CANADIAN FORCES COLLEGE / COLLÈGE DES FORCES CANADIENNES

CSC 30 / CCEM 30

MASTERS OF DEFENCE STUDIES/MAÎTRISE EN ÉTUDES DE LA DÉFENSE

LEVERAGING NETWORK STRENGTHS TO DEFEAT TERRORIST NETWORKS

By /par Cdr Guy Desjardins

ABSTRACT

A network is an effective and robust form of organization based on relationships from which non-state actors can garner a significant amount of influence. Arquilla and Ronfeldt have coined as 'netwar' the use of network and information age doctrines and strategies to conduct conflicts. The events of 9/11 have demonstrated that in netwar, a criminal network such as Al-Qaeda can be a potent adversary to stove-piped, non-networked organizations, such as government hierarchies. It takes a network to fight a network and to succeed in the Global War on Terrorism, governments need to employ all instruments of national power and must reorganize some of their assets to leverage the potential offered by that organizational form and reduce barriers between themselves. Within that networked environment, conventional forces should only be used in a supporting role to intelligence and law enforcement agencies. The brunt of the military effort must come from small and agile Special Operations Forces that rely on relations, rather than weapons, to operate within the lawful network.

TABLE OF CONTENTS

We want our land to be free of enemies. We want our land to be freed of the Americans. – Osama bin Laden, 1998[1]

Our duty is to rouse the Muslim nation for jihad against the United States, Israel and their supporters, for the sake of God. – Osama bin Laden, 1998[2]

INTRODUCTION

The bombing of US military barracks in Saudi Arabia in 1996, the bombing of American embassies in Kenya and Tanzania in 1998, the attack against the USS COLE in Yemen in 2000, the attacks of 11 September 2001 (9/11) on US soil and the bombings in Bali, Jakarta, Casablanca and Madrid were all perpetrated by a network of Islamic terrorist groups in which Osama bin Laden is predominant. While bin Laden has yet to be successful at annihilating US involvement in the Muslim world, he has managed to terrorize an entire country by serving blows to two pillars of American society: its economy and its military. When compared to most wars, the number of lives lost and the destruction caused by the attacks of 11 September 2001 were relatively small. However, the US was not at war and its population was certainly not expecting to become a victim of such brutal attacks at home. The terrorizing effect of 9/11 transcended borders; grief and insecurity were felt the world over. Naturally, this sense of insecurity was at a peak in the US due to the shock caused by the first attack on US soil since World War II. How is it possible that a small non-state actor could inflict so much damage and cause so much fear to the sole remaining super power? How could one man supported by a group of terrorists strike such a blow to the mighty US and its well-resourced

[1] Jane Corbin, Jane. *Al-Qaeda, In Search of the Terror Network that Threatens the World* (New York: Thunder's Mouth Press, 2002), 26.

[2] Ibid, 41.

intelligence and security services? Better yet, how can the US and other countries rid themselves of the threat posed by terrorist networks?

This research will reveal that criminal groups derive tremendous synergy from their organizational structure: the network. A review of organizational theory will highlight the characteristics of networks and will demonstrate the inherent strength of that type of organization, its resiliency and its ability to exploit the weaknesses of traditional hierarchies. Events leading to the attacks of 9/11 will be used to show the inability of traditional government hierarchies to defend against well-organized, networked groups such as Al-Qaeda. This will lead to the central thesis of this research: it takes a network to defeat another network. As such, it will be argued that the best way to counter terrorist networks is to emulate their organizational structure in an effort to fill the gaps between hierarchies and to leverage the strengths of networks. This research will conclude with a section dedicated to the role of the military within that networked environment. It will be argued that the military can play an important role in the war on terrorism; however, unlike other wars, the use of kinetic military force should be limited and politicians should seek instead to employ networked military competencies to establish global order and security.

SECTION 1 – BACKGROUND AND FRAMEWORK

The end of the Cold War has resulted in significant changes in the global political, strategic and military landscape. Through the nineties, as western democracies realized that the communist threat had waned, most countries reviewed their Defence Policies and proceeded to cash-in the so-called peace dividends brought about by the end of the War. This was done by reducing military forces, infrastructure and equipment and by reconsidering commitments to Alliances such as NATO. Nevertheless, the last decade of the Twentieth century had its share of conflicts that did not spare any continent; a sober reminder that despite the end of the Cold War, global peace had yet to be achieved and highlighting that the ability to project and employ credible military forces remained one of the tools favoured by politicians. Interventions in Kuwait, Bosnia, Kosovo, Somalia, Ethiopia, Rwanda, Haiti and East-Timor represent some of the examples where the use of military force by third parties was deemed necessary to restore order. The United States, as the sole remaining superpower, seldom hesitated to take the lead and wield its impressive military, economic and diplomatic might to protect its interests. However, American foreign policy, values and standards were not universally accepted.

Over the years, the US pro-Israeli position in the Middle East has resulted in increased tensions between Arab states and the US. In many circles, American involvement in Arab affairs is considered an assault on their right for self-determination and self-governance. In addition, American values are now omnipresent around the world due to globalization and the explosion in the area of telecommunications. Indeed,

these two phenomena have contributed to spreading the liberal and permissive American culture to predominantly Muslim countries that have difficulty tolerating pluralism. The result is that many Muslim fundamentalist organizations unilaterally reject American hegemony and everything that is American. These groups' inability to peacefully influence the superpower has led them to resort to violence to harass and weaken them. Osama bin Laden and his Al-Qaeda network of terrorists examplify how terrorists have targeted American diplomatic and military facilities located outside the US.

On 11 September 2001, the Al-Qaeda network continued to live up to its threats and managed to exploit some of the weaknesses of the United-States by delivering bold and carefully planned attacks in New York and Washington. The tragic events of 9/11 were neither perpetrated by military forces nor states but they had a de-stabilizing effect on peace nonetheless. Following these terrorist attacks, President Bush has vowed to defeat terrorist groups and countries that harbour them by declaring War on Terrorism. On 20 September 2001, he stated, "Our war on terror begins with Al-Qaeda, but it does not end there. It will not end until every terrorist group of global reach has been found, stopped and defeated."[3] Since then, two significant military campaigns have taken place in Afghanistan and in Iraq. To date and from an American point of view, the Global War on Terrorism (GWOT) and the introduction of various security measures in the US and around the world have been effective since they have precluded the recurrence of significant terrorist attacks against the US. Nevertheless, given the recent bombing in Madrid, it is clear that the terrorist threat has yet to be quashed; many members of Al-

[3]President Bush Address to a Joint Session of Congress and the American People, 20 September 2001 http://www.whitehouse.gov/news/releases/2001/09/20010920-8.html; accessed 25 February 2004.

Qaeda, including its leader, continue to be on the loose and present a serious threat to global security. Is the defeat of global terrorism an achievable goal or does it belong to utopia along with the eradication of drug trafficking?

Rather then attempting to answer the preceding question, it is worthwhile at this point to draw a few parallels between the war on drugs and the war on transnational terrorism to highlight some of the challenges at hand. Both of these illegal activities are underground and as such, they do not present clearly defined head offices or organizations that can easily be targeted. Generally, these organizations consist of a complex web of actors that have a high degree of autonomy but which depend on one another for the accomplishment of mutually satisfying goals. Unlike most other organizations, terrorist networks and drug rings do not exist for the sole benefit of the organization. The organization is not an end unto itself; it is a means to an end, which could be a political cause in the case of tey 9 Tm(f)Tj12 0 906lancise gaian case of te

across the public, private, and civic sectors is both highly important and very difficult."[4] In sum, the war on terrorism, much like the war on drugs, represent a confrontation between governments and fluid organizations that are difficult to pin down. These organizations derive their strength from their basic construct: the network.

The study that follows is based on ideas and concepts regarding networks as organizational structures proposed by John Arquilla and David Ronfeldt of the RAND's National Defense Research Institute.[5] For over a decade, these two authors have used the concept of computer networks to demonstrate "the rise of network forms of organizations… across the spectrum of conflict, including among ethno nationalists, terrorists, guerrillas, criminals, and activists."[6] Since the study of the network as an organizational form is relatively new, literature on the subject is very limited. The subject is commonly discussed in the fields of computer science and business (self-managed teams) but it is seldom discussed in regards to criminal organizations. Arquilla and Ronfeldt are two of the most published authors in the field of network organizations and their work is recognized by many including Phil Williams, a leading authority on transnational criminal networks. Given the limited sources available on this subject, the discussion on network theory and netwar rely heavily on the work of Arquilla and Ronfeldt.

[4] Jonathan P. Caulkins, Mark A.R. Kleiman and Peter Reuter. "Lessons of the War on Drugs for the War on Terrorism." In *Countering Terrorism* ed. Arnold M. Howitt and Robyn L. Pangi (Cambridge: Harvard University, 2003), 73.

[5] RAND® is an American nonprofit institution, created by the US Air Force to help improve policy and decision making through research and analysis.

[6] John Arquilla and David Ronfeldt, *Networks and Netwars* (Santa Monica: Rand, 2001), 19.

The focus of this study is to demonstrate that transnational terrorists draw their strength from their networked organization and that to opposed them effectively, authorities will need to adjust their hierarchical organizations and form responsive and flexible networks of their own. To narrow the scope of this work, the terrorist network studied will be Al-Qaeda and the 'authority' to be networked will focus on the United States and its response to counter transnational terrorist networks with an emphasis on the role of the military in the Global War on Terrorism.

SECTION 2 –NETWORKS

This section consists of a review of some of the theory that pertains to networks and a comparison between networks and hierarchies. This will be accomplished initially by defining networks and reviewing briefly their evolution over time. Using Al-Qaeda as a case study, organizational networks as we know them today will then be studied to provide a common understanding of the characteristics and inherent strengths of this type of organization. The discussion will then conclude with the demonstration that networked organizations enjoy a net advantage over those that are organized along traditional hierarchical lines. These findings will subsequently be used in this study to substantiate the need to network resources in order to successfully counter the terrorist threat.

2.1 Networks Defined

The word *network* is not new to the English language. In 1913, it was defined as "any system of lines or channels interlacing or crossing like the fabric of a net; as, a network of veins; a network of railroads."[7] Later, the term was utilized by social scientists to characterize relationships between individuals and organizations. Since then, the term network has been used in telecommunication to characterize groups of broadcasting stations (radio and television) and more recently, it has been adopted by computer science to represent a web of interconnected computers.[8] As will be

[7] Webster Dictionary, 1913, http://machaut.uchicago.edu/cgi-bin/WEBSTER.sh?WORD=network accessed 28 February 2004.

[8] The Pocket Oxford Dictionary, 8th Ed.

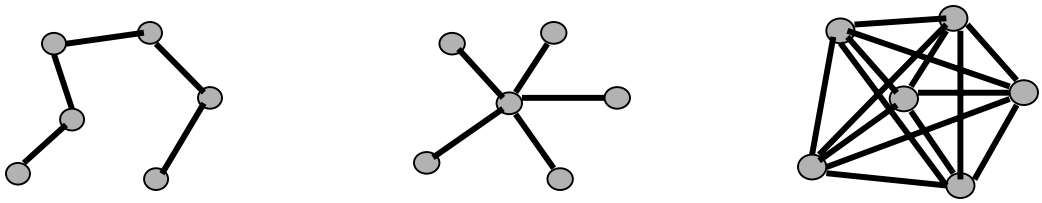
demonstrated below, it is not by coincidence that networks have become omnipresent; they constitute a robust construct that can optimize the effectiveness of individuals, businesses, equipment and terrorists alike. Notwithstanding the merits of all types of network, this study will focus on the social aspects of networks.

Networks are one of the most common forms of social organization. They are simultaneously pervasive and intangible, ubiquitous and invisible, everywhere and nowhere.[9]

A network is a series of nodes, which represent individuals or organizations that are connected or tied through some form of relationship.[10] As depicted in Figure 1, there are three basic types of network: the line or chain network, the hub, star or wheel network and the all-channel network. In the chain network, people, goods or information move in a sequential fashion between nodes as is the case in smuggling activities.[11] In the hub (star or wheel) network, nodes in the periphery must go through one central actor in order to coordinate or communicate with other nodes as in a franchise or a cartel.[12] In the all-channel network, communication is possible between every single node as in a collaborative network of militant groups where everybody is connected to everybody else.[13] In practice, networks seldom resemble perfectly any of these three types and they will likely take a hybrid form. The all-channel type of network is the form that is the

[9] Phil Williams. "Transnational Criminal Networks". In *Networks and Netwars ed.* John Arquilla and David Ronfeldt (Santa Monica CA: Rand, 2001), 64.
[10] Ibid, 66.
[11] John Aquilla and David Ronfeldt. *Networks and Netwars*…7.
[12] Ibid.
[13] Ibid, 8.

most difficult to establish and sustain but once in place, it has boundless potential;[14] that will become evident as the discussion progresses.



Line or Chain | Hub, Star or Wheel | All-Channel

Figure 1 – Types of networks

2.2 Components of Networks

The ties between nodes can be strongly coupled or loosely coupled.[15] In the former, the ties are well established, well oiled and there is strong co dependence between the nodes. Such ties can be highly effective when all goes well but this type of arrangement may engender chaos within the network if it is disrupted. When the nodes in a network are loosely coupled, any node can be adjusted, repositioned or removed without affecting the whole network.[16] For this reason, loosely coupled ties offer the most flexibility and resiliency to the network. Ties can also be strong or weak. Strong ties are present in established relationships that involve a sense of obligation or indebtedness; weak ties represent acquaintances or casual relationship.[17] A mixture of both strong and weak ties is necessary in an effective network since it is likely to promote balance, flexibility and redundancy.

---

[14] Ibid, 9.

[15] John Urry, *Global Complexity* (Cambridge: Polity *Press: 2003),* 52.

[16] Gernot Grabher and David Stark, "Organizing Diversity: Evolutionary Theory, Network Analysis and Postsocialism." *Regional Studies*, Vol. 31, Iss. 5 (July 1997): 538.

[17] Ibid.

THE CORE

As indicated earlier, a network will likely have a hybrid shape that could resemble the structure shown below in Figure 2. Once again, nodes may represent individuals or organizations, or parts of organizations that could be hierarchies or even networks. Within the entire network, some of the nodes are located under layers of nodes and represent the core of the network. Nodes positioned away from the core represent the networks' periphery. The core is characterized by dense connections between nodes and it generally provides leadership within the network through direction and coordination.[18] Depending on the nature of the network, the leadership provided by the core can be strong, providing clear and precise directions on activities to be conducted or it can be loose, providing general guidance on the desired effect that is sought. The core of Al-Qaeda is Osama bin Laden and his close associates. Together, they elaborate broad strategies for the network and they provide resources for their accomplishment. The leadership in Al-Qaeda is loose and de-centralized; the sub-components of the network have freedom to manoeuvre but, whenever necessary, the components interact, merge or cooperate ideologically, financially and technically.[19]

While strong leadership may lead to a quicker achievement of results, it may inhibit creativity and decrease flexibility if it provides too much direction. Strong centralized leadership is therefore not desirable since it may negate some of the strengths inherent to the network, such as flexibility and creativity. A centralized network may

[18] Phil Williams. "Transnational Criminal Networks"…, 72.
[19] Rowan Gunaratna. *Inside Al Qaeda* (New York: Columbia University Press, 2002), 57.

also present a centre of gravity (a heart or head that can be targeted), thus decreasing its resiliency.[20] Loose leadership may be less efficient but it will allow the network to determine on its own the best means of achieving the desired effect through the selection of the most effective means available within the network. Therefore, a network that is loosely led, such as Al-Qaeda, is likely to be more potent and effective than if it is led and directed in a firmer manner. Regardless of the leadership style, in an effective network, the relationship between core and periphery "is often underpinned by bonding mechanism that help to create high degrees of trust and cohesion."[21] Within Al-Qaeda, that bond comes from shared ideology and religion and past service in conflicts or training camps. The social bonds that exist within the network constitute the glue that keeps its components tied together.

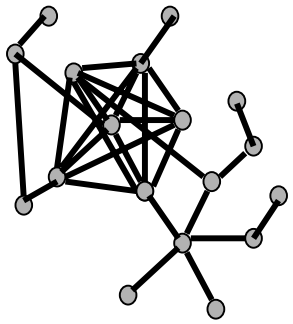


Figure 2 – Hybrid network

THE PERIPHERY

The core of the network acts as its nervous system and the periphery acts as its eyes, ears, mouth and limbs. Just like the limbs of the human body, the periphery plays

[20] John Aquilla and David Ronfeldt. *Networks and Netwars*…9.
[21] Phil Williams. "Transnational Criminal Networks"…, 72.

essential roles within networks. It can act in a sensorial role and be used to collect information that will be transmitted to the appropriate nodes in the network. It can also be used to transmit information from the network to the 'world' outside of the network. Therefore, the periphery of the network can be used as an interface between the network and the environment in which it exists. Assuming that the network exists to further illicit interests, the periphery will be used as a gateway to the licit world. This may not be the sole purview of the periphery and other nodes will likely span borders also. However, the periphery's position away from the core of the network makes it ideally suited to evolve simultaneously as part of the network and outside of it.

Loosely connected nodes, such as the Hamburg cell of Al-Qaeda, which contributed perpetrators to 9/11, also operate in the periphery. Their members lead a normal life without raising any kind of suspicion from their surroundings and wait to be called upon when their services are required. Further, some very useful nodes in the periphery are those that belong to licit organizations (such as law enforcement agencies) that must be bypassed, used or defeated by the network in order to achieve its objectives. These people who support a criminal network while continuing to operate in licit institutions (government, businesses, financial) are called crossovers[22]. Crossovers can be established in one of three ways: bribes/blackmailing, recruiting and infiltration. "By operating in a different sphere from most of the network, they [crossovers] are able to provide invaluable information and protection."[23]

[22] Phil Williams. "Transnational Criminal Networks"…, 83.
[23] Ibid.

2.2 Network Protection

Criminal networks have defence mechanisms that are peculiar to that form of organization. They are intangible because they are based on social ties between people and organizations, and because they seldom rely on large infrastructure. These social ties are extremely difficult to discern and therefore provide the network with its first line of defence. It may be possible to uncover and target a portion of the network but its diversity and redundancy will decrease the likelihood that the entire network will be disclosed and confronted at once.[24] Given its diffused construct, attacks on the network will likely result in limited damages to the organization.

As stated earlier, the core of the network is its nervous system and as such, it can be a centre of gravity or vulnerability for the network. However, the core of the network is protected by one or more layers of nodes that will act as sensors and shields that can absorb or deflect such attacks. This is the second line of defence which is referred to as a 'self-healing network' in modern telecommunication. Indeed, given their remoteness from the core, nodes on the periphery of the network would therefore become expendable if they came under attack or if they were to be captured or destroyed. This could disrupt the activities of the network, but it would adjust to the blow by mutating its organization and its activities.

Similarly, the network may be constructed with circuit breakers between its components. Figure 3 depicts three cells that belong to a larger network. Each of the

[24] John Aquilla and David Ronfeldt. "Osama bin Laden and the Advent of Netwar." *New Perspectives Quarterly*, Vol. 18 Iss. 4 (Oct 2001): 30.

cells are composed of a number of nodes that are integrated in an all-channel fashion within the cell. The cells interact with other cells through very specific ties. For instance, Cell A's interaction with Cell B can only be conducted through the tie between nodes A1 and B1. The nodes in Cell A do not know or interact with any other nodes in Cell B and, if node A1 were to be compromised, the extent of the damages would potentially be limited to the nodes in Cell A and nodes B1 and C1 in Cells B and C. The circuit breakers in place between cells isolate their components and constitute a third line of defence. This type of defence is used by Al-Qaeda whereby a cell leader is the only member in the cell to maintain a tie to the network through a controller who acts as the interface with the remainder of the network.[25]

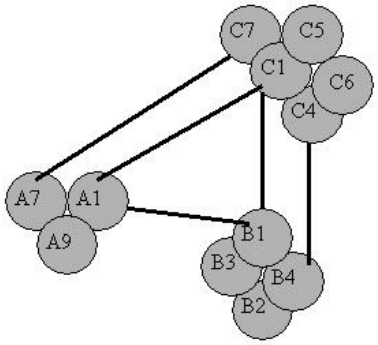


Figure 3 – Circuit Breaker

The fourth line of defence of the network is as intangible as the network itself. It resides in the culture of the network. This can take the form of unwritten rules or informal codes of conduct that transcend the network. Since networks are based on social ties, adhesion to the network is not universal; one does not decide to join a

[25] Rowan Gunaratna. *Inside Al Qaeda* …, 97-98.

network, one is chosen. Naturally, those who are asked to join the network will have earned trust and will have demonstrated that they possess some of the attributes, be it ideology, religion, race or skills that are sought by the network. In criminal circles, ethnicity and language are often used as a protective armour that limits the infiltration of the network by unwanted individuals.[26] In sum, networks are hard to discern, difficult to target as a whole and difficult to infiltrate. These characteristics protect the networks and make them adversaries that are hard to defeat.

2.4 The Al-Qaeda Network

Following the theoretical study of networks, the time has come to take a closer look at Al-Qaeda from a practical perspective. More specifically, Al-Qaeda will be used to illustrate how terrorist organizations have managed to leverage the strengths of its organizational construct. Al-Qaeda consists of an extremely large and complex network of people, cells and organizations; the aim is not to describe that organization in details but rather to provide a sense of how that network operates.

"Al-Qaeda… represents more than a decade of organizational development built upon relationships that were first established in the 1980s."[27] The Genesis of Al-Qaeda comes from the call to jihad against the Soviets in Afghanistan,[28] which later transformed into Islamic movements opposed to ruling regimes in the Middle East.[29] Today, Al-Qaeda consists of a complex web of loosely connected organizations that are dedicated in

[26] Phil Williams. "Transnational Criminal Networks"…, 75.
[27] Brian Michael Jenkins. *Countering al Qaeda* (Santa Monica: Rand, 2002), 18.
[28] Richard Bernstein. *Out of the Blue* (New York: Times Books, 2002), 16.
[29] Rowan Gunaratna. *Inside Al Qaeda*…, 55.

one way or another to promoting Islam and annihilating the dominance of non-believers over the Muslim population. This global network is reportedly established in at least sixty countries spanning every continent on the globe.[30] It is well organized, it has access to a wealth of financial and human resources and its members are trained and dedicated to their cause. Martyrdom is encouraged and as a result, violence is often used indiscriminately to terrorize and sensitize Muslims and non-believers to the grievances of the Islamic radicals in the network.

Networks such as Al-Qaeda cannot exist in a vacuum, oblivious to their environment. In order to maintain their livelihood and to maximize their effectiveness, they will attempt to extend the reach of their periphery as much as possible into the realm of the licit world. Al-Qaeda achieves this by maintaining close ties with Muslim communities. These ties are critical when it comes to intelligence gathering for both offensive and defensive purposes. In an offensive mode, intelligence gathering will allow the network to gain a thorough understanding of its environment and to identify weaknesses that can be exploited. On the defensive front, good intelligence will give the network the opportunity to identify threats early, thus allowing it to adjust its plans or mutate in order to minimize the effects of the blows. Crossovers also have access to the licit organizations and can collect intelligence, provide official documents (such as passports, registrations, custom documents) and assist the network in the procurement of goods, money laundering or the movement of people, goods and money.

[30] Brian Michael Jenkins. *Countering al Qaeda* …, 9.

The Al-Qaeda network relies on a variety of funding sources that allows it to support its operations, which are estimated to cost more than US$36M per year.[31] In order to raise, control and distribute a budget of that magnitude, the network has in place an elaborate system that spans both the lawful and the illicit domains. The main source of funding for the network is thought to be the contributions received from wealthy Arab benefactors.[32] In addition, the network has a well-developed periphery and it draws resources from legitimate businesses and investments that are owned in part or in total by Al-Qaeda and sympathetic organizations around the world.[33] It also relies on criminal activities, as is the case in its European financial network where the Algerians are heavily involved in credit card fraud and credit card counterfeiting,[34] and it siphons funds from legitimate and illegitimate Islamic charities and Non-Governmental Organizations, which it has infiltrated.[35] To bring it all together, Al-Qaeda uses a combination of legitimate banks, informal banking systems (hawala) and couriers to safeguard and transfer its funds.[36]

Al-Qaeda's high level of sophistication is not limited to its ability to generate and move funds around the world. The network also possesses elaborate means of recruiting, indoctrinating and training its most valuable resource: its members. "Al-Qaeda is a political group driven by an interpretive religious ideology, it operates on the basis of a

[31] Rowan Gunaratna. *Inside Al Qaeda* …, 61.
[32] Jason Burke. *Al-Qaeda: Casting a Shadow of* Terror (New York: I.B. Tauris &Co Ltd, 2003), 224.
[33] Rowan Gunaratna. *Inside Al Qaeda* …, 67.
[34] Ibid, 65.
[35] Ibid, 62 and 112.
[36] Ibid, 63.

cultural network, recruiting known persons…"[37] In recent years, it has targeted educated young men of keen intelligence and religious zeal who have the ability and language skills to operate in a non-Islamic environment.[38] Before the birth of Al-Qaeda in the nineties, thousands were recruited and trained to fight the Soviets in Afghanistan. The lessons drawn from that campaign have been compiled in a thirteen volume Encyclopaedia of Jihad and one volume Jihad Manual, which cover such topics as tactics, topography, intelligence, handguns and explosives.[39] [40] This Encyclopaedia was also used to train guerrillas who have fought in Chechnya, Bosnia, Kashmir, the Philippines and the Horn of Africa. While many young Muslim mercenaries have been trained and have taken part in guerrilla warfare, it is important to recognize that only a portion of them have continued to be members of Al-Qaeda.[41] Nevertheless, this training and war fighting in Afghanistan and elsewhere have created long lasting relationships that can be used by the network to recruit new members when the need arises.

2.5 Globalization and Failed States: Enablers

In the last two decades, the phenomenal progresses in the field of telecommunications have enabled networks to broaden their scope and transcend borders. Technological developments in cellular phones and the Internet provide the means to keep nodes connected to the network no matter where they are situated geographically. Moreover, the decrease of barriers between states has benefited networks by facilitating

[37] Ibid, 57.
[38] Ed Blanche, "Al-Qaeda Recruitment." *Jane's Intelligence Review*, January 1, 2002, 28.
[39] Rowan Gunaratna. *Inside Al Qaeda* …, 70.
[40] Bruce Hoffman, *Al-Qaeda, Trends in Terrorism and Future Potentialities: An Assessment*. (Santa Monica CA: RAND, 2002), 13.
[41] Rowan Gunaratna. *Inside Al Qaeda* …, 72.

the movement of people, funds and goods between countries. Since networks are based on relationships, they need not be established in a specific country. Nevertheless, criminal networks may seek to establish their nodes in countries that are favourable, or at least not unilaterally opposed to the network and its operations. For terrorist networks, failed states provide a wide array of opportunities that can be leveraged by the outlaws.

Failed states provide four main attractions: the ability to acquire territory, weak law- enforcement, a potential pool of recruits and, the protection and legitimacy of a sovereign state.[42] If there is a strong relationship between the network and the failed state, as was the case between Al-Qaeda and the Talibans in Afghanistan, then it can evolve into a mutually supporting relationship where both players benefit from the interaction with the other.[43] Infrastructure is generally shunned away by terrorist networks since it offers a centre of gravity that can be targeted. Nevertheless, if the environment is favourable, terrorist networks may choose to expand their footprint from the traditional safe houses to a territory that can support training facilities, arms depots and communication facilities.[44] Through payoffs or the exchange of services, the terrorists may be allowed to work away from the scrutiny of the government and may exist outside the rest of society.[45] Failed states are prone to having lax laws and weak law-enforcement agencies, thus permitting the network to engage in smuggling and trafficking all kinds of goods to finance its activities.[46] Weak laws and weak law-

[42] Ray Takeyh and Nikolas Gvosdev. "Do Terrorist Networks Need a Home?" *The Washington Quarterly*, Vol. 25 No 3 (Summer 2002), 98-100.

[43] Jeffrey Record, *Collapsed Countries, Casualty, Dread and the New American Way of War*. Parameters, Vol 32, Iss. 2, Summer 2002, 5.

[44] Ray Takeyh and Nikolas Gvosdev. "Do Terrorist Networks Need a Home?"…, 98.

[45] Ibid, 98-99.

[46] Ibid, 99.

enforcement agencies also mean that the movement of personnel, weapons and capital to, from and within the failed state will not be subjected to the controls that are normally in place in other states; therefore limiting the obstacles in the path of the network.

"Failed states create pools of recruits and supporters for terrorist groups, who can use their resources and organizations to step into the vacuum left by the collapse of civil society."[47] The lack of employment and the financial strife that ensues will increase the attraction of the network in the eyes of unemployed, adventurous young men who will accept employment within the network. Difficult economic conditions will also facilitate the bribing of officials or authorities still in place. Finally, one of the main features of failed states is that they legally remain sovereign states. As such, the United Nations Charter prevents the intervention of states in the internal affairs of another state thus limiting the possibility of external attacks against terrorist groups established in a failed state. As a sovereign state, a failed state retains the right to issue official documents that can be used by terrorists to obtain passports that will enable them to dissimulate their real identity and their movements around the world.[48] Finally, failed-states may retain the ability to legitimately procure weapons, which can subsequently be sold to terrorists. Otherwise, arms trafficking within the failed state will likely be rampant.

Al-Qaeda was first based in Khartoum, Sudan from its creation in 1991 until May 1996.[49] While in Sudan, it established numerous training camps, it infiltrated various

[47] Ibid, 100.
[48] Ibid, 101.
[49] Rowan Gunaratna. *Inside Al Qaeda* …, 95.

government agencies and it used military facilities to test and develop weapons.[50] Sudan was also used by Al-Qaeda as a transfer point for weapons.[51] When increasing pressure was put on Sudan by the US, Saudi Arabia and Egypt for its support of Islamic radicalism, the support for Al-Qaeda started to wan and Osama bin Laden relocated to Afghanistan where the political situation was more favourable.[52] The establishment of Al-Qaeda in Afghanistan was certainly beneficial for a number of years but the massing of personnel and equipment in that country facilitated the disruption of the network by American forces. To date, the blows have not been fatal but they have demonstrated why criminal networks need to remain flexible, mobile and relatively free of infrastructure.

In summary, progresses in telecommunications and the advent of globalization mean that wireless networks can now easily span geographical borders without too much difficulty. By definition, criminal networks have an element of mobility and can reconfigure and relocate themselves as required. While they need some support infrastructure to operate, they do not need large infrastructure. Nevertheless, failed states provide networks with the opportunity of establishing themselves in a specific location where the inherent weaknesses of the state can be leveraged extensively to further the interests of the networks. For this reason alone, components of criminal networks will continue to migrate to failed states where they enjoy support and freedom of action.

[50] Ibid, 157-8.
[51] Ibid, 158.
[52] Jason Burke. *Al-Qaeda: Casting a Shadow of* Terror …, 141.

2.6 Network Strengths

Networks display various other strengths, many have been alluded to already. They are compiled here to provide a basis for comparison between networks and hierarchies. These strong attributes include the following.

Diversity: Networks can be composed of a collection of individuals and organizations that cover a wide breadth of disciplines. Al-Qaeda has members from all walks of life spanning lawful and illicit organizations. The nodes that are incorporated in the network will vary based on the nature of the network and the tasks to be accomplished. This diversity will allow the network to perform a wide array of activities spanning the lawful and illicit spectrums.

Redundancy: Networks that have a high density of ties between nodes offer a variety of paths that can be taken to communicate information or transfer goods and services. In addition, the ties between the network and a plethora of nodes on the periphery act as a buffer and a guarantee that the required skills are always available to the network. "Network redundancy makes it possible to maintain organizational integrity in an extremely inhospitable environment."[53]

Flexibility: A high density of ties between nodes also provides flexibility because there is more than one way to connect the dots. Therefore, the permanent or temporary elimination of a node does not necessarily disrupt network activities since the network

[53] Phil Williams. "Transnational Criminal Networks"…, 81.

can mutate and adopt a new configuration when some of its components are no longer accessible. In addition, diversity and redundancy provide a significant amount of flexibility and adaptability when the environment surrounding the network evolves as a result of new laws or new opponents for instance.

Responsiveness: The web of ties between nodes provides the potential to quickly disseminate information and goods throughout the network. Decentralized decision-making, mission command and the flexibility inherent to the network allow the use of initiative when unexpected opportunities arise.

Stealthiness: Since networks are based on social relationships and do not have a large infrastructure, they cannot be identified and located easily. Criminal networks are naturally hidden under a veil of secrecy that can also be armoured by foreign cultures and languages.

Protection: Criminal networks in general and Al-Qaeda in particular are shielded by social ties, layers of nodes, circuit breakers and a culture of their own. Since the beginning of the GWOT, a large number of cells belonging to the Al-Qaeda network have been identified and neutralized. However, the network's creator has yet to be captured and Al-Qaeda continues to claim attacks, thus indicating that components of the network remain intact.

Lawlessness: By definition, criminal networks are not constrained by a legal framework thus providing them freedom to manoeuvre and the ability to retain the initiative. While this feature is quite attractive for the recruitment of radicals, it can also be viewed as a weakness because of its failure to rally moderate individuals and the public at large. Nevertheless, Al-Qaeda does not hesitate to break laws to attack and terrorize its enemies. For Al-Qaeda, lawlessness means that opportunities are plentiful.

Global nature: Telecommunications and globalization benefit networks, which can now operate and move more freely between states. They are not limited to the boundaries of a country and they benefit immensely by having nodes in various geographic locations, whether these locations are friendly or hostile. Al-Qaeda is present on every continent in more than sixty countries where it maintain ties with moderate and radical Muslim organizations.

2.7 Networks versus Hierarchies

Armed with a good understanding of networks and Al-Qaeda, networks will be compared to another form of organization, the hierarchy. The aim of this discussion is to highlight the main differences between the two types of organizations and to demonstrate that criminal networks have a net advantage over their opponents, which are typically organized in a hierarchical fashion.

HIERARCHIES

The Oxford dictionary defines hierarchy as a "system of grades of status or authority ranked one above the other."[54] In hierarchical organizations, power is concentrated at the top of the pyramid. This type of organization is favoured because it allows unity of command, which translates in the ability to lead and coordinate the efforts of large organizations that work on complex and on-going activities such as programs and projects.[55] In a hierarchy, authority and accountability flow from the top down, responsibilities are generally well defined, and it is possible to attribute outcomes to specific members or units of the organization. In a nutshell, hierarchies fulfill the need for structure and accountability and they get big jobs done.[56] However, hierarchies and more specifically those that belong to governments since they are the ones opposed to criminal networks, have their share of shortcomings, including sluggish bureaucracies and the creation of silos within and between state agencies.

Hierarchies are essential in governments given the scope and the complexity of administrating states' programs in accordance with the applicable legislation. Hierarchies are also necessary to assign responsibilities, authorities and accountabilities. Given the legal foundation of governments and the constant scrutiny of the public, it is not surprising that these organizations are extremely risk adverse and focused on their survival, or that of their leader, as much as the program they are responsible to deliver. This concern for survival leads to the creation of a variety of controls, which necessitate

[54] The Pocket Oxford Dictionary, 8th Ed.

[55] Harold J. Leavitt. "Why Hierarchies Thrive." *Harvard Business Review*, Vol. 81 Iss. 3 (March 2003): 101.

[56] Ibid, 98.

large bureaucracies that are heavy and lack responsiveness. Left unchecked, government hierarchies can become self-serving, inflexible and ineffective in the delivery of their programs.

With the assignment of specific responsibilities, authority and accountabilities, government officials often get mandates that are decreed by government acts, which clearly define their playing field. Officials are evaluated on how well they control the environment that is assigned to them and they are emphatically discouraged to step outside of their jurisdictions. These boundaries, whether they are legal or self-imposed, are organizational silos that limit the overall effectiveness of hierarchical organizations.

The silos can dissuade interaction between organizations and can act as blinders, preventing workers from focusing on the big picture rather than the boss' limited vision. Silos promote tribalism, limit initiative and are responsible for the creation of seams between government agencies. Ideally, these seams should be strong and state agencies should have good communication between themselves, and procedures and systems that interface seamlessly. Unfortunately these agencies may be in competition for power and resources and the seams between them may be weak, thus providing opportunities that can be exploited by savvy criminal networks. These opportunities have the potential to grow significantly as activities cross geographical borders, thus increasing the number of seams that can be exploited.

AL-QAEDA VERSUS HIERARCHIES

We had not been attacked in our homeland since Pearl Harbor and we didn't feel that America itself was the target of terrorist activities. There were serious breakdowns in our systems – and they had a fatal impact. -Senator Bob Graham, Chair, Senate Intelligence Committee, November 2002[57]

The attacks of 9/11 were the result of breakdowns between a variety of international and American agencies that were exploited by a shrewd terrorist network. Some experts contend that as many as a dozen agencies can be blamed at least partially for their failure to detect the attacks.[58] The following examples demonstrate the blatant lack of networking between some of the hierarchical agencies.

The perpetrators of the attacks were carefully chosen for their lack of association with Islamic radical organizations in the US and abroad, therefore limiting the chance that they would be tracked by intelligence agencies before the attacks.[59] They came from dormant cells situated on the periphery of the Al-Qaeda network. Nevertheless, they committed mistakes that were not noticed on the spot but that were eventually discovered when detailed investigations took place following 9/11. For instance, a newly trained Lebanese pilot left Florida to go to Afghanistan via Pakistan in December 2000, probably to report progress on the operation or to obtain further instructions from the network.[60] His travel pattern must have raised suspicions since the CIA requested that Emirates authorities question him on his return journey due to suspicions of his relationship with

[57] Jane Corbin, *Al-Qaeda, In Search of the Terror Network…,* 165.
[58] Jonathan P. Caulkins, Mark A.R. Kleiman and Peter Reuter. "Lessons of the War on Drugs for the War on Terrorism"…; 87.
[59] Rowan Gunaratna. *Inside Al Qaeda* …,103.
[60] Jane Corbin, *Al-Qaeda, In Search of the Terror Network…,* 173.

Islamic extremists.[61] When interviewed, Jarrah stated that he had spent two months in Afghanistan, that he was a pilot and that he was on his way back to the US.[62] While that information was relayed to the CIA, there are no indications that the information was communicated to the FBI to be added on the US watch list at ports of entry.[63] Jarrah re-entered the US a few days later and was never questioned. According to Senator Graham, head of the Senate Intelligence Committee, this was not an isolated case and "it was a breakdown in the hand-off of information from the intelligence agencies to the domestic law-enforcement agencies."[64]

In July 2001, an FBI agent from Phoenix noted a pattern of suspect men from the Middle East signing up at flight schools in Arizona.[65] He submitted a memo suggesting that Osama bin Laden might be backing the pilots and recommending that an investigation be conducted nationwide to determine if their were any linkages with Al-Qaeda.[66] The memo reached two units in FBI headquarters but did not make it to senior levels and was not disclosed to other agencies involved in counter-terrorism.[67] Similarly, the FBI in Minnesota questioned Zacharias Moussaoui in August 2001 after his flight instructor had reported suspicious behaviour.[68] Moussaoui was in violation of his visa and the FBI turned him over to the INS (Immigration and Naturalization Service) and he was arrested.[69] The FBI informed the CIA of the situation, continued investigating

[61] Ibid.
[62] Ibid, 174.
[63] Ibid.
[64] Ibid, 172.
[65] Bernstein. *Out of the Blue*…,164.
[66] Michael Elliott, et al. "They had a Plan," *Time*, August 12, 2002: 35.
[67] Michael Hirsh and Michael Isikoff. "What Went Wrong," *Newsweek*, May 27, 2002: 31.
[68] Bernstein. *Out of the Blue*…,161.
[69] Ibid.

Moussaoui and discovered from their French counterparts that he was associated with Islamic terrorist groups.[70] Due to the barriers between all the agencies involved in counter-terrorism, the information could not be fused into a clear warning. Indeed, the White House Counter-terrorism Security Group (CSG) officials led by Richard Clarke were obsessed with Al-Qaeda long before 9/11 but they were not told about the Phoenix memo nor were they informed of the Moussaoui arrest.[71] Once again, hierarchical barriers favoured Al-Qaeda.

The idea of crashing airplanes into buildings was not a novelty in September 2001. Following the light aircraft crash landing on the White House lawn in 1994 and the failed attempt by the Algerian terror group, the Groupe Islamique Armé (GIA), to blow up the Eiffel Tower with a hijacked aircraft, Secret Services were aware of the potential threat.[72] In 1999, "the National Intelligence Council, a think-tank affiliated to the CIA, warned that terrorists associated with bin Laden might hijack an aircraft and crash it into an American government building." In the wake of the terrorist attacks on American embassies and the USS Cole, President Bush was briefed by the CIA in August 2001 that bin Laden might have a plan to hijack American airliners.[73]

Despite indicators of the threat vis-à-vis the airline industry, the Federal Aviation Authority (FAA) was not informed and it was not on the lookout for any anomaly that would involve foreign pilots. Naturally, flying schools were not in the know and they

[70] Michael Elliott, et al, "They had a Plan"…, 36.
[71] Michael Elliott, et al, "How the U.S. Missed the Clues," *Time Canada*, May 27, 2002, 20.
[72] Jane Corbin, *Al-Qaeda, In Search* …,160-1.
[73]Michael Hirsh and Michael Isikoff, "What Went Wrong"…, 31.

continued to enrol and license students who did not have the required student visas.[74] On 26 December 2000, Mohamed Atta and Marwan al-Shehhi flew a small plane to Miami International airport where it was abandoned just off the main runway when it failed to start, blocking access to a big jet.[75] What were two newly qualified pilots doing in a small craft at one of the busiest airport in the US during the busiest time of the year? An angry FAA official contacted the flying school, but that was the extent of official inquiries. The incident was not investigated further and a report was not filed. Six months later, the FAA issued at least two warnings to the aviation industry during the summer that specifically mentioned the possibility of hijackings.[76] This is an indication that the FAA was aware of the threat. However, it was not deemed to be serious enough to compel airlines to take concrete action to lower the risk of hijacking. The message was sent but it was not communicated. Since the FAA, flying schools and airline officials were not aware of the threat, they could not be part of the team that would fend it off.

ASSESSMENT

It is likely that through previous experience gained from groups that operate in the periphery of Al-Qaeda in the US, that the operatives were aware of some of the weaknesses in the American 'systems'. Some of these weak spots, such as FBI/CIA rivalries and lack of cooperation are quite apparent from discussions available in the public domain while others, such as airport security, were probably tested in person. The perpetrators of the attacks were well trained and well informed. However, they

[74] Jane Corbin, *Al-Qaeda, In Search*…,176.
[75] Ibid, 162.
[76] Michael Hirsh and Michael Isikoff, "What Went Wrong"…, 32.

committed a number of mistakes prior to the attacks that were missed by non-networked authorities. Due to poor communication and coordination between themselves, American agencies have lowered their chance of identifying an attack that many knew was coming. The Al-Qaeda network was superior that time, because it managed to exploit the weaknesses of the American giant.

Based on the network strengths discussed previously, a comparison with government hierarchies is in order. When it comes to diversity and redundancy, both types of organizations could be considered equal. Given their quasi-unlimited resources and their breadth of activity, governments certainly have an edge on the ability to access large quantities of diversified talents. With regards to redundancy, governments also have an advantage but in this case, duplication of effort does not necessarily translate into effectiveness as pointed out in the discussion on organizational silos and their offspring, the exploitable seams. Networks are undeniably more flexible and more responsive, while hierarchies need to adjust to their environment to survive and are bound by rigid legal framework. Further, the bureaucracy and centralized decision making generally inhibit initiative and creativity in hierarchies. As for networks, they operate based on a well-understood set of rules referred to as protocols. Within the parameters of these protocols, networks can adjust easily and react quickly because they are not constrained by a rigid chain of command.

In the area of stealthiness and lawlessness, networks have an advantage over government hierarchies. Hierarchies need to demonstrate a fair amount of transparency

to the taxpayers whom they serve, combined with the need to operate within the constraints of the law. Some agents of the government may operate covertly but the cultural divide and the reclusive nature of criminal networks will keep them hidden or totally inaccessible. It could be argued that the reverse applies to government agencies, however; most government agencies operate in the open, in the view of the general public, thus making them more vulnerable and less protected than networks. The last factor to compare is the strength that networks derive from their global nature. Here again, government hierarchies are somewhat disadvantaged because of jurisdictional barriers that cause a number of seams, and the limited actions they can take on the soil of other sovereign states.

Overall, criminal networks have a net advantage over government hierarchies. There are certainly areas where government hierarchies excel but the aim of this comparison was to demonstrate how relatively small criminal networks could leverage their inherent strengths to oppose large hierarchies. Finally, two of the most significant advantages that terrorist networks have over government hierarchies is that they are not constrained by laws and that they retain the initiative: their imagination and the weaknesses presented by hierarchies will determine where and how they will strike next. The following section will explore means of opposing such an agile and invisible enemy.

SECTION 3 – NETWAR

As shown in the previous section, criminal networks such as Al-Qaeda are well poised to exploit the weaknesses that traditional hierarchical authorities present. For the last decade, John Arquilla and David Ronfeldt have been studying the increasing role played by networks in activities ranging from social activism to global terrorism. They have concluded that "the information revolution is fostering the rise of network forms of organization, whereby small previously isolated groups can communicate, link-up, and conduct coordinated joint actions as never before."[77] They have coined this concept of using a network to further a cause as 'netwar'.[78]

3.1 Netwar Defined

The advent of netwar stems from technological advances that have increased the ability of like-minded people to meet, stay connected and coordinate their efforts. More precisely, netwar is defined 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 command.[79]

---

[77] John Arquilla and David Ronfeldt. "The Advent of Netwar: Analytic Background," *Studies in Conflict and Terrorism*, Vol. 22, Iss. 3 (Jul-Sep 1999): 193.

[78] Ibid.

[79] John Arquilla John and David Ronfeldt. *Networks and Netwars*…, 6.

The information revolution has precipitated netwar through the creation of a multitude of new ties between nodes (people and organizations) and has facilitated the transfer of information within the network. To realize its full potential, the network relies on a variety of information and telecommunication technologies (cellular phones, fax machines, e-mail, encryption, world wide web sites) to sustain a constant and dense flow of information.[80] However, technology is not an end in itself, it is a means that enables netwar.[81] Whether the relations between nodes are weak, strong or loose, it is those relations, and not how they are effected (i.e. using technology or not) that is important to the livelihood of the network. Accordingly, netwar actors can benefit significantly from the use of technology; however, technology alone is not a crucial component of netwar.[82]

In the same vein, it must be understood that netwar is not limited to the surreal domain of cyberspace. While it is true that technology allows netwar to evolve in the virtual world and garner a fair amount of synergy from it, netwar is much more than war through the Internet.[83] Beyond the dissemination of information through the use of enabling technologies, netwar involves real people who will take concrete actions,[84] be it by showing up at a demonstration, by financing an extremist organization or by taking up arms to fight an enemy that is hostile to their cause. The networking of these real people is the reason why netwar is so effective.

---

[80] John Arquilla and David Ronfeldt. "The Advent of Netwar: Analytic Background,"…, 195.
[81] Ibid, 196.
[82] Ibid.
[83] John Arquilla John and David Ronfeldt. *Networks and Netwars*…, 11.
[84] Ibid.

Additionally, it is important to point out that netwar is not restricted to criminal activities; it can be used to rally peaceful opponents, as was the case in the protests against globalization in Seattle in 1999, as much as it can be a means to oppose government and military forces with violence, as in Chechnya in the first half of the nineties.[85] However, no matter why netwar is employed, people and organizations that had limited reach, and therefore limited means to influence their environment in the past, can now muster considerable support and influence through global networks. As a result of this phenomenon, "power is migrating to non-state actors, because they are able to organize into sprawling multi-organizational networks… more readily than traditional, hierarchical, state actors."[86] When used for criminal purposes, this shift in power presents a threat to states, which cannot be ignored and which warrants further study if it is to be countered successfully.

Netwar is here today and in the hands of such organizations as Al-Qaeda, it is lethal and extremely difficult to defeat. Since hierarchies are weak when opposed to networks, Arquilla and Ronfeldt contend that it will take networks to fight networks because hierarchies alone will not succeed.[87] Therefore, governments who want to oppose networks may benefit from the reorganization of some of their resources in a network fashion to emulate their enemy and leverage the full potential offered by that

[85] Ibid, 16-19.
[86] John Arquilla and David Ronfeldt. "Osama bin Laden and the Advent of Netwar," *New Perspectives Quarterly*, Vol. 18 Iss. 4 (October 2001): 24.
[87] Ibid, 31

organizational form.[88] The sections that follow will focus on the development of networks to defeat terrorism and will study the role of the military within that network.

3.2 Governments and Netwar

Governments consist of specialized and departmentalized units that operate within a rigid legal framework and they are slow and ill equipped to respond to attacks that cross boundaries, as is often the case in netwar. Governments have worked hard to develop effective hierarchical processes and will therefore be very reluctant to transform to a network that exhibits diluted and decentralized controls.[89] On the positive side, governments have access to a tremendous amount of resources and talent; they are pervasive and diversified. In addition, the legal framework that binds a government together generally provides legitimacy, which should be leveraged as much as possible to gain and sustain public support at home and abroad. As will be discussed later, that legitimacy is a force multiplier that ought to be exploited in a well-coordinated information campaign. Governments also have a global reach due to embassies and diplomatic missions worldwide and multilateral agreements of all sorts. Notwithstanding this, governments face significant challenges on the way to network their assets, and it is unlikely that the legal framework in which they operate will ever promote the creation of a fully networked government. Realistically, the only way to network government might be to network selected nodes with sufficient authority, influence and connections to ensure the timely exchange of information and services between the various components of the bureaucracy.

[88] Ibid.

[89] Matt Begert and Dan Lindsay. *Intelligence Preparation for Operations*, in Non-State Threats and Future Wars, ed. Robert J. Bunker (London: Frank Cass & Co. Ltd, 2003), 135.

The concept of 'operating in the seams' was broached earlier when networks and hierarchies were compared. Therefore, it comes as no surprise that the exploitation of seams, or boundaries between organizations figures as one of the predominant features of netwar. In addition to what has been discussed already, Arquilla and Ronfeldt state that "netwar 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."[90] As a result of this blurring of responsibilities, governments have tremendous difficulties in dealing with multidisciplinary threats or attacks through their single purpose agencies that are not designed to operate as networks.[91]

In the US, many contend that the country needs a multidisciplinary organization that draws on all elements of national power to bring all forces to bear on asymmetric enemies such as terrorist networks.[92] This could be achieved through the elimination of barriers between agencies and the networking and integration of all organizations (political, judiciary, administrative, diplomatic, financial, economic, social and military) that play a role in the GWOT. While some may argue that the Office of Homeland Security (OHS) was established with that purpose in mind, critics[93] claim that the OHS has limited powers to act as Lead Agency and actually coordinate the efforts of the

[90] John Arquilla John and David Ronfeldt. *Networks and Netwars*…, 14.
[91] Ibid.
[92] Cdr R.V. Gusentine. "Asymmetric Warfare- On Our Terms," *U.S. Naval Institute Proceedings*, August 2002: 60.
[93] See Philippe Bionditti. "L'organisation de la lutte anti-terroriste aux Etats-Unis, " *Cultures et Conflits*, no. 44 (Hiver 2001): 75.

American bureaucracy. In the same vein, the creation of the National Security Coordination Council (NSCC) by the US Department of Justice to "identify, disrupt and dismantle terrorist networks"[94] appears to be yet another stovepipe solution with limited scope, reach and authority.[95] On a more positive note, the enactment of the Patriot Act by the US Congress is considered a step towards networking since it facilitates the sharing of information and intelligence between departments and agencies. However, in light of the breakdowns in controls and information sharing that have preceded the attacks of 9/11, many still argue that the US needs a structural reform to at least enhance the coordination between the FBI and the CIA.[96] The debate over the integration of the FBI and the CIA is not new and will not be solved here but it highlights, the need for cooperation and networking within governments and arguably between states.

Arquilla and Ronfeldt contend that in addition to operating in the seams, swarming is another potent technique that is employed in netwar. "Swarming occurs when the dispersed nodes of a network of small (and perhaps some large) forces can converge on a target from multiple directions."[97] Contrary to the massing of forces, swarming involves the use of independent but coordinated forces to overwhelm an objective; "it will work best…if it is designed mainly around the deployment of myriad, small, dispersed, networked manoeuvre units."[98] This technique allows networks to

[94]Attorney General John Ashcroft, #03-05-02 Transcript News Conference on the National Security Coordination Council, 5 March 2002, accessed 14 Mar 2004 http://www.usdoj.gov/ag/speeches/2002/030502newsconferencenationalsecuritycoordinationcouncil.htm

[95] Cdr R.V. Gusentine. "Asymmetric Warfare- On Our Terms"…, 60.

[96] Robert Bryant, et al, "America Needs More Spies," *The Economist* July 12, 2003: 30.

[97] John Arquilla and David Ronfeldt, "The Advent of Netwar: Analytic Background"*...,* 198.

[98] John Arquilla John and David Ronfeldt. *Networks and Netwars*…, 12.

harness the strength of their diversity in an offensive posture while offering a limited front that can be attacked.

On the global scene, the US promulgated its 'National Strategy for Combating Terrorism' in February 2003, which expresses clearly the US resolve to use every instrument of its national power - diplomacy, economics, law enforcement, financial information, intelligence and military - to fight terrorist networks and those who support their efforts.[99] To achieve this, the strategy proposes a non-sequential four-prong approach (defeat, deny, diminish and defend) that places a heavy emphasis on the necessity to forge and maintain ties with partners and allies. In sum, this strategy is well aligned along the concepts of netwar and it proposes to swarm terrorist networks from all directions "across the geographic spectrum to ensure that all linkages between the strong and the weak organizations are broken, leaving each of them isolated, exposed and vulnerable to defeat."[100]

For many,[101] the key to success in the GWOT depends heavily on the availability of good domestic and foreign intelligence. The US may be self-sufficient in the field of domestic intelligence; however, chances are that the assistance of allies, especially Muslim and Arab allies,[102] is quite useful when fighting terrorist networks. To foster dialogue, governments must be deliberately sensitive in their foreign policies and must

---

[99] US National Strategy for Combating Terrorism, February 2003, accessed 20 March 2004 http://usinfo.state.gov/topical/pol/terror/strategy/

[100] Ibid.

[101] See Anatol Lieven, "The Cold War is Finally Over," in *How Did This Happen? Terrorism and the New War*, ed. James F. Hoge and Gideon Rose (New York: PublicAffairs, 2001) 298. and Thomas A. Stewart, *America's Secret Weapon,* Business 2.0 December 10, 2001. http://proquest.umi.com accessed 5 April 2004

[102] Anatol Lieven, "The Cold War is Finally Over"..., 298.

attempt to reach consensus. Unilateral actions, such as the war in Iraq in 2003, are not conducive to cooperation and will likely make new enemies and lose old friends that are crucial for intelligence and logistics support (such as in the basing of troops and equipment, over-flight rights, etc.).[103] Sharing intelligence between allies is essential because of network defence, "small cells of fanatics tied by religion and blood are difficult to penetrate, especially for Western spies."[104]

While it is accepted that intelligence is the cornerstone of the war on terrorism, only networking will eliminate the weak seams between organizations and states, thus allowing governments to fully leverage their true potential against terrorist networks. This networking of assets goes well beyond intelligence agencies; it needs to integrate the appropriate mix of intelligence, conventional military forces, Special Forces, police, civil protection and non-governmental organizations.[105] "This network of operators will need to synchronize its response across jurisdictional boundaries, disciplinary lines, services and (increasingly) across borders."[106] The network needs to encompass all instruments of national power, civil and military.

---

[103] C.J. Dick. *Conflict in a Changing World: Looking Two Decades Forward*. Conflict Studies Research Centre, February 2002; 16.

[104] Evan Thomas, Mark Hosenball, Michael Isikoff, Owen Matthews, Sami Kohen, Sami, Yousafzai, and Liat Radcliffe. "Moving Targets," *Newsweek*, December 1, 2003; 22.

[105] John P. Sullivan. "Networked Force Structure C4I," in *Non-State Threats and Future Wars*, ed. Robert J. Bunker (London: Frank Cass & Co. Ltd, 2003), 154.

[106] Ibid.

3.3 Armed Forces and Netwar

Since the attacks of 9/11, governments have relied heavily on their armed forces to wage the Global War on Terrorism. Two significant military campaigns have taken place to date. The first consisted of defeating the Talibans in Afghanistan whom were strong supporters of Al-Qaeda and dismantling the terrorist network established in that country. The second was the attack against Iraq to remove Sadam Hussein from power, put an end to his development of Weapons of Mass Destruction (WMD), end his support to terrorists, and free the Iraqi population from his ruthless dictatorship. From an American perspective, the War on Terror has been effective to date since it has prevented the recurrence of significant terrorist attacks against the US. Nevertheless, bombings in Jakarta, Bali, Casablanca and Madrid have all been linked to the Al-Qaeda network. These are sad reminders that the network has survived such setbacks as the destruction of its training camps in Afghanistan, the seizure or freeze of substantial financial assets and the arrest of thousands of members all over the world[107]. The network is resilient and it continues to thrive even though many of its nodes have been maimed, disrupted or dismantled over the past thirty months.

Now that two rogue states have been brought to order by military forces without annihilating the Al-Qaeda network, the time is ripe to assess the role of the military in the GWOT. Accordingly, three areas will be covered. The first is whether armed forces should be the tool of choice to wage the GWOT or not. The second will deal with the

[107] According to Jane's Intelligence Digest, more than 4000 suspects associated with Al-Qaeda have been arrested worldwide. "Al-Qaeda Influence Spread," *Jane's Intelligence Digest*, December 5, 2003. http://www4.janes.com accessed 3 April 2004.

capabilities that the military can bring to netwar. The third will deal with the employment of Special Operations Forces in the GWOT and will assess in broad terms how it measures up against netwar doctrine.

MILITARY AS THE TOOL OF CHOICE?

For decades, western militaries have focused their efforts to counter the Soviet threat. They have developed doctrine, structures, tactics and equipment to deter and fight a huge and identifiable enemy on a well-defined battlefield, using the Law of Armed Conflict as a guiding principle. As a result of the Cold War mindset, states and militaries continue to take for granted that their principal opponents would be organized and armed much like them and they have neglected to transform themselves to face the growing threat posed by non-state actors.[108] Terrorist networks are not contained within the borders of a single state and they do not field armies; as a result, they cannot be subjected to large conventional military destruction.[109] The point to be made here is not that army divisions, bombers and aircraft carriers are no longer required to deter and counter a military threat. The point is that militaries in general are not well equipped, trained nor organized to oppose terrorist networks.[110] The main shortcomings identified are that: their weapons are too cumbersome, their organizations too large and too complex, and their decision-making too rigid and centralized to oppose small, dispersed and agile units.

---

[108] Martin Van Creveld. "In wake of Terrorism, Modern Armies Prove to be Dinosaurs of Defense," *New Perspective Quarterly* Vol. 13, Iss. 4 (Fall 1996): 57.

[109] Jeffrey Record. *Bounding the Global War on Terrorism*. (Carlisle PA: Strategic Studies Institute, U.S. Army War College, 2003), 3.

[110] See C.J. Dick, *Conflict in a Changing World* …; Van Creveld, "In Wake of Terrorism"…; Jeffrey Record. *Bounding the Global War on Terrorism*…

By nature, terrorist networks derive their strengths from social ties. They are diversified, flexible, stealth, dispersed, pervasive and they exploit the seams between hierarchical organizations and states. It is no surprise that military forces tailored to fight one another within a nation-state framework do not measure up against networks.[111] After all, combating terrorism is primarily a political, intelligence and law enforcement role, not a military one.[112] C.J. Dick endorses that point of view and contends that in the GWOT, military should only be involved when absolutely necessary, in a supportive role to law enforcement.[113] Politicians and military leaders need to realize that military forces, despite their wide-ranging capabilities and competences, should not be used as the arm of choice to fight terrorism. Armed forces should be integrated in a networked array of capabilities and called upon when required. If armed forces are to be effective players in netwar, politicians and military leaders need to reconsider how they employ the military.

MILITARY CONTRIBUTION

In the GWOT, military forces have been quite useful in hostile environments where terrorist networks have sufficient leeway to operate freely, without fear of intervention, due to supportive or weak government authorities. As discussed earlier, rogue states such as Afghanistan, failed states such as Somalia, and weak states such as Pakistan and its troubled Afghan border, offer safe havens where networks may establish themselves to train and reconstitute their forces. This massing of terrorists in one

[111] John P. Sullivan. "Networked Force Structure C4I"…, 145.
[112] Jeffrey Record. *Bounding the Global War on Terrorism*…, 3.
[113] C.J. Dick. *Conflict in a Changing World: Looking Two Decades Forward*…, 17.

geographical area is a definite weakness of their network, one that military forces have exploited in the past, as in Afghanistan for example, and must continue to exploit in the future. Unfortunately, the pervasive nature of networks implies that their components will seldom be massed neatly, waiting to be attacked.

There will be instances when armed forces are deemed to be the best resource available to fight, capture or dismantle terrorist cells. In such instances, military intervention should be limited and solely centred on the enemy and its fluid network. Politicians and military planners need to remain focused on the enemy and avoid at all cost the temptation to conquer and hold ground. That strategy is costly, labour intensive and difficult to sustain over time. "Imperial policing" and nation building are responsibilities that fall outside the military's traditional portfolio.[114] They divert limited resources from fighting networks and simply result in the displacement of flexible and mobile terrorists. In the end, it may be more effective, cheaper and less intrusive to infiltrate and monitor closely what is going on in weak states rather than attempting to impose democratic values and democratic institutions upon mildly receptive, fragmented populations who may rally and turn against westerners in the process. The intent here is not to assess the effectiveness of the military interventions in Afghanistan and Iraq; it is merely to point out that the conduct of large-scale military campaigns may not be effective and sustainable over time and, to propose that considerations be given to limiting military intervention to discreet and focused hits against terrorist networks. That being said, military forces have a wide-range of capabilities, beyond kinetic force, that the lawful network could use to its advantage in the GWOT.

[114] Jeffrey Record. "Bounding the Global War on Terrorism"…, 3.

In its supporting role, the military has a phenomenal amount of expertise and equipment that can be harnessed to support actors involved in counter terrorism. Expertise in the fields of intelligence, communications, communication intercept, electronic warfare, mapping and logistics are often unique military capabilities that must be shared rather than being retained for the sole benefit of the military. The sheer ability to deploy and sustain personnel and equipment away from their normal place of employment is a contribution that the military can make to civilian agencies (government agencies and non-government organizations) chosen to deploy abroad to partake in the GWOT. Military aircraft could be used to airlift personnel and equipment. Naval ships could be used for transport also, or as remote and mobile headquarters where a wide array of experts would be housed safely when not busy labouring ashore. The military can also make a worthwhile contribution in the field of information operations (IO). Its expertise and resources in that area can be made available and pooled with similar resources of other agencies to devise a potent and coordinated IO campaign directed at terrorist networks and those who support them.

By design, armed forces are accustomed to being in the lead in theatres of operation where they deploy. The war that is currently being fought is global and the theatre is fluid. Depending on the circumstances, a variety of organizations, including the military, may have the lead at any given time, while others will assume a supporting role. Within a networked environment and as a supporting element therein, the military will need to be responsive to the demands of a host of agencies that could be both domestic

and foreign. This is a fundamental change in mindset for commanders and military members who are used to operating within rigid and well-defined chains of command. That vision will not be easy to achieve. However, the migration of power to networked non-state actors has taken place and the benefits of opposing that threat with a network must be recognized by all. Therefore, to remain responsive and relevant in this new security environment, armed forces may need to adapt their doctrine, training and structures to increase their interoperability with civilian authorities.

3.4 Special Operations Forces and Netwar

As arms of governments, militaries rely heavily on chains of command or hierarchies to dispense authority and enforce accountability. This construct has numerous advantages in conventional warfare but it quickly becomes less effective when confronted with an asymmetric foe such as a network. However, it is very probable that military forces will continue to be called upon to conduct strikes and possibly campaigns against terrorist networks. When that occurs, the enemy will not be massed and the military will therefore need to operate in a lean collection of dispersible units that are suited to match the mobility and flexibility of their opponents.[115] The military needs to start thinking in terms of small and many instead of few and large.[116] To be effective, these small groups will need autonomy and freedom of action. Instead of direct orders, they will be given the commanders' intent and a set of Rules of Engagements.[117] To

[115] Nina Bernstein. "The Strategists Fight a War About the War," *New York Times*, 6 April 2003, 4.

[116] Thomas A. Stewart, "America's Secret Weapon," *Business 2.0* Vol. 2, Iss. 10. Dec 2001; available from http://proquest.umi.com; accessed 5 April 2004.

[117] Ibid.

capitalize on opportunities, command and control will have to be instantaneous[118] and decentralized. Based on these characteristics, it could be argued that Special Operations Forces (SOF) are there today, ready for netwar.

Over the last six months, the American Special Operations Command (SOCom) has employed new approaches that could indicate that network doctrine is being introduced in SOF. "This community needs to morph. We need to look more like them than we do like us," stated LtGen Schwartz from SOCom when referring to SOF's composition and capabilities.[119] While the integration of SOF and its responsiveness within a networked environment remains to be seen, it appears to be moving in that direction. Networking is crucial because it is very unlikely that "a purely military organization will have the diversity of experience and expertise among its members to conceptualize collaborative, multifaceted approaches to complex threats overseas."[120] Examples of competencies that may not be readily available to military units are varied and may include, linguists, anthropologists, information systems experts, international banking and securities specialists, forensic accountants, lawyers, scientists and criminal laboratory technicians.[121]

The idea of organizing diverse and multidisciplinary teams to collect intelligence and conduct special operations is not new and was used extensively by the Office of

[118] Ibid.
[119] Robert Wall, "Sharpening the Sword." *Aviation Week & Space Technology*, February 23, 2004: 80.
[120] Cdr R.V. Gusentine, "Asymmetric Warfare- On Our Terms"…, 60.
[121] Ibid, 61.

Strategic Services (OSS) during World War II.[122] The OSS was the predecessor of the CIA and SOF and its members included military members, women, foreign nationals and ethnically diverse personnel, who were well-trained polymath.[123] Today, while striving to create a networked environment, many of the features and characteristics of the OSS teams could be retained, but the added benefit would be that most of its members would remain connected to domestic and foreign government agencies, thus increasing the synergies between agencies, and eliminating the seams between them, through the establishment of a networked environment. Ironically, last November, the US created Task Force 121, which is a covert commando team, composed of Special Operations Forces and Central Intelligence Agency officers.[124] Task Force 121 was created to hunt high-value targets in Iraq and Afghanistan and it has demonstrated its worth through its involvement in the capture of Saddam Hussein in December 2003.[125]

SOF have been employed extensively since the beginning of the GWOT and it is not by coincidence. Its members have a wide breadth of competencies, they are well trained, they operate in small teams and they have the ability to remain in a hostile environment for extended periods of time without extensive logistics support. They can maintain a low profile and their presence on foreign soil is less intrusive than conventional forces.[126] SOF are flexible, versatile, rapidly deployed and they have the small footprint required to hunt down and root out terrorist networks. It was very

---

[122] Ibid, 60.
[123] Ibid, 61.
[124] David E. Sanger and Eric Schmitt, "New US Effort Steps Up Hunt for bin Ladden;" *New York Times*, 29 February 2004.
[125] Ibid.
[126] LCol Bernd Horn. "A Self-Evident Truth: Special Operations Forces and Intelligence in Asymetric Warfare," *The Army Doctrine and Training Bulletin*, Vol. 5, No 4 (Winter 2002-03): 22.

effective in Afghanistan and since then, SOF have been employed in various roles in the GWOT and have become the US military tool of choice.

SOF tasks are varied and range from direct action (attacks, interdiction, capture of personnel or material, rescue of personnel), to military assistance (train, equip, support other forces) and include IO and special reconnaissance. By employing SOF and network doctrine, the Americans have managed to rally the assistance of Afghan militias and destroy the Taliban government and Al-Qaeda bases in Afghanistan.[127] They were also employed in that country for swarming when they were used to direct B-52 air strikes "that took a matter of minutes from call to completion compared with the many hours it usually took to identify a target in Desert Storm…"[128] SOF have been used in Afghanistan to train a new Afghan national army; they have trained and advised the Filipino army in fighting the Abu Sayyaf terrorist group in the southern part of that country and they have been employed to train army troops in the former Soviet republic of Georgia to fight Chechen and Al-Qaeda guerrillas.[129]

In January 2003, the Pentagon has designated SOCom as its lead organization in combating terrorism.[130] This was much more than a title and for SOCom, it meant an increase in authority, personnel and budget enabling SOF to take on greater

---

[127] Frederick W. Kagan, "War and Aftermath," *Policy Review*, No 120 (August and September 2003); 4.

[128] Arquilla quoted in David Hughes, "Swarming: Sting like a Bee," *Aviation Week Space & Technology*, September 29, 2003: 53.

[129] Glenn W. Goodman Jr., Expanded Role for Elite Commandos, *Armed Forces Journal*, Vol. 140 (February 2003): 38.

[130] Ibid, 34.

responsibilities in the GWOT.[131] Up to then, SOCom had functioned as a supporting command, performing missions to meet the demands of regional commanders.[132] In January 2003, SOCom was granted the authority to plan and carry out independent missions thus moving SOCom's status from being solely a supporting command to becoming both a supporting and a supported command.[133] Therefore, in certain circumstances, SOCom could plan a mission and have access to Navy, Army or Air Force units in the region, which would act in response to its direction and control.[134] This increase in authority puts SOCom on an equal footing with Combatant Commands and may increase the degree of networking between SOF and conventional forces. The designation of SOCom as the lead military organization in the war on terror is a positive step towards netwar since it ensures that the SOF, and their high propensity to network, will continue to be employed against terrorist networks.

SOCom is working towards a networked environment but its commander, General Brown, recognizes that there is room for improvement in the domain of information sharing with coalition partners.[135] In addition, senior personnel in SOCom also recognize the need to increase SOF capabilities in all aspects of intelligence: human, signals and UAV imagery. Notwithstanding the importance that continues to be placed on technology in the GWOT, whether it is smart bombs, satellite imagery or UAVs, leaders and soldiers must not forget that their opponents' biggest strength is their network and the human relationships that keep it together. Advance technology and equipment may

[131] Ibid.
[132] Ibid, 36.
[133] Ibid.
[134] Ibid.
[135] Robert Wall, "Sharpening the Sword"…, 80.

facilitate netwar but SOF's greatest contribution will remain the people it brings to the fight, not its machines.[136] Just as terrorists derive more power from their organizational construct than from technology, so too must the military rely more on people, organizations and doctrine than on advanced technical systems.[137] SOF and military planners must remain cognizant of that fact when they organize forces and plan operations. Only humans can forge relationships and the key to netwar is to forge, exploit, disrupt and destroy relationships.

SOF will continue to be a potent contributor to netwar as long as the human factor continues to play a predominant role in its operations. SOF is not a panacea; to be effective, it needs to be integrated in a diverse network composed of government agencies and NGOs that can be used to swarm terrorist networks and exploit the seams between their components. Both sides can wage netwar and SOF is well poised to contribute to the fight.

[136] Frederick W. Kagan, "War and Aftermath"…27.

[137] Arquilla, John and David Ronfeldt, "The Underside of Netwar," *Review – Institute of Public Affairs*, Vol. 54, Iss. 4 (December 2002). http://proquest.umi.com accessed 5 April 2004.

CONCLUSION

A well-financed, well-organized and well-trained terrorist network perpetrated the attacks of 9/11. This study was focused on networks as an organizational form and the means of countering them. It has explained how networks operate and it has highlighted how criminal networks rely heavily on interpersonal relationships to operate. When compared to the government hierarchies that oppose them, criminal networks were found to have a net advantage especially in the areas of flexibility, responsiveness, global nature and stealthiness. Some of the events leading to the attacks of 9/11 were used to illustrate the weaknesses of stovepipe bureaucratic government agencies vis-à-vis the Al-Qaeda network. The concept of netwar – the use of network forms of organization and related doctrine, strategies and technologies in conflicts – proposed by John Arquilla and David Ronfeldt further explains the potency of criminal networks. Technology may be utilized as an enabler to netwar but relationships within the network retain a central role in the exploitation of the network's potential by allowing it to swarm and to operate in the seams. Because of the inherent weaknesses of hierarchies vis-à-vis networks, it was concluded that it would take a network to counter netwar effectively.

The roles that governments can play in waging netwar are varied and encompass the deployment of all elements of national power encompassing the political, judiciary, administrative, diplomatic, financial, economic, social and military domains. Far from suggesting that governments should forego hierarchies and adopt a network construct blindly, it was suggested that governments and nations must strive to network their assets in manners that will decrease their vulnerability to swarming and the exploitation of

seams. Progresses towards that vision were noted in the American Patriot Act, the Office of Homeland Security, the National Security Coordination Council and the National Strategy for Combating Terrorism. However, it was also noted that more work would be required, in the US and globally, to achieve the synchronization and coordination of all instruments of national power.

Notwithstanding the recognition that the war against terrorist networks is primarily a political, intelligence and law enforcement role, it was recognized that military forces, as arms of governments, must also be integrated in the 'lawful' network. While it was argued that conventional forces, as a result of the Cold War, were too large, too complex, too rigid and too centralized to oppose the dispersed and agile units that compose terrorist networks, it was suggested that conventional forces could make a meaningful contribution in the GWOT if it were to be employed in a supporting role. This would necessitate a change in mindset and doctrine but it could greatly enhance the capabilities of the lawful network.

Finally, it was determined that within the military, Special Operations Forces supported by conventional forces were best poised to wage and counter netwar. Given their div0 12 301.32001 97.279290 212.21936 Tmressyts, m

ee

networks. The networking of SOF assets must continue to grow and barriers between all warriors in the GWOT, whether they are in uniform or not, must continue to come down.

Over the past decade, terrorist networks have repeatedly been a threat to world order and security. They have managed to exploit the weaknesses of hierarchies that are notoriously parochial and ill equipped to oppose the pervasive, ubiquitous and resilient enemy they face. Networks are based on relationships and they derive a tremendous amount of strength from these relationships. The war on terror is about people and relationships, not weapons. To win the war, governments and military forces must strive to reduce barriers between their assets, to create and nurture a global networked environment that will allow the exploitation of their full potential. The eradication of terrorism belongs to utopia. The annihilation of terrorist networks, however, is within the realm of the possible if all instruments of national power are networked. It takes a network to fight a network, and whoever has the largest and most effective organization will be best positioned to win the war.

BIBLIOGRAPHY

Arquilla, John and David Ronfeldt. *Networks and Netwars.* Santa Monica CA: Rand, 2001.

Arquilla, John and David Ronfeldt. "Osama bin Laden and the Advent of Netwar." *New Perspectives Quarterly*, Vol. 18 Iss. 4 (Oct 2001): 23-33.

Arquilla, John and David Ronfeldt. "The Underside of Netwar." *Review – Institute of Public Affairs*, Vol. 54, Iss. 4 (Dec 2002).
Available from http://proquest.umi.com; accessed 11 February 2004.

Arquilla, John and David Ronfeldt. "The Advent of Netwar: Analytic Background." *Studies in Conflict and Terrorism*, Vol. 22, Iss. 3 (Jul-Sep 1999):193-206.

Ashkanasy, Neal M., Celeste P.M. Wilderom, and Mark F. Peterson. *Organizational Culture & Climate.* Thousand Oaks CA: Sage Publications, Inc, 2000.

Begert , Matt and Dan Lindsay. "Intelligence Preparation for Operations." In *Non-State Threats and Future Wars*, ed. Robert J. Bunker, 133-143. London: Frank Cass & Co. Ltd, 2003.

Bernstein, Nina. "The Strategists Fight a War About the War." *New York Times*. 6 April 2003.

Bernstein, Richard. *Out of the Blue*. New York: Times Books, 2002.

Bionditti, Philippe. *L'organisation de la lutte anti-terroriste aux Etats-Unis.* Cultures et Conflits, no. 44 (Hiver 2001): 65-76.

Blanche, Ed. "Al-Qaeda Recruitment." *Jane's Intelligence Review*. January 1, 2002: 27-32.

Bryant, Robert, J. Hamre, J. Lawn, J. MacGaffin, H. Shapiro, J. Smith. "America Needs More Spies." *The Economist*. July 12, 2003: 30-31.

Burke, Jason. *Al-Qaeda: Casting a Shadow of Terror*. New York: I.B. Tauris &Co Ltd, 2003.

Corbin, Jane. *Al-Qaeda, In Search of the Terror Network that Threatens the World.* New York: Thunder's Mouth Press, 2002.

Caulkins, Jonathan P., Mark A.R. Kleiman and Peter Reuter. "Lessons of the War on Drugs for the War on Terrorism." In *Countering Terrorism* ed. Arnold M. Howitt and Robyn L. Pangi, 73-93. Cambridge: Harvard University, 2003.

Dick, C.J. *Conflict in a Changing World: Looking Two Decades Forward*. Conflict Studies Research Centre, February 2002.

Elliott, Michael, Massimo Calabresi, James Carney, Michael Duffy, Elaine Shannon, Douglas Waller, Michael Weisskopf, David Schwartz, Bruce Crumley, J.F.O. McAllister. "How the U.S. Missed the Clues." *Time Canada*. May 27, 2002: 18-26.

Elliott, Michael, Massimo Calabresi, John F. Dickerson, Mark Thomson, Elaine Shannon, Douglas Waller, Michael Weisskopf, David Schwartz, Bruce Crumley, Hannah Bloch, Tim McGirk, Cathy Booth, Thomas, Wendy Cole, Marguerite Michaels, James Graff, Michael Ware. "They had a Plan." *Time.* August 12, 2002: 22-37.

Goodman, Glenn W. Jr. *Expanded Role for Elite Commandos*. Armed Forces Journal, Vol. 140, (February 2003): 34-38.

Grabher, Gernot and David Stark. *Organizing Diversity: Evolutionary Theory, Network Analysis and Postsocialism.* Regional Studies, Vol. 31, Iss. 5 (July 1997): 533-545.

Gunaratna, Rowan. *Inside Al Qaeda*. New York: Columbia University Press, 2002.

Gusentine, Cdr R.V. "Asymmetric Warfare- On Our Terms." *U.S. Naval Institute Proceedings*. August 2002: 58-61.

Hirsh, Michael and Michael Isikoff. "What Went Wrong." *Newsweek*. May 27, 2002: 28-35.

Hoffman, Bruce. *Al-Qaeda, Trends in Terrorism and Future Potentialities: An Assessment*. Santa Monica CA: RAND, 2002.

Horn, Lieutenant-Colonel Bernd. "A Self-Evident Truth: Special Operations Forces and Intelligence in Asymmetric Warfare." *The Army Doctrine and Training Bulletin*. Vol. 5, No 4 (Winter 2002-03): 20-29.

Hughes, David. "Swarming: Sting like a Bee." *Aviation Week Space & Technology*. September 29, 2003: 52-54.

Jane's Intelligence Digest. *Al-Qaeda Influence Spreads, 5 December 2003.* Available from: http://www4.janes.com; accessed 3 April 2004

Jenkins, Brian Michael. *Countering al Qaeda*. Santa Monica: Rand, 2002.

Kagan, Frederick W. *War and Aftermath*. Policy Review, No. 120 (August and September 2003): 3-27.

Leavitt, Harold J. "Why Hierarchies Thrive." *Harvard Business Review*, Vol. 81, No.3 March 2003: 96-102.

Lieven, Anatol. "The Cold War is Finally Over." In *How Did This Happen? Terrorism and the New War*, ed. James F. Hoge and Gideon Rose 246-306. New York: PublicAffairs, 2001.

Record, Jeffrey. *Bounding the Global War on Terrorism*. Carlisle PA: Strategic Studies Institute, U.S. Army War College, 2003.

Record, Jeffrey. "Collapsed Countries, Casualty, Dread and the New American Way of War." *Parameters*, Vol. 32, Iss. 2 (Summer 2002): 4-23.

Sanger, David E. and Eric Schmitt. "New US Effort Steps Up Hunt for bin Ladden." *New York Times*. 29 February 2004.

Stewart, Thomas A. "America's Secret Weapon." *Business 2.0*. December 10, 2001. Available from: http://proquest.umi.com; accessed 5 April 2004.

Sullivan, John P. Sullivan. "Networked Force Structure C4I." In *Non-State Threats and Future Wars*, ed. Robert J. Bunker, 144-155. London: Frank Cass & Co. Ltd, 2003.

Takeyh, Ray and Nikolas Gvosdev. "Do Terrorist Networks Need a Home?" *The Washington Quarterly*, Vol. 25 No. 3 (Summer 2002): 97-108.

Thomas, Evan, Mark Hosenball, Michael Isikoff, Owen Matthews, Sami Kohen, Sami, Yousafzai, and Liat Radcliffe. "Moving Targets." *Newsweek*. December 1, 2003: 22-26.

United States. US National Strategy for Combating Terrorism, February 2003, Available from: http://usinfo.state.gov/topical/pol/terror/strategy/ ; accessed 20 March 2004.

United States. President Bush Address to a Joint Session of Congress and the American People, 20 September 2001. Available from: http://www.whitehouse.gov/news/releases/2001/09/20010920-8.html; accessed 25 February 2004.

United States. Attorney General John Ashcroft, #03-05-02 Transcript News Conference on the National Security Coordination Council, 5 March 2002. Available from: http://www.usdoj.gov/ag/speeches/2002/030502newsconferencenationalsecuritycoordinationcouncil.htm; accessed 14 Mar 2004.

Urry, John. *Global Complexity*. Cambridge: Polity Press, 2003.

Van Creveld, Martin. "In wake of Terrorism, Modern Armies Prove to be Dinosaurs of Defense." *New Perspective Quarterly* Vol. 13, Iss. 4 (Fall 1996). Available from: http://weblinks3.epnet.com; accessed 10 March 2004.

Wall, Robert. "Sharpening the Sword." *Aviation Week & Space Technology*. February 23, 2004: 80-83.