CANADIAN FORCES COLLEGE/COLLEGE DES FORCES

CANADIENNES AMSC 6/CSEM 6

CANADIAN MILITARY DOMESTIC RESPONSE TO TERRORIST NETWORKS

By /par Col Bob Bertrand

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

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

ABSTRACT

This paper contends that Canadian government departments and other agencies, responsible for domestic security, are unprepared to deny al-Qaeda and other terrorist networks the ability to operate within Canada. These networks have stated they intend to attack the interests of the western world and specifically the United States of America wherever and whenever they can.

Canada is likely not a major target for these networks. There is however a very real possibility that Canada will be used as a staging point to attack the US. The threat to Canada would be US loss of confidence in its border security with Canada resulting in restriction in the movement of goods between Canada and the US. The resulting loss of export sales would have a disproportionate economic impact on Canada's economy since it is more reliant on export trade.

This paper explores the nature of the threat to the US and Canada, proposes an analytical model to understand terrorist networks, reviews the state of US and Canadian defence and finally recommends some structures to develop the required intelligence assessments and domestic Canadian military capabilities to counter terrorist networks.

INTRODUCTION

> "It is every Muslim's duty to wage war against the US and Israeli citizens anywhere in the world"
>
> Osama bin Laden[1]

> September 11, 2001 — Nineteen young men, sponsored by an Islamic terrorist group with connections to an Islamic Fundamentalist theocracy in Afghanistan and an Islamic Fundamentalist sect in Saudi Arabia, hijack four aircraft over the United States. They fly two of them into the twin towers of the World Trade Center in New York City, ultimately causing the buildings to collapse. A third plane is flown into the Pentagon in Washington, DC, the nation's capital. They crash the fourth plane into an open field in Pennsylvania when the passengers, who by then had found out the fate of the other aircraft via in-flight telephone calls to relatives, tried to retake control of the plane**.** [2]

The September 11, 2001 terrorist attacks shattered the United States of America's sense of security. The event served as a wake-up call to the American and Canadian governments that, in the future their enemies would not always directly confront their conventional armed forces in battle. The enemy, in this case the al-Qaeda network, could also resort to asymmetrical tactics using network organizational structures to exploit and attack their weaknesses and centers of power.

The aim of this paper is to demonstrate new international and domestic network organizations are required to develop intelligence assessments and conduct information warfare to counter the terrorist network threat.

The paper will explore the nature of the threat to the US and Canada by reviewing past American and Canadian Defence Department assessments. The threat will be situated in the context of the post Cold War world order, the Revolution in

[1] V. Crawley, "Terror Alert," *Army Times,* November 6, 2000.
[2] J.A.H. Futerman, "The New World War", www.dogchurch.org, April 2002

Military Affairs, the military and economic ties between Canada and the US and the correlation between the rise of terrorist networks using asymmetric tactics and the post Cold War order. To better understand the threat, an analytical model that includes two global forces conducive to the gestation of terrorist networks and a review of terrorist network organization, communication and information systems, strategy and tactics and funding will be used to develop counter-measure recommendations. A review of the state of American and Canadian defence and actions since 11 September 2001 will be used to propose there is still much work to do. Finally, structures upon which to develop the required intelligence assessments and domestic Canadian military capabilities to counter terrorist networks will be recommended.

NATURE OF THE THREAT

Cold war intelligence policies and organizations with their compartmentalized acquisition, analysis, and dissemination of information methods are ill suited to countering networked terrorist threats. This new threat poses a dilemma for intelligence and counter-terrorism agencies on both sides of the border. How do you defend against a threat that is not understood, where means of attack are unpredictable and the range of targets appears limitless? A necessary first step is to understand the nature of this threat and what to expect from this new type of warfare.[3]

[3] James B. Steinberg et al, "Building Intelligence Networks to Fight Terrorism", Brookings Institute – Policy Brief # 125, 2003, 1

What Is the Threat?

The terrorist threat to the US and Canada is not new and was recognized as early as 1996 in the American military's Joint Vision 2010 document, which identified the risk as an asymmetric threat to the American military. The 1997 Quadrennial Defence Review restated the threat and identified ballistic missiles, weapons of mass destruction, terrorism and information warfare as possible avenues for terrorist attacks.[4] In Canada, Strategy 2020, published in 1999, provided strategic direction to develop a joint capability to deal with weapons of mass destruction, information operations and other asymmetrical threats.[5] The DCDS's 1999 Future Operations Study identified asymmetric actions against Canada, as a potential threat, that had significant potential to affect Canada's security and could move into the foreground in the next 5 – 10 years.[6]

Canada and the US remain vulnerable to terrorist attacks, weapons of mass destruction, or unpredictable actions in unpredictable places as evidenced by the attack on the USS COLE.[7] The threat against the US is higher, due to its position as the lone world super power. The US is a major target of radical Islamic terrorist networks for a number of reasons:

[4] Canada, Department of National Defence, "Strategic Assessment 2002" (Ottawa: Public Works and Government Services Canada), August 2001

[5] Canada, Department of National Defence, "Shaping the Future of Canada's Defence: A Strategy for 2020" (Ottawa: Public Works and Government Services Canada) June 1999, 2

[6] Canada, Department of National Defence, "Threat Definition: Asymmetric Threats and Weapons of Mass Destruction" (Ottawa: Public Works and Government Services Canada), 2002, 1

[7] Author Unknown, "Asymmetric Warfare, the USS Cole and the Intifada", The Estimate – Political and Security Analysis of the Islamic World and its Neighbours, Vol XII, Number 22, Nov 3, 2000, 1

- attacking the US provides terrorist networks with regional and world-wide publicity and recognition since the US projects the most power in the world,

- the terrorists are attempting to drive out US military forces that are forward based on the Arabian peninsula and provide authoritarian secular regimes with security,

- the US supports Israel and has played a lead role in brokering peace initiatives with her neighbors. By attacking Israel or the US, the terrorist networks are attempting to break up Arab-Israeli peace negotiations and continue the war to return holy sites within Arab borders, and

- the US's cultural and consumer values are perceived to corrupt Islamic values**.** Terrorist network attacks are aimed as blows against American influence in the region.[8]

While the US pursues development of a high tech military with a low-casualty combat doctrine, third world nations are suffering from a series of low-intensity conflicts with no quick-fix solutions. Against this backdrop, an understanding of the new world order, Canada's place in it relative to the US and the nature of the terrorist threat is useful to identify possible areas to attack terrorist networks.

New World Order

With the breakup of the Soviet Union in 1991, the US assumed the mantle of the world's lone super-power. No potential adversary has the US military's global

[8] Anthony H. Cordesman, "Transnational Threats From the Middle East: Crying Wolf or Crying Havoc", January 1999, page 45

reach and advanced conventional weaponry such as stealth bombers, cruise missiles, laser-guided bombs, supporting navigation, surveillance, target-acquisition and communication systems. Given this supremacy in conventional forces, it is not surprising the US's enemies prefer not to engage their conventional military forces.

The US and its allies, in the next decade, will likely be faced with an increasing number of what may be called "brush-fire" wars where casualties will pale in comparison to the potential damage a Cold War exchange of nuclear weapons or engagement of conventional forces in Europe could have resulted in.[9] The small wars will no longer be proxy campaigns of influence by the old Cold War adversaries. While western militaries have pushed toward high-tech, low casualty combat, war has gone in the opposite direction toward low-tech small arms engagements with no regard for civilian casualties. A few current examples include the Israeli – Palestinian and Balkan ethnic conflicts. The US and its allies will enter into these conflicts at their own risk since a conventional military campaign will not correct the complex cultural, religious and historical background problems at their core and the exit strategy or point will have to be clearly defined to avoid becoming embroiled in a long term commitment or conflict.[10] In Western security policy, there is a dangerous gulf between the dominant thinking about security based on "old wars", like the Second World War and the Cold War, and the reality in the field. The so-called Revolution in Military Affairs, the development of 'smart' weaponry to fight wars at long distance, the proposals for the National Missile Defense Program, were all

[9] Clark L. Staten "Asymmetric Warfare, the Evolution and Devolution of Terrorism; The Coming Challenge for Emergency and National Security Forces." 27 April, 1998, 1

predicated on out-dated assumptions about the nature of war, the idea that it is possible to protect territory from attacks by outsiders.[11] The military requirement for "brush-fire" wars will likely be mobile, lethal packages of sea, land and air capabilities with special operations forces. Political decisions will be required to determine whether nations engage in these conflicts to neutralize a direct threat or in an enforcement or peace-keeping role.

Canada and the US.

Canada and the US share a longstanding defence relationship supported by more than 80 treaty level defence agreements, 250 memorandums of understanding and joint bi-national command of NORAD.[12] Canada's economy is also highly integrated with the US's. The US is Canada's largest export market. Eighty percent of Canada's exports, consisting largely of motor vehicles, lumber, crude metals, natural gas, wheat and other agricultural products, go to the U.S. Those exports totaled approximately $250 billion in 2001.[13] Canada, with a population less than one-ninth the size of that of the United States, bought an average of $5,254 worth of U.S. goods per capita. The United States bought $219 billion worth of Canadian merchandise, approximately $768 for every American. The US-Canada current account, the balance of trade in goods, services and income flows, has shifted back

[10] David L. Grange, "Asymmetric Warfare: Old Method, New Concern", National Strategy Forum Review, Winter 2000, 3

[11] David Held, "Violence, Law and Justice in a Global Age", Social Science Research Council, 5 November, 2001, 8

[12] Canada, Department of National Defence, A Time for Transformation (Ottawa: Public Works and Government Services Canada, 2003) 26

[13] http://www.clearfacts.com/Canada/Canada_profile.htm

and forth over the past few decades. In 2001, Canada's current account surplus decreased from $30 billion to $27 billion.[14] While both countries are co-signatories of a comprehensive free trade agreement, Canada as an exporting nation is highly reliant on its access to the U.S. market. Border closure or restrictions would have a disproportionate impact on Canada given our greater dependence on cross-border trade.

Asymmetry and Terrorist Network Warfare

> "When conventional tactics are altered unexpectedly according to the situation, they take on the element of surprise and increase in strategic value"
> "Greater powers and resources do not guarantee tactical superiority"
>
> Sun Bin – The Lost Art of War

There are many definitions of asymmetry, however, Steven Metz, a research professor of National Security Affairs at the US Army War College, Carlisle Barracks, Pennsylvania, has published a definition which will be used in this paper due to its comprehensiveness.

> "In military affairs and national security, asymmetry is acting, organizing and thinking differently from opponents to maximize relative strengths, exploit opponents' weaknesses or gain greater freedom of action. It can be political-strategic, operational or a combination, and entail different methods, technologies, values, organizations or time perspectives. It can be short-term, long-term, deliberate or by default. It can be discrete or pursued in conjunction with symmetric approaches and have both psychological and physical dimensions".[15]

Asymmetric warfare is not new. In general, all military tactical, operational and strategic planning and execution focuses on applying your strength at the enemy's weakest point. Opponents seldom have identical military forces, nor do they

[14] Canada, Department of Foreign Affairs and International Trade, "Canada – United States – The World's Largest Trading Relationship, http://www.canadianembassy.org/trade/wltr2002-en.pdf, 2002

behave identically. Today, a clear-cut military victory is very difficult to achieve because the advantages of supposed superior technology have been eroded in many contexts. As the Russians discovered in Afghanistan and Chechnya, the Americans in Vietnam, and the Israelis in the current period, conquering people and territory by military means has become an increasingly problematic form of warfare. These military campaigns have all been lost or suffered serious and continuous setbacks as a result of the:

- stubborn refusal of movements for independence or autonomy to be suppressed,
- refusal to meet the deployment of the conventional means of interstate warfare with similar forces which play by the same set of rules,
- terrorist having little regard for civilian casualties and collateral damage,
- constantly shifting use of irregular or guerrilla forces which sporadically but steadily inflict major casualties on states (whose domestic populations become increasingly anxious and weary), and
- risks of using high-tech weapon systems, carpet bombing and other very destructive means of interstate warfare are very high.[16] [17]

The September 11th attack did not destroy America's political, military or financial hegemony. The attack demonstrated how a well-planned action using asymmetric tactics could result in damage, in this case to American prestige, largely disproportionate to the terrorist effort. The attacks resulted in much military and

[15] Steven Metz, "Strategic Asymmetry", Military Review, Jul-Aug 2001, 3

[16] David Held, "Violence, Law and Justice in a Global Age", Social Science Research Council, 5 November, 2001, 8

academic review of the causes with recommendations to prevent future attacks. The post-attack debate has ranged from the apocalyptic view of events, concluding there is no defence against these networks, to more optimistic views.

The optimists conclude that while the rules of engagement with these networks will be different, they still have to recruit, train, plan, gain support, move, stage, attack and regroup during any operation or pursuit of a cause. This requirement presents opportunities to attack the network and cause it to fail anywhere along this process, preferably prior to the attack phase. The terrorist network's smaller size, secretive nature, deliberate attempts to avoid becoming predictable and network structure will make them hard to detect and counter.[18] What is clear, is that the terrorist networks are waging a different kind of war. This network warfare or netwar is targeting the weaknesses of conventional military forces and democratic countries. John Arquilla and David Ronfeldt, in the The Advent of Netwar, define network warfare as,

> ”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. These protagonists are likely to consist of dispersed organizations, small groups, and individuals who communicate, coordinate, and conduct their campaigns in an internetted manner, often without a precise central command.”[19]

[17] Anthony H. Cordesman, “Transnational Threats From the Middle East: Crying Wolf or Crying Havoc”, January 1999, 113

[18] Collin A. Agee, “Leadership Notes Army Intelligence Master Plan” Military Professional Bulletin, Fort Huachuca, Jul-Sep 2002, Volume 28, Issue 3, 47

[19] John Arquilla et al. ”The Advent of Netwar” 6

ANALYTICAL MODEL

Understanding your enemies is essential if you plan to defeat them. Developing a solution to any problem must necessarily begin with an analysis phase. Fortunately there are numerous military and academic reviews upon which to base this analysis. Defeating terrorist networks will require a thorough understanding of the forces or events that led to their formation, how they are organized, communication and information systems, strategy, tactics and funding.

Globalization

Globalism has resulted in the growth of a world market, increasingly penetrating and dominating national economies, resulting in a loss of sovereignty and control due to common currencies, exchange rates and free market access. Another result has been the accelerating gap between rich and poor states as well as the populations participating in and benefiting from globalization. Widespread Muslim misgivings about globalization are not a figment of anyone's imagination. Just as there are anti-globalists across America and Europe, so there are many in Egypt, Pakistan, and Indonesia. But for the most part, the observed Muslim resentment is less an expression of opposition to modern capitalism than it is a cry of desperation. Middle Easterners who have acquired skills to compete in the global economy, when given opportunities to participate in it, usually prefer peaceful production to hateful destruction. The Hebron crowd that danced in the streets on September 11 consisted overwhelmingly of people pushed by modern technologies to the fringes of the global economy.[20] It is no coincidence that the marginalized Muslim populations are a prime source of recruits for terrorist networks.

Failed States and Radical Islam

Many third world Muslim countries have failed to develop stable political and economic systems. These secular regime failures triggered the rise of numerous Islamic terrorist networks. While some target their own country or government, some have also targeted the West and western interests. Many of the US's terrorist network enemies are non-state actors that operate with a different mind-set, believing they are continuously at war. For terrorists, violence is a way of life and they know it is an effective tactic against democratic populaces worried about preserving their way of life. Their values are different than ours, which makes it difficult for us to understand why they value human life so little and are prepared to commit atrocities against the civilian populace. Most of these organizations are predatory, taking refuge in weak states and their sovereignty and using the local discontented population as a base for recruitment. Once established, these networks use the country as an operating base from which to deliver terrorist attacks and train other terrorists for export to other conflict areas.[21]

Al-Qaeda is a product of the resistance campaign to eject the Soviets from Afghanistan. That campaign, portrayed as a holy war against the "godless" Soviets brought together thousands of volunteers and financial support from the Islamic

[20] Timur Kuran, "The Religious Undercurrents of Muslim Economic Grievances", Social Science Research Council, 2001, 1

[21] David L. Grange, "Asymmetric Warfare: Old Method, New Concern", National Strategy Forum Review, Winter 2000, 3-4

global community. Volunteers from different Muslim countries fought together and gained confidence in the merits of their cause with the eventual withdrawal of the Soviet Union and its subsequent collapse (for which they assumed credit). Osama bin Laden provided this potent but unfocussed group a sense of vision, mission and strategy by recasting all the separate national conflicts into a single struggle. The enemy was the west, particularly the US, since without US support, corrupt regimes would fail allowing a return of Islamic based regimes. Linking all of the individual struggles into one against the US and the West allowed bin Laden to establish a much larger base from which to recruit and finance anti-western activities. In addition to the thousands of veterans from the Afghanistan war, al-Qaeda was now able to draw thousands of new recruits from every Islamic conflict area.[22] While their religious conviction gives the terrorist networks strength, it is the armed struggle that holds them together. Violent actions against western countries and the US provides status, power and psychological satisfaction and also attracts new recruits. The September terrorists who left messages and testaments described their actions as being in the name of Allah. They made this their explicit appeal and defence. Bin Laden himself, no longer disclaiming culpability for their actions, clothes their murders and their suicides in religious glory. This version of Islam, not typical and a minority, but undeniably Islamic, endorses the hatred for America.[23] It would be easy to link terrorist network threats into an indictment of all Arabs and all of Islam. However,

[22] Brian M. Jenkins, Countering al-Qaeda, Washington: RAND 2002, 4-5

[23] Hugo Young, "It May Not be PC to Say" The Guardian, 8 October, 2001

Islam is a powerful force for both morality and stability and the vast majority of Middle Eastern Arabs have no interest in violence.[24]

Terrorist Network Organization

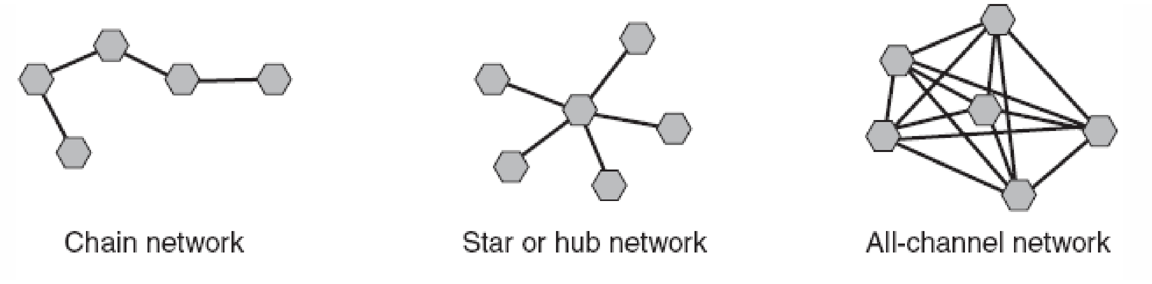
In general, terrorist networks share a set of general ideas, philosophies or ideology to which all members subscribe providing them a common motive for their actions.[25] Terrorist organizations often operate on a network structure. The network structure is not unique to terrorist organizations but is a characteristic of the new transnational terrorist networks. The network structure gives organizational flexibility, reduces the possibility of penetration, makes it more difficult to identify leaders and provides greater efficiency. The terrorist networks' organizational structures resemble more modern legitimate business structures than older hierarchical corporate structures. The terrorist network structures feature many design variants. In order to defend against and attack these networks, analysts will have to first understand what kind of network they are confronting and then develop tactics to neutralize it. Networks can be categorized into three kinds of structures that may be large or small, specialized or generic in function or loosely or tightly aligned with the network including the following pictured in Figure 1:[26]

- the chain or line network where information must move sequentially through a series of nodes or separated contacts. This is a hierarchical model,

[24] David Held, "Violence, Law and Justice in a Global Age", Social Science Research Council, 5 November, 2001, 7
[25] John Arquilla et al. "The Advent of Netwar", 7
[26] Ibid, 8

- the hub, star or wheel network where members, info and materiel are linked to a central, but not hierarchical node. This is typical of sophisticated criminal enterprises, and
- the all-channel or full matrix network, where every member is connected to every other member to enhance functionality. This model is collaborative in nature, quick acting and effective. It can be difficult to maintain given the high level of communication required. This is the network of the information age and when used by terrorists can launch multiple repeated attacks from many points. It can be difficult to identify since there is no traditional leader but multiple heads. It can be difficult to destroy because pathways as well as nodes are highly redundant. This model also provides opportunity for attack by counter-terrorist agencies since it is highly reliant on communications.[27]

FIGURE 1



To complicate matters there may be hybrids of the above structures such as hierarchical organization with all-channel networks for tactical operations.[28]

[27] Lee S. Strickland, “Fighting Terrorism With Information”, The Information Management Journal, July-August 2002, 28

Communications and Information Systems

Modern communication media can facilitate co-ordination of network node activities. Dispersed networks require effective communication links to pass information and to co-ordinate activities between nodes. Modern communication such as cell phones, satellite links, e-mail, computer conferencing and chat rooms that process and store this information provide opportunities for western governments. They can be targeted through conduct of passive and active information operations against the terrorist network communication links and the information systems used to communicate between nodes.[29]

Strategy and Tactics

Another important element of the counter-terrorism intelligence analyst's work is to determine what kind of doctrine or tactics the network is likely to employ. Most terrorist networks have the ability to or are moving towards swarming. Arquilla and Rondfelt define swarming as:

> "a seemingly amorphous, but deliberately structured, co-ordinated , strategic way to strike from all directions at a particular point or points, by means of a sustainable pulsing of force and/or fire, close-in as well as from stand-off positions".[30]

The approach is very different from the symmetrical and conventional mass and maneuver doctrine used by western military forces. Swarming occurs when dispersed terrorist network nodes converge on a site or target from many different directions or locations, striking the target and dispersing ready to again swarm a future target.

[28] John Arquilla et al. "The Advent of Netwar", 50
[29] Ibid, 10-11
[30] Ibid, 12

Intelligence and information operations are capabilities that can be used to counter the terrorist network before a swarming attack can be launched.

Funding

New terrorist networks are less likely to be state-sponsored although they may use failed and sympathetic states as an operating bases and/or training sites. Without traditional state support the new networks sought new funding sources. Al-Qaeda, for example, differs from traditional, state-sponsored terrorist groups in one critical way: it is financially robust. This financial security provides independence from the control of any government and the ability to maintain its organizational infrastructure, communications systems, training programs, and operations. This has allowed al-Qaeda to operate from failed states and even provide financial support to their hosts.[31] Osama bin Laden built al-Qaeda's financial network from the foundation of a system originally designed to channel resources to the mujahideen fighting the Soviets. This financial network permitted movement of the operations base from Saudi Arabia, Sudan and Afghanistan while still maintaining a capacity to attack Americans around the world. Al-Qaeda's financial network is as decentralized and compartmentalized as its organization and is characterized by layers and redundancies.[32] It raises money from a variety of sources and moves money in a variety of ways. The most important source of al-Qaeda's money however, is its continuous fund-raising efforts.

Al-Qaeda's global fund-raising network is built upon a world-wide foundation of charities, nongovernmental organizations, mosques, web-sites, intermediaries,

[31] United States, Council on Foreign Relations, Terrorist Financing: Report of an Independent Task Force, (Washington D.C.: US Government Printing Office, 2001) 3

[32] Ibid, 1

facilitators, banks and other financial institutions.[33] This network extends to all corners of the Muslim world and includes everyone from wealthy Persian Gulf Arabs (who can be solicited directly to give huge sums themselves), to the masses (who make regular charitable donations as part of their religious obligations, the zakat). The zakat is a religious duty of all Muslims to give at least 2.5 percent of their income to humanitarian causes and is one of the pillars of Islam, *"My mercy encompasses all things, but I will specify it for the righteous who give Zakat (Koran 7:156)".*[34] Al-Qaeda and other Islamic terrorist groups have taken advantage of this enormous source of funds for their own ends. In many communities, the zakat is often provided in cash to prominent, trusted community leaders or institutions, which then commingle and disperse donated moneys to persons and charities they determine to be worthy. These widely unregulated, seldom audited, and generally undocumented practices allow the diversion of huge sums of money. Some contributors know full well the violent and illicit purposes their money will further. In other cases, donors believe their money will help fund legitimate humanitarian efforts, but the money is nonetheless diverted to al-Qaeda.[35]

For years, al-Qaeda has been particularly attracted to operating in under-regulated jurisdictions, places with limited bank supervision, no anti–money laundering laws, ineffective law enforcement institutions, and a culture of "no-questions-asked" bank secrecy. Al-Qaeda moves its funds primarily through the global financial system, the Islamic banking system and the underground hawala

[33] Ibid, 1

[34] http://www.submission.org/zakat.html

[35] United States, Council on Foreign Relations, Terrorist Financing: Report of an Independent Task Force, (Washington D.C.: US Government Printing Office, 2001) 5

system.[36] The ancient hawala underground banking system allows money transfer without actual money movement, or any wire transfer. Here is how it works. Customers in one city pass their local hawaladar money. The hawaladar then contacts his counterpart across the world, who then dispenses money out of his own resources to the intended recipient. The volume of transactions flowing through the system in both directions is such that the two hawaladars rarely have to worry about settlement. The trust between and among hawaladars, who are in many cases related through family, clan or ethnic associations, allows them to carry each other's debts for long periods before finding ways to clear them.

There is nothing illegal about the hawala system. It offers critically needed financial services in many remote corners of the globe and is used extensively by millions of law-abiding persons. In Pakistan, for instance, government officials estimate that $7 billion enters the country each year through the hawala system, the true number is likely to be significantly higher.[37] Its nature also makes it particularly susceptible to abuse by terrorists and other criminals and appears custom-made for al-Qaeda. It is a cash business that leaves behind few, if any, written or electronic records for use by investigators in following money trails. It operates out of nondescript storefronts and countless bazaars. It reaches both small villages throughout the region and large cities around the world. It is quick, efficient, reliable, and inexpensive. All the hawala system needs to operate are a network of hawaladars, trust, and open phone lines. Al-Qaeda also uses its global network of businesses and charities as a cover for moving funds, as well as such time-honored

[36] Ibid, 7
[37] Ibid, 8

methods as bulk cash smuggling and the global trade in gold and other commodities to move and store value. Al-Qaeda is not the only terrorist organization to make use of these mechanisms. Other terrorist organizations have long used charities to help raise and move their funds, as the Irish Republican Army (IRA) did for decades in American cities such as Boston and New York.[38] The funding network which supports al-Qaeda and other terrorist networks is another potential target for intelligence and information operations. Success in reducing terrorist fundraising will limit the number of recruits that can be trained, equipped and sent out against western targets. As long as al-Qaeda retains access to a viable financial network, it remains a lethal threat to the United States.[39]

STATE OF OUR DEFENCES

The events of 11 September 2001, provided a stark warning to the US that it had some serious gaps in its international and domestic intelligence and counter-terrorism capabilities. Canada as the US's major military ally and trading partner also had reason for concern since there had been several arrests at Canada-US border checkpoints of suspected terrorists bound for the US. Much has been done by both countries since the fall of 2001. However, much work remains to develop the organizations, intelligence sources and new counter-terrorism capabilities to defeat terrorist networks.

[38] Ibid, 1
[39] Ibid, 9

US Actions Since September 11, 2001 (9/11)

Homeland Security has taken on heightened importance within the US since 9/11. The Office of Homeland Security was legislated with a mandate to produce a National Strategy for Homeland Security and create a comprehensive plan for using America's talents and resources to enhance their protection and reduce their vulnerability to terrorist attacks.[40] The security plan calls for new intelligence efforts to protect the nation's borders, defend against threats within the US, minimize infrastructure vulnerabilities and improve emergency responses.[41] Specific actions resulting from 9/11 include tightening of border, port and airfield security, allocation of additional resources to intelligence gathering and counter-terrorism capabilities.[42] A bilateral agreement, the Smart Border Declaration, was signed by Canada and the US in December 2001. This agreement, which acknowledges the importance of trade between the two countries, allowed Canada to remain within the US's security perimeter in exchange for closer co-operation with the US in four areas: transit of people, transit of goods, infrastructure protection and information sharing in enforcement. The intention of the agreement is to pool resources, share information and adopt common standards and policies to attempt to intercept terrorists before they can mount an attack.[43]

American defence initiatives included the creation of Northern Command (NORTHCOM) within the Unified Command Plan. Northern Command consolidates

[40] President Bush, Letter to all Americans, July 16, 2002
[41] James B. Steinberg et al, "Building Intelligence Networks to Fight Terrorism", Brookings Institute – Policy Brief # 125, 2003, 1
[42] Canada, Department of National Defence, "Strategic Assessment 2002" (Ottawa: Public Works and Government Services Canada) August 2001, 1
[43] Ibid, 4

all military homeland security responsibilities under one commander. The new command will have responsibility for US maritime, land and air defence, with an area of responsibility that encompasses Canada, the US and Mexico and its approaches out to 500 miles off-shore. NORTHCOM will also be responsible for providing military assistance to first responder civilian authorities under the Office of Homeland Security.[44] American Secretary of Defence Rumsfeld is also pursuing an initiative to transform the US military to ensure it is equipped, manned and trained to support US domestic and international policy.

Canadian Actions Since 9/11

The CDS's 2002-2003 Annual Report identified a number of transformation initiatives, funded and announced in prior Federal Budgets and Defence Planning documents, that recognized the importance of domestic security against terrorist networks and conventional enemies. The report implicitly recognizes the importance of defending our portion of the US security perimeter. First there is a recognition that the Canadian Forces must develop the ability to operate as part of collaborative human networks that include all war fighters, the three military environments, headquarter military and civilian staff and staff from other Government security portfolios as well as allies.

Second a number of new capabilities were to be stood-up or augmented under a Strategy 2020 target to develop new task tailored capabilities to deal with asymmetric threats and weapons of mass destruction.[45] including:

[44] Ibid, 3

[45] Ibid, 5

- doubling the capacity of Joint Task Force 2 (JTF2) to conduct counter-terrorism and special operations, both domestically in support of police and internationally, as part of a Canadian contribution to UN or coalition operations,
- the Joint Nuclear, Biological and Chemical Defence Company stood-up in December 2002 with a capability to respond to both domestic and international terrorist activities,
- the Disaster Assistance Response Team (DART) improved its capacity to respond rapidly to humanitarian crisis such as natural disasters both domestically and abroad,
- the Communication Security Establishment (CSE) continued to expand its counter-terrorism capabilities including, government network security and enhancing its ability to co-ordinate efforts and share info with other security agencies,
- the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) is leading a program to co-ordinate critical infrastructure protection with provinces, municipalities and the private sector,
- a new Counter Terrorism Technology Centre is being constructed to train first responders from across Canada to react to incidents involving biological and chemical agents, and
- the US and Canada will work together as apart of a bi-national military planning group, led by the Canadian Deputy Commander in Chief NORAD,

to develop contingency plans to respond to natural disasters and deter and respond to potential terrorist threats or attacks.[46]

The above incremental activities by the US and Canada have still not produced a new intelligence system that breaks down the formal and hierarchical structures and organizations that currently exist nor has it produced offensive capabilities to disrupt and attack terrorist communications.

Some Assumptions

A number of political and strategic assumptions are required to scope possible recommendations for Canadian military domestic responses to terrorist network threats. Discussion of each of these assumptions is beyond the scope of this paper due to space limitations:

- the US will play the lead role in attacking strategic terrorist network targets outside of North America targets including actions against nations supporting the terrorist networks. Canada will choose to participate on a case by case basis,
- no Canadian agency has a mandate to conduct intelligence operations outside of Canada. The US can be expected to share intelligence on terrorist activities that threaten the US security perimeter especially if there is a possibility threats may emanate from Canada. Canada will identify a lead agency for the collection, analysis and assessment of all international and domestic intelligence. That agency will be responsible to for reducing the barriers to sharing information, improving technology capabilities for all users,

[46] Canada, Department of National Defence, A Time for Transformation (Ottawa: Public Works and Government Services Canada) 2003, 5

coordinating analysis of intelligence data, collecting information on the nation's critical infrastructure vulnerabilities especially where they will impact the US and supporting federal, provincial and municipal communications,

- the Liberal government is attempting to run a balanced budget, pay down some of the country's deficit and address under funded public sector institutions such as health care. The Department of National Defence has received some budget baseline increases however must undergo a capability review to ensure its force generation and sustainment capabilities are affordable. These funding constraints will likely limit Canada to developing niche military capabilities to contribute to domestic security and international anti-terrorist coalition operations,
- Canada does not have the same security concerns as the US as the terrorist threat is not as high. Canada must try and balance US concern about gaps in the North American security perimeter within available resource constraints and also deny terrorists the use of Canada as a base from which to attack the US. Canada will provide a best effort here understanding that failure to do so would likely result in restrictions to the flow of goods and people across our borders which would severely affect our economy, and
- Canada willbet hrd- p edh to ddr

> adoption of clear, public guidelines governing the collection, retention, and dissemination of information and the development of strong procedures for oversight and accountability.[47] [48]

What Are We Trying to Fix?

> "Surprise, when it happens to a government, is likely to be a complicated, diffuse, bureaucratic thing. It includes neglect of responsibility but also responsibility so poorly defined or so ambiguously delegated that action gets lost. It includes gaps in intelligence, but also intelligence that, like a string of pearls too precious to wear, is too sensitive to give to those who need it. It includes the alarm that fails to work, but also the alarm that has gone off so often it has been disconnected. It includes the unalert watchman, but also the one who knows he'll be chewed out by his superior if he gets higher authority out of bed. It includes the contingencies that occur to no one, but also those that everyone assumes somebody else is taking care of. It includes straightforward procrastination, but also decisions protracted by internal disagreement. It includes, in addition, the inability of individual human beings to rise to the occasion until they are sure it is the occasion-- which is usually too late. (Unlike movies, real life provides no musical background to tip us off to the climax.) Finally, as at Pearl Harbor, surprise may include some measure of genuine novelty introduced by the enemy, and possibly some sheer bad luck.
>
> The results, at Pearl Harbor, were sudden, concentrated, and dramatic. The failure, however, was cumulative, widespread, and rather drearily familiar. This is why surprise, when it happens to a government, cannot be described just in terms of startled people. Whether at Pearl Harbor or at the Berlin Wall, surprise is everything involved in a government's (or in an alliance's) failure to anticipate effectively."

Thomas C. Schelling,

Forward to Pearl Harbor; Warning and Decision,

by Roberta Wohlstetter

[47] Department of National Defence, Directorate of Strategic Analysis - Policy Planning Division, "Strategic Assessment 2002 – Functional Issues", August 2001, 5

[48] James B. Steinberg et al, "Building Intelligence Networks to Fight Terrorism", Brookings Institute – Policy Brief # 125, 2003, 3

The above forward, written in hind site, provided vivid parallels between the surprise attack on Pearl Harbor in 1941 and the World Trade Centre and Pentagon attacks in 2001. Both events occurred during a time when the US was complacent with respect to possible domestic threats and lacked the integrated intelligence system to raise the alert. There had been some warning of the possibility of both events however the intelligence systems and organizations in place failed to react. Then as now, the US is focused on preventing further surprises and took concrete actions to ensure they are not caught completely unprepared again.

While Canada does not face the same threat it must develop the intelligence systems and domestic capabilities to deny terrorist networks the use of Canada as a staging point for attacks against the US.

RECOMMENDATIONS

The Office of Homeland Defence has been provided a mandate to co-ordinate all American government actions. There is no equivalent lead department in Canada. The Privy Council Office (PCO) is the logical entity to provide the national grand strategy that integrates military and civilian agency efforts and specifies rules of engagement for defensive as well as offensive terrorist operations.[49] Terrorist networks have to recruit, train, plan, gain support, move, stage, attack and regroup during any operation or pursuit of a cause. Ideally there will be an opportunity to

[49] Elaine M. Grossman "Key Review Offers Scant Guidance On Handling '4th Generation' Threats", Inside the Pentagon, 4 October, 2001, 4

attack the network's organizational structure, communication and funding to cause it to fail anywhere along this process prior to the attack.

New Structures to Combat Terrorist Networks

The network theory and netwar concept should be employed in developing and implementing the inter-agency network organizations to provide domestic intelligence and military anti-terrorist capabilities.

Civil service bureaucracies, where employees are unionized and pay scales are linked to hierarchical level rather than function or merit, offer resistance at the very thought of flattening. The Canadian Federal Government and military have approximately 15 grades of civil service/uniformed employees. It is unlikely that al-Qaeda has more than three or four, and its terrorists don't belong to civil service unions. In a bureaucratic organization, we can often observe, that the measures taken to struggle with increasing internal and external complexity are reflected by increasing internal complexity, i.e. more complex information flows through the organizational element.[50]

Toffler, Arquilla and Rondfelt have suggested that hierarchical organizations are unsuitable to combating networks since they do not understand network organizational forms or the importance of identifying key nodes and gateways for attack, furthermore they are too rule bound and too slow to address terrorist networks threats. Only flat cross-organization/agency networks have the ability and speed to combat the terrorist networks in a netwar.

[50] Alvin Toffler, Heidi Toffler, "The War of Pyramids vs. Pancakes and How It Will Shape the Future",
2002

Restricting terrorist network activity in Canada will require the cooperation of numerous domestic security stakeholder departments and agencies. Vertical information stovepipes will have to be cooperatively shared between the multiple stakeholders to put together the best possible threat assessments to combat terrorist networks.

Enhanced Capabilities to Combat Terrorist Networks

The Solicitor General and its agencies (RCMP/CSIS) have the lead for Canadian domestic security. The Canadian military has a support role in this task and has established links with the RCMP and CSIS to assist them when required. The following two capabilities currently exist but will require further development to assist in combating terrorist networks.

Intelligence.

Excellent intelligence is the best defence and weapon against terrorist networks. Terrorist networks, due to their organizational structure, will offer few targets. This will require a variety of intelligence types and sources to be fused together to develop threat assessments. There are many types of intelligence ranging from technical forms such as signal intelligence (SIGINT), which includes communication and electronic intelligence, to human intelligence (HUMINT). Unfortunately Canada has no offshore intelligence operations. Canada does have domestic SIGINT and HUMINT capabilities resident in CSIS and DND agencies like CSE contribute to that capability. The US will likely share international intelligence with Canada to assist in protecting the US defence perimeter to stop terrorists before they enter the US. Canada can take advantage of the US need to protect their borders and push the requirement to develop US and Canadian inter-agency interoperable intelligence networks. The only way for Canada to develop the required threat assessments is to improve intelligence sharing between RCMP, CSIS, CSE, NSA, CIA and the FBI especially for out of country HUMINT. This will of course affect numerous domestic security departments and agencies necessitating horizontal working network structures to establish contact with the security stakeholders, collate and organize the massive amounts of information and develop the threat assessments and exploitation opportunities for action. The list of potential stakeholders is extensive and includes the following Federal Government Departments. It will be important to include equivalent Provincial and Municipal Government agencies as well:

- Department of Foreign Affairs and International Trade,
- Department of National Defence and its portfolio agencies, OCIPEP, CSE and DRDC,
- Solicitor General and its portfolio agencies, RCMP and CSIS,
- Canada Customs and Revenue Agency,
- Transport Canada,
- Immigration Canada, and
- Fisheries and Oceans including the Coast Guard.[51]

Information Operations.

A Canadian military information operations capability is resident in CSE. It is tightly controlled since information operations against individuals and groups require legal approval. CSE received new funding to enhance their technical capability however approval to increase their responsibilities in the information operations niche has been delayed since the summer of 2001 due to political and legal issues.[52] This capability is essential in combating terrorist networks and would allow Canadian intelligence to seize the initiative from terrorist networks by conducting computer network attack (CNA).   The CNA capability would provide voice and data communication monitoring of suspected individuals and groups thereby denying them the use of electronic, wire or informatics.ck (Ckey07 abl5994 Tm(Thdi)Tj0.00211 Tc -0.00011 Tw 12 0 0 4

- passive attacks where software code is deployed throughout the internet to monitor data transfer and e-mail traffic between suspected nodes,[54] and
- analysis of the above data to identify terrorist nodes, traffic patterns, decryption and translation to confirm intent and data consolidation to prepare further active and passive.

Information operations will not completely destroy the terrorist organizations as they will likely adapt to whatever methods are used, such as increasing use of internet cafes where it is almost impossible to trace users. However impeding and denying terrorist communication will force use of other more cumbersome or manual methods that may in turn provide other opportunities for identification since the anonymity of the net will be denied. This will in turn disrupt their communication flows, fund raising and over time their will to fight as the terrorist networks are blocked from proceeding to their attack phase and funding to recruit train, equip and support offensive operations dries up. CSE will have to remain abreast of terrorist technology and tactics to ensure a technology gap does not occur and it maintains its ability to collect and exploit terrorist information as well as providing computer network defence and attack capabilities. We will have little chance of successfully neutralizing terrorist networks if we yield the initiative. Excessive vulnerability invites attack.[55]

[54] Ibid, 29

[55] Anthony H. Cordesman, "Transnational Threats From the Middle East: Crying Wolf or Crying Havoc", January 1999, 65

CONCLUSION

The terrorist network threat is real and a thorough understanding of the forces behind their creation, organizations, means of communicating, tactics and funding is essential to combat them. The best weapon against terrorist networks is cross-organizational networks and excellent intelligence. Excellent intelligence is essential to avoid over reaction and ensure measured actions are taken. Canada does not have the domestic and global intelligence to combat these networks and so will have to develop inter-agency networks between Canadian and American intelligence services. Network structures will be essential to permit interoperability with other Canadian and US intelligence agencies. Information operations will also be essential to successfully attack terrorist networks in this netwar. Inter-operability with Other Government Departments (OGD) and other military organizations is a requisite for success. Without a focus on inter-operability implementation of any PCO grand strategy will be dispersed among the numerous departments and agencies and the focus of the overall strategy will be lost.

Organized across fast acting network structures and armed with intelligence, technology and personnel to conduct information operations against the terrorist networks, Canada can seize the initiative and defend its sovereignty. By doing so, Canada will limit threats to the US from its territory and preserve the free flow of goods and services across its border.

BIBLIOGRAPHY

Agee, Collin A. "Leadership Notes Army Intelligence Master Plan" Military Professional Bulletin, Fort Huachuca, Volume 28, Issue 3, July-September 2002

Arquilla, John et al. The Advent of Netwar, accessed from http://www.comw.org/rma/fulltext/asymmetric.html October 2003

Author Unknown. "Asymmetric Warfare: the USS Cole and the Intifada" The Estimate Volume XII, Number 22, 3 November, 2000

Bergen, Peter L. Holy War Inc.:Inside the Secret World of Osama bin Laden. New York: The Free Press, 2001

Canada, Department of Foreign Affairs and International Trade, "Canada – United States – The World's Largest Trading Relationship", 2002

Canada, Department of National Defence, Strategic Assessment 2002 (Ottawa: Public Works and Government Services Canada), August 2001

Canada, Department of National Defence, "Shaping the Future of Canada's Defence: A Strategy for 2020" (Ottawa: Public Works and Government Services Canada) June 1999

Canada, Department of National Defence, Threat Definition: Asymmetric Threats and Weapons of Mass Destruction (Ottawa: Public Works and Government Services Canada), 2002

Canada, Department of National Defence, A Time for Transformation (Ottawa: Public Works and Government Services Canada) 2003

Charters, Dr. David. "The Future of Military Intelligence Within the Canadian Forces" Canadian Military Journal, Winter 2001-2002

Cordesman, Anthony H. "Transnational Threats From the Middle East: Crying Wolf or Crying Havoc." Center for Strategic and International Studies, 15 January 1999

Cordesman, Anthony H. "Asymmetric Warfare Versus Counterterrorism: Rethinking CBRN and CIP Defence Response" Center for Strategic and International Studies, December 2000

Crawley, Vince "Terror Alert," Army Times, 6 November, 2000

Futerman, J.A.H. "The New World War", April 2002

Gould, Harold A. and Spinney, Franklin C. "Fourth Generation Warfare Is Here" University of Virginia Center for South Asian Students, Fall 2001 Newsletter

Grange, David L. "Asymmetric Warfare: Old Method, New Concern." National Strategy Forum Review, Winter 2000

Gray, Colin S. "Thinking Asymmetrically in Times of Terror", Parameters, Spring 2002

Greenberg, Maurice R. "Terrorist Financing: Report of an Independent Task Force Sponsored by the Council on Foreign Relations", 14 November, 2002

Grossman, Elaine M. "Key Review Offers Scant Guidance On Handling '4th Generation' Threats", Inside the Pentagon, 4 October, 2001

Held, David. "Violence, Law and Justice in a Global Age", Social Sciences Research Council, 5 November, 2001

Jenkins, Brian M. Countering al-Qaeda. Washington: RAND, 2002

Kastoryano, Riva. "The Reach of Transnationalism", Social Sciences Research Council, 2001

Kuran, Timur. "The Religious Undercurrents of Muslim Economic Grievances", Social Sciences Research Council, 2001

Lesser, Ian O. et al. Countering the New Terrorism. Washington: RAND, 1999

Metz, Steven. "Strategic Asymmetry." Military Review, July – August 2001

National Defence Panel, "Transforming Defence: National Security in the 21st Century" Joint Force Quarterly, Summer 1997

Schneider, James L. "A New Form of Warfare." Military Review, January – February 2000

Staten, Clark L. "Asymmetric Warfare, the Evolution and Devolution of Terrorism: The Coming Challenge for Emergency and National Security Forces." 27 April, 1998

Steinberg, James B. et al. "Building Intelligence Networks to Fight Terrorism", Brookings Institute – Policy Brief # 125, 2003

Strickland, Lee S. "Fighting Terrorism With Information", The Information Management Journal, July-August 2002

Toffler, Alvin. et al. "The War of Pyramids vs. Pancakes and How It Will Shape the Future", *2002*

Tucker, Jonathan B. "Asymmetric Warfare." Forum for Applied Research and Public Policy, Summer 1999

United States, Department of Defence, Quadrennial Defence Review Report, Washington D.C. US Government Printing Office, 1997

United States, Department of Defence, Quadrennial Defence Review Report, Washington D.C. US Government Printing Office, 2001

United States, Department of Defence, Joint Chiefs of Staff, Joint Vision 2010, Washington D.C. US Government Printing Office, 1997

United States, Department of Defence, Network Centric Warfare: Department of Defence Report to Congress, Washington D.C. US Government Printing Office, 2001`

United States, Council on Foreign Relations, Terrorist Financing: Report of an Independent Task Force, Washington D.C.: US Government Printing Office, 2001

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

Van Creveld, Martin. Technology and War. New York: Free Press, 1989

Vatis, Michael A. "Cyber Attacks During the War on Terrorism: A Predictive Analysis." 22 September, 2001

Young, Hugo. "It May Not be PC to Say" The Guardian, 8 October, 2001