien occupation in a unifying objective that defies a coherent strategy rooted in political ideology.[6] Take for example the adversaries in Iraq: a loosely affiliated network of Shi'ite and Sunni extremists, Ansar al-Islam, Baathist loyalists, disgruntled military and security elements, al-Qaeda, and criminal elements such as Saddam fedayeen all joined in temporary alliance with no unifying purpose other than to drive the United States out. These factions have no coherent plan for the political future of Iraq and will likely plunge the country into a chaotic civil war for power if the Coalition withdraws before a stable government is established. How does one win such a melee? What does winning look like?

The categorization of insurgencies into one of these two forms is unfortunately not so cut-and-dried. An insurgent struggle can demonstrate elements of both national and liberation insurgencies, often with the emphasis shifting over time from one to the other. In South Vietnam for example, the Viet Cong and North Vietnamese insurgency grew out of liberation, becoming more national in focus prior to extensive American involvement in the conflict only to emphasize again the liberation element from 1965 to the early 1970s, and finally reverted to a national form following the withdrawal of the American forces.[7]

Historically, successful insurgencies were those that prevented the counterinsurgents – be they the national ruling regime or foreign occupiers – from achieving strategic decision in the military battlespace until the balance of power shifted to favour the insurgents. In

---

[6] *Ibid*., 3, 14.

[7] *Ibid*., 3.

other words, while avoiding a crushing military defeat, successful insurgents pursued their objectives through the political and psychological realms, postponing decisive military encounters until they developed a critical mass of capability and support that would enable them to effectively strike at a weakened regime. This strategy was introduced with great success under Mao in the People's War and has since been widely used as a model to generically explain the doctrine of insurgency.

The People's War was a national insurgency that called for the seizure of power and the creation of a communist state. Seeing political power as the key to insurgency, Mao prescribed a strategy of three merging phases, expanding or contracting over time as necessary, which enabled his guerrillas to overcome the Nationalist Chinese government's superior conventional military and economic strength.

> **Phase I:** The insurgents concentrate primarily on building political strength. Military action is limited to selected, politically motivated assassinations. Any other military action must have a propaganda purpose to cement the population's support of the insurgents.
>
> **Phase II:** The insurgents gain strength and consolidate control of base areas. They begin to actively administer some portions of the contested area. And, because Mao had no outside sponsor providing weapons, they conducted military operations both to capture arms and to wear down government forces.
>
> **Phase III:** The insurgents commit regular forces (which have been carefully husbanded up to this point) in a final offensive against the government. This phase can succeed only if the "correlation of forces" has been shifted to the insurgents during the early phases.[8]

In Mao's vision, the first two phases served primarily to build the political, social, and economic power required to shift the "correlation of forces" from the government to the insurgents. It was only after this shift that the insurgents would be ready to complete the destruction of the government by conventional military action. National insurgencies since have refined Mao's strategy to bring about the defeat of superior regimes, as seen both in

---

[8] Colonel Thomas X. Hammes, *The Sling and the Stone: On War in the 21st Century* (St. Paul, MN: Zenith Press, 2004), 52.

Vietnam and in Nicaragua. But there is a danger here in extending Mao's model to explain the nature of all insurgencies, particularly those of liberation, as it can lead to the development of a one-size-fits-all counterinsurgency doctrine that is applied to far more complex struggles and adversaries.

The Thesis and Roadmap

Due to the Darwinian nature of warfare, some nations have adapted their war machines in response to the Maoist model, developing effective strategies, doctrine and forces to counter it. In turn however, insurgency continues to evolve and while some of the age-old characteristics remain unchanged, there are key variations or discontinuities that are not yet fully understood, particularly in cases of liberation insurgencies. Tarring all insurgencies with the Maoist brush will inevitably deceive our recognition of their true and unique natures and ultimately dupe nations into pursuing strategies that are insufficient and destined to fail. The aim of this paper is to *frame the problem* posed by evolved forms of insurgency and to *highlight the challenges of adapting* organizational, doctrinal, and strategic frameworks to beat insurgents at their own game.

This will be accomplished in four chapters. The first chapter establishes that "mainstream warfare" is now, and is likely to remain for the foreseeable future, irregular and that conventional warfare, into which we've invested extensive military, political, and economic capital, has become "marginal warfare." The antagonists in the mainstream have emerged as masters of what William Lind calls "the fourth generation of warfare": an evolved form of insurgency that relies on ". . . all available networks – political, economic,

social, and military – to convince the enemy's political decision makers that their strategic goals are either unachievable or simply too costly for the perceived benefit."[9]

Enabled by the Information Age, these adversaries have adapted their organizational designs, doctrines, and strategies to effectively wage a form of warfare that has become synonymous with Lind's fourth generation: netwar. As a comprehensive approach to conflict, netwar represents the migration of power to smaller, non-state actors who can capitalize on the inherent benefits offered by the Information Age and networked organizations – greater flexibility, agility, adaptivity, and connectivity. Chapter Two of this paper examines networks in detail, both as an organizational feature of netwar adversaries and as a strategic enabler in the political and psychological domains.

Chapter Three of this paper is a case study analysis that illustrates how the Shi'a fundamentalist trans-national organization Hezbollah, a master of strategic netwar, aptly leveraged all available networks to conduct a strategic communications campaign, supported by guerrilla and terrorist operations, in an insurgency of liberation to force the unilateral withdrawal of the Israeli war machine from South Lebanon in 2000.

The final chapter of this paper examines the merits of emerging concepts that are being developed to combat the asymmetric, unconventional, Information Age opponents that are frustrating nation-states in the complex conflicts of today and those forecasted for the coming decades. The challenges that confront these concepts will be highlighted to show that they are less technological than they are cultural and institutional. Key to successfully meeting these challenges will be overcoming the bureaucratic, cultural, doctrinal, and organizational inertia that inhibits interoperability, information sharing, and mission effectiveness.

---

[9] *Ibid.,* 2.

CHAPTER 1
OLD WINE, NEW BOTTLE?

Like a man who has been shot in the head but still manages to stagger forward a few paces, conventional war may be at its last gasp.[10]

When we think of warfare *per se*, we think of it, certainly initially, almost by default in both the traditional and the conventional sense. That is to say, we see warfare traditionally as a confrontation between nation-states, or coalitions of nation-states, exemplified by force-on-force military engagements where conventional military capabilities are employed in the air, land, maritime, space and cyberspace domains.[11] The objective of these military engagements is typically to convince or coerce key military or political decision makers, to defeat an enemy's armed forces, to destroy an adversary's war-making capacity, or to seize or retain territory in order to force a change in an adversary's government or policies.[12] To these ends we have developed a level of comfort with this traditional characterization of warfare that has shaped the development of most Western nations' war-fighting capabilities, doctrines and organizations to the extent that the United States, and any coalition it leads, has achieved overwhelming dominance in the conventional arena.

Consequently, this conventional dominance has led to a resurgence in the appearance of *unconventional warfare* as the means to effect change in the conflicts of the recent past involving states of conventionally inferior military and economic strength opposing comparative Goliaths. By mixing modern technology with ancient techniques of insurgency

---

[10] Martin van Creveld, *The Transformation of War* (New York: Free Press, 1991), 205.

[11] United States, Secretary of the Air Force, *Air Force Doctrine Document 2-3: Irregular Warfare* (Washington, DC: U.S. Government Printing Office, August 1, 2007), 1 [electronic publication]; available from http://www.e-publishing.af.mil/; Internet; accessed 1 March 2008.

[12] United States, Joint Chiefs of Staff, JP 1 *Doctrine for the Armed Forces of the United States* (Washington, DC: U.S. Government Printing Office, 14 May 2007), I-6 [electronic publication]; available from http://www.dtic.mil/doctrine/jel/new_pubs/jp1.pdf; Internet; accessed 8 March 2008.

and terrorism, today's truly dangerous foe to powerful nation-states can avoid the contest of contemporary military might and instead aim to exhaust its opponent's national will, achieving its goals by undermining and outlasting public support.[13] This chapter sets out to establish the relevance of unconventional warfare and the irregular activities that typify insurgencies not because they represent a new or independent type of warfare – quite to the contrary as irregular warfare has a long history that pre-dates Westphalia – but because they represent a major and pervasive form of warfare that has overtaken the conventional inter-state conflict that we have mastered and in doing so threaten to negate our military capabilities and organizations.

UNCONVENTIONAL WARFARE

> The U.S. Department of Defence defines unconventional warfare as:
>
> A broad spectrum of military and paramilitary operations, normally of long duration, predominantly conducted through, with, or by indigenous or surrogate forces who are organized, trained, equipped, supported, and directed in varying degrees by an external source. It includes, but is not limited to, guerrilla warfare, subversion, sabotage, intelligence activities, and unconventional assisted recovery.[14]

Unconventional warfare is an irregular activity that is typical of the violent struggles between state and non-state actors for legitimacy and influence over relevant populations.[15] These complex, nasty, prolonged conflicts avoid the decisive engagements pitched between

---

[13] United States, Department of the Army, FM 3-24 *Counterinsurgency* (Washington, DC: U.S. Government Printing Office, 15 December 2006), ix [electronic publication]; available from http://www.fas.org/irp/doddir/army/fm3-24.pdf; Internet; accessed 8 March 2008.

[14] United States, Joint Chiefs of Staff, JP 1-02 *Department of Defence Dictionary of Military and Associated Terms* (Washington, DC: U.S. Government Printing Office, 12 April 2001 as amended through October 17 2007), 564 [electronic publication]; available from http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf; Internet; accessed 8 March 2008.

[15] Definition of Irregular Warfare, quoted in United States, Secretary of the Air Force, *Air Force Doctrine Document 2-3: Irregular Warfare* . . .

conventional forces and instead focus on undermining their opposition's resolve, at least until the correlation of forces can be swung in their favour, to effect significant change. In the Canadian context these conditions describe the essence of an *insurgency*: "a competition involving at least one non-state movement using means that include violence against an established authority to achieve political change."[16]

Unconventional Warfare: The New Black

Since the Second World War numerous examples have showcased how unconventional warfare has led to major changes in the political, social, and economic fabrics of the territories involved. The Communist Revolution in China, the Indochinese wars, the Algerian War of Independence, the Sandinista struggle in Nicaragua, the Iranian revolution, the Afghan-Soviet War of the 1980s, the first Intifada, and Chechnya all demonstrated how the irregular and unconventional behaviour of militarily and economically inferior adversaries challenged state authority and forced significant change.[17] Low-intensity conflict, a term often used to describe unconventional war, has become the predominant instrument for bringing about political change, particularly in the Third World, and has frustrated the most modern and technologically advanced conventional forces of the industrialized world.

Contrast the political change resulting from these unconventional conflicts with the relative return to the strategic status quo following conventional wars of the same period: the Korean War, the Israeli-Arab Wars of 1956, 1967, and 1973, the Falklands War, the Iran-Iraq

---

[16] Definition as developed by a counter-insurgency study group during USMC Joint Urban Warrior 2005, quoted in Department of National Defence, B-GL-323-004/FP-003 *Counter-Insurgency Operations* (Kingston: Army Publishing Office, 2007).

[17] Colonel Thomas X. Hammes, *The Sling and the Stone: On War in the 21st Century* (St. Paul, MN: Zenith Press, 2004), 4.

War, and the first Gulf War. While some of these conventional clashes resulted in regime change or the to-and-fro of territorial frontiers, for the most part the political, social and economical structures of each of these states changed very little.[18]

This contrast is reinforced in Martin van Creveld's *The Transformation of War* as he illustrates the relative successes of unconventional wars against conventional opponents and argues that the trend since 1945 points to an eventual return to a pre-Westphalian kind of war; that is to say, a form of war where the principle constituents are not states, but are sub-national and trans-national groups whom we label today as terrorists, insurgents, guerrillas, and criminals.[19] "Their organizations are likely to be constructed on charismatic lines rather than institutional ones, and to be motivated less by 'professionalism' than by fanatical, ideologically-based, loyalties."[20] Conventional militaries have generally failed to adapt to effectively counter the threats posed by such groups, particularly as the distinction between governments, armies, and citizens has become more and more obscure.[21]

The dissimilarity between the strategy of the conventional army and the unconventional warrior has contributed significantly to this failure, a fact which was perhaps best articulated over a century ago by the British military theorist Colonel Charles E. Callwell: ". . . the key problem in the conduct of irregular warfare . . . is the difficulty of persuading or coercing an irregular enemy to come out and fight so that he could be duly

---

[18] *Ibid.,* 4.

[19] van Creveld, *The Transformation of War*, 192-197.

[20] *Ibid.,* 197.

[21] *Ibid.,* 192-195.

slaughtered in satisfactorily large numbers."[22] Van Creveld asserts that classical strategy – the eternal writings of Jomini and Clausewitz through Moltke to Liddell Hart as preached dogmatically at command and staff colleges – is inadequate to understand a war without fronts and will continue to lose relevance, along with conventional militaries and technologically advanced weaponry, as low-intensity conflict rises to dominance.[23]

Van Creveld's theory that in an ever less state-centric world the Clausewitzian strategic view of war has become obsolete is contested by Colin S. Gray in his work *Another Bloody Century*. Essentially, Gray examines a dozen theories that offer useful frameworks to explain the nature of war – including the rise and fall of total war, the obsolescence of major interstate war, and revolutions in military affairs to name but a few – and concludes that it would be in grave error to throw the baby out with the bath water when trying to characterize conflicts on the horizon. As he cautions about the perils of prediction he establishes that the alleged obsolescence of major conventional wars between states remains unproven. His assessment of the likely nature of future warfare does, however, grant that irregular, unconventional, low-intensity conflict may be dominant for some years. Interestingly, Gray's definition of irregular warfare is inclusive of terrorism and "[a]s such it is subject to the same lore of war and strategy as are other forms of warfare, both regular and irregular."[24] While holding onto his reservation that we have not seen the last of conventional major

---

[22] Colonel Charles E. Callwell, *Small Wars: A Tactical Textbook for Imperial Soldiers* (London: Greenhill Books, 1990), quoted in Colin S. Gray, *Another Bloody Century: Future Warfare* (London: Weidenfeld and Nicolson, 2005), 224.

[23] van Creveld, *The Transformation of War*, 27, 205, 207.

[24] Colin S. Gray, *Another Bloody Century: Future Warfare* (London: Weidenfeld and Nicolson, 2005), 214.

interstate war, Gray concedes that it has been overtaken in frequency by unconventional, irregular combat more akin to the conflicts in Afghanistan and Iraq today.[25]

The decline of large-scale state-on-state warfare in favour of protracted, ambiguous, unconventional conflicts, as introduced by van Creveld and acknowledged by Gray, is a theme that the U.S. Army War College has picked up on as well. A March 2003 monograph from the Institute of Strategic Studies' Dr Steven Metz and Lieutenant Colonel Raymond A. Millen concludes that ". . . the costs and risks associated with cross-border aggression will mount to the point that most states will not consider it . . ." in the traditional context.[26] The corollary to this decline is that the tensions that generate violence will, if anything, increase in the coming decades for primarily three reasons. One is the continuing clash of ethnic groups, sects, and clans that results from the long process of decolonization and the dissolution of national borders, which reflected the interests of colonial powers more so than the economic, religious, and ethnic realities on the ground.[27] A second is the effect of globalization as it enlightens the disparity between the haves and the have-nots in the world and sparks the disillusionment, frustration, resentment, and anger that fuel radicalism in non-state entities.[28] The third is likely to manifest itself in the poorer regions of the world through the competition for resources, whether arable land, water, or capital. As states are discouraged from traditional cross-border aggression by the high political and economical

---

[25] Gray, *Another Bloody Century* . . ., 170.

[26] Steven Metz and Raymond Millen, *Future War/Future Battlespace: The Strategic Future of American Landpower,* Report Prepared for the U.S. Army War College Strategic Studies Institute (Carlisle, PA: Strategic Studies Institute Publishing, March 2003), 3 [electronic publication]; available from http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB214.pdf; Internet; accessed 8 March 2008.

[27] *Ibid.,* 9.

[28] *Ibid.,* 9.

costs, the antagonists in these resource competitions will likely be sectarian or ethnic proxies.[29] These factors lead Metz and Millen to conclude:

> As states themselves are constrained from overt military aggression, the armed forces of all nations will be involved in promoting internal stability and confronting internal enemies, whether separatists, militias, insurgents, terrorists, armed criminal cartels, or something similar. The first two decades of the 21st century will be dominated by protracted, complex, ambiguous armed conflicts rather than short, politically and ethically clear ones leading to decisive outcomes.[30]

While van Crevald's speculation that the low-intensity conflict typical of unconventional warfare has become the prevailing method of war has earned the begrudging endorsement of the likes of Colin Gray, it has also been widely embraced by many theorists, such as Metz and Millen, as a signpost pointing to the strategic, operational and even tactical characteristics future war will take. To summarize the important commonality between these theorists, we can look to Colonel Thomas X. Hammes, an advocate of the importance of the unconventional in the evolution of warfare, who offers that "[t]he message is clear for anyone wishing to shift the political balance of power: only unconventional war works against established powers."[31]

A FRAMEWORK FOR THE EVOLUTION TO THE UNCONVENTIONAL

In order to discuss the nature of the unconventional conflict the Canadian Forces finds itself in today in Afghanistan and the challenges posed by such conflicts in the foreseeable future, it is necessary to use a framework upon which one can hang terminology that illustrates the evolution of warfare to present day and beyond. For that purpose, this paper will use an architecture that was developed in 1989 by the American theorist William

---

[29] *Ibid.,* 11.

[30] *Ibid.,* 14.

[31] Hammes, *The Sling and the Stone . . .*, 4.

S. Lind and a team of four officers from the U.S. Army and Marine Corps and has since been expanded upon most significantly by Colonel Hammes, cited above. *The Changing Face of War: Into the Fourth Generation* provides a theory that is congruent with van Creveld's as it reflects linearly upon three distinct generations of warfare that support the rise of a fourth generation where protracted, asymmetric insurgencies overshadow the traditional, decisive conventional campaigns.[32]

The First Three Generations of Warfare

Lind's framework commences at the Peace of Westphalia in 1648 where the state established a monopoly on war.[33] The First Generation reflected the order of the battlefield in the order of the military culture. Battles were formal engagements of line and column tactics where mass armies were deployed at the point of main effort to vanquish the enemy's formation.

Advances in weaponry such as breach-loaders, the rifled musket, machine guns, and indirect firepower broke down order on the battlefield in the mid 19th century, making the line and column tactics an advance into certain death. Second Generation warfare was the solution to the chaos and it culminated in World War I as the French developed a mass firepower doctrine of attrition where "[t]he artillery conquers, the infantry occupies."[34] Linear tactics based on the principles of fire and movement set the conditions for the formal

---

[32] William S. Lind, Colonel Keith Nightengale, Captain John F. Schmitt, Colonel Joseph W. Sutton, and Lieutenant Colonel Gary I. Wilson, "The Changing Face of War: Into the Fourth Generation," *Marine Corps Gazette* 73, no. 10 (October 1989): 22-26 [electronic publication]; available from http://www.d-n-i.net/fcs/4th_gen_war_gazette.htm; Internet; accessed 2 March 2008. In this framework, the term "generation" is used to describe a dialectically qualitative shift or change in the evolution of warfare.

[33] Prior to Westphalia marking the end of the Thirty Years War, wars were not fought exclusively by states; rather, they were fought by families, tribes, clans, sects, cities, religious groups and even business enterprises using means not limited to armies and navies.

[34] William S. Lind, "Understanding Fourth Generation War," 6 January 2004, http://www.lewrockwell.com/lind/lind3b.html; Internet; accessed 1 March 2008.

adoption of the operational art, initially by the Prussian Army, and the replacement of massed manpower with massed firepower.[35] The set-piece battle emerged with the careful synchronization of centrally controlled firepower orchestrating the movement of armies onto objectives. The culture of order was preserved through disciplined adherence to rules, processes and procedures, which enabled meticulous synchronization of effects. Interestingly, it can be argued that Second Generation warfare remained the basis of U.S. doctrine until the 1980s and to an extent is still germane today as the "American way of war" in both Afghanistan and Iraq where troops-in-contact quickly and decisively "put steel on target."[36]

Borne of the First World War, Third Generation warfare was developed by the German Army and reached its maturity over twenty years later in the form of Blitzkrieg or manoeuvre warfare.[37] Speed, surprise, and mental and physical dislocation became tenets for the German Army in 1939 as they capitalized on new capabilities presented by reliable armour, motorized infantry, mobile artillery, close air support, and radio communication. Third Generation warfare emphasized the use of initiative over obedience and embraced non-linear tactics to infiltrate, bypass and collapse the enemy from the rear forward. The evolution of the Third Generation's manoeuvre warfare commenced over 90 years ago and the "manoeuvrist approach" to tactical and operational thinking has been ingrained in Western doctrine for at least the last 20 years or so.[38]

---

[35] Lind, Nightengale, Schmitt, Sutton, and Wilson, "The Changing Face of War . . .," 23.

[36] Lind, "Understanding . . . "

[37] *Ibid.*

[38] This observation is based on the professional experience of the author, whose initial tactical training as a troop commander in the Canadian Army was based on manoeuvre doctrine.

The first three generations of this framework provide insight as to the logical progression of warfare, not by sudden transformations, but as gradual evolutions sparked by the advancement of ideas and technology that emerged during conflicts that proceeded each generation. The ideas and technological advancements enabled engagements of each successive generation to reach deeper into the enemy's territory in an effort to defeat his military force. It follows that the Fourth Generation reaches further still, as warfare shifts from the Industrial-Age focus on the physical destruction of conventional military capability to an Information-Age focus capable of attacking a society's very culture and breaking their political will.[39]

Fourth Generation Warfare

> *"You know you never defeated us on the battlefield," said the American colonel.*
> *The North Vietnamese colonel pondered this remark a moment.*
> *"That may be so," he replied, "but it is also irrelevant."*[40]

Fourth Generation Warfare (4GW) is not a new concept; in fact, Lind specifies ". . . that the 4th Generation is not novel but a return, specifically a return to the way war worked before the rise of the state."[41] It represents an evolution of warfare from the short, decisive campaigns of conventional forces to the protracted asymmetric struggles characteristic of small wars across the globe. Rooted in the philosophy of Mao Tse-Tsung, 4GW has matured over the last 80 years and continues to evolve as the only effective means for today's Davids to slay the Goliaths that dominate the arena of conventional warfare. It is the only kind of war that America has ever lost, and she has done so not once, but three times: first in

---

[39] Hammes, *The Sling and the Stone . . .,* 30, 208.

[40] Conversation in Hanoi, April 1975 quoted in Colonel Harry G. Summers Jr., *On Strategy: A Critical Analysis of The Vietnam War* (New York: Dell Publishing Co., 1984), 21.

[41] Lind, "Understanding . . ."

Vietnam, then in Lebanon, and again in Somalia.[42] It toppled the French in both Vietnam and Algeria and likewise overwhelmed the Soviets in Afghanistan. It stymied the Russians in Chechnya and it continues to affront the Americans in Iraq and NATO in Afghanistan. The track record of fourth generation proponents against major powers is telling; and failure to understand and adapt to this form of warfare will be at the peril of not only conventional militaries, but also nation-states that are opposed by 4GW practitioners.

The Nature of Fourth Generation War

It's important to recognize that 4GW is war; and as such, Colin S. Gray suggests that ". . . there is no avoiding the judgement that 4GW is a rediscovery of the obvious and familiar."[43] What this means is that like all wars, 4GW seeks to change an enemy's political position and makes use of all available means to achieve that end.[44] And like all modes of warfare, it was borne of necessity and innovation; however, 4GW matured under the practice of those who were grossly disadvantaged on the conventional battlefield.

One of the most important characteristics that differentiates 4GW from more conventional forms of war is the concept of time. 4GW is a complex struggle that is measured in decades vice months or years and its practitioners are determined to pit superior political or ideological will against great economic and military power over the long haul. From its inception under Mao, the Chinese Communists fought a fourth-generation campaign for twenty-seven years; the Vietnamese for thirty years; and the Sandinistas for eighteen years. Al-Qaeda has been fighting for their ideology since 1984. The Palestinian fight

---

[42] Hammes, *The Sling and the Stone* . . ., 3.

[43] Gray, *Another Bloody Century* . . ., 142.

[44] Hammes, *The Sling and the Stone* . . ., 3.

continues after more than thirty years while the insurgent battle in Afghanistan approaches the thirty-year mark following the Soviet invasion of 1979.[45]

As an evolved form of insurgency 4GW relies on ". . . all available networks – political, economic, social, and military – to convince the enemy's political decision makers that their strategic goals are either unachievable or simply too costly for the perceived benefit."[46] Its methodology is a mainstay strategy for the insurgent warriors of today in Palestine, Iraq, and Afghanistan where the military might of conventionally superior forces is avoided on the battlefield in favour of a much more "comprehensive approach" that leverages networks to attack, degrade, and eventually destroy their enemies' political will.

The following discussion examines the characteristics of 4GW across the levels of conflict, as defined by the Canadian Forces, based on an analysis by Hammes in his work *The Sling and the Stone: On War in the 21st Century*. This examination will serve to develop a broader understanding of the adversary, his methods, and in particular his extensive use of networks to shape the operating environment and further his aims. But first, a segue to the levels of conflict . . .

Levels of Conflict

In the Canadian context, the translation of policy goals into military action flows across three levels of military activity: strategic, operational, and tactical. At the strategic level, the top of this hierarchical model, national security objectives are determined and resources of national power – political, economic, scientific, technological, psychological, and military – are allocated to accomplish those objectives. At the operational level strategic intent is translated into effective military plans. At this vital link between strategy and

[45] *Ibid.,* 14, 221.

[46] *Ibid.,* 2.

tactics, campaigns and major military operations are designed, conducted, and sustained through operational objectives, providing the means for tactical successes to be exploited to achieve the overarching strategic objectives. At the tactical level, forces are deployed for battle and combat power is applied directly to defeat an enemy at a particular time and place.[47]

It is important to recognize at this juncture that the concept of levels of conflict is a conventional Western paradigm. It is presumptuous to assume that 4GW adversaries necessarily categorize their activities across distinct levels that mirror the Western paradigm. That said, this paradigm will be used as a framework to facilitate our understanding 4GW activities and to illustrate that there is more to 4GW than merely tactics.

Strategic 4GW

Strategically, 4GW sets out to change the minds of enemy policy makers. This is in keeping with Clausewitz's definition of war as ". . . an act of force to compel our enemy to do our will."[48] The nuance conceptually lies in the application of force. The 4GW adversary does not attempt to achieve traditional military superiority on the battlefield through mass, firepower, or manoeuvre; rather, he targets policy makers and those that influence them by employing all available networks to transmit specific messages convincing them that their war aims are either unachievable or too costly.[49] The conflicts in both Iraq and Afghanistan are illustrative of how adept the belligerents have become at tailoring messages to various audiences – one to the supporters of insurgency, another to the mass of neutral population,

---

[47] Department of National Defence, B-GG-005-300/FP-000 *Canadian Forces Operations* (Ottawa: DND Canada, 2005), 1-5.

[48] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 75.

[49] Hammes, *The Sling and the Stone* . . ., 208.

and a third to the Coalition decision-makers – all with a view to achieving their greater purpose.[50] In addition to tailoring messages to supporters (the power base) and the population, 4GW warriors will use networks to extend messages to the decision-makers of the target nation (often members of provisional authorities or transitional governments), to the allies of the target nation and even to neutral nations in order to preserve their neutrality or solicit their tacit support.[51]

It is important to recognize that the emphasis on strategic messaging via networks does not imply the absence of violence. Quite to the contrary, 4GW promises brutal and bloody conflict as civilian populations are drawn into the fray. As we have witnessed in Iraq, Lebanon and Afghanistan, these casualties are caused not so much by engagement of conventional military weaponry as they are the result of unconventional methods such as improvised explosive devices and suicide bombing attacks.

Hammes points out that the strategic significance of these tactics is important. As 4GW warriors resort to developing the tools to deliver violence from materials that are readily found in the society they are attacking, they avoid the requirement to build the massive war-fighting infrastructures that propelled the previous generations. Bombing campaigns can be supported locally without the reliance on heavy logistics, vulnerable lines of communication, or the necessity to defend core production assets. In short, the 4GW warrior's strategic focus can be primarily on the offence.[52]

---

[50] *Ibid.,* 209.

[51] *Ibid.,* 214.

[52] *Ibid.,* 209.

This offensive focus often finds a soft target in the underbelly of democracy. From a Canadian, American or British perspective, most 4GW adversaries of today are directly engaged by expeditionary operations and the violence is contained abroad (the attacks of 9/11 notwithstanding). Unfortunately, expeditionary operations are far from the "splendid little wars"[53] of the past and the 4GW warrior has recognized the strategic value in targeting "national interest." More specifically, the 4GW adversary has recognized the strategic merits of exploiting violent attacks via the media to cast doubt upon national interests of the countries involved. If a nation's vital national interests are clearly not at stake, images on CNN of a downed pilot being dragged through the streets of Mogadishu or the occasional beheading of a contractor will just as likely result in withdrawal as retaliation.[54]

As a comprehensive approach to conflict, 4GW has a well developed strategic-political side as well, which makes extensive use of international, trans-national, national, and sub-national networks to further its aims. A 4GW campaign will consider the roles of international organizations, such as the United Nations, NATO, the World Bank, the World Trade Organization, and the International Monetary Fund to name but a few, and can leverage these networks to achieve political paralysis on the international stage or specifically in the target nation's government process. Consider the causal connection between a nation's security situation and its ability to secure loans. A 4GW adversary need only to threaten to disrupt a target nation's security, communicate that message to the IMF and foreign investors, and measure the effect.[55]

---

[53] A popular reference to U.S. Secretary of State John Hay's reference to the 1898 Spanish-American War, which gave the US dominion over Guam, Puerto Rico and the Philippines.

[54] Hammes, *The Sling and the Stone* . . ., 210. Images of U.S. soldiers being abused in the streets of Mogadishu precipitated the end of the U.S. commitment to Somalia.

[55] *Ibid.,* 211-212.

Trans-national elements ranging from belief-based organizations such as the Islamic jihad, to nationalistic organizations such as the Palestine Liberation Organization, to humanitarian organizations such as Médecins Sans Frontières, to economic structures, to even criminal organizations all provide excellent networks for the 4GW adversary. Their organizations span borders, but are not subject to national control, and have diverse memberships whose loyalties vary. These organizations are often a source of recruits, funding, or even legitimacy for their cause.[56]

National organizations, both internal and external to the target nation, can be leveraged in a 4GW campaign as well. For example, the Congress of the United States, a national organization, was both a target of and a network for the North Vietnamese and the Sandinistas.[57] Non-governmental national groups such as churches, businesses, and lobbyists have all provided the networks to transmit the strategic messages in 4GW conflicts.[58]

On the sub-national level, there are many organizations that represent nations in the absence of states. These sub-national elements are typically minorities in their traditional homelands who readily align themselves with whoever best serves their interests.[59] The Palestinians, the Bosnian Serbs, the Kosovo Albanians, and the Kurds all exemplify sub-national groups who have played significant roles in recent conflicts demonstrating 4GW

---

[56] *Ibid.,* 212-213. This does not suggest that Médecins Sans Frontières supports 4GW adversaries or their campaigns. It merely serves to illustrate that humanitarian organizations provide another network that 4GW actors can exploit.

[57] Both the Vietnamese and the Sandinistas targeted their efforts to neutralize U.S. military power through Congressional action to remove funding for their opponents, the South Vietnamese and the Somoza regime respectively. For more information, see chapters 6 and 7 of Hammes, *The Sling and the Stone* . . .

[58] *Ibid.,* 213.

[59] *Ibid.,* 213.

strategy. These groups may be used as a social network to gather intelligence, provide logistical support, camouflage militant activity, or even conduct information operations amongst the greater population.

All of these networks have grown to take on a larger and larger strategic role in 4GW, particularly due to globalization, the increased awareness of the power of the media, and of course, the Internet. Colonel Hammes published an article in 2007 updating his original book and in it he suggests that 4GW is undergoing a strategic shift whereby ". . . insurgent campaigns have shifted from military campaigns supported by information operations to strategic communications campaigns supported by guerrilla and terrorist operations." [60]

Operational 4GW

At the level which links strategic goals to tactical execution, the 4GW adversary designs his campaign to ensure that tactical events target selected audiences and deliver specific messages that will influence decision-makers on the strategic level. From a Canadian military perspective, this concept is analogous to an Effects Based Approach to Operations: the 4GW opponent's operational design ". . . attempts to establish a link between action and effect in war . . . It defines success through the impact on human psychological and sociological behaviour, as opposed to a mechanistic approach focussed only on physical material and quantitative effects."[61]

To this end,

---

[60] Colonel Thomas X. Hammes, "Fourth Generation Warfare Evolves, Fifth Emerges," *Military Review* 87, no. 3 (May-June 2007): 14 [journal on-line]; available from http://www.proquest.com/; Internet; accessed 9 March 2008.

[61] Colonel Craig King, "Effects Based Operations: Buzzword or Blueprint?," in *Operational Art: Canadian Perspectives Context and Concepts*, ed. Allan English, Daniel Gosselin, Howard Coombs, and Lawrence M. Hickey, 313-330 (Kingston: Canadian Defence Academy Press, 2005), 314.

> . . . the 4GW operational planner must determine the message he wants to send, the networks available to him, the types of messages those networks are best suited to carry, the action that will cause the network to send the message, and the feedback system that will tell him if the message is being received.[62]

4GW opponents have proven to be capable of integrating this understanding of networks into highly sophisticated and complex campaigns designed to attack cultural and societal vulnerabilities that are the foundation of political will. What's more, the 4GW adversary understands how to attack networks to achieve far-reaching effects. Hammes asks his readers to consider the effect on the international trade network that would result if a high-yield explosive or weapon of mass destruction were delivered to North America via a commercial seaborne shipping container. The economic impact alone would have a staggering effect on society; arguably enough to sway political decision-makers to leave well enough alone or at the very least question their "vital national interests" of pursing expeditionary operations against a 4GW opponent.[63]

The First Intifada provides an excellent illustration of 4GW at the operational level. The Palestinian strategic messages needed to reach three different audiences: their Palestinian supporters, the international community, and of course, Israel. The operational design relied on 4GW techniques to communicate messages tailored to each of these audiences. For their power base, the message was that they could sustain the resistance to Israeli occupation and the Palestinians reinforced this message by providing economic, medical and social support to their people while continuing to demonstrate and agitate before Israeli authority. For international consumption, the message portrayed the Palestinians as an oppressed, impoverished people struggling for human dignity in their homeland. Israel was

---

[62] Hammes, *The Sling and the Stone* . . ., 216.

[63] *Ibid.,* 216-218.

no longer cast as the underdog amongst the Arab states; rather, it was portrayed as an occupying power. The Palestinian decision to limit violence and not take up arms was instrumental to this end as the media repeatedly showed the world young Palestinians armed with rocks and bottles confronting tanks and heavily armed professional Israeli soldiers. For Israel, the message was simply that as long as the territories remained occupied, there would be no peace. The Israeli people began to question the value of the occupation since the Palestinians confined the limited violence to the occupied territories, deliberately avoiding spill-over into Israel proper. The operational application of 4GW during the First Intifada effectively won concessions, forcing the Israelis to the negotiating table. "[It] neutralized U.S. support for continued Israeli action in the territories, froze the Israeli defence forces, and affected the Israeli national election."[64]

Tactical 4GW

4GW will tactically unfold in the complex, ambiguous environment of low-intensity conflict not unlike that described by Martin van Creveld. As Metz and Millen have written, "[t]he era of the 'stupid' enemy is over."[65] 4GW adversaries are all too aware of the conventional military might that can be brought to bear against them. They have adapted their tactics and continue to refine the lessons of Somalia, Afghanistan, Nicaragua, and Palestine. Tactical military action, primarily guerrilla or terrorist and occasionally even conventional, will be supportive of strategic messages targeting specific audiences.[66]

---

[64] *Ibid.,* 104-110, 216.

[65] Metz and Millen, "Future War/Future Battlespace . . .," viii.

[66] Hammes, *The Sling and the Stone* . . ., 220.

However, tactical activities in 4GW are not limited to strictly military action. The 4GW adversary will use a more comprehensive approach to deliver messages by various means, including through business, religious, economic, academic, artistic, and even social networks. These messages will likely be far less violent than the bloody images that are used for shock-value on political decision-makers. As van Creveld forecasts, the distinction between combatant and non-combatant in low-intensity conflict becomes very obscure, challenging conventional forces. Non-violent actors will play a critical role at the tactical level of 4GW as ". . . protestors, media interviews, web sites, and other 'nonviolent' [sic] resources . . . can create tactical dilemmas . . ." that will frustrate political will.[67]

A FINAL NOTE ON THE NATURE OF 4GW

> The first, the supreme, the most far-reaching act of judgement that the statesman and commander have to make is to establish . . . the kind of war on which they are embarking; neither mistaking it for, nor trying to turn it into, something that is alien to its nature.[68]

4GW is indicative not only of the nature of the fight the Canadian Forces are experiencing today in Afghanistan, but also of the nature of the conflicts that in all likelihood lie before the Canadian Forces in the future. It is essential that the nature of 4GW is recognized and well understood so that the Canadian Forces can avoid the pitfall of embarking upon a Third Generation campaign of manoeuvre to combat adversaries who are well versed in this evolved form of networked insurgency. Rather than play into our conventional strengths, the 4GW warrior will seek to fight a netwar that will frustrate our "manoeuvrist approach" and affront our political will. They will remain committed to their cause for the long term and will accept numerous tactical and operational setbacks in pursuit

---

[67] *Ibid.,* 219.

[68] von Clausewitz, *On War* . . ., 88.

of their strategic objectives. Winning on the battlefield may be irrelevant in terms of the strategic approach to winning the war.[69]

[69] Hammes, *The Sling and the Stone* . . ., 222.

CHAPTER 2
INFORMATION AGE ADVERSARIES

The previous chapter established that low-intensity, asymmetric, unconventional warfare has manifested itself as the dominant form of conflict confronting nation-sates and conventional militaries today. The protagonists in these conflicts have emerged as masters of Fourth Generation Warfare (4GW), an evolved form of insurgency that relies on all available networks – political, economic, social, and military – to conduct strategic communications campaigns, supported by guerrilla and terrorist operations, to convince the enemy's political decision makers that their strategic goals are either unachievable or simply too costly for the perceived benefit. This chapter will examine networks as an organizational feature of Information Age adversaries and their abilities to wage a form of warfare that has become synonymous with the Fourth Generation: netwar.

NETWAR

Defining Netwar

As the framework in Chapter One portrayed, the nature of warfare has shifted from the Industrial-Age focus on decisive battlefield engagements to the Information-Age focus on winning complex wars. The information age has affected more than the types of targets and weaponry at the disposal of fourth generation adversaries; it has significantly shaped their organization, doctrine, and strategy. Just as the information age has given rise to networked forms of organization in private sector commerce as an effective alternative to traditional hierarchical bureaucracies, it has also encouraged 4GW adversaries to disaggregate from

centralized revolutionary movements built along Marxist lines to flatter, decentralized webs of groups united by common goals.[70]

The rise of networked organizations is one of the single most important effects of the information age on the dimensions that Hammes identifies as key to a 4GW campaign: political, economic, social, and military.[71] John Arquilla and David Ronfeldt explain the impact of this effect in a RAND report as the shift to netwar.

> Netwar refers to an emerging mode of conflict (and crime) at societal levels, short of traditional military warfare, in which the protagonists use network forms of organization and related doctrines, strategies, and technologies attuned to the information age.[72]

As a comprehensive approach to conflict based on the centrality of information, netwar represents the migration of power to smaller, non-state actors who can capitalize on the inherent benefits offered by networked organization – greater flexibility, agility, adaptivity, and connectivity – with far greater ease than comparatively rigid, traditionally hierarchical, nation-states. For professional military forces whose cores are formed by classical hierarchies, these nimble networked foes pose a serious threat to conventional field operations.[73]

---

[70] Michelle Zanini and Sean J.A. Edwards, "The Networking of Terror in the Information Age," in *Networks and Netwars: The Future of Terror, Crime, and Militancy*, ed. John Arquilla and David Ronfeldt, 29-60 (Santa Monica, CA: RAND, 2001), 30.

[71] John Arquilla and David Ronfeldt, "A New Epoch – and Spectrum – of Conflict," in *In Athena's Camp: Preparing for War in the Information Age*, ed. John Arquilla and David Ronfeldt, 1-20 (Santa Monica, CA: RAND, 1997), 5.

[72] John Arquilla and David Ronfeldt, "The Advent of Netwar (Revisited)," in *Networks and Netwars: The Future of Terror, Crime, and Militancy*, ed. John Arquilla and David Ronfeldt, 1-25 (Santa Monica, CA: RAND, 2001), 6.

[73] Arquilla and Ronfeldt, "A New Epoch – and Spectrum – of Conflict," . . . 5.

A Metaphor for Netwar

The following metaphor is borrowed from Arquilla and Rondfeldt as it aptly describes the contrast between the natures of conventional warfare and netwar. The metaphor uses chess to reflect conventional warfare and the Chinese game *Wei Qi*, commonly known as *Go*, to represent netwar.[74]

The chess analogy is quite straightforward and really not much of a stretch for any student of military history. The opponents each form their pieces up on fronts defined by hierarchical worth on opposite sides of the board. They exchange manoeuvres to control the "no-man's land" that is the board's centre, threaten or capture their opponent's pieces, shield their own valuable pieces, and deliver victory through the decapitation of their opponent's one and only king. It is a game of linear strategy and the parallels to the first three generations of warfare are evident.

Netwar is not so linear and consequently is much more akin to *Go*, which, unlike chess, starts with an empty board. The board resembles a vast grid of many small squares. Opponents each take turns placing "stones" anywhere on the board, one by one, but not on the squares like chess; rather, on the intersections of the grid lines. There is no king, only stones of equal value. Stones cannot move once placed; they can only be removed if captured by becoming completely surrounded by the opponent's stones. However, the game is not about capturing the opponent's stones; it is about controlling territory or, in a conceptual military context, dominating the battlespace. Once played, stones form connected groups or chains to surround as many empty points of intersection, or opponent's stones, as

[74] *Ibid.,* 11. Invented in China in about 2000BC, *Go* has been played in Japan since 740AD, in Europe since 1880 and in Britain since 1930. As a game of strategy, chess can be viewed as 'battle' whereas *Go* is irregular warfare. For more information on *Go*, see http://www.tradgames.org.uk/games/Wei-Chi.htm.

possible. As a result, there is rarely a front line and opponents may act anywhere on the board at any time. The real battles are not for domination of the board's centre, but for the peripheries as they are easier to secure. The game is won by he who controls the most territory, not by toppling a king.[75]

Go, therefore, differs from chess much like netwar differs from conventional war. *Go* is not about manoeuvre or massed concentrations; it is more about proactive insertion and presence; it is more about deciding where to stand than whether to advance or withdraw; it is more about developing web-like links than about developing the set-piece battle; it is more about creating networks of pieces than about protecting hierarchies of pieces. *Go* illustrates netwar's simultaneity of offence and defence as a single action may both attack and defend.[76]

With its simple rules governing the incredible complexity of play, *Go* is a relatively accurate metaphorical representation of the nature of netwar as it is practiced by 4GW adversaries today. But netwar is not a game; it represents a form of conflict that ". . . spans economic, political, and social as well as military forms of 'war'."[77] The challenge that confronts Western war machines is how to defeat an adversary who is effectively playing *Go* with an organization, doctrine, and strategy that have been conceptualized to win at chess.

Netwar Actors

Netwar is likely to involve non-state, paramilitary, insurgent or other irregular forces who may be both sub-national and trans-national in scope. While netwar strategies and tactics have been adopted by enlightened civil-society action groups and many non-

---

[75] *Ibid.,* 11.

[76] *Ibid.,* 11.

[77] John Arquilla and David Ronfeldt, "Cyberwar is Coming!," in *In Athena's Camp: Preparing for War in the Information Age*, ed. John Arquilla and David Ronfeldt, 23-60 (Santa Monica, CA: RAND, 1997), 28.

governmental organizations (NGOs), this chapter will confine its discussion to those actors who resort to violence as a means to deliver their messages and further their goals.

Historically, there are many examples of netwar actors that resorted to irregular or unconventional tactics; however, these actors were forced to adapt to their tactical environments by evolving as social networks. These were not organizational designs that were progressed by specific doctrines or could be sustained over great distances.[78] Newer militant groups and terrorist organizations (i.e. post-1970s) have evolved from the nationalist or Marxist agendas of relatively hierarchical organizations, such as the Palestine Liberation Organization, to more loosely organized assemblies with religious or ideological motives and horizontal coordination mechanisms that allow for tactical independence while providing strategic direction.[79] Examples such as Hamas, the Palestinian Islamic Jihad, Algeria's Armed Islamic Group, and the Egyptian Islamic Group are all representative of netwar actors that have capitalized on the information revolution and steady rise of network designs.

Many netwar actors are anarchistic or nihilistic revolutionaries who advocate post-industrial, information-age ideologies, such as Osama bin Laden's multi-national alliance of Islamic extremists, al-Qaeda.[80] It is important to recognize at this juncture that netwar actors such as bin Laden do not necessarily represent the centre of gravity of mature and well developed 4GW adversaries. While a key figure in the Islamic terror network, he does not play a direct command-and-control role over all operatives. The network conducts many

---

[78] John Arquilla and David Ronfeldt, "The Advent of Netwar," in *In Athena's Camp: Preparing for War in the Information Age*, ed. John Arquilla and David Ronfeldt, 275-293 (Santa Monica, CA: RAND, 1997), 278. Arquilla and Rondfedlt expand on examples deriving from North America's French and Indian Wars, the American Revolution, and Spanish guerrillas fighting Napoleonic occupation in the early nineteenth century.

[79] Zanini and Edwards, "The Networking of Terror in the Information Age," . . . 32-33.

[80] Arquilla and Ronfeldt, "The Advent of Netwar," in *In Athena's Camp* . . . 278.

operations without his leadership and has the resilience to persevere should he be killed or captured.[81] Archetypal netwar organizations are characterized by multiple leaders diffused throughout their network acting in coordination with each other, but in the absence of central control.

> [T]he kind of leader who may be most important for the development and conduct of netwar is not the "great man" or the administrative leadership that people are accustomed to seeing, but rather doctrinal leadership – the individual or set of individuals who, far from acting as commander, is in charge of shaping the flow of communications, the "story" expressing the netwar, and the doctrine guiding its strategy and tactics.[82]

NETWORKS

Networked Organizational Design

Netwar is enabled principally by the organizational dynamics of networks.[83] One of the most common forms of social interaction, networks are ". . . simultaneously pervasive and intangible, ubiquitous and invisible, everywhere and nowhere."[84]

Netwar organizations consist generally of dispersed small groups who communicate, coordinate, and act in an internetted manner, often without the guidance of a defined headquarters element or central leadership.[85] The dispersal of these groups can be viewed as

---

[81] Zanini and Edwards, "The Networking of Terror in the Information Age," . . . 34.

[82] David Ronfeldt and John Arquilla, "What Next for Networks and Netwars?," in *Networks and Netwars: The Future of Terror, Crime, and Militancy*, ed. John Arquilla and David Ronfeldt, 311-362 (Santa Monica, CA: RAND, 2001), 327.

[83] David Ronfeldt and John Arquilla, "Networks, Netwars, and the Fight for the Future," in *First Monday* 6, no. 10 (October 2001): 5 [journal on-line]; available from http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/; Internet; accessed 14 March 2008. Rondfedlt and Arquilla expand upon both the social and organizational analysis of networks and conclude that while both provide significant insight as to how well a network is designed to execute netwar strategies and tactics, the decisive factor is its organizational design.

[84] Phil Williams, "Transnational Criminal Networks," in *Networks and Netwars: The Future of Terror, Crime, and Militancy*, ed. John Arquilla and David Ronfeldt, 61-97 (Santa Monica, CA: RAND, 2001), 64.

[85] Arquilla and Ronfeldt, "The Advent of Netwar," in *In Athena's Camp* . . . 277.

interconnected "nodes" sharing a set of common values, ideas, and interests.[86] The configuration of these networks is generally derived from the following three models depicted in Figure 1:

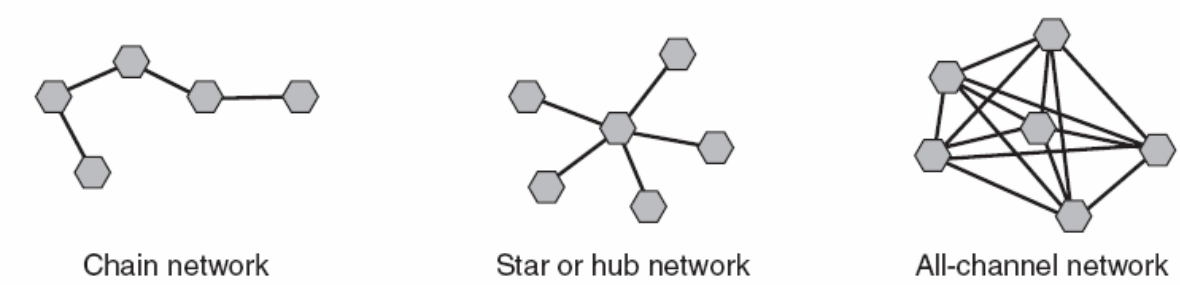

Figure 1 - Basic Models of Networks
Source: Arquilla and Ronfeldt, "The Advent of Netwar (Revisited)," in *Networks and Netwars* . . . 8.

The simplest model is represented by the chain network, which is a linear design where end-to-end communication must travel through intermediate nodes. The star, hub, or wheel network is a non-linear design where a central node, which is not indicative of a hierarchical design, serves as the intermediary for communication and coordination with other nodes. The most complex model is the all-channel, or full-matrix network, where all nodes are connected to one another. Conceptually, Arquilla and Rondfeldt explain that "[e]ach node in the diagrams may refer to an individual, a group, an organization, part of a group or organization, or even a state."[87] It follows then that these nodes may vary in size, function, and membership. The cohesion of the interconnecting links may be tight or loose, spanning boundaries that may be well-defined, obscure or even porous in relation to the external environment.[88] While these links are most often viewed as relationships between

[86] Arquilla and Ronfeldt, "The Advent of Netwar (Revisited)," in *Networks and Netwars* . . . 7.

[87] Ibid., 8.

[88] *Ibid*., 8.

actors, they may in some cases be nothing more than common ideas, giving the network a nebulous character that makes it particularly ill-structured; that is to say, making it interactively complex, non-linear, and chaotic.[89]

While the most difficult to organize and sustain, the all-channel model yields the greatest potential for collaborative undertakings thanks to the information revolution. Despite its geodesic representation in Figure 1, the ideal organizational design of the full-matrix network is conceptually quite flat, with no single, central leadership node, no discernable chain of command structure, and no headquarters *per se*. This means that there is "no precise head or heart that can be targeted."[90] Writ large, the all-channel network demonstrates no hierarchies; however, this is not necessarily true of its individual nodes. Multiple leaders sharing common principles, interests, goals, and often an overarching doctrine or strategy, enjoy relative autonomy, which enables tactical decentralization. Consequently, ". . . the design may sometimes appear acephalous (headless), and at other times polycephalous (Hydra-headed)."[91]

Netwar actors reflect attributes of these models based largely upon the functional requirements of their organizations. Chain networks are conducive to smuggling operations; hub networks are found at the core of cartels, criminal syndicates, and terrorist organizations; and all-channel networks serve highly internetted, decentralized militant groups. Larger and more complex organizations, such as radical trans-national terrorist groups, may incorporate

---

[89] United States, Department of the Army, TRADOC Pamphlet 525-5-500 *The U.S. Army Commander's Appreciation and Campaign Design* (Washington, DC: U.S. Government Printing Office, 28 January, 2008), 9.

[90] *Ibid*., 9.

[91] *Ibid*., 9.

combinations of these models to form hybrid networks with fully-matrixed councils at their strategic core and hub or chain networks executing tactical operations at their peripheries.

The concept of network cores and peripheries is particularly germane to highly developed trans-national 4GW adversaries as it reflects the asymmetries of power, influence, and interests within the larger network.[92] Generally, the core is characterized by dense connections amongst individuals who may provide strategic direction to nodes on the periphery or play a key role in their coordination and support. The peripheries on the other hand, are characterized by looser relationships and less dense patterns of interaction than those of the core.[93] American sociologist Mark S. Granovetter emphasizes the cohesive power of "weak ties" such as these loose relationships in extending the network beyond its core: "weak ties are more likely to link members of *different* small groups than are strong ones . . . ."[94] Phil Williams translates the significance of these weak links to the trans-national threat network, explaining how they give the network diversity and resilience, enabling it " . . . to operate at a far greater distance – both geographically and socially – than would otherwise be the case, facilitating more extensive operations, more diverse activities, and the capacity to carry out effective intelligence collection."[95]

The complexity of the organizational designs increases as hybrids form within networks, often coexisting with or even including traditional hierarchies. The configurations

---

[92] Williams, "Transnational Criminal Networks," . . . 72. While Dr. Williams' work analyzes trans-national criminal networks, much of the analysis is equally applicable to militant groups, terrorist organizations, and 4GW practitioners, many of whom incorporate criminal endeavours in their operations as a source of funding.

[93] *Ibid.,* 73.

[94] Mark S. Granovetter, "The Strength of Weak Ties," in *The American Journal of Sociology* 78, no. 6 (May 1973): 1370, 1371, 1376 [journal on-line]; available from http://www.jstor.org/; Internet; accessed 13 March 2008.

[95] Williams, "Transnational Criminal Networks," . . . 73.

are unique to each organization, making the analytical mapping of netwar adversaries and the identification of their centers of gravity very challenging.[96] To illustrate this complexity, consider a "spider-web" network that features a small number of highly connected actors functioning as key hubs in the core, around which are arrayed a large number of actors, linked to the hubs but only loosely connected in the periphery to one another, yet with frequent all-channel information-sharing across all actors.[97] This configuration proves to be very resilient to attack, forcing its opponents to identify and target one or more of the key hubs, while remaining highly agile and collaborative in pursuing its strategic vision.

This section has focused on the organizational design of netwar actors; however, it is important to recognize that the effectiveness of these actors relies upon more than just the foundation of their configuration. The strength of their performance depends on their ability to function across five dimensions Arquilla and Rondfeldt describe as the:

- Organizational dimension – the netwar actor's organizational design;
- Narrative dimension – their story being told or the message delivered;
- Doctrinal dimension – their shared strategies and tactics;
- Technological dimension – the information systems at their disposal; and,
- Social dimension – the personal ties that assure trust and loyalty.[98]

These dimensions are not viewed as mutually exclusive levels; they are entwined such that the characteristics of each are likely to affect the others. The strongest netwar actor, therefore, is the one whose ". . . organizational design is sustained by a winning story and a

---

[96] *Ibid.,* 8,9.

[97] Ronfeldt and Arquilla, "Networks, Netwars, and the Fight for the Future," . . . 9.

[98] Ronfeldt and Arquilla, "What Next for Networks and Netwars?," . . . 324.

well-defined doctrine, and in which all this is layered atop advanced communications systems and rests on strong personal and social ties at the base."[99]

Networks versus Hierarchies

Netwars differ from the more traditional conflicts, such as those that Lind would describe as forms of Second or Third Generation Warfare, in which the actors prefer formal, stand-alone, hierarchical organizations, doctrines, and strategies.[100] In their book *Power to the Edge,* Alberts and Hayes attribute hierarchy to the ". . . organizational consequence of Industrial Age specialization . . ." and reason that large organizations require many layers of middle management to coordinate and integrate specialists and specialized sub-organizations due to the limits of effective span of control.[101] In an effort to transform the complexity of war and reduce the fog and friction of battle into a collection of manageable tasks and problems, Industrial Age militaries resorted to the optimization of processes,[102] which decomposed operations by creating layered organizations based on specializations organized along hierarchical lines.[103] Nowhere is this more evident than in the present-day architecture of the U.S. Army, which can trace its lineage back to the U.S. Civil War. The more unwieldy the organization – like the Department of National Defence – the greater is the requirement

---

[99] *Ibid.,* 234.

[100] Zanini and Edwards, "The Networking of Terror in the Information Age,". . . 30.

[101] David S. Alberts and Richard E. Hayes, *Power to the Edge: Command, Control, in the Information Age* (Washington, DC: CCRP Publications, 2003), 41.

[102] Recall the description of Second Generation Warfare in Chapter One and the reliance on process.

[103] Alberts and Hayes, *Power to the Edge* . . ., 44.

for bureaucratic structures to permit personal interface between responsible managers, or commanders in the military context, and individuals at the next layers.[104]

These antiquated structures increase the time required for information to flow, increase the probability of error or distortion in that flow, and decrease the speed and agility of the organization to react to changes in information as it flows. The integration of powerful, high-tech information systems seeks to remedy these conditions and optimize the military's efficiency; however, the nature of the hierarchical organization effectively hamstrings this potential. Consider a typical commander's requirement for intelligence today in the most modern of militaries. Intelligence requirements are submitted up the chain of command where at each level they are validated, consolidated, prioritized and then passed through a centralized staff system that synchronizes the tasking of information collection assets. Once the information is collected, it is then fed through a level of analysis, transformed into usable product, and disseminated back down through the chain of command. The cumbersome vertical bureaucracy of the organization effectively nullifies the potential of advanced information systems to provide near real-time intelligence.[105]

Potential 4GW adversaries are not constrained by structured bureaucracies. They have evolved into sprawling, loose, leaderless networks, overcoming the vulnerability posed by small, isolated hierarchies headed by "great men".[106] What's more, networking has enabled the 4GW adversary to not only overcome isolation and suppression, but to

---

[104] *Ibid*., 42.

[105] The capabilities of military hierarchies in contrast to 4GW networks are discussed at length in Hammes, *The Sling and the Stone* . . . Chapter 13. The specific analogy to intelligence collection is expanded upon at pages 192-200.

[106] Arquilla and Ronfeldt, "The Advent of Netwar (Revisited)," in *Networks and Netwars* . . . 4.

effectively vie against nation-states and powerful hierarchically oriented actors.[107] Networked adversaries enjoy a freedom of action that exploits the constraints of their hierarchical opponents:

> It tends to defy and cut across standard boundaries, jurisdictions, and distinctions between state and society, public and private, war and peace, war and crime, civilian and military, police and military, and legal and illegal. This makes it difficult if not impossible for a government to assign responsibility to any single agency – e.g. military, police, or intelligence – to be in charge of responding.[108]

Nation-states are therefore challenged by netwar actors largely because of the differences in their organizational structures. As government tools for the exercise of sovereignty and authority, bureaucracies have difficulty fighting networks that can operate in the nebulous areas where the ". . . operational paradigms of politicians, officials, soldiers, police officers, and related actors get fuzzy and clash."[109] The conclusion that Arquilla and Rondfeldt draw from these observations is one that will be developed further in Chapter Four: *It takes networks to fight networks.*

NETWORKS, NETWAR ACTORS AND TECHNOLOGY

"Netwar is not mainly about technology – but good information technology sure makes a difference."[110] Generally speaking, networked organizations are better situated to exploit new technological opportunities in the information and communications domains than

---

[107] *Ibid*., 15.

[108] *Ibid*., 14.

[109] *Ibid*., 14.

[110] Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," in *Networks and Netwars: The Future of Terror, Crime, and Militancy*, ed. John Arquilla and David Ronfeldt, 239-288 (Santa Monica, CA: RAND, 2001), 239.

most bureaucratic hierarchies, and trans-national adversaries have exploited these opportunities, turning them into force multipliers.

Technological advancement in these domains has greatly reduced transmission times, which in turn has enabled networks to plan, coordinate, and execute operations amongst geographically dispersed constituents. The extensively networked organizations of today are in fact only viable because new technologies have significantly reduced the cost of sustaining information-intensive organizational designs.[111]

Netwar and the Internet

Perhaps the most significant of these technologies, the Internet has emerged as a resilient and effective means to communicate across networks, through the strategic cores and out to the peripheries, while providing a physical separation that adds to their operational security. As an unparalleled integration medium, the Internet offers networked adversaries the advantages of:

> . . . easy access; little or no regulation, censorship, or other forms of government control; potentially huge audiences spread throughout the world; anonymity of communication; a rapid flow of information; the inexpensive development and maintenance of a web presence; a multimedia environment; and the ability to shape coverage of the traditional mass media.[112]

In Gabriel Weimann's report, *www.terror.net: How Modern Terrorism Uses the Internet*, he identifies eight different, though often overlapping, ways Information Age adversaries use the Internet to target current and potential supporters, international public opinion, and enemy publics.

---

[111] Zanini and Edwards, "The Networking of Terror in the Information Age,". . . 36.

[112] Gabriel Weimann, "Special Report: www.terror.net – How Modern Terrorism Uses the Internet," in *United States Institute of Peace* Special Report 116 (March 2004): 3 [journal on-line]; available from http://www.usip.org/pubs/specialreports/sr116.pdf; Internet; accessed 15 March 2008.

As an instrument of psychological warfare, "[t]he Internet – an uncensored medium that carries stories, pictures, threats, or messages regardless of their validity or potential impact – is peculiarly well suited to allowing even a small group to amplify its message and exaggerate its importance and the threat it poses."[113]

As an instrument of publicity and propaganda, the Internet offers ample opportunity for the netwar adversary to shape how they are perceived and to manipulate their own image and the image of their enemies.[114]

As a vast source of information, the Internet is a colossal intelligence data-base where subversive groups can legally collect, collate, and analyze details about targets, organizations, and even opposing military force dispositions, tactics, techniques and procedures.[115]

Additionally, the Internet provides effective mechanisms for fundraising, recruitment and mobilization, networking and information sharing.[116] Finally, and perhaps most importantly, as a mechanism for planning and coordination, the Internet is used in the direction and execution of attacks. As an example, the militant Islamic group Hamas has made extensive use of chat rooms to plan operations and e-mail to coordinate actions in Gaza, the West Bank, and Lebanon.[117]

---

[113] *Ibid*., 5.

[114] *Ibid*., 6.

[115] *Ibid*., 7.

[116] *Ibid*., 7-9. In terms of information sharing, the Internet provides a virtual "How-To" manual for militants and terrorists, including such titles as *The Terrorist's Handbook*, *The Anarchist Cookbook*, *The Mujahadeen Poisons Handbook* published on the official Hamas website, and al Qaeda's *The Encyclopaedia of Jihad*.

[117] Zanini and Edwards, "The Networking of Terror in the Information Age,". . . 37.

For all intents and purposes, the Internet has become Mao's "sea" and the messages within it the "fish" that enjoy the relative security to which his guerrilla fighters grew accustomed.[118] Actors with common agendas can collaborate, mobilize, coordinate, execute, propagate effects, and quickly dissolve into the electronic ether much to the chagrin of counterterrorism intelligence organizations who have realized that it is impossible to monitor the flow and content of all Internet traffic. However, while the Internet itself has proven to be an effective environment in which to hide communications, it is not an entirely secure medium for the netwar adversary. Recognizing the vulnerability of electronic communication to monitoring, sophisticated commercially available encryption programs protect much of the 4GW practitioner's information flow. Coded e-mails are becoming increasingly difficult to break and more and more militant groups have established web sites where instructions in the form of maps, photographs, directions, and technical details of how to use explosives can be disguised using technologies such as steganography.[119]

Low-Tech Netwar

Western populations tend to view modern conflict from a futuristic, high-tech perspective. Clausewitz's caution to neither mistake war for, nor try to turn it into, something that is alien to its nature remains valid when preparing to combat a 4GW opponent in a netwar.[120]

---

[118] In Mao's theory of insurgency, he metaphorically refers to guerrilla fighters as fish swimming in a sea of people. The cloak of invisibility that a population once provided to a guerrilla fighter can be replicated in the Information Age by the internet as communications are immersed in the volume of legitimate electronic correspondence.

[119] Zanini and Edwards, "The Networking of Terror in the Information Age,". . . 38. Steganography is a method of embedding data within graphic files. Through steganography, insurgents can hide messages in a single dot in a digital picture, or even in the period at the end of a sentence.

[120] Carl von Clausewitz, *On War* . . ., 88.

Netwar is not simply a function of the Internet, and by extension it is not solely about Internet war. That is to say, the netwar battlefield is not limited to the electronic arena. Quite to the contrary, while it is increasingly likely that some activity will occur in cyberspace, the overall conduct of netwar will occur in the "real world" where its effects can be observed, felt, and measured qualitatively. New technologies, however enabling for organizational networking, are not absolutely necessary for a netwar actor.[121]

As an example, consider the utility of a relatively low-tech tool such as the television. In the war-torn Balkans of 1995, the Bosnian Serb leadership relied on their television sets as near real-time information collection assets to measure the Western reaction to their seizure of U.N. hostages. After chaining the hostages to potential NATO targets, they invited the media to film the scene. Within hours the footage reached the U.N. headquarters in New York, and the Bosnian Serb message was in the New York Times:

> Television footage supplied by the Bosnian Serb forces after the raid showed eight unarmed United Nations officers chained to doors or posts and a bridge near the site of the attack. In a radio recording released to Reuters by the United Nations, one of the officers said, "We've been advised that the next bomb that falls, we'll be killed."[122]

Bosnian Serb leadership was able to again watch their televisions to gauge the reactions of key players in the U.N. assembly as national positions were aired over CNN. Consequently, the Bosnian Serbs were able to measure the effects of their actions before the U.N. commanders on the ground had received any official guidance through their chain of command. Compared to the use of encryption programs and web sites, the television was a

---

[121] Arquilla and Ronfeldt, "The Advent of Netwar (Revisited)," in *Networks and Netwars* . . . 11.

[122] Roger Cohen, "Conflict in the Balkans: The Overview; After 2d Strike from NATO, Serbs Detain U.N. Troops," *New York Times*, 27 May 1995 [electronic publication]; available from http://www.nytimes.com/; Internet; accessed 15 March 2008.

low-tech tool that a relatively flat organization leveraged to dislocate the decision-action cycle of an organization renowned for its bureaucratic process.[123]

Similarly, Somalia warlords used a combination of cell phones, runners, and drum codes to pass information and coordinate the efforts of dispersed clans and sub-clans across Mogadishu in 1993. The use of simple codes, nicknames, and slang increased their security when using cell phones and provided them with effective local and worldwide communications.[124]

4GW adversaries have proven that they are adept not only at leveraging high technology, but any available technology to carry out their activities. The platforms to sense targets, process information, communicate securely, and deliver precision weapons are not the prerogative of high-tech conventional forces. Insurgent groups use people, open-source reporting, Internet mining and commercially available imagery as sensors; their processor is the human mind; the worldwide web provides secure global connectivity; and their precision weapons are martyrs willing to ride the ordnance to the target.[125]

Emerging Netwar Doctrine

Just as warfare can be seen to have evolved through Lind's generational framework, so too has the doctrine of the war-fighters. The traditional doctrines of the melee (the chaotic, undirected free-for-all form of primeval warfare), massing, and manoeuvre evolved in concert with advances in organizational designs and their abilities to structure and process

---

[123] Hammes, *The Sling and the Stone* . . ., 196.

[124] *Ibid.,* 197.

[125] *Ibid*., 202.

information.[126] It follows that with the evolution of 4GW in the Information Age new doctrinal concepts are bound to keep pace. Arquilla and Rondfeldt introduce an approach that has emerged with the shift to netwar: *swarming*.

Swarming is the ". . . systematic pulsing of force and/or fire by dispersed, internetted units, so as to strike the adversary from all directions simultaneously."[127] The key active process of swarming is "sustainable pulsing" of either a concentration of force, such as a small group of fighters, or a concentration of fire, such as multiple bombing attacks. Like fish in Mao's sea, forces will be widely dispersed, but internetted such that they can swiftly come together to concentrate their force or fires on selected or opportune targets from all directions. After striking, they will again disperse, blanketing the battlespace, ready to "pulse" to attack again when the conditions are favourable. It is important to recognize that the concept of swarming "fires" is not limited to kinetic weapons effects; non-kinetic "fires" such as media-oriented messages and propaganda can swarm an opponent with considerable effect.[128]

Swarming relies on two fundamental requirements: a large number of tightly internetted small units of manoeuvre; and the capability of those forces to not only strike, but also sense, providing operational and strategic awareness.[129]

---

[126] John Arquilla and David Rondfeldt, *Swarming and the Future of Conflict*, Report Prepared for the Office of the Assistant Secretary of Defence (Command, Control, Communications, and Intelligence) project "Swarming and Information Operations" (Santa Monica, CA: RAND, 2005.), 7-8 [electronic publication]; available from http://rand.org/pubs/documented_briefings/2005/RAND_DB311.pdf; Internet; accessed 16 March 2008. The evolution of these doctrines is expanded on in detail in Chapter One of the report.

[127] *Ibid*., 8.

[128] *Ibid*., 21-22, 39.

[129] *Ibid*., 22.

Swarming is a natural doctrine for networked organizations to apply. Since most netwar actors are operating as non-state, trans-national or sub-national antagonists engaged in low-intensity, unconventional conflict, swarming is likely to become a widespread methodology in the coming years. It is a flexible approach that allows those who apply it to shift easily and swiftly between the offence and the defence and promises high potential as an offset to conventional hard power.[130]

The blurring of the lines between offence and defence complicates the nature of the conflict as it becomes increasingly difficult to distinguish between attacking and defending actions. Take for example, an enemy that attacks in the name of self-defence. The blending of offence and defence mires the understanding of the conflict as it often mixes the strategic and tactical levels of operations. In the war of the Mujahadeen in Afghanistan in the 1980s, guerrilla fighters were strategically on the defensive yet were tactically offensive.[131]

A FINAL NOTE ON INFORMATION AGE ADVERSARIES

This chapter has established that the Information Revolution is altering the way people fight, shifting the focus from decisive battlefield engagements to netwar campaigns aimed at winning wars. The rise of networked organizations is one of the single most important effects of the information age, facilitating the reorganization of militant, insurgent, and terrorist groups into decentralized arrays of trans-national groups, linked to others with similar agendas or beliefs, communicating and coordinating horizontally rather than vertically, with speed and complexity. Netwar actors have evolved into sprawling, loose, leaderless networks capable of vying against powerful nation-states by exploiting the

[130] *Ibid*., 43-44.

[131] Arquilla and Ronfeldt, "The Advent of Netwar (Revisited)," in *Networks and Netwars* . . . 13.

comparative rigidity of bureaucratic hierarchies. Embracing technology, netwar organizations have leveraged the Internet to further their goals in various ways ranging from psychological warfare and propaganda campaigns to highly instrumental uses such as fundraising, recruitment, data mining, and coordination of tactical actions. Netwar is, however, a function of more than just technology. Technology is an enabler that, when married to a networked organizational design, compliments a shared narrative, well-defined doctrine, and strong social ties to empower a 4GW adversary to pursue a netwar campaign.

CHAPTER 3
HEZBOLLAH: THE A-TEAM OF 4GW ADVERSARIES

Hezbollah, as an organization with capability and worldwide presence, is [al Qaeda's] equal, if not a far more capable organization. I actually think they're a notch above in many respects.[132]

Chapter One demonstrated the decline of large-scale conventional state-on-state conflicts in favour of unconventional, asymmetric, low-intensity insurgencies featuring non-state, trans-national actors. As war has evolved over time, so too has insurgency: from garden variety guerrilla warfare to strategic communications campaigns empowered by the Information Age and enabled by militias and terrorists. The methodology of the most dangerous insurgents leverages all available networks – political, economic, social, and military – to convincingly demonstrate to conventional military and economically superior states the futility of the continued pursuit of their strategic objectives. This comprehensive netwar is the way of the Fourth Generation and it is best illustrated by the Shi'a fundamentalist organization, Hezbollah (the Party of God).

The aim of this chapter is to use Hezbollah to exemplify 4GW as it was used in South Lebanon to force the unilateral withdrawal of the Israeli war machine in 2000. The nature of 4GW as discussed in Chapter One and the ability of its practitioners to function across the organizational, narrative, doctrinal, technological, and social dimensions introduced in Chapter Two, will serve as a guide to illustrate Hezbollah's emergence as a master of strategic netwar.

---

[132] George Tenet, former CIA Director George Tenet in a statement to the U.S. Congress in 2003, quoted in Daniel Byman, "Should Hezbollah be Next?," *Foreign Affairs* 82, no.6 (November-December 2003): 54 [journal on-line];available from http://proquest.umi.com/pqdweb?RQT=318&pmid=6; Internet; accessed 17 March 2008.

The Genesis of Hezbollah

"Hizbollah is the quintessential organizational manifestation of violent Shi'a reaction to westernization and secularization in Muslim societies; it epitomizes the radical Shi'a response to the modern state in general and contemporary Lebanon in particular."[133] Hezbollah emerged in the wake of Israel's massive invasion of Lebanon in 1982, which sought to destroy the PLO as a coherent political and military force. The PLO withdrawal from Beirut placed Israel in control of Lebanon from Beirut southward. The subsequent assassination of Lebanon's President-elect Bashir Gemayel, an Israeli protégé, in September 1982 sparked the U.S. to broker a peace agreement in May of 1983 between Israel and the Lebanese Republic that virtually ceded southern Lebanon to Israel in the form of a "security zone".[134]

In the beginning, Hezbollah could not be labelled a popular movement; rather, it was more of a conspiracy of a handful of clerics and lay Shi'a, sponsored by the nascent Islamic Republic of Iran in an effort to progress their campaign to spread the message of "Islamic revolution." With the Israeli troops consolidating their occupation of southern Lebanon and Hezbollah's popularity on the rise, by 1984 an Islamic resistance took shape with Hezbollah emerging as a dominant player amongst the radical Shi'a. Moving boldly to strike at "imperialist" influence in Lebanon, Hezbollah, or groups linked to Hezbollah, targeted dozens of westerners in a series of abductions, using them as barter for the release of Lebanese prisoners held in Germany, Israel, and Kuwait. Hezbollah embarked upon a

---

[133] Carl Anthony Wege, "Hizbollah Organization," *Studies in Conflict and Terrorism* 17, no. 2 (January 1994): 151 [journal on-line]; available from http://web.ebscohost.com; Internet; accessed 18 March 2008.

[134] Augustus Richard Norton, "Hizbollah and the Israeli Withdrawal from Southern Lebanon," *Journal of Palestine Studies* 30, no. 1 (Autumn, 2000): 23 [journal on-line]; available from http://www.jstor.org/view/0377919x/di020211/02p01053/0; Internet; accessed 17 March 2008.

journey into martyrdom, pursuing a jihad that included a series of impressive suicide bombing attacks on the U.S. embassy, the U.S. embassy annex, the headquarters of Israeli intelligence located in then-occupied Tyre, the U.S. marine barracks at the Beirut airport, and the French embassy.[135]

The sudden withdrawal of the U.S. from Lebanon following the devastating attacks on their embassy and the Marine barracks was labelled by Hammes' as one of three American losses to a 4GW adversary.[136] But Hezbollah was arguably still a fledgling organization; one which was to mature from a rigidly ideological organization reputed for kidnappings, hijackings, and suicide bombings into " . . . not only a highly professional guerrilla force, but also an impressive political organization with a broad and varied constituency, a pragmatic leadership, and a clearheaded strategy."[137]

HEZBOLLAH AS A NETWAR ACTOR

Leadership and Organizational Design

Hezbollah is far from what was believed to be a monolithic proxy of Iran or Syria. It resembles much more a coalition of Lebanese Shi'a clerics, who each have their own views, networks of followers, and personal links back to Iranian clergymen.[138] Although the modern structure of Hezbollah, particularly that of the political party, is formal, interactions among members are volatile and do not follow rigid lines of control. What's more, the

---

[135] *Ibid*., 24-25.

[136] Hammes, *The Sling and the Stone* . . . 3.

[137] Norton, "Hizbollah and the Israeli Withdrawal from Southern Lebanon,". . . 23.

[138] Magnus Ranstorp, "Hizbollah's Command Leadership: Its Structure, Decision-Making and Relationship with Iranian Clergy and Institutions," *Terrorism and Political Violence* 6, no. 3 (Autumn 1994): 303 [journal on-line]; available from http://web.ebscohost.com; Internet; accessed 16 March 2008.

organization serves as an umbrella to radical Shi'a groups and therefore is in many respects a hybrid of networked arrangements within a hierarchical design.[139]

Figure 2 depicts the structure of Hezbollah's organization as Magnus Ranstorp described it in his 1994 monograph on Hezbollah's command leadership. While somewhat dated, it remains a valid reflection of the hybrid nature of Hezbollah's multitudinous components stemming from the core of the organization.

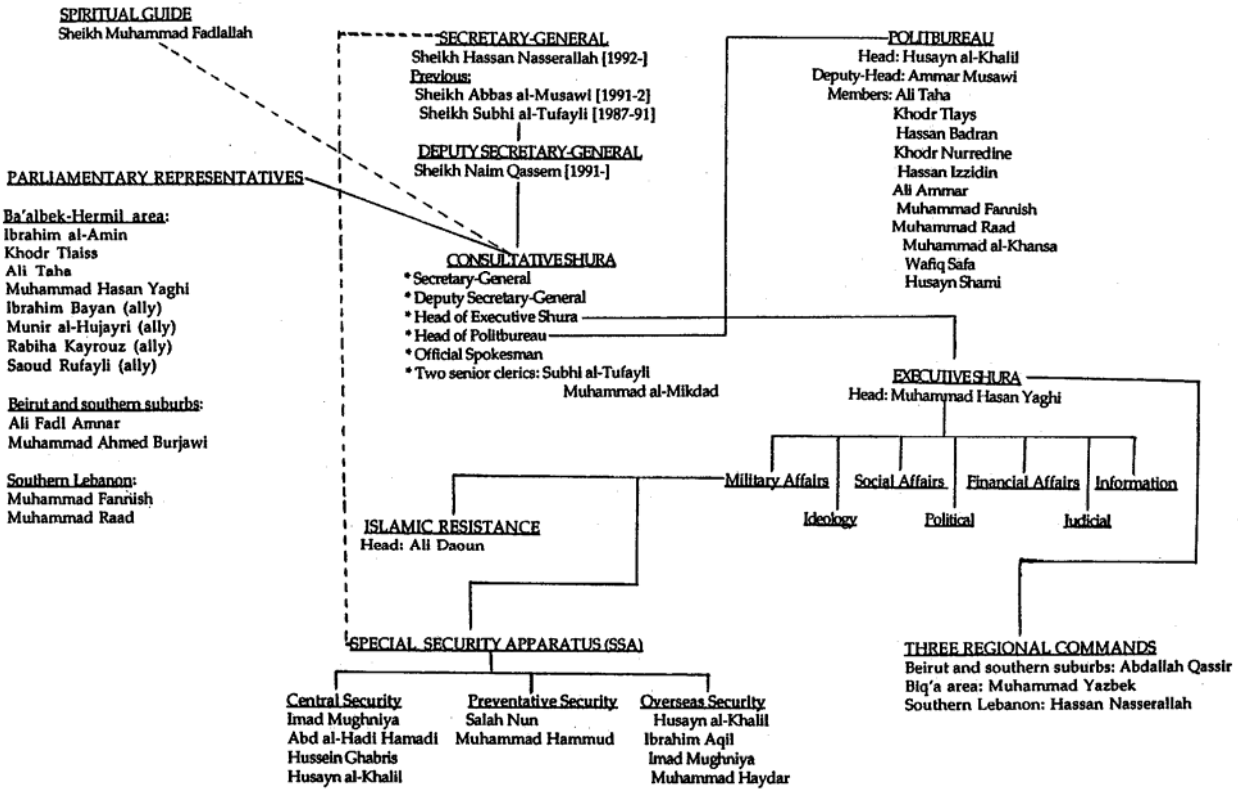

Figure 2 - The Structure and Leadership of Hezbollah (1994)
Source: Ranstorp, "Hizbollah's Command Leadership . . .," 306.

Typified by continuous clerical factionalism between its leading members over the direction of the movement, Hezbollah was never a uniform body; it was secretly governed by

[139] Zanini and Edwards, "The Networking of Terror in the Information Age,". . . 34. For more on the dynamic of the clerical factionalism within the organization, see Ranstorp, "Hizbollah's Command Leadership . . .," 312-313.

a supreme religious body fashioned upon the upper echelons of Iran's clerical leadership.[140] The organizational design of the core is based on a loose religious hierarchy that is governed by a decision-making council of a dozen clergymen and military commanders that form the *Majlis al-Shura*, or Consultative Shura. The *Majlis al-Shura* includes the Secretary General, Sheikh Hassan Nasserallah, his deputy and spokesman, the religious authority Sheikh Muhammad Fadlallah, two senior clerics, and two supervisory organs: the Executive Shura, which strategically administers seven specialized committees overseeing military, social, political, financial, information and judicial affairs as well as the party's ideology; and the Politbureau, which coordinates the recruitment, propaganda, and support services on regional and local levels.[141] The Executive Shura and its specialized committees are replicated regionally by three Hezbollah cells in the southern suburbs of Beirut, the Bekka, and south Lebanon.[142]

The leadership provided by the *Majlis al-Shura* exemplifies the "doctrinal leadership" that was described in Chapter Two as essential to a netwar actor. While Sheikh Muhammad Fadlallah presides over the *Majlis al-Shura* as Hezbollah's spiritual oracle, the main clergymen who are responsible for specific committees or portfolios wield significant power in the control of the movement.[143] Multiple leaders diffused throughout Hezbollah's network act in coordination with each other through loosely organized assemblies governed by common religious and ideological motives while horizontal coordination mechanisms allow

---

[140] Ranstorp, "Hizbollah's Command Leadership . . .," 305.

[141] *Ibid*., 308, 313.

[142] Marius Deeb, "Shia Movements in Lebanon: Their Formation, Ideology, Social Basis, and Links with Iran and Syria," *Third World Quarterly* 10, no. 2 (April 1988): 692-693 [journal on-line]; available from http://www.jstor.org; Internet; accessed 29 March 2008.

[143] Ranstorp, "Hizbollah's Command Leadership . . .," 308.

for tactical independence of committees, clans, factions, and cells operating within the strategic context of the party. Nasserallah, as Secretary General, is less the "great man" than he is:

> . . . the kind of leader who may be most important for the development and conduct of netwar . . . the individual or set of individuals who, far from acting as commander, is in charge of shaping the flow of communications, the "story" expressing the netwar, and the doctrine guiding its strategy and tactics.[144]

Hezbollah's Military and Security Organizations

As a committee within the Executive Shura, there exists a separate body responsible for intelligence and security called the Special Security Apparatus. This body is further subdivided into a central security apparatus responsible for the majority of the kidnapping operations of foreigners in Lebanon; a preventative security apparatus responsible for personal security of prominent Hezbollah clergymen; and an overseas security apparatus responsible for special operations abroad. The strong personal ties required by a netwar actor to ensure trust and loyalty, as discussed in Chapter Two, are achieved within these security apparatus by relying primarily on family members from the Mughniya and Hamadi clans. These family bonds ". . . ensure loyalty to the senior commanders and secrecy surrounding [hostage-taking] operations."[145]

Following the Ta'if Accords in 1989, an Islamically oriented military wing splintered from the main party of Hezbollah, which was beginning to involve itself in secular Lebanese politics. Hezbollah military units are lead by local commanders who are organized into

---

[144] David Ronfeldt and John Arquilla, "What Next for Networks and Netwars?," in *Networks and Netwars: The Future of Terror, Crime, and Militancy*, ed. John Arquilla and David Ronfeldt, 311-362 (Santa Monica, CA: RAND, 2001), 327.

[145] Ranstorp, "Hizbollah's Command Leadership . . .," 308.

regional cells and communicate directly with Hezbollah party members, bypassing intervening levels of bureaucracy. These self-contained cells of fighters share common operational objectives that support Hezbollah's strategic objective – the creation of an Islamic republic free from the oppression of American-Zionist hegemony – without reliance on close tactical oversight. Coalescing to attack and disintegrating immediately afterward in a manner similar to the pulsing swarms described in Chapter Two, the cells of the Islamic Resistance, Islamic Jihad, Islamic Jihad for the Liberation of Palestine, Revolutionary Justice Organization, and the Organization of the Oppressed on Earth[146] are not ". . . led by commanders – by a Mr X or a Mr Y, as the media say – [they are] directed by the ideas of Islam."[147] Quite literally in fact,

> [t]he village Imams . . . were asked to mention certain words in their sermons. These requests came from Beirut, often from Hezbollah; sometimes, not always, the code-words were devised by Iranians. These words – 'great books', 'olive groves', 'sweet fruits', there was no limit to the combinations – would mean nothing to the village sheikhs. Nor to most of their worshippers. But a few, perhaps only one man, in the mosque would understand their import. They would be a message. That is how the suicide bombers of Lebanon used to receive their orders.[148]

A loosely structured system of fluctuating operational cells, Hezbollah's military and security organizations clearly exemplify the essence of a complex, networked adversary.

Securing a Power Base: Hezbollah's Comprehensive Social Networks

Domestically, Hezbollah has emerged as a dominant order among Lebanese Shi'a. Why? Hezbollah's political and social activities operate as an integrated and holistic network, delivering an array of services to Shi'a groups, which in turn develops the strong

---

[146] Wege, "Hizbollah Organization," . . . 157.

[147] Robert Fisk, *Pity the Nation: The Abduction of Lebanon* (New York: Thunder's Mouth Press/Nation Books, 2002), 578.

[148] *Ibid*., 578.

social dimension discussed in Chapter Two that is essential to a netwar actor; and, it legitimizes their party as an organization that is beyond the common perception of terrorists-cum-politicos.[149]

Hezbollah's Executive Shura created a central social services unit that consists of institutions that either provide services related to armed resistance or cater to a wider group of users requiring social, economic, or urban services. These institutions are essentially Non-Governmental Organizations (NGOs) that function autonomously but depend administratively on Hezbollah and therefore must respect the overall sense of the Hezbollah mission.[150]

Two NGOs – the association of the Martyr (*al-Shahid*) and the association of the Wounded (*al-Juraha*) – manage schools, hospitals, dispensaries, and leverage a wider network of relationships to stabilize families committed to armed resistance. In 2005, *al-Shahid* provided services for 2500 relatives of martyrs, prisoners and missing individuals, while *al-Juraha* provided care for more than 3000 wounded.[151]

Similarly, for the greater population not directly involved in armed resistance, Hezbollah sponsors a diversity of NGOs that manage social, educational, medical, urban, economic, cultural, and religious policy sectors. The Educational Institute (*al-Mu'assasa al-Tarbawiyya*) reaches some 5300 students through nine schools in an effort to redefine the structure of Shi'a society through Islamic learning. The Good Loan (*al-Qard al-Hassan*)

---

[149] Mona Harb and Reinoud Leenders, "Know Thy Enemy: Hizbullah, 'Terrorism' and the Politics of Perception," *Third World Quarterly* 26, no. 1 (February 2005): 187 [journal on-line]; available from http://web.ebscohost.com; Internet; accessed 17 March 2008.

[150] *Ibid*., 187, 188.

[151] *Ibid*., 187.

provides micro-credit at drastically reduced rates to an average 750 clients monthly.[152] The network of service providers encompasses aid for the poor and deprived, public health, and even reconstruction aid to compensate for the substantial urban devastation that resulted from Israeli occupation. In addition to sponsoring a research centre that studies social, economic, political, financial, administrative, and development issues, Hezbollah's reach extends right through to youth and sports programs as well as women's activism.[153]

While Hezbollah's institutions are autonomous and structured as hierarchies, they form a holistic network that relies on horizontal coordination mechanisms to optimize their efficiency by sharing information and expertise across the entire array of service providers. Not only does this network permit the NGOs to capitalize on resources and shared knowledge, but it also serves to disseminate codes, norms, and values that progress what Hezbollah has called the Resistance Society.[154]

As a non-state actor, Hezbollah has certainly managed to provide services that the state could not, or would not, and in doing so has cemented an indigenous and highly networked support base. Its fighters, many of them part-timers, are local men with strong family ties, homes, jobs, hopes and aspirations for Lebanon. They choose the resistance because it suits their ideals and provides them networks of social support.[155]

The Narrative of the Resistance Society

Over the last two decades, Hezbollah has carefully cultivated a variety of institutions in Lebanon that operate today as a holistic and integrated network that engenders sets of

---

[152] *Ibid*., 187.

[153] *Ibid*., 188.

[154] *Ibid*., 188.

[155] Norton, "Hizbollah and the Israeli Withdrawal from Southern Lebanon,". . . 26-27.

values and meanings embedded in an interrelated religious and political framework. These ideals are disseminated daily amongst the Shi'a community through Hezbollah's institutionalized networks and ". . . serve to mobilize them into 'the society of Resistance' in order to consolidate the foundation of an Islamic sphere."[156]

> Key to Hezbollah's narrative is the concept of Muslim oppression by the West.
>
> Colonialism and imperialism are singled out as the major constants of how countries like France, Britain and, more recently, the USA have trampled on the Muslim peoples and approached the latter with contempt, double standards and brutal force in order to impose their hegemony.[157]

With the rise of the U.S. as a unilateral world power, the French and British colonial influence has steadily declined in the region over the past two decades. According to Sheik Naim Qassem, Hezbollah's Deputy Secretary General and media spokesman, contemporary U.S. foreign policy has aimed to promote the existence of the Israeli entity, furnishing it with justifications for financial, military or political power, and nodding favourably towards Israeli intermediate and long-term strategic objectives.[158] Coupled with what Qassem characterizes as flagrant U.S. hostility towards any movement that either denounces or resists Israeli occupation, U.S. policy endorses ". . . an 'American-Zionist project' that threatens to usurp the entire region, impose its hegemony and complete the destruction of Palestine."[159]

To Hezbollah, therefore, the Israeli state and the U.S. government represent the manifestation of colonial and imperialist oppression of Muslims. Hence, resistance to this

---

[156] Harb and Leenders, "Know Thy Enemy . . .," 173.

[157] *Ibid*., 181.

[158] Naim Qassem, *Hizbullah: The Story from Within* trans. Dalia Khalil (London: SAQI, 2005), 246.

[159] Speech by Hezbollah's Secretary General Hasan Nasrallah in Beirut, as cited in Al-Safir 22 May 2004, quoted in Harb and Leenders, "Know Thy Enemy . . .," 181.

oppression is believed to be the mission and responsibility of every Shi'a: it is a choice of life that embraces not only armed resistance, but social and political resistance as well.

The Shi'a constituency that subscribes to this view is the product of Hezbollah's holistic network and this emergent society serves to disseminate the concept of *jihad*, a basic behaviour in a Muslim's life that signifies struggle, either spiritual struggle or the physical struggle against an enemy. In the Islamic context, *jihad* has a broader meaning than armed resistance, which is a lesser test in comparison to spiritual jihad, as illustrated below.

> The Prophet (PBUH) expressed this meaning upon reception of a group of Muslims just back from combat: 'Welcome to a troop that has fulfilled that smaller *jihad* (battle) and whom the bigger *jihad* still awaits.' When asked of that bigger challenge, the Prophet (PBUH) answered: '*Jihad* with the soul.'[160]

Jihad with the soul is the greater endeavour as it is a constant and permanent struggle that manifests itself internally as the conflict between virtue and vice. In contrast, combat with an enemy is a periodic calling to ". . . the triumph of principles, morals, righteousness and the victory of the nation, when the nation is subject to oppression, occupation, or humiliation."[161]

Both military jihad and spiritual jihad are therefore essential components in the perpetuation of Hezbollah's resistance society. Together the "smaller" and "bigger" jihads form a comprehensive dogma that takes the meaning of resistance beyond righteous combat and transforms it to signify an individual process characterized by humanitarian, moral, and religious duty. Hence, Hezbollah uses resistance as a strategy to empower Lebanese Shi'a, providing them an opportunity to reject victimization and instead embrace a culture of

---

[160] Naim Qassem, *Hizbullah: The Story from Within* trans. Dalia Khalil (London: SAQI, 2005), 34.

[161] *Ibid*., 36.

solidarity, commitment, and sacrifice; a culture that offers the prospect of justice in God's name.[162]

> We want to disseminate the culture of religious commitment (*iltizam*). We insist on culture, because this is what makes identity. Resistance is not an aim, it is the result of a culture.[163]

This identity and culture are not only disseminated formally through Hezbollah's institutions, they also permeate Shi'a society via an extensive social network ranging from women volunteers to local clerics. These social networks are reinforced by media campaigns that broadcast to its power base the core elements of Hezbollah's resistance society: martyrdom, Shi'ism, and the Israeli occupation. The net result is a collective identity that generates a strong sense of belonging, which in turn gives meaning and social importance to Shi'a individuals. The collective product is known as *al-hala al-islamiyya* – the Islamic sphere – and though it, Hezbollah's power and influence are deeply entrenched.[164]

Both a Trans-national and Sub-national Actor

Hezbollah's network extends well beyond Lebanon and even the Middle East. Its operatives have been located in France, Spain, Cyprus, Singapore, the "tri-border" region of South America, the Philippines, and a fundraising cell was even discovered in 2001 in North Carolina.[165]

However, Hezbollah's regional ties to Iran, Syria, and the Lebanese government play a most significant role in the movement's organizational definition and ability to conduct

---

[162] Harb and Leenders, "Know Thy Enemy . . .," 189, 190.

[163] Vice president of Hezbollah's Educational Institute, interviewed by Harb and Leenders, 8 September 1998, quoted in *Ibid*., 190.

[164] Harb and Leenders, "Know Thy Enemy . . .," 190-192.

[165] Daniel Byman, "Should Hezbollah be Next?," *Foreign Affairs* 82, no. 6 (November/December 2003) n.p. [journal on-line]; available from http://proquest.umi.com; accessed 29 March 2008.

netwar. Syria, at odds with Israel over the Golan Heights, emerged as hegemonic regional power in Lebanon following the Israeli 1985 withdrawal to the Security Zone in south Lebanon. The Syrian regime established a Lebanese coalition leadership and attempted to control militant Shi'a Islam in Lebanon; however, Hezbollah, wanting to replace the Lebanese political system with an Islamic state, could not be contained. It was in Syria's national interest to foster an alliance with the Party of God for two reasons: first, it was important to Syria's grand strategy since Hezbollah was sponsored by the Republic of Iran; and second, Syria envisioned the regulation of Hezbollah as a means to apply pressure and influence upon Israel. Syria therefore became a major Hezbollah supporter, furnishing them with Iranian supplied arms, missiles, and rockets. Coincidentally with the evolution of the Syrian relationship, the Lebanese coalition leadership recognized the utility of Hezbollah's presence as a means to pressure Israeli to accept the UN Security Council Resolution (UNSCR) 425, which called upon Israel to immediately cease its military action against Lebanese territorial integrity and withdraw its forces from all Lebanese territory.[166] It was therefore in the Lebanese government's interest to at least tacitly endorse Hezbollah.[167]

As previously stated, Hezbollah is far from a monolithic proxy of Iran. Its relationship with Iran is influenced largely by the impact of Iranian clerical factionalism on its institutions, which is often divergent from the official position and policy of Iran's ruling clerical elite.[168] Strong personal relationships between individual Iranian clergymen and

---

[166] United Nations Security Council Resolution 425 (1978) of 19 March 1978; available from http://domino.un.org/unispal.nsf; Internet; accessed 29 March 2008.

[167] Simon Murden, "Understanding Israel's Long Conflict in Lebanon: The Search for an Alternative Approach to Security During the Peace Process," *British Journal of Middle Eastern Studies* 27, no. 1 (May 2000): n.p. [journal on-line]; available from http://proquest.com; Internet; accessed 29 March 2008.

[168] Ranstorp, "Hizbollah's Command Leadership . . .," 316.

Hezbollah's command leadership have politically intertwined institutions in both the Party of God and the Islamic Republic of Iran. These connections are particularly evident amongst the more radical clergy who hold senior positions within Iran's Ministry of Foreign Affairs, such as the Director of Arab Affairs who placed members of the Pasdaran (Iranian Revolutionary Guards Corps) in Iranian embassies abroad to participate in operations coordinated by Hezbollah's overseas security apparatus. Incidentally, the Pasdaran has proven to be the most reliable and loyal ally of Hezbollah, as it is not only the most radical Iranian institution, but also enjoys relative autonomy from the Iranian civilian political control. This is most apparent in the Pasdaran contingent based in Lebanon, which has provided extensive training, resources and military support to Hezbollah, even in the face of contrary direction from Iran's political leadership.[169]

In addition to Iranian funding for military capacity building, the Hezbollah-Iranian network also incorporates the comprehensive social institutions described in the preceding section. Hezbollah's social services receive significant funding from the Iranian government, religious trusts and from income generated by the confiscation of exiled Iranians' properties. The Iranian Ministry of Islamic Culture and Guidance provides sponsorship to many of Hezbollah's mosques, religious schools, and NGOs such as the Association of the Martyr and the Foundation of the Oppressed. Iran's generous financial support has been essential to Hezbollah's campaign to secure the hearts and minds of the Lebanese Shi'a.[170]

Figure 3 illustrates the network of Iranian institutions linked to Hezbollah, on the political, social and military fronts, all of which are leveraged by this 4GW practitioner to further its grand strategy and build its society of resistance.

---

[169] *Ibid*., 319-322.

[170] *Ibid*., 320-321.

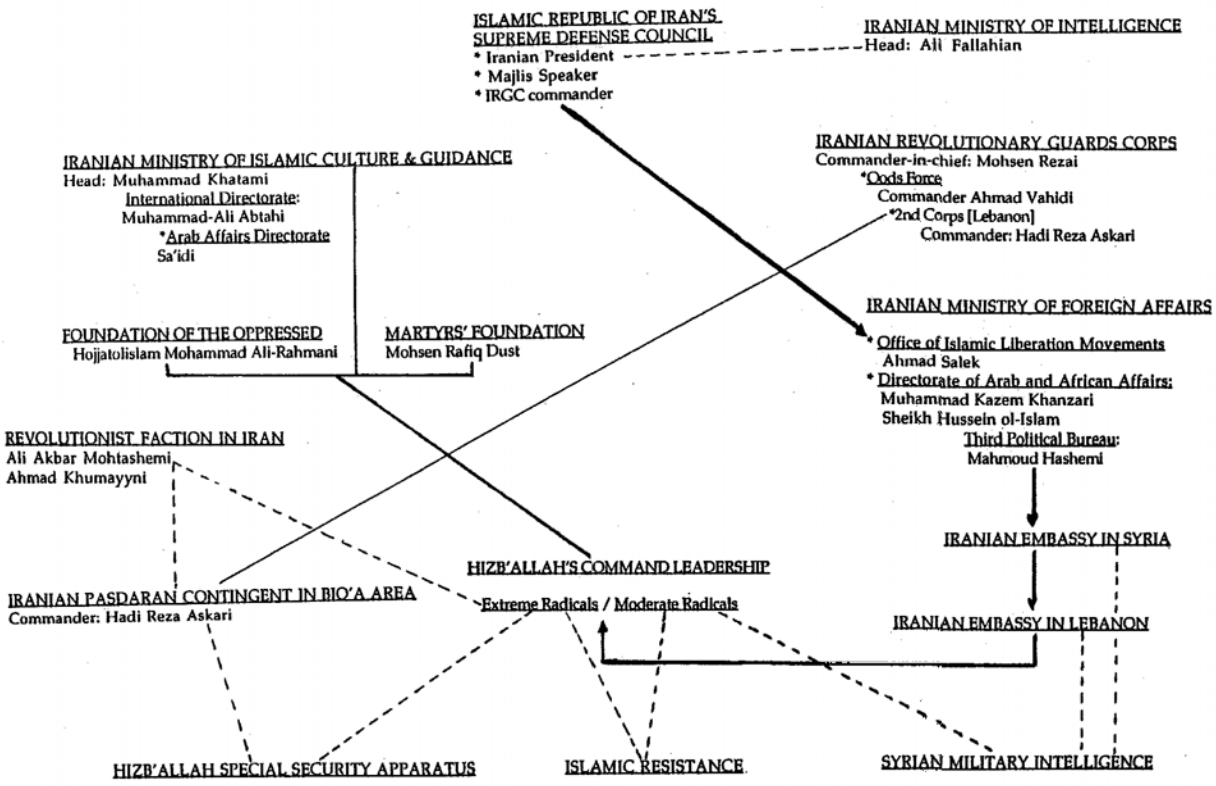

Figure 3 - The Network of Iranian Institutions and Hezbollah
Source: Ranstorp, "Hizbollah's Command Leadership . . .," 318.

Hezbollah and the Information Age

Hezbollah, as a mature netwar actor, is a media-savy organization that leverages information technology as a comprehensive system to propagate its agenda, ideology, and propaganda, enabling its strategic communications campaign to reach a global audience in near real-time.

Visual media has been an important weapon system in Hezbollah's information operations arsenal since the early days of the resistance. Hezbollah has since developed this capability to what must be seen as the envy of militant organizations worldwide. One of the most important components of this system is Hezbollah's television station *al-Manar* (The Beacon). Commencing with broadcasts in 1991, the station has evolved over the years into a

leading news station in the Arab world that is transmitted via satellite worldwide.[171] The station serves as a primary conduit for Hezbollah's messages to its constituents, enemies and neutral audiences, particularly in times of intensified conflict. Similarly, Hezbollah operates a radio station, *al-Nur*, which compliments *al-Manar* by broadcasting five daily Arabic news programs, now downloadable from *al-Nur's* website.[172]

Together these stations provide Hezbollah ready access to not only their subscribers, but also national and international media networks, broadcasting programmes aimed at informing viewers about the nature of Israeli and U.S. societies and politics. *Al-Manar* frequently broadcasts footage of Israeli political discourse, including in-house commentary on the workings of the Israeli legislature and policies regarding the Palestinians. On the lighter side, but in keeping with Hezbollah's ideology, *al-Manar* also broadcasts a prime-time game show that offers the virtual possibility of conquering Jerusalem by answering a series of questions on resistance operations, Islamic thought, the Palestinian cause, Western conspiracies, and Israeli plots. The prize money from this radical *Jeopardy* spin-off is split between the winner and the Palestinian Intifada.[173]

Hezbollah's first website, *hizbollah.org*, appeared in 1996 and since then Hezbollah has expanded its Internet presence to at least fifty active websites that provide the Party of God ". . . with a forum for direct, two-way communication between audiences and

---

[171] Gabriel Weimann, "Hezbollah Dot Com: Hezbollah's Online Campaign," in *New Media and Innovative Technologies*, ed. D. Caspi and T. Azran, 17-38 (Beer Sheva: Ben-Gurion University Press, 2008), n.p. In 2004 Hezbollah was officially listed as a terrorist organization and consequently paid advertisement on *al-Manar*, such as the Coca-Cola commercials that aired on the station in the 1990s, and satellite transmission of *al-Manar's* signal in Europe and North America were banned. For more info on *al-Manar*, visit http://www.almanar.com.lb/NewsSite/News.aspx?language=en.

[172] *Ibid*., n.p.

[173] Harb and Leenders, "Know Thy Enemy . . .," 182.

operatives, according the group an interactive channel for contact with its local and international constituency."[174] Hezbollah maintains websites in Arabic, English, German, and French, which may be broadly classified into six domains based on content. In the first domain Hezbollah operates between six and eight news and information websites that

> . . . provide listings of articles on issues like the influence of Christian fundamentalism on U.S. policies towards Israel, the Jewish lobby in Washington, Israel's evolving notion of national security, Jewish political philosophy, interviews with Israeli academicians and political activists taken from the Israeli press and, indeed, investigations into how the notion of terrorism shapes US foreign policy.[175]

In the second domain several websites provide welfare and social service information to Lebanese Shi'a, reinforcing Hezbollah's social values and channelling social activity towards political and militant commitment. In the third domain Hezbollah websites are devoted to religious education and the presentation of Shi'a religious principles to core cadres and potential converts. In the fourth domain Hezbollah administers several personal websites offering photos, biographies, and selected writings of key party figures. The fifth domain is dedicated to anti-Israeli websites, promoting a narrative of Israeli conquest and occupation, American-Zionist cooperation, and Hezbollah's jihad against colonialism. The sixth domain consists of open online bulletin boards providing virtual connectivity for Hezbollah members and sympathizers. The seventh and final domain targets children and adolescents via online gaming. Hezbollah developed a game called Special Force that simulates terrorist attacks on Israeli targets, based on scenarios derived from actual Hezbollah battles. The game also features a training program in which players can practice their virtual marksmanship on former Israeli Prime Minister Sharon and other Israeli political and military personalities.

---

[174] Weimann, "Hezbollah Dot Com: Hezbollah's Online Campaign," . . . n.p.

[175] Harb and Leenders, "Know Thy Enemy . . .," 183.

The game ends with a tribute to Hezbollah martyrs, giving the young player a sense of the resistance.[176]

Hezbollah's presence on the Internet has been remarkably resilient to Israeli and American hackers for reasons elaborated on in Chapter Two. Interestingly, when Hezbollah sites were assaulted virtually by Israeli hackers, Hezbollah hijacked the websites of cable service providers in south Texas and Virginia as well as web hosting servers in Delhi, Montreal, Brooklyn, and New Jersey by adding an extension to their Internet Protocol addresses. This permitted Hezbollah to then run recruitment videos, post *al-Manar's* feed online, and post bank account numbers for sympathizer donations. While many Hezbollah sites have moved to Dubai-based servers, some continue to operate from U.S. and Canadian-based servers.[177]

As stated in Chapter Two, netwar is not simply a function of the Internet; it is not solely about Internet war. That said, Hezbollah has proven to be a master of leveraging information technology and its media empire, including the Internet, to broadcast propaganda, conduct psychological operations, and communicate its messages to a global audience.

---

[176] Weimann, "Hezbollah Dot Com: Hezbollah's Online Campaign," . . . n.p. For more information on the computer game Special Forces, see the article at http://www.worldnetdaily.com/news/article.asp?ARTICLE_ID=31323

[177] *Ibid*., n.p.

HEZBOLLAH'S NETWAR

David Becomes Goliath: The 2000 Israeli Withdrawal from South Lebanon

> *The Hezbollah fighter wakes up in the morning, drinks his coffee, takes a rocket out of his closet, goes to his neighbour's yard, sticks a clock timer on it, goes back home and then watches CNN to see where it lands.*[178]

The Israeli invasion of Lebanon in 1982 met the operational objective of routing the Palestine Liberation Organization; however, the unanticipated second and third order effects of the invasion drew Israel into a long and costly quagmire of an insurgency led by the emergent Hezbollah. A seemingly relentless campaign of guerrilla and terrorist attacks aimed at ousting the Israeli Defence Force (IDF) from the country forced a withdrawal into southern Lebanon in 1985. The IDF established a security zone encompassing ten percent of Lebanon and was determined to remain there until the security of Israel's northern border could be underpinned with some guarantees against terrorist border incursions and rocket attacks from Lebanon. This occupation, a clear rejection of UNSCR 425, resulted in the IDF and its ally, the South Lebanon Army (SLA), adopting a static defence of fortified company-sized outposts throughout the zone.[179]

Hezbollah, determined to drive the IDF back into Israel, developed an operational plan to:

> . . . stampede the Israelis and the SLA into as disorderly and costly a withdrawal as possible by imposing casualties that further eroded the troops' morale and increased domestic pressure for their departure. Strategists

---

[178] LTC Ishai Efroni, Deputy Commander, Baram Brigade, quoted in Matt M. Matthews, *We Were Caught Unprepared: The 2006 Hezbollah-Israeli War*. The Long War Series Occasional Paper 26 (Washington, DC: CSI Press, 2008), 33 [electronic publication]; available from http://usacac.army.mil/CAC/csi/RandP/CSIpubs.asp; Internet; accessed 29 March 2008.

[179] Matthews, *We Were Caught Unprepared* . . . , 7.

> therefore aimed at clever operations that would emphasize Hezbollah's implacability and long reach and demonstrate the enemy's vulnerability.[180]

Key to Hezbollah's successful implementation of this plan would be the strategic communications campaigns supported by guerrilla and terrorist operations that typify 4GW. Hezbollah had developed considerable experience in information operations as was demonstrated in 1997 when Hezbollah communications experts uncovered an Israeli plot to infiltrate a force of elite naval commandos into Lebanon in order to kidnap or assassinate a Hezbollah party member. Not only did Hezbollah ambush and annihilate the force as it made its way into Lebanon, but a Hezbollah camera crew provided video footage of the incident to the international media. The video was a "propaganda coup" for Hezbollah as they were able to brand the covert Israeli operatives as terrorists caught in the act of a presumed kidnapping or assassination attempt.[181]

In keeping with the design of their operational plan, Hezbollah continued to engage the IDF and SLA in the security zone through similar tactical strikes that achieved operational effects in support of Hezbollah's strategic purpose. By March of 1999, Israeli citizens had grown weary of over twenty years of conflict in Lebanon and Hezbollah, according to plan, was capitalizing on the "increased domestic pressure."[182] Martyrs in action, sophisticated ambushes, and resistance assaults on the IDF and SLA positions were sste in iositiD 81ƀBDC BT/TT0 0001 Tc 410.0023 Tw ppolth0l-M pponarositiD 8 ƀBDC BT/. Bya

television."[183] Israeli antiwar groups, politicians, and citizens called for the unilateral withdrawal from Lebanon, compelling the Prime Ministerial candidate Ehud Barak to endorse this sentiment as a campaign promise, which, he assured the Israeli people upon his election in 1999, he would affect within twelve months of assuming office.[184]

Twelve more months of occupation were twelve too many for Hezbollah. Conscious of the opportunities presented by the SLA's crashing morale, Hezbollah attempted to dislocate the SLA by advertising leniency to all SLA members who surrendered prior to the commencement of the withdrawal. Concurrently, the tempo of assaults on the IDF and SLA positions in the security zone increased amidst SLA defections, increasing the pressure to withdraw.[185] These defections became a serious matter for the Israelis to contend with as they precipitated the closure of SLA outposts in the vicinity of the large Christian town of Jezzine and the subsequent disorderly withdrawal of SLA militiamen into the depth of the security zone in June 1999.[186] The security zone was beginning to shrink as the IDF hunkered down in a handful of heavily fortified positions, leaving the majority of them to the SLA.

Even the fortifications failed to dissuade Hezbollah's efforts to erode the enemy's morale and expose its vulnerabilities as they fired tube-launched, optically-tracked, wire-guided (TOW) anti-tank missiles into the narrow slits of the bunkers. Adding insult to injury, the American-made TOWs were reportedly supplied by Israel to Iran in the 1980s as

---

[183] Norton, "Hizbollah and the Israeli Withdrawal from Southern Lebanon,". . . 31.

[184] Augustus Richard Norton, *Hezbollah: A Short Story* (Princeton: Princeton University Press, 2007), 88.

[185] Matthews, *We Were Caught Unprepared* . . . , 9.

[186] Harik, *Hezbollah: The Changing Face of Terrorism*, 126-127.

part of the Iran-Contra deal.[187] The number of Israeli casualties to TOW missile attacks (less than seven in January and February of 2000) was far less significant than the psychological effect on the IDF and the Israeli people watching the footage in their homes.

On 30 January 2000, despite heavy security precautions, the SLA's second highest ranking officer, Colonel Akl Hashim, was assassinated in his home in the security zone by a Hezbollah bomb. A week later, Israeli news stations repeatedly broadcast Hezbollah video footage of an ambush that resulted in not only the deaths of several IDF soldiers, but also the death of the medic trying to save them. Three weeks later, regional newscasts aired another Hezbollah video of the assassination of Brigadier General Eretz Gerstein, the commander of all Israeli forces in south Lebanon, whose convoy was targeted by a roadside bomb attack. Hezbollah was demonstrating more than guerrilla prowess; it was sending a strategic message to Israel that no Israeli soldiers were safe so long as they remained on Lebanese soil.[188]

The message was received. By March 2000, Prime Minister Barak announced that "by July 2000, the army will withdraw to the international border, and it is from the international border that we will defend the north of the country."[189] The announcement further discouraged the SLA and by 21 May the SLA began to disintegrate as their center brigade collapsed, abandoning their positions in fear of being left to the Hezbollah. The IDF was forced to accelerate its withdrawal timetable as the SLA withdrew, or surrendered, destroying their bunkers and outposts as they fled. *Al-Manar* televised the withdrawal for the

---

[187] Norton, "Hizbollah and the Israeli Withdrawal from Southern Lebanon,". . . 30.

[188] Harik, *Hezbollah: The Changing Face of Terrorism*, 131.

[189] Prime Minister Ehud Barak, quoted in Norton, "Hizbollah and the Israeli Withdrawal from Southern Lebanon,". . . 31.

world to witness. By 23 May the disintegration of the SLA was complete with the eastern and western brigades collapsing to the Israeli border. The IDF abandoned much of its military equipment as it withdrew while Hezbollah planted triumphant yellow flags atop each of the vacated outposts.[190]

The Israeli retreat from Lebanon was a complete fiasco as Hezbollah stampeded them into as disorderly and costly a withdrawal as possible. Hezbollah's protracted resistance to a militarily and economically superior nation-state exemplified 4GW as cells totalling at any given time only about 500 Hezbollah fighters wore down Israel over the years and begot ". . . the collapse of what had been a corps of 1500 well-armed Israeli regulars and 2,500 SLA militiamen."[191]

A FINAL NOTE ON HEZBOLLAH AS A 4GW ACTOR AND ITS NETWAR OF 2000

In 2000, Israel suffered a rout at the hands of a 4GW adversary. Hezbollah is clearly a movement that boasts a complex organizational design that is a hybrid of a trans-national network coexisting with a core hierarchy that extends to a loosely structured system of committees and fluctuating operational cells. Hezbollah's organizational design is sustained by a winning narrative and a well-defined doctrine of psychological operations, which is enabled by advanced information technologies and rests on the strong ties of the comprehensive social networks at its base. Hezbollah aptly leveraged all available networks – political, social, military, and economic – to conduct a strategic communications campaign, supported by guerrilla and terrorist operations, to convince Israel that continued occupation of the security zone was too costly for any perceived benefit.

---

[190] Matthews, *We Were Caught Unprepared . . .* , 11.

[191] Harik, *Hezbollah: The Changing Face of Terrorism*, 132.

CHAPTER 4
STUDENTS OF THE FOURTH GENERATION

Where an Army cannot pass, a donkey laden with gold often will.[192]

While Hezbollah may be the A-Team of 4GW adversaries, its principle utility in the context of this paper is to illustrate the complexity of a netwar actor's organization and the effectiveness of its *modus operandi* – an evolved form of insurgency, empowered by the Information Age, that leverages all available networks in a strategic communications campaign supported by guerrilla and terrorist operations – to defeat the political will of militarily and economically superior nation-states. By contrast, Western powers, led by the mighty war machine of the U.S., have by and large focussed their vision of warfare for the last three decades on the European concept of conventional battlefield dominance over near-peer competitors. The great danger to this conceptual disparity is exasperated by Western initiatives to improve upon this forte, believing that a capabilities-based approach to defence will enhance existing second and third generation capabilities sufficiently to defeat all-comers, including those of the fourth generation such as Hezbollah.

The aim of this final chapter is to examine the merits of emerging concepts that are being developed to combat the asymmetric, irregular, unconventional opponents that are frustrating nation-states in the complex conflicts of today and those forecast in the coming decades. The influence of netwar actors and the fourth generation are clearly evident in these concepts; however, this chapter will also highlight the magnitude of the challenges confronting the contemporary militaries and nation-states aiming to adopt concepts based on netwar organizational designs and strategies.

---

[192] Phillip II, father of Alexander the Great quoted in van Creveld, *The Transformation of War*, 212.

The Canadian Army and the Future Security Environment

Key to a nation's ability to succeed in the future security environment is its evaluation of the future threat. The good news is that rise of unconventional conflict and the decline of inter-state warfare as described in Chapter One has been formally recognized by the Canadian Army in its guide for Land Force development, *Land Operations 2021*. Not only has the reality of today's asymmetrical security environment been recognized as the likely norm for future conflict, but the publication also heeds Colin Gray's caution regarding the perils of prediction, conceding that the prospect of contemporary warfare, while improbable, is not entirely obsolete. The result is a well balanced perspective of the challenges confronting Western nations today and well into the near future:

> While the prospect of inter-state war will not disappear, the future challenges will be more diverse – with asymmetric attacks launched by transnational terror groups, and the political instability, civil war and humanitarian crises characteristic of fragile countries making up the lion's share of turmoil in the early 21st century.[193]

The capstone document goes on to describe the nature of future adversaries, acknowledging the rise to dominance of the characteristics attributed in Chapter One to the Fourth Generation warrior:

> Increasingly, the likelihood of large force-on-force exchanges will be eclipsed by irregular warfare conducted by highly adaptive, technologically enabled adversaries; media-savvy foes intent less on defeating armed forces than eroding an adversary's will to fight, rogue states bent on challenging the status quo, and transnational criminal organizations ready, willing and able to but, sell, and trade everything from drugs to armaments for their own gain.[194]

---

[193] Department of National Defence, B-GL-310-001/AG-001 *Land Operations 2021: Adaptive Dispersed Operations, The Force Employment Concept for Canada's Army of Tomorrow* (Ottawa: DND Canada, 2007), 4.

[194] *Ibid*., 4.

The consequence of this evaluation of the future security environment is that the operating concept for Canada's Army of Tomorrow must seek to

> . . . create and sustain operational advantage over adept, adaptive, adversaries through the employment of . . . networked and integrated land manoeuvre forces – supporting and supported by [Joint, Interagency, Multinational, Public] effects – alternatively dispersing and aggregating over extended distances to identify, influence, and defeat full spectrum threats throughout the multidimensional battlespace.[195]

The parallels in the articulation of this operating concept to the networked nature of 4GW adversaries and the swarming doctrine of netwar are clearly evident. These parallels are not all that surprising as Martin van Creveld explains that the outcome of any drawn-out conflict has always been a mutual learning process, as belligerents who may have been originally very dissimilar come to gradually resemble one another, first in tactics and then in other respects. Van Creveld illustrates this explanation by citing the 1989 Israeli kidnapping of three Hezbollah leaders in Lebanon, thus implying that he who fights terrorists for any period of time risks becoming one himself.[196] That is not to say that the Canadian Army is about to embrace terrorist or even guerrilla tactics in the future. What it does suggest is that the Canadian Army is learning from its own military experiences, history, and observable trends emerging from David-versus-Goliath insurgencies and it recognizes the requirement to adapt and engage 4GW threats in the future security environment using very the same political, social, economic and military networks that the netwar adversary has thus far exploited to his advantage.

---

[195] *Ibid*., 18, 19.

[196] van Creveld, *The Transformation of War*, 195, 201.

EVOLVING TO COUNTER NETWAR

Adaptive Dispersed Operations

In response to the evaluation of the emergent threat in the future security environment, the discussion of Adaptive Dispersed Operations (ADO) has become de rigueur in the Canadian Army. ADO aims to ". . . provide the [military] commander with enhanced capability to create operational and strategic level effects through the use of dispersed teams able to make rapid decisions in order to achieve the commander's desired end state."[197] ADO relies on *adaptive forces* that are agile, lethal and non-lethal, net-enabled, and multipurpose across the full spectrum of conflict, illustrated in the common doctrinal representation below, from peacetime military engagements to major combat operations.

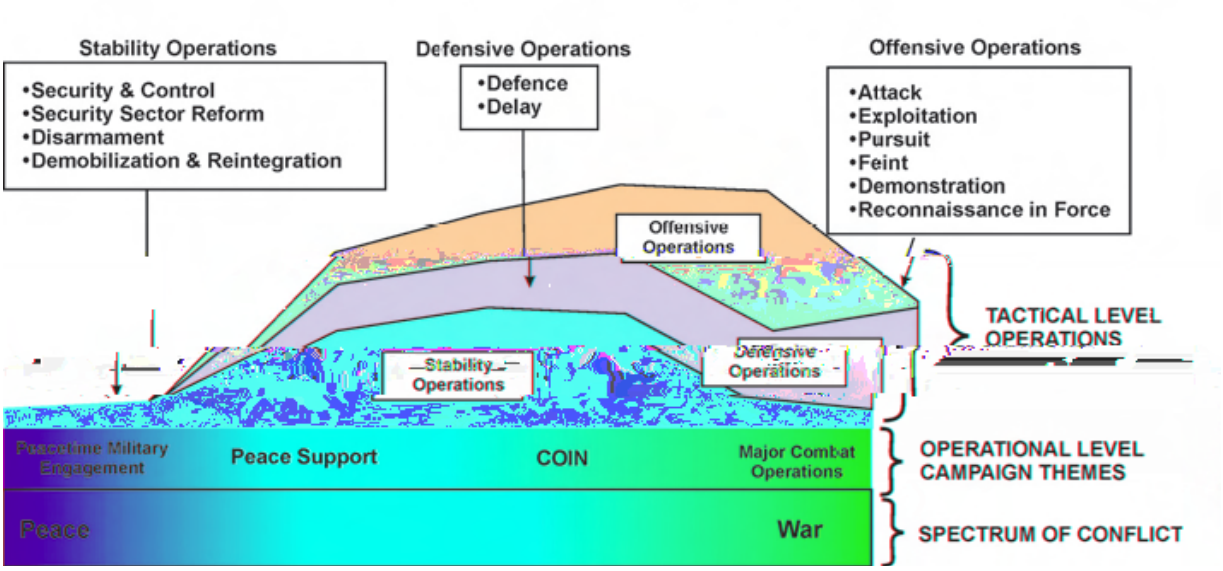

Figure 4 - The Spectrum of Conflict
Source: Department of National Defence, B-GL-310-001/AG-001 *Land Operations 2021* . . . , 7.

[197] Department of National Defence, B-GL-310-001/AG-001 *Land Operations 2021* . . . , 22.

Agile forces are capable of planning, executing, and reacting faster than the adversary. Operating across the full spectrum of conflict, the ability to achieve both lethal and non-lethal battlespace effects at the time and place of one's choosing is deemed of paramount importance to success in the future security environment. These effects are to be enabled by a network of joint sensor, fire support, and command and control (C2) systems linked to create an acute level of situational awareness and mobility that combine to overwhelm the adversary's cognitive awareness and ability to react. The agile forces that deliver these effects will be founded upon leading edge technologies that enhance their deployability, mobility, survivability, lethality, and modularity, thereby ensuring their multipurpose employability in support of a whole-of-government campaign plan.[198]

ADO will employ these adaptive forces, dispersed in terms of time, space, and purpose, throughout a non-contiguous battlespace to create effects and exploit opportunities. "The essence of ADO is the ability to conduct coordinated, interdependent, full spectrum actions by widely dispersed teams across the moral, physical and informational planes of the battlespace, ordered and connected within an operational design created to achieve a desired end state."[199]

The ability to disperse land forces across the battlespace will provide the commander with many of the same advantages a netwar adversary exploits through the doctrine of swarming introduced in Chapter Two. Recall that as a natural doctrine for networked organizations, swarming is the ". . . systematic pulsing of force and/or fire by dispersed,

---

[198] *Ibid*., 18.

[199] *Ibid*., 18.

internetted units, so as to strike the adversary from all directions simultaneously."[200] Swarming forces may be widely dispersed, but internetted such that they can swiftly come together to concentrate kinetic or non-kinetic actions on selected or opportune targets from all directions. Swarming relies on two fundamental requirements: a large number of tightly internetted small units of manoeuvre; and the capability of those forces to not only strike, but also sense, providing operational and strategic awareness.[201] Similarly, the dispersed forces in ADO will develop a greater understanding of the battlespace through the enhanced capability to collect information, while enabling the commander to find, fix, and strike lucrative targets at the time and place of his choosing.[202] The synchronization of these dispersed forces to sense and prosecute effects will rely heavily on the functional concept of Network Enabled Operations discussed in the following section.

Network Enabled Operations (NEOps)

The U.S. concept of networked operations is called Network Centric Warfare (NCW) and it ". . . seeks to maximize advances in information technology in military operations by linking all sensors, platforms, and decision makers through an integrated system of robust networks, thereby lifting the fog and friction of war."[203] Seizing upon the potential of NCW as a central concept for shaping military transformation to address the emergent threats in the future security environment, Canada is developing its own functional concept ". . . that has the potential to generate increased combat power by networking sensors, decision makers

---

[200] Arquilla and Rondfeldt, *Swarming and the Future of Conflict*, 8.

[201] *Ibid*., 22.

[202] Department of National Defence, B-GL-310-001/AG-001 *Land Operations 2021* . . . , 21.

[203] Michael H. Thompson and Barbara D. Adams, *Network Enabled Operations: A Canadian Perspective*, Report Prepared for the Defence Research and Development Canada – Toronto (Guelph: Humansystems Incorporated, 2005), 3.

and combatants to achieve shared battlespace awareness, increased speed of command, higher operational tempo, greater lethality, increased survivability, and greater adaptability through rapid feedback loops."[204] This Canadian concept, which is deemed key to ADO, is called Network Enabled Operations and it is founded on the following basic tenets:

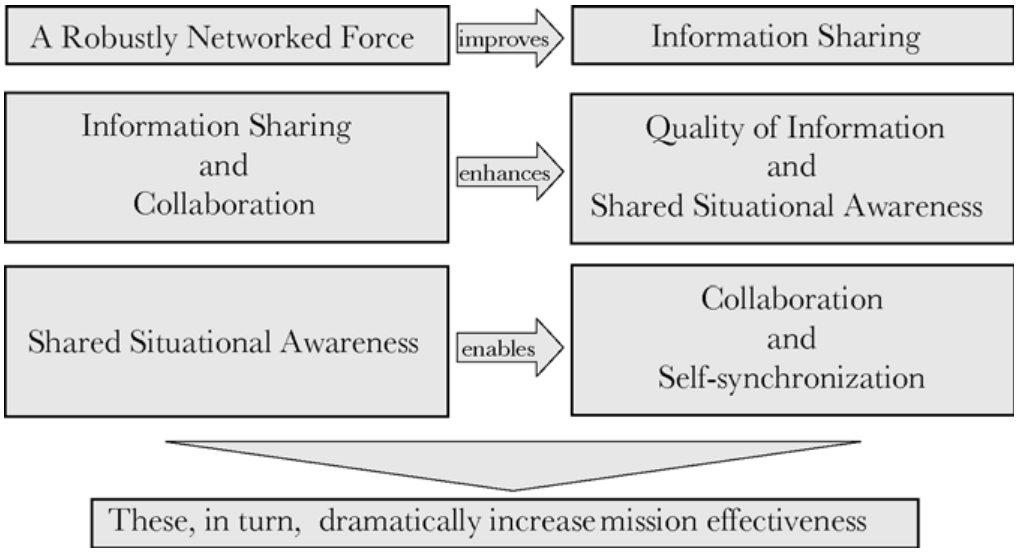

Figure 5 - The Tenets of NEOps
Source: Alberts and Hayes, *Power to the Edge* . . ., 108.

From Figure Five above, it is clear that a networked enabled operation requires first and foremost a robustly networked force. Such a force can only be achieved if there is a high level of interoperability – the ability to work together, to communicate, to share information, and to collaborate with one another – among the mission participants and the systems that support them. Consequently, the effectiveness of NEOps, and by extension ADO, is directly related to the degree of interoperability among not only the military forces, but all of the other government and non-governmental organizations participating in the mission. To achieve the highest level of interoperability, all players must be connected to the net, they must be able to post information to those on the net, they must be able to find, retrieve, and

[204] *Ibid*., 5.

understand the information drawn from the net, and they must be able to participate in collaborative processes via the net. A lack of connectivity or limited interoperability will result in the marginalization of entities as they are less able to contribute to mission effectiveness.[205]

In the military context, NEOps offers considerable benefits that promote its ultimate objective of increasing mission effectiveness. The primary effect of NEOps is an increase in shared situational awareness, the ability to regularly translate information and knowledge into a common understanding, or a common operating picture among the forces. This common operating picture provides dispersed forces with access to high quality information with minimum latency, thereby compressing decision-making cycles, increasing the speed of command, increasing the tempo of operations, and ultimately disrupting the adversary's ability to react to the evolving situation. A critical component to the common operating picture shared across the network is the complete understanding of the commander's intent. Knowing the higher commander's promulgated common intent will allow ". . . individual unit commanders to synchronize their unit's individual efforts in order to mutually support other commander's units, and accomplish the overall shared goal."[206] This ability is termed self-synchronization and it implies that dispersed forces will be able to operate almost autonomously, re-tasking themselves based on shared situational awareness and knowledge of the commander's intent. NEOps also offer dispersed tactical forces the capability to "reach-back" and access valuable resources such as databanks, intelligence, and imagery despite physical separation from operational or even strategic information sources. The

---

[205] Alberts and Hayes, *Power to the Edge* . . ., 107-108.

[206] Thompson and Adams, *Network Enabled Operations* . . ., 10.

corollary to reach-back is "reach-forward", which is the ability of commanders far removed from tactical operations to leverage the network infrastructure to monitor tactical events as they unfold in near-real time. Finally, NEOps offers commanders a capability beyond information superiority; it provides commanders with the capability to successfully translate superior information into knowledge upon which sound and timely decisions can be based.[207]

Joint, Interagency, Multinational, Public (JIMP) Effects

For the NEOps concept to "dramatically increase mission effectiveness" as envisioned, it must be inextricably linked to the JIMP framework. Military operations increasingly require coordinated joint efforts across the environmental services, cooperation with other agencies, and multinational collaboration to achieve effective results, particularly in 4GW campaigns. Military power alone will simply be insufficient to achieve national objectives. All instruments of power – diplomatic, economic, military, and informational – will be required to be brought to bear in the complex, unconventional, asymmetric conflicts on the horizon. Arguably, this realization was arrived at decades ago as non-state 4GW actors began leveraging the political, economic, military, and social networks as part of their insurgencies to take on nation-states.

The Canadian Forces requires an enhanced ability to operate in the framework illustrated in Figure 6 below. The broad notion of a harmonious framework such as this infers that all partners will benefit from the prospects of increased cooperation and the development of unity of purpose across the diverse constituents.

---

[207] *Ibid*., 8-12.

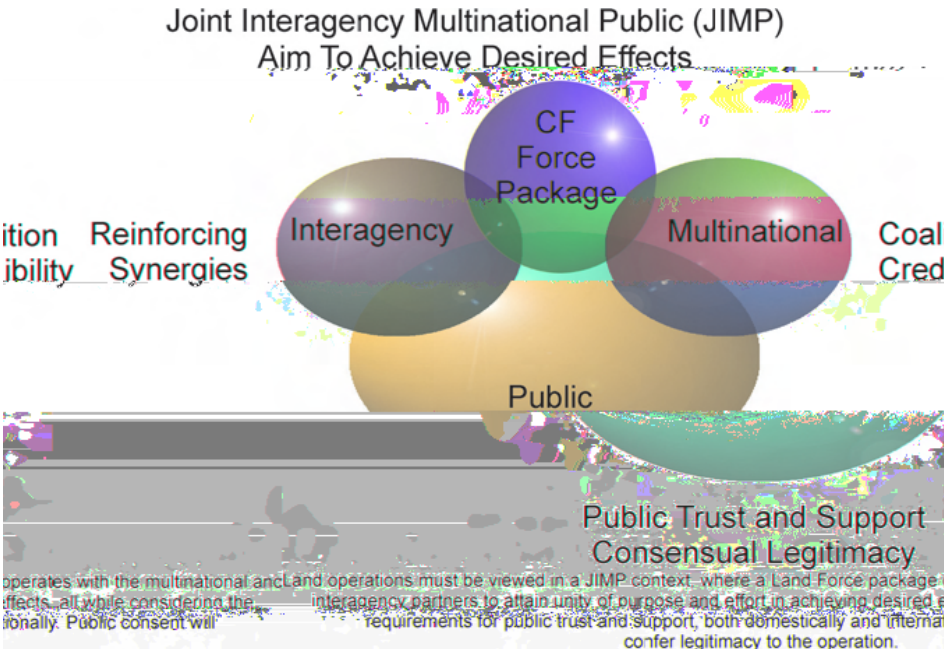

Figure 6 - JIMP Framework
Source: Department of National Defence, B-GL-310-001/AG-001 *Land Operations 2021* . . . , 7.

The JIMP framework compliments Canada's comprehensive whole-of-government approach to operations, recognizing that the Canadian Forces will participate to varying degrees in all aspects of such an approach – diplomatic, defence, development, and commerce. These aspects, aligned with the resources and influence of countless other agencies, will be integrated into a campaign plan to achieve a shared end state. In addition to integrating governmental and non-governmental agencies into the operational architecture, the JIMP framework seeks to embrace a network that 4GW practitioners, such as Hezbollah, have learned to exploit to great advantage: the public media. The incorporation of the media serves to effectively communicate mission goals, objectives and actions to the public, thereby promoting a culture of transparency, legitimacy and ultimately insulating the campaign from propaganda.

Ultimately, the JIMP framework will provide the mechanism to permit the "donkey laden with gold" to pass where the Army cannot. It is envisioned that NEOps will enable this

framework by offering ". . . the means to improve the ways that people throughout the system (i.e. the soldier, the diplomat, and the developer) work together, promoting information sharing and greater cooperation in a variety of defence, diplomatic, and developmental contexts."[208]

RHETORIC OR ROADMAP?

Earlier in this chapter, it was pointed out that the good news was that the Canadian Army has formally recognized the rise of unconventional conflict and the decline of inter-state warfare in *Land Operations 2021*. And it certainly is good news that the concepts that fall out from this recognition reflect the agility, robustness, resilience, responsiveness, flexibility, innovation, and adaptation required by forces pitted against netwar adversaries in the future security environment. But are these concepts truly achievable? Can conventional forces and nation-states effectively prosecute netwar or even combat against it? The challenges that confront these concepts are significant and a failure to address them will result not in the paradigm shift suggested by ADO; rather, it will exchange the roadmap for transformation to The Army of Tomorrow for rhetoric, cloaking technologically enhanced second and third generation capabilities.

Challenges to ADO

While the technological capability to execute ADO is essentially available, the challenges to this dynamic and decentralized doctrine lie primarily in the human and social domains. The requirement for dispersal means that relatively junior leaders must make rapid and bold decisions based on the principles of mission command; that is to say, decision-making must be decentralized through common situational awareness and a clear

[208] *Ibid*., 5.

understanding of the commander's intent in order to effectively disrupt the adversary's decision-action cycle and create opportunities for exploitation.[209] Given the military culture of clear chains of command, one has to wonder if the organization is prepared to devolve the requisite authority and trust to junior leaders to make those bold and rapid decisions.

The U.S. Marine Corps have recently experimented with dispersed operations in Iraq and a *Marine Corps Gazette* article concludes that the Marines are not yet ready for this doctrine due to localized rules of engagement and command restrictions. Tactically dispersed manoeuvre units are currently hamstrung by the very technology that is intended to enable dispersed operations. The capability to "reach-forward", which promises to be a very powerful tool to enhance a higher commander's situational awareness, has resulted in a dangerous level of micromanagement superimposed upon tactical elements. This is explained simply as human nature: if a decision-maker is required to authorize a kinetic action, he'll naturally want to know why he has been asked to do so, who the action is targeting, where the action will occur, how it will unfold, the potential collateral damage associated with the action, and if the action satisfies his superior's criteria for execution.[210] Essentially, the kill chain[211] is elongated such that decisions to execute kinetic actions must be solicited through multiple levels of a hierarchical command structure and the inherent advantages of dispersal, primarily agility, are effectively negated. Restrictive rules of engagement, restraints on authority, and the very military ethos of responsibility and

---

[209] Department of National Defence, B-GL-310-001/AG-001 *Land Operations 2021* . . . , 21.

[210] Major Michael D. Grice, "Distributed Operations: Is the Marine Corps Ready?" *Marine Corps Gazette* 92, no. 3 (March 2008), 21 [journal on-line]; available from http://proquest.umi.com/pqdweb?RQT=318&pmid=27962; Internet; accessed 6 April 2008.

[211] The "kill chain" is a U.S. Air Force analogy to the process of Find, Fix, Track, Target, Engage, Assess.

accountability fettered by the chain of command are anathema to the concept of truly dispersed operations.

The U.S. Air Force has turned to high-tech solutions to compress its kill chain and despite great success with data processing links, enhanced multi-mission platforms, and web-based situational awareness software, it has not been able to overcome the cultural stovepipes of the intelligence, space, surveillance, reconnaissance, and communications communities that contribute data to a Joint Force Commander. Each of these communities has its own systems and methods that are guarded almost tribally, creating seams across which data cannot flow freely.[212] Add to these cultural barriers the centralized command authority to prosecute individual targets using air power and optimization of the kill chain will never be realized.

Overcoming these challenges will demand a significant cultural shift in military leadership; a shift that is not required of Hezbollah or other 4GW adversaries who are not so constrained culturally or organizationally. In the interim, since ADO is grounded in manoeuvre warfare theory and an effects-based approach,[213] what has been accomplished is the technological "advancement" of the commander's ability to tactically orchestrate third generation manoeuvre from afar to efficiently achieve a desired effect. What has not been realized is the ability to distribute decision-making amongst a dispersed force in order to achieve self-synchronization.

Another potential drawback to ADO is the doctrinal requirement for dispersed forces to maintain local superiority over the adversary. While it is clearly advantageous to be able

---

[212] Adam J. Herbert, "Compressing the Kill Chain," *Air Force Magazine Online* 86, no. 3 (March 2003) n.p. [electronic publication]; available from http://www.afa.org/magazine/March2003/0303killchain.asp; Internet; accessed 6 April 2008.

[213] Department of National Defence, B-GL-310-001/AG-001 *Land Operations 2021* . . . , 21.

to disperse and aggregate forces in response to the changes in the tactical environment, the proposed concept suggests that:

> . . . in situations where the adversary can locally mass more combat power than the dispersed force . . . the potential threat to a dispersed force would outweigh the potential gain and the force would operate aggregated. Given the inherent risks of operating in a dispersed posture, a dispersed element should overmatch the adversary it is likely to encounter in terms of firepower, mobility, protection, information, and leadership. For example, in situations where local overmatch is unlikely at the team or section level, dispersion should be limited to the platoon or company level.[214]

This demonstrates a degree of general risk aversion and a first generation reliance on mass to dominate an adversary. This was certainly not a doctrine espoused by Hezbollah when it forced the Israeli withdrawal from the security zone in 2000. In fact, Hezbollah fighters were effectively outnumbered by about 8:1 throughout the entire campaign. This illustrates a significant divergence between the swarming doctrine of netwar actors and ADO, where the former is a seemingly amorphous and sustained pulsing attack from all directions by small networked units and the latter is more akin to a dispersed economy of effort, massing a concentration of force to overmatch a local adversary at a particular time and place. The comparative analogy of *Go* to chess introduced in Chapter Two comes to mind when this divergence is conceptualized.

Developing ADO to its fullest potential implies, among other things, dramatic changes in current military organizational structures. From command and control of line units to logistics, profound shifts will have to occur to nurture this concept. Such shifts, though monumentally challenging, would give a networked ADO force a deliberately

---

[214] *Ibid*., 21.

structured, coordinated, strategic way to strike from all directions, kinetically or non-kinetically, from close-in as well as from stand-off positions.[215]

Challenges to JIMP

To respond to 4GW adversaries in the JIMP framework requires a genuine, effective interagency process.[216] That process is yet to have emerged in the Canadian context. As a result, there is a risk that the instruments of Canada's national power will be applied in an uncoordinated and disjointed fashion. In the absence of a process that articulates a unifying strategy, government departments are contained within their stovepipes, working towards their self-defined objectives, at times even at cross purposes with other agencies. In order to effectively engage a 4GW adversary across the political, military, economic, and social domains leveraged in a netwar, Canada must develop a mechanism to coordinate a comprehensive whole-of-government response. Hezbollah has such a mechanism in the form of the Executive Shura, which strategically administers military, social, political, financial, information and judicial affairs as well as the party's ideology.

The Canadian approach in Afghanistan to integrate diplomatic, defence, and developmental efforts is on the right track at the tactical and even operational levels; however, it is challenged at the strategic level by the stovepipes of DFAIT, DND, and CIDA as they preserve their bureaucratic functions, adhere to rigid personnel policies, and remain driven by budgetary process.

These stovepipes lead to one of the most significant challenges to operating within the JIMP framework: building trust amongst the various governmental departments and

---

[215] Arquilla and Rondfeldt, *Swarming and the Future of Conflict*, vii.

[216] Hammes, *The Sling and the Stone . . .*, 227.

agencies. To this end, the social network becomes far more important than a technologically enabled network as the huge cultural differences that exist between governmental departments can only be overcome by establishing personal relationships, reputations, and a recognizable shared purpose. Unfortunately, the development of NEOps, the functional concept that will enable the soldier, the diplomat, and the developer to work together, was developed ". . . largely in isolation, without substantive interagency involvement, which is, ironically, exactly counter to what the idea entails."[217]

High-Tech versus the Right-Tech

In the last decade the world's most technologically sophisticated militaries have been confronted by three seemingly primitive foes in Lebanon, Afghanistan and Iraq – and have failed to win on all three occasions. Technology has driven militaries to develop networked platforms, sensors, and capabilities that have focussed on accelerating the kill chain to mere instants. The problem with this network-enabled process of killing is that it only provides technological solutions to problems at the tactical level of war. It does not provide solutions to the complex political, economic and social aspects of 4GW conflicts.[218]

Unlike the U.S. concept of NCW, which overtly seeks to maximize advances in information technology in military operations, the Canadian concept of NEOps places a greater emphasis on the human elements and the need for cooperation and collaboration.[219] This recognition that netwar extends well beyond information technology and well into the

[217] Thompson and Adams, *Network Enabled Operations* . . ., 15.

[218] Hammes, *The Sling and the Stone* . . ., 191.

[219] Thompson and Adams, *Network Enabled Operations* . . ., 6.

domain of social networks has been exemplified by Hezbollah and serves as a reminder for Canada to resist getting drawn into the quest for technological dominance.

The systems of Western militaries are without a doubt the most powerful, most capable, and most technologically advanced in the world and their potential to amass information from across the spectrum of emissions continues to grow. But this technological prowess does not translate directly into inherent tactical, operational or strategic advantage due largely to the antiquated hierarchical organizational design of Western militaries.[220]

Will the transformation of the Canadian Forces to meet the threat in the future security environment be driven by the high-tech evolution of systems, or will the leadership of the Canadian Forces pursue "the right-tech" solutions to enable transformation of the organization, pushing power to the edge[221] and integrating other agencies? If the former is allowed to flourish, high-tech systems will continue to provide militaries with incredible means to achieve tactical level victories. But in the complex conflicts of the fourth generation, strategic victory is *not* the sum of incredible tactical victories.[222] The incorporation of technologies must support the strategic imperatives of today's conflicts, which are typically low-tech, protracted, man-power intensive struggles vice futuristic high-tech precision engagements or rapid-decisive operations. For those that espouse high technology as a panacea, they tempt the fate of winning battles but losing wars. Technology may be the answer, but what was the question?

---

[220] *Ibid*., 192.

[221] The hierarchical organization is a centralized status-power topology with a small but powerful center, a significant middle that serves to operationalize command and exercise control, and an edge that has very limited means and opportunity (power). See Alberts and Hayes, *Power to the Edge* . . ., 176.

[222] Hammes, *The Sling and the Stone* . . ., 191.

Organizational Design

Arquilla and Ronfeldt posit that "it takes networks to fight networks."[223] This infers that to defend or disrupt a netwar adversary, nations may have to adopt similar netwar organizational designs and strategies. This does not mean mirroring the adversary; governments cannot, and should not, attempt to reject all hierarchies in favour of full-matrix networks simply because an adversary such as al Qaeda has exploited their use with great success. It does mean that organizational designs in the JIMP framework should benefit from the principles demonstrated by netwar actors and embrace the advantages of networks and the information age in hybrid interagency architectures. These principles will depend not only on technological innovation, but also on a willingness to innovate organizationally, culturally, and doctrinally.[224]

Unfortunately, military and government hierarchies are by their very nature impediments to this innovation as they are commonly composed of stovepipes that compartmentalize the organization, creating fiefdoms that resist amalgamation into a coherent interoperable design. Alberts and Hayes explain that these stovepipes are optimized to achieve narrowly focussed objectives, which consequently encourages local loyalties and almost tribal rivalries. Consequently, as hierarchies evolve, they tend to do so as a federation of individually evolved stovepipes as opposed to as an integrated organization.[225]

The topology of the traditional Industrial Age hierarchy therefore largely restricts interactions and information flow across the breadth of the organization. In the NEOps

---

[223] Arquilla and Ronfeldt, "The Advent of Netwar (Revisited)," in *Networks and Netwars* . . . 15.

[224] *Ibid*., 15.

[225] Alberts and Hayes, *Power to the Edge* . . ., 216.

concept, the organizational culture must shift from the need-to-know paradigm of today's hierarchies to the need-to-share paradigm of networks. Unfortunately, information hoarding is an inherent characteristic of organizational stovepipes as information flow is typically confined to the stovepipe that originated or collected the information. Interestingly, even when subjected to considerable pressure, exchanges of information and collaborations are considered to be an exception to be accommodated rather than a basic organizational principle.[226]

A FINAL WORD ON ADAPTING TO THE FUTURE SECURITY ENVIRONMENT

The Canadian Army has accurately, and rather boldly, portrayed the asymmetric nature of the future security environment and unconventional threat that will dominate it. ADO, as the overarching employment concept for the Army of Tomorrow, reflects the networking strategies and swarming doctrine exemplified by 4GW adversaries today. The challenges that confront this concept, as well as the key functional concept of NEOps and the enabling JIMP framework, are less technological than they are cultural and institutional. Flattening hierarchical organizations and eliminating bureaucratic stovepipes will be essential to developing interoperability, sharing information, and dramatically increasing mission effectiveness. Perhaps the greatest challenge facing this employment concept initially is the fact that it has been introduced and developed in relative isolation from the Army rather than from within a JIMP framework. 4GW is a holistic threat, and as such, it requires an integrated, holistic response.

---

[226] *Ibid*., 216.

CONCLUSION

Although the global superiority of the United States – and by extension the relative national powers of its Western allies – has continued to increase since the end of the Cold War, the world has become arguably far less stable, more chaotic, and grossly more complex. Consequently, the likelihood of large-scale conventional war between states has been eclipsed by protracted asymmetric unconventional struggles dominated by highly agile, networked adversaries that exploit the advantages of the Information Age in their organizational design, doctrines, and strategies to dislocate political will from the traditional strengths of military and economic power.

Recent history has demonstrated what happens when large, Industrial Age militaries, even those of superpowers, attempt to combat a fourth generation adversary using a second or third generation formula for war: they lose. The Chinese communists, the Vietnamese, the Sandinistas, Hezbollah, the Palestinians in the first Intifada, and the Chechnyans all crippled militarily and economically superior nation-states by adapting unconventional warfare to suit their particular form of fourth generation insurgency.[227]

Conventional forces have generally failed to adapt to effectively counter the threats posed by such groups, particularly as the distinction between governments, armies, and citizens has become more and more obscure.[228] The Canadian Army has recognized the potency of netwar and is attempting to shape the Canadian Forces, and by extension Canadian national power, to adapt to the future security environment by adopting

---

[227] Hammes, *The Sling and the Stone* . . ., 204.

[228] *Ibid.,* 192-195.

organizational and cultural principles that will enable the nation to engage netwar adversaries comprehensively and coherently via political, social, economic and military networks.

Unfortunately, shifts in organizational structures and cultures are often compromised by a tremendous bureaucratic resistance to change. As the old saying goes, "bureaucracies do what bureaucracies do; when that doesn't work, they do more of it."[229] The inertia of bureaucratic resistance is reinforced by entrenched investments in the defence industry, competing government budgets, alliances, and partisan politics. Add to these factors the degree of uncertainty involved in predicting the nature of future warfare and it becomes culturally and pragmatically difficult to develop an honest appreciation for future threats beyond the status quo of third generation manoeuvre on the Polish plains or the familiar Maoist model of 20th century national insurgency. These prejudices must be overcome in order to transform the instruments of national power into a more agile and resilient entity that can combat and defeat insurgents in the fourth generation.

The "So What?" of it All

The "so what?" of it all is that for the most part we are still trying to play chess while the truly dangerous foes are playing *Go*. Failure to truly understand the mutations and unique context of insurgencies will be at the peril of both conventional regular militaries and the nation-states drawn into such complex, protracted, asymmetric conflicts expecting a short and decisive commitment. Effectively adapting to the future security environment requires first and foremost an honest, holistic appreciation of the nature of the likely threats on the horizon. That appreciation should shape the transformation of organizational, doctrinal, and strategic concepts, considering the art of the possible while recognizing the unachievable.

---

[229] *Ibid*., 247.

The scope of this paper focused on *framing the problem* posed by evolved forms of insurgency and *highlighting the challenges of adapting* organizational, doctrinal and strategic frameworks to beat insurgents at their own game. These tasks can be summarized graphically via the following conceptual model, which is derived from the discussions presented in the preceding four chapters and illustrates the *tensions*[230] that exist when attempting to optimize a national security organization for wars of counterinsurgency. These natural tensions can be attributed to the divergence between the conventional linear threat, which the organizational, doctrinal and strategic frameworks have been optimized to mitigate, and the complex emergent threats of fourth generation insurgencies and netwars that will demand the adaptation of these frameworks from the status quo.

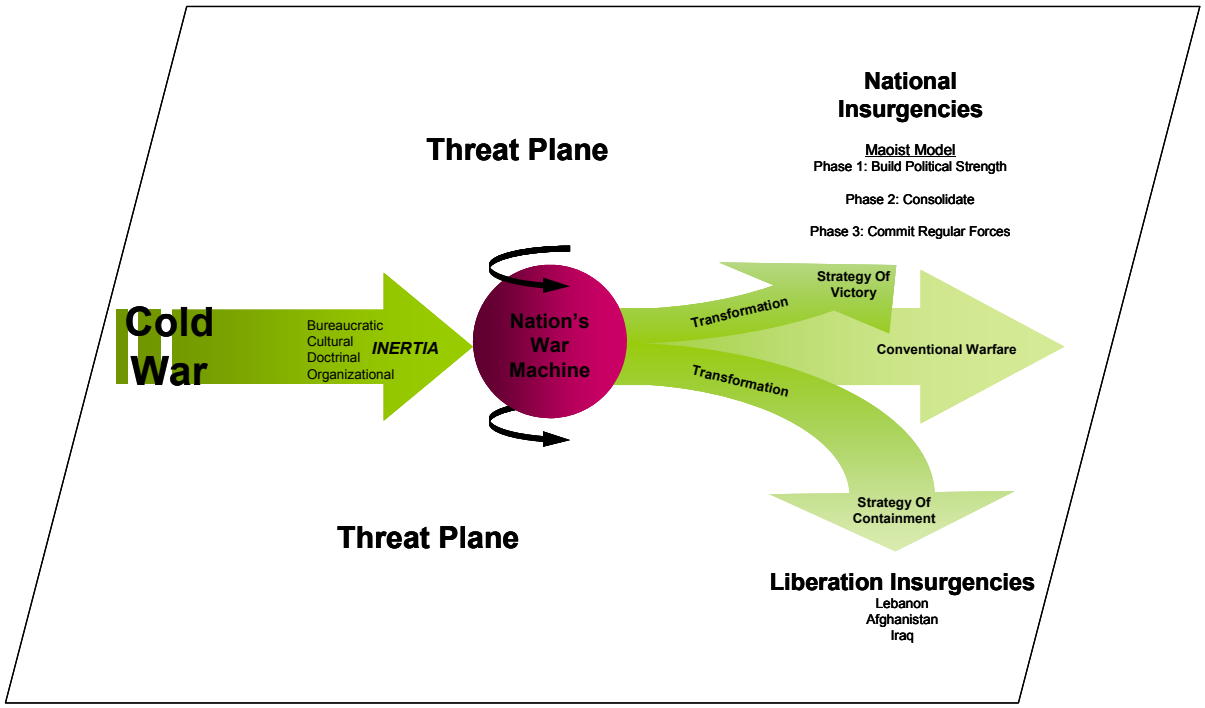

Figure 7 - The Trajectory of the Nation's War Machine

[230] The concept of tension is derived from Systemic Operational Design and illustrates opposing or conflicting goals, actions, or paradigms.

In this model the nation's war machine is the combination of all of the instruments of national power that can be applied to achieve strategic objectives in the national interest. The nation's war machine is conceptualized as a ball bearing rolling across a "threat" plane on a trajectory towards conventional linear conflict. The ball's trajectory is determined by the combined bureaucratic, cultural, doctrinal, and organizational inertia of each of the instruments of national power. For the most part this inertia stems from a Cold War legacy, where military capabilities, foreign policies, cultural perspectives, and institutional organizations were conceived and developed for a world that no longer exists today. The nation's war machine must now cope with the emergent threats across the plane without neglecting some of the traditional ones that lie before it. How the war machine will cope with these threats implies that the trajectory of the ball must change. This change, or adaptation to new threats, is often labelled as "transformation" in military jargon. And that transformation may be slight, or quite fundamental depending on two factors: the amount of force present to overcome the inertia (i.e. the will to change); and, the bearing of the new trajectory (i.e. the complexity of the threat in relation to conventional warfare).

For the first factor, the will to change will be determined by the national interest. If the interests at stake are high enough, it follows that there will be sufficient motivation to transform organizationally, doctrinally, and conceptually. Arguably, it would take a clear threat to the nation's vital interest to overcome the present inertia and precipitate a fundamental transformation in the near term. The current conflict in Afghanistan has not yet posed what would be considered a clear threat to Canada's vital national interest, and therefore transformation to meet the threat in that theatre will be incremental and largely capabilities based. As discussed in Chapter One and later demonstrated in Chapter Three's

case study of the Hezbollah, 4GW adversaries have also recognized the strategic merits of casting doubt upon a nation's national interests and will leverage all available networks in strategic communications campaigns, supported by violent guerrilla and terrorist actions, to target that interest.

For the second factor, the model illustrates two trajectories diverging from the conventional. The first implies a transformation to counter a nationalist form of insurgency based on the Mao model. In this case, the nation can pursue a strategy of victory, aiming to apply the instruments of national power to set the conditions for the insurgent force to be defeated in its final phase; that is, when the insurgent believes the correlation of forces has shifted to his favour and he commits to a conventional fight. Transformation to meet this threat would conceivably not be that dramatic as the Maoist model is well understood and nations have developed effective strategies, doctrine and forces to counter it.

Of the two broad forms of insurgency introduced, those of liberation are generally more difficult to counter. A strategy of victory that seeks a definitive end and has proven successful against national insurgencies is far less likely to succeed against a liberation insurgency, particularly one that exploits 4GW or netwar techniques. "Traditional thinking is that victory, defined as the eradication of the insurgency as a political and military force and the amelioration of the factors that allowed it to emerge in the first place, is the appropriate goal."[231] But this counterinsurgency strategy is based on the ideas and concepts central to the understanding of a Maoist-type national insurgency. It fails to acknowledge that in cases of most liberation insurgencies, such as Iraq, Afghanistan and Lebanon, no matter how much

[231] Metz and Millen, *Insurgency and Counterinsurgency in the 21st Century* . . ., 23.

political, economic and military capital that is invested by a foreign nation, it will always be perceived as a foreign imposition of a solution.

This appreciation of the threat therefore suggests that when a nation recognizes that it cannot ameliorate the root cause of the insurgency, a strategy of containment is more appropriate, where the problem can be cauterized by strengthening the states surrounding the state facing the insurgency. In this way, the strategic damage could be contained as the national efforts would focus on managing the problem, ensuring that the insurgents do not become effectively trans-national and that the conflict does not escalate. The tension between these two strategies is evident. In the model depicted as Figure 7, the trajectory leading towards liberation insurgencies implies dramatic transformation of the organizational, doctrinal and strategic frameworks. This transformation includes the integration of the emergent concepts discussed in Chapter Four (ADO, NEOps and JIMP). But to achieve such a complete transformation will require a significant threat to vital national interests in order to overcome the bureaucratic, cultural, doctrinal, and organizational inertia of the status quo.

Where to From Here?

An evolved form of insurgency is indicative not only of the nature of the fight the Canadian Forces is experiencing today in Afghanistan, but also of the nature of the conflicts that in all likelihood lie before the Canadian Forces in the future. While not all conflicts in the future will be of the fourth generation, the most dangerous to Western powers likely will be. The Information Age is altering the way people fight, shifting the focus from decisive battlefield engagements between armies to blurred, protracted conflicts prosecuted by decentralized arrays of trans-national groups, linked to others with similar agendas or beliefs,

communicating and coordinating horizontally rather than vertically, with speed and complexity. The Information Age has affected more than the types of targets and weaponry at the disposal of these adversaries; it has significantly shaped their organization, doctrine, and strategy to mitigate the effectiveness of Western military power. To extrapolate the ideas, strategies, doctrine, and operational concepts from several decades ago and apply them to the complex insurgencies of the 21st century is a recipe for ineffectiveness that will ultimately ensure that Canada's war machine becomes the *sharpest knife in the gunfight*.

To avoid this fate of irrelevance, the nation's leaders must heed Clausewitz's admonition and understand the nature of the threats of today and tomorrow for what they really are, not for what we wish them to be. They must distinguish the universal themes and concepts of insurgencies from the context specific ones and jettison those which no longer apply.[232] The Canadian Forces can be an advocate and a locomotive to not only shape this understanding, but to also overcome the bureaucratic, cultural, doctrinal, and organizational inertia that inhibits interoperability, information sharing, and mission effectiveness. The Army has started in the right direction with its capstone guide for Land Force development, *Land Operations 2021*. But neither the Army nor the Canadian Forces can be expected to independently resolve the tensions of fundamental institutional transformation that would enable the diplomat, the soldier and the developer to effectively work together in the face of an evolved and complex insurgency. These struggles require an integrated and holistic approach; hopefully it will not take a vital threat to our national interest to spark such a transformation.

---

[232] *Ibid*., 34.

BIBLIOGRAPHY

al-Qurashi, Ubeid. Quoted in "Bin Laden Lieutenant Admits to September 11 and Explains Al-Qa'ida's Combat Doctrine." *The Middle East Media Research Institute Special Dispatch Series,* no. 344 (10 February 2002). Journal on-line; available from http://www.memri.org/bin/articles.cgi?Page=archives&Area=sd&ID=SP34402; Internet; accessed 9 April 2008.

Alberts, David S. and Richard E. Hayes. *Power to the Edge: Command, Control, in the Information Age*. Washington, DC: CCRP Publications, 2003.

Arquilla, John and David Ronfeldt. "A New Epoch – and Spectrum – of Conflict." In *In Athena's Camp: Preparing for War in the Information Age*, edited by John Arquilla and David Ronfeldt, 1-20. Santa Monica, CA: RAND, 1997.

Arquilla, John and David Ronfeldt. "Cyberwar is Coming!" In *In Athena's Camp: Preparing for War in the Information Age*, edited by John Arquilla and David Ronfeldt, 23-60. Santa Monica, CA: RAND, 1997.

Arquilla, John and David Rondfeldt. *Swarming and the Future of Conflict*. Report Prepared for the Office of the Assistant Secretary of Defence (Command, Control, Communications, and Intelligence) project "Swarming and Information Operations." Santa Monica, CA: RAND, 2005. Electronic publication; available from http://rand.org/pubs/documented_briefings/2005/RAND_DB311.pdf; Internet; accessed 16 March 2008.

Arquilla, John and David Ronfeldt, "The Advent of Netwar." In *In Athena's Camp: Preparing for War in the Information Age*, edited by John Arquilla and David Ronfeldt, 275-293. Santa Monica, CA: RAND, 1997.

Arquilla, John and David Ronfeldt. "The Advent of Netwar (Revisited)." In *Networks and Netwars: The Future of Terror, Crime, and Militancy*, edited by John Arquilla and David Ronfeldt, 1-25. Santa Monica, CA: RAND, 2001.

Byman, Daniel. "Should Hezbollah be Next?" *Foreign Affairs* 82, no.6 (November-December 2003): 54. Journal on-line; available from http://proquest.umi.com/pqdweb?RQT=318&pmid=6; Internet; accessed 17 March 2008.

Callwell, Colonel Charles E. *Small Wars: A Tactical Textbook for Imperial Soldiers*. London: Greenhill Books, 1990.

Canada. Department of National Defence. B-GG-005-300/FP-000 *Canadian Forces Operations*. Ottawa: DND Canada, 2005.

Canada. Department of National Defence. B-GL-310-001/AG-001 *Land Operations 2021: Adaptive Dispersed Operations, The Force Employment Concept for Canada's Army of Tomorrow.* Ottawa: DND Canada, 2007.

Canada. Department of National Defence. B-GL-323-004/FP-003 *Counter-Insurgency Operations.* Kingston: Army Publishing Office, 2007.

Cohen, Roger. "Conflict in the Balkans: The Overview; After 2d Strike from NATO, Serbs Detain U.N. Troops." *New York Times*, 27 May 1995. Electronic publication; available from http://www.nytimes.com/; Internet; accessed 15 March 2008

Deeb, Marius. "Shia Movements in Lebanon: Their Formation, Ideology, Social Basis, and Links with Iran and Syria," *Third World Quarterly* 10, no. 2 (April 1988): 683-698. Journal on-line; available from http://www.jstor.org; Internet; accessed 29 March 2008.

Denning, Dorothy E. "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy." In *Networks and Netwars: The Future of Terror, Crime, and Militancy*, edited by John Arquilla and David Ronfeldt, 239-288. Santa Monica, CA: RAND, 2001.

Fisk, Robert. *Pity the Nation: The Abduction of Lebano.* New York: Thunder's Mouth Press/Nation Books, 2002.

Granovetter, Mark S. "The Strength of Weak Ties." In *The American Journal of Sociology* 78, no. 6 (May 1973): 1360-1380. Journal on-line; available from http://www.jstor.org/; Internet; accessed 13 March 2008.

Gray, Colin S. *Another Bloody Century: Future Warfare*. London: Weidenfeld and Nicolson, 2005.

Grice, Major Michael D. "Distributed Operations: Is the Marine Corps Ready?" *Marine Corps Gazette* 92, no. 3 (March 2008), 20-21. Journal on-line; available from http://proquest.umi.com/pqdweb?RQT=318&pmid=27962; Internet; accessed 6 April 2008.

Hammes, Colonel Thomas X. *The Sling and the Stone: On War in the 21st Century.* St. Paul, MN: Zenith Press, 2004.

Hammes, Colonel Thomas X. "Fourth Generation Warfare Evolves, Fifth Emerges." *Military Review* 87, no. 3 (May-June 2007): 14-23. Journal on-line; available from http://www.proquest.com/; Internet; accessed 9 March 2008.

Harb, Mona and Reinoud Leenders. "Know Thy Enemy: Hizbullah, 'Terrorism' and the Politics of Perception." *Third World Quarterly* 26, no. 1 (February 2005): 173-197.

Journal on-line; available from http://web.ebscohost.com; Internet; accessed 17 March 2008.

Harik, Judith Palmer. *Hezbollah: The Changing Face of Terrorism*. New York: I.B. Tauris and Co Ltd, 2004.

Herbert, Adam J. "Compressing the Kill Chain," *Air Force Magazine Online* 86, no. 3, March 2003, n.p. Electronic publication; available from http://www.afa.org/magazine/March2003/0303killchain.asp; Internet; accessed 6 April 2008.

King, Colonel Craig. "Effects Based Operations: Buzzword or Blueprint?" In *Operational Art: Canadian Perspectives Context and Concepts*, edited by Allan English, Daniel Gosselin, Howard Coombs, and Lawrence M. Hickey, 313-330. Kingston: Canadian Defence Academy Press, 2005.

Lind, William S. "Understanding Fourth Generation War." 6 January 2004. http://www.lewrockwell.com/lind/lind3b.html; Internet; accessed 1 March 2008.

Lind, William S., Colonel Keith Nightengale, Captain John F. Schmitt, Colonel Joseph W. Sutton, and Lieutenant Colonel Gary I. Wilson. "The Changing Face of War: Into the Fourth Generation." *Marine Corps Gazette* 73, no. 10 (October 1989): 22-26. Electronic publication; available from http://www.d-n-i.net/fcs/4th_gen_war_gazette.htm; Internet; accessed 2 March 2008.

Matthews, Matt M. *We Were Caught Unprepared: The 2006 Hezbollah-Israeli War.* The Long War Series Occasional Paper 26. Washington, DC: CSI Press, 2008. Electronic publication; available from http://usacac.army.mil/CAC/csi/RandP/CSIpubs.asp; Internet; accessed 29 March 2008.

Metz, Steven and Raymond Millen. *Future War/Future Battlespace: The Strategic Future of American Landpower*. Report Prepared for the U.S. Army War College Strategic Studies Institute. Carlisle PA: Strategic Studies Institute Publishing, March 2003. Electronic publication; available from http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB214.pdf; Internet; accessed 8 March 2008.

Metz, Steven and Rayond Millen. *Insurgency and Counterinsurgency in the 21st Century: Reconceptualizing Threat and Response*. Report Prepared for the U.S. Army War College Strategic Studies Institute. Carlisle PA: Strategic Studies Institute Publishing, November 2004.

Murden, Simon. "Understanding Israel's Long Conflict in Lebanon: The Search for an Alternative Approach to Security During the Peace Process." *British Journal of Middle Eastern Studies* 27, no. 1 (May 2000): 25-48. Journal on-line; available from http://proquest.com; Internet; accessed 29 March 2008.

Norton, Augustus Richard. "Hizbollah and the Israeli Withdrawal from Southern Lebanon." *Journal of Palestine Studies* 30, no. 1 (Autumn, 2000): 22-35. Journal on-line; available from http://www.jstor.org/view/0377919x/di020211/02p01053/0; Internet; accessed 17 March 2008.

Qassem, Naim. *Hizbullah: The Story from Within* translated by Dalia Khalil. London: SAQI, 2005.

Ranstorp, Magnus. "Hizbollah's Command Leadership: Its Structure, Decision-Making and Relationship with Iranian Clergy and Institutions." *Terrorism and Political Violence* 6, no. 3 (Autumn 1994): 303-339. Journal on-line; available from http://web.ebscohost.com; Internet; accessed 16 March 2008.

Ronfeldt, David and John Arquilla. "Networks, Netwars, and the Fight for the Future." In *First Monday* 6, no. 10 (October 2001). Journal on-line; available from http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/; Internet; accessed 14 March 2008.

Ronfeldt, David and John Arquilla. "What Next for Networks and Netwars?" In *Networks and Netwars: The Future of Terror, Crime, and Militancy*, edited by John Arquilla and David Ronfeldt, 311-362. Santa Monica, CA: RAND, 2001.

Summers, Colonel Harry G. Jr. *On Strategy: A Critical Analysis of The Vietnam War*. New York: Dell Publishing Co., 1984.

Thompson, Michael H. and Barbara D. Adams. *Network Enabled Operations: A Canadian Perspective*. Report Prepared for the Defence Research and Development Canada – Toronto. Guelph: Humansystems Incorporated, 2005.

United Nations Security Council Resolution 425 (1978) of 19 March 1978. Available from http://domino.un.org/unispal.nsf; Internet; accessed 29 March 2008.

United States. Department of the Army. TRADOC Pamphlet 525-5-500 *The U.S. Army Commander's Appreciation and Campaign Design.* Washington, DC: U.S. Government Printing Office, 28 January 2008.

United States. Department of the Army. FM 3-24 *Counterinsurgency*. Washington, DC: U.S. Government Printing Office, 15 December 2006. Electronic publication; available from http://www.fas.org/irp/doddir/army/fm3-24.pdf; Internet; accessed 8 March 2008.

United States. Joint Chiefs of Staff. JP 1 *Doctrine for the Armed Forces of the United States.* Washington, DC: U.S. Government Printing Office, May 14, 2007. Electronic publication; available from http://www.dtic.mil/doctrine/jel/new_pubs/jp1.pdf; Internet; accessed 8 March 2008.

United States. Joint Chiefs of Staff. JP 1-02 *Department of Defence Dictionary of Military and Associated Terms*. Washington, DC: U.S. Government Printing Office, April 12, 2001 as amended through October 17 2007. Electronic publication; available from http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf; Internet; accessed 8 March 2008.

United States. Secretary of the Air Force. *Air Force Doctrine Document 2-3: Irregular Warfare.* Washington, DC: U.S. Government Printing Office, August 1, 2007. Electronic publication; available from http://www.e-publishing.af.mil/; Internet; accessed 1 March 2008.

van Creveld, Martin. *The Transformation of War.* New York: Free Press, 1991.

von Clausewitz, Carl. *On War*, Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976.

Wege, Carl Anthony. "Hizbollah Organization." *Studies in Conflict and Terrorism* 17, no. 2 (January 1994): 151-164. Journal on-line; available from http://web.ebscohost.com; Internet; accessed 18 March 2008.

Weimann, Gabriel. "Hezbollah Dot Com: Hezbollah's Online Campaign," in *New Media and Innovative Technologies*, edited by D. Caspi and T. Azran, 17-38. Beer Sheva: Ben-Gurion University Press, 2008.

Weimann, Gabriel. "Special Report: www.terror.net – How Modern Terrorism Uses the Internet." In *United States Institute of Peace* Special Report 116 (March 2004). Journal on-line; available from http://www.usip.org/pubs/specialreports/sr116.pdf; Internet; accessed 15 March 2008.

Williams, Phil. "Transnational Criminal Networks." In *Networks and Netwars: The Future of Terror, Crime, and Militancy*, edited by John Arquilla and David Ronfeldt, 61-97. Santa Monica, CA: RAND, 2001.

Zanini, Michelle and Sean J.A. Edwards. "The Networking of Terror in the Information Age." In *Networks and Netwars: The Future of Terror, Crime, and Militancy*, edited by John Arquilla and David Ronfeldt, 29-60. Santa Monica, CA: RAND, 2001.