CANADIAN FORCES COLLEGE / COLLÈGE DES FORCES CANADIENNES
JCSP 33 / PCEMI 33

MASTER OF DEFENCE STUDIES THESIS

AL QAEDA – A LESSON IN NETWORKED WARFARE?

By /par Wg Cdr A T Martin RAF

CONTENTS

Table of Contents ii

Abstract iv

Chapter

1. Introduction 1

2. The Military Approach to Networked Warfare 3

- Underlying Concepts 5
- Overview of Networked Warfare 7
- Benefits of Networked Warfare 8
- Key Enablers 11
- Principal Challenges and Issues 14
- Summary of Networked Warfare 16

3. Understanding Al Qaeda 19

- The Origin of Al Qaeda 20
- Ideological Roots 23
- Al Qaeda's 'Mission' 25
- Catalysts for Evolution 26
- Current Structure 28
- Conclusions 30

4. Al Qaeda's Use of Networking 32

Part 1 – 'Classic' Networking 33

- Information Sharing 33
- Networked Training 35
- Developing Shared Intent 37
- Central Control – Dispersed Guidance 39
- Operational Planning and Research 44
- Comparison with the Military Concept 47

Part 2 - Using the Internet as an Enabler 50

- The Internet as a 'Global Grid' 50
- Additional Benefits of the Internet 51
- Opportunities for Security Forces 53
- Al Qaeda's Security Precautions 55
- Summary of Enabling Internet Use 60

Part 3 - Extending the Use of the Network 62

Networked Support – Recruiting and Finance 63
Online Information Warfare 66
Enhancing Effect – Influencing the Media 71
Cyber Attack 73
Summary of Extended Network Use 77

5. Conclusion 79

Lessons for Military Networking 79
Al Qaeda's Online Vulnerabilities 82
The Future of Networked Warfare 84

Bibliography 86

ABSTRACT

This paper illustrates how Al Qaeda's use of the Internet to support and enhance its operational capability can provide useful lessons to military practitioners of networked warfare. After an initial examination of the British, Canadian and American military approaches to networked operations, an analysis of Al Qaeda's origin, ideology, aims and structure provides an understanding of how these unique characteristics result in a different approach to networked warfare in some key areas. Next, Al Qaeda's use of networks to improve its operational effectiveness, for recruiting and fundraising, and as a weapon are demonstrated, along with both the benefits it gains from its use of the Internet as its information bearer, and the measures it employs to solve the problems this creates. The paper concludes that the methods which give Al Qaeda its continued success underline the value of the concepts and techniques contained in military networked warfare doctrine, and highlight enablers that are essential to maximize the benefits it offers. The paper also identifies areas where Al Qaeda's networked operations could be challenged, before closing with the argument that Western militaries should expand their implementation of networked warfare across government departments and beyond to enable a 'Full Spectrum Response' to complex modern conflicts.

INTRODUCTION

Networked warfare is an enabling concept that seeks to take advantage of modern technology to increase the speed of command and combat effectiveness of military operations. By sharing information across a force, a common level of understanding can be achieved that, in turn, allows individual units that may be dispersed geographically to achieve synchronized effects in time and space. A further benefit of this concept is that the dispersal of forces it enables increases their survivability in a hostile environment.

Although it is not a military organization, the modern Al Qaeda provides a clear example of the success that an organization can achieve through the use of networked warfare techniques. Having come into existence in the 1980s to support Arabs fighting in the Afghan war against the Soviet Union, it has since developed into arguably the most dangerous terrorist organization in history. During that time, Al Qaeda's growth from a regionally based Islamic resistance group into a radical Islamist organization with global reach is an achievement that is impressive in its own right. What is more significant is that this evolution has taken place despite concerted attacks on its bases and senior leadership since its attack on the World Trade Center in 2001. The resilience Al Qaeda continues to demonstrate, along with the effectiveness it currently achieves through its ability to mobilize and co-ordinate not only its core members, but also a more diffuse global network of jihadi supporters, are a direct result of its practise of networked warfare.

This paper will demonstrate that Al Qaeda's networked operations have a significant amount to teach the Western military. A brief summary of the military concept of networked warfare will outline its aims and benefits, along with the conditions that must be met for an organization to implement it successfully. Next, the context for understanding Al Qaeda's use of networks will be provided by an examination of its origins, ideology, aims, and structure, highlighting how its organizational characteristics differ from the military in key areas relevant to networked warfare. The remainder of the analysis will consider Al Qaeda's operations in three parts. First, its 'traditional' use of networking to enhance its operations will be demonstrated. Next, the benefits and challenges that arise from its reliance on the Internet to provide its information exchange network will be assessed, along with the solutions it has found to the problems it faces. Lastly, Al Qaeda's extended use of the Internet for recruiting, financing, and as a weapon will be examined. The analysis will illustrate that throughout its implementation and extension of networked warfare, Al Qaeda demonstrates an ability to learn from and adapt to its surroundings that combines with an awareness of the strategic environment within which it is operating to underpin its success as a networked organization. In closing, Al Qaeda's methods will be used to underline the validity of military networked concepts, to illustrate how its use of networking can be challenged, and to indicate the direction for future development of the Western approach to networked warfare.

THE MILITARY APPROACH TO NETWORKED WARFARE

Modern military operations involve the co-ordinated activity of forces that are increasingly distributed over a wide geographic area. Whether due to the enhanced performance of modern weapons and sensors or to ever scarcer resources, force elements are either responsible for larger operating areas or are compelled to be more dispersed to ensure their survival. Under such conditions, communications between elements (and in particular the transfer of critical command and control information) can have a significant impact on operational success. In the same way that commanders were dependant on runners to deliver messages during the First World War, today's leaders rely on communications networks to deliver their intent to those under their command. As the speed of information transfer has increased, the quest for improved operational performance has shifted to other components of the command and control process. For example, once orders and intent are received, force elements must act in a coherent manner to achieve optimum effect. In a constantly evolving and often confused battlespace, commanders must therefore provide either continuous direction to their subordinates, or allow them to exercise delegated authority in an attempt to synchronize their actions. If self-synchronization is to be attempted, the greater the difference between co-operating subordinate commanders' perceptions of the battlespace, the lower the likelihood of effective co-ordination between them.

The potential contribution of network technology to military operations is described in a variety of ways by different nations. In the United Kingdom, the concept is referred to as Network Enabled Capability (NEC), which "offers decisive advantage through the timely provision and exploitation of information and intelligence to enable effective decision-making and agile actions."[1] In Canada, the idea is referred to as Network-Enabled Operations (NEOps), which is defined in a more detailed fashion as:

> An evolving concept aimed at improving the planning and execution of operations through the seamless sharing of data, information and communications technology to link people, processes and ad hoc networks in order to facilitate effective and timely interaction between sensors, leaders and effects.[2]

In a similar way, the United States concept of Network-Centric Warfare (NCW) "links sensors, communications systems, and weapons systems in an interconnected grid that allows for a seamless information flow to warfighters, policy makers, and support

---

[1] United Kingdom, Ministry of Defence, *Network Enabled Capability (JSP 777)* (United Kingdom: Ministry of Defence, January 2005), 2; available from http://www.mod.uk/NR/rdonlyres/E1403E7F-96FA-4550-AE14-4C7FF610FE3E/0/nec_jsp777.pdf; Internet; accessed 19 February 2007.

[2] Canada, Department of National Defence, *DND/CF Network Enabled Operations Working Paper* (Ottawa: Defence R&D Canada, 31 January 2006), 4/46; available from http://pubs.drdc.gc.ca/inbasket/dstpol3.060407_0959.p525133.pdf; Internet; accessed 19 February 2007.

personnel."[3] Whilst the various national expressions of networked warfare may appear to be different, this is not the case. The concepts share a common core, which is summed up in the statement that the networking of forces can deliver increased combat power, increased lethality, survivability and responsiveness through better synchronization of effects and greater speed of command.[4]

Although many nations are now pursuing networked operations, it is the United States' NCW concept that provides the broadest view of what modern technology can do in the military context. This is illustrated in a US Department of Defense study by David Alberts, John Garstka and Frederick Stein, which describes networked warfare as generating increased combat power by "networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization."[5] The reason the US military has achieved such a broad view of the potential offered by networks is that, in addition to the advantages of size and superior funding, its approach is also the most mature, having begun its development in the early 1990s. Since that time, the implementation of networked warfare has seen American capability, technology and procedures leading the way in creating the ability rapidly to achieve shared situational awareness and to synchronize operational activity to enhance its effect. Consequently, the NCW model will form the core of the following analysis of networked warfare, supplemented by information from the UK and Canadian models where the latter are clearer, differ substantially or simply add value.

UNDERLYING CONCEPTS

In order to understand how networking can generate improved performance, it is necessary to consider the processes and interactions that take place to support or achieve the application of combat power. These are described in the book *Understanding Information Age Warfare*[6] as taking place simultaneously across the physical, information, and cognitive domains of the battlespace. In that analysis, the physical domain represents the various physical environments of land, sea, air and space, and is the traditional arena of warfare where events take place and objects exist. In contrast, the information domain is the abstract arena where information is created, manipulated, and

---

[3] United States, Department of Defense, *Network Centric Warfare – Department of Defense Report to Congress* (Washington DC: Department of Defense, 27 July 2001), 1-1; available through http://www.dodccrp.org/html3/research_ncw.html; Internet; accessed 22 January 2007.

[4] David S Alberts, John J Garstka, Richard E Hayes and David A Signori, *Understanding Information Age Warfare 2nd Edition (Revised)* (Washington, DC: Department of Defense Command and Control Research Program, August 2001), 58; available through http://www.dodccrp.org/html3/research_ncw.html; Internet; accessed 15 January 2007.

[5] David S Alberts, John J Garstka and Fredrick P Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority* (Washington, DC: Department of Defense C4ISR Cooperative Research Program, August 1999), 2; available through http://www.dodccrp.org/html3/research_ncw.html; Internet; accessed 20 January 2007.

[6] Alberts, Garstka, Hayes & Signori, *Understanding Information Age Warfare*, 10-13.

shared; it is where command and control is achieved, and in particular where the commander's intent is communicated. Finally, the cognitive domain represents the mind of the warfighter and his or her supporting populace; it is where the commander's intent, doctrine, tactics, techniques, and procedures reside.

Once these three domains are recognized, the next step in understanding networked warfare is to examine how the interactions between them affect the execution of military operations. Although it is in the physical domain where objects exist and actions take place to achieve effects, it is in the cognitive domain where decisions take place and from which orders, direction and intent originate. Whilst an individual action (such as a soldier observing and subsequently engaging the enemy with a personal weapon) involves only the cognitive and the physical domains, modern military activity increasingly involves the information domain. With forces distributed over large geographic areas, remote sensors that provide information to various force elements, and command that is often exercised at a distance, large amounts of information must be moved around the battlespace through the information domain. The effect of this linking is that the ability of the information domain to function in both a timely and accurate fashion is critical to mission success, and that the combined performance of linked elements can be enhanced through an improved exchange of information.[7] Furthermore, as battles can now be won or lost as a result of events in all three domains, the ability to influence decision makers through activity in the information and cognitive domains has created attractive new targets, particularly to practitioners of asymmetric warfare.

OVERVIEW OF NETWORKED WARFARE

The basis of networked warfare is that it demands a change of approach to the conduct of operations. Essentially, rather than viewing the battlespace in terms of the platforms within it and the individual capabilities these platforms possess, a more holistic approach is required that links each of the various, often widely separated elements of a military force (referred to by Alberts, Garstka and Stein as “entities”). Once connected to the network, entities are able develop a high level of shared awareness of their environment to assist them in achieving the commander’s intent.[8] The mechanism for developing and using this shared situational awareness is spelled out in what the US command and control research program identifies as the tenets of networked warfare, which state that:

- A robustly networked force improves information sharing.
- Information sharing and collaboration enhance the quality of information and shared situational awareness.
- Shared situational awareness enables self-synchronization.

---

[7] For a more detailed analysis, see Alberts, Garstka, Hayes, & Signori, *Understanding Information Age Warfare*, Chapter 2.

[8] Alberts, Garstka & Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 88.

- These, in turn, dramatically increase mission effectiveness. [9]

The key idea is that by allowing the entities within a network to share and improve the quality of their information, the level of understanding of the whole force is increased, not just individually, but to a common level. This raised, but common level of awareness is critical to the success of networked warfare, as increasing the understanding of individuals to different levels would not be sufficient. It is only when unity of purpose is supported by a common perception of the environment that a force can begin to gain an advantage through networked operations.

BENEFITS OF NETWORKED WARFARE

Although the primary effect of networking is to increase the shared awareness of the force, simply possessing shared situational awareness will not in itself win battles. Rather, it is the way that this shared awareness is used that gives networked warfare its power. First, from the command perspective, the ability to access high quality information with minimum latency leads to improved decision making, not just in terms of the time required to reach a decision, but also in the accuracy of those decisions. This effect is highlighted in the US Joint Vision 2020 which recognizes that, whether in combat or in operations other than war, an information advantage creates a competitive advantage when it enables commanders to reach and implement better decisions faster than an opponent can react or a situation develop.[10] The potential fundamental change induced by networked warfare is therefore that "Information Age technologies will [also] enable continuous Command and Control processes" and "replace the cyclical processes of the Industrial Age."[11]

In addition to an increase in linear decision making processes, networking also provides the means to achieve a step-change in effectiveness. Empowering the entities within a network by devolving the power to make decisions allows them to act or react with increased speed, and to self-synchronize according to their shared understanding of the task in hand. In the military context, this represents "Mission Command relevant to the information age, [exercised] through the network-wide expression of command intent and an adaptive command and control process."[12] In other words, by developing shared situational awareness that specifically includes a full understanding of the commander's intent, the decision making cycle can be radically shortened with a corresponding increase in the tempo and effectiveness of operations. In taking this last step, it should be noted that networked warfare "has the potential to contribute to the coalescence of the

---

[9] United States Command and Control Research Programme, "Research: Network Centric Warfare," http://www.dodccrp.org/html3/research_ncw.html; Internet; accessed 30 January 2007.

[10] United States, Department of Defense, *Joint Vision 2020* (Washington, DC: US Government Printing Office, June 2000), 8; available through http://www.dtic.mil/jointvision/jvpub2.htm; Internet; accessed 10 February 2007.

[11] US DoD, *Network Centric Warfare - Report to Congress*, 2-2.

[12] UK MoD, *Network Enabled Capability (JSP 777)*, 3.

tactical, operational, and strategic levels of war"[13] by devolving higher level authority to well informed tactical elements.

In attempting to self-synchronize, one of the principal problems faced by force elements is that plans often do not survive contact with the enemy, which is due in part to the fact that situational awareness does not last very long in modern combat.[14] In this context, the shared situational awareness provided by networking serves directly to reduce the "fog of war." At its simplest, knowledge of the location of other friendly forces can improve their geographic co-ordination, and will significantly reduce the possibility of friendly fire incidents. When an accurate picture of enemy dispositions and friendly unit activity is blended into the operational picture, the resulting understanding of the battlespace serves to reduce uncertainty and friction, and is the means for effective self-synchronization of effort.[15] In addition to enabling self-synchronization, the achievement of enhanced awareness across a widely dispersed force combines with the performance of modern weapons and sensors to give the commander the ability to mass effects in time and space without the need to mass force elements.[16] This ability of co-operating units to remain dispersed whilst providing mutual support by proximity also serves to increase their survivability and to reduce risk.

KEY ENABLERS

In order effectively to achieve shared situational awareness and to practise devolved mission command, force elements require "a steady diet of timely, accurate information, and the processing power, tools, and expertise necessary to put battlespace information into context and turn it into battlespace knowledge."[17] This requirement was underlined in the US Department of Defense's July 2001 Report to Congress on networked warfare, which also identified a number of key organizational enablers. These included a requirement for technological improvements, the continued evolution of organizations and doctrine, and the development of relevant training.[18]

---

[13] Alberts, Garstka & Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 88.

[14] Vice Admiral Arthur K Cebrowski, U.S. Navy, and John J Garstka, "Network-Centric Warfare: Its Origin and Future," *Proceedings* Vol 124, Issue 1 (January 1998) [journal online]; available through http://www.usni.org/Proceedings/Articles98/PROcebrowski.htm#InfoSuper; Internet; accessed 18 January 2007.

[15] For detailed examples of the effect of NCW, see US DoD, *Network Centric Warfare – Report to Congress*, Chapter 8.

[16] Alberts, Garstka & Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 90.

[17] Alberts, Garstka & Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 91.

[18] US DoD, *Network Centric Warfare - Report to Congress*, 2-5.

From the technological perspective, the 'entry fee' to a networked posture is the network itself, which has been characterized as "a high performance information grid that provides a backplane (sic) for computing and communications."[19] Within that grid, the principal components are the hardware that forms the network and the software that hosts, processes and distributes the information the network contains. In the military context, both must be secure, deployable and interoperable with coalition partners. Furthermore, in order to prevent users from becoming overloaded (thereby reducing potentially useful information to mere data that is of no value because it cannot be used), network software must enable and assist the user to access information in a clear and concise manner. The requirement to develop a "Global Information Grid" (GIG) is identified in the US Joint Vision 2020, which defines it as "the globally interconnected, end to end set of information capabilities, associated processes, and people to manage and provide information on demand to warfighters, policy makers, and support personnel."[20] The concept of a GIG is echoed in UK and Canadian doctrine along with the obligation to achieve interoperability not just with potential coalition militaries, but across the spectrum of interagency activity.

Turning next to the evolution of policy and organizations, Alberts, Garstka and Stein comment that "the power of a new technology cannot be fully exploited to create competitive advantage without the simultaneous coevolution (sic) of organization and process."[21] The need for change is also recognized in the emerging Canadian policy, which states that "Traditional views of command and control may change…. Co-operation, collaboration and initiative will become more dominant attributes."[22] Although recognized in Western networked warfare doctrine, the size and fundamental depth of the change required is best indicated by Vice Admiral Arthur K. Cebrowski, U.S. Navy, and John J. Garstka, who comment that, whilst the traditional military approach to command is top-down and command-directed, a bottom-up organizational style is more effective at generating self-synchronization.[23] They illustrate their point by citing examples of network enabled business activity in companies as large as Wal-Mart and Deutsche Morgan Grenfell, whose operations now function intuitively and deliver a significant competitive advantage. From the military perspective, these examples are instructive. Although the networks these companies employ specifically do not require the conscious intervention of managers or leaders, the command and control capability that is essential to military operations is built into their systems. Managers retain the option to "command at all times and control when appropriate"[24] as they share situational

---

[19] Cebrowski & Garstka, *Network-Centric Warfare: Its Origin and Future*.

[20] US DoD, *Joint Vision 2020*, 9.

[21] Alberts, Garstka & Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 26-7.

[22] DND/CF, *Network Enabled Operations Working Paper*, 12/46.

[23] Cebrowski & Garstka, *Network-Centric Warfare: Its Origin and Future*.

[24] UK MoD, *Network Enabled Capability (JSP 777)*, 4.

awareness with the rest of the network and possess the tools to intervene. The challenge that remains for military commanders is the need to strike the balance between excessive interference and a lack of engagement, "between micromanagement of subordinates and excessive independence from commanders that may be possible through the broad asset visibility achievable through NEOps."[25] Consequently, whilst the changes made by business demonstrate that improvement within the military is possible on the scale required, they underline the need for specific policy and doctrine to support the evolution of networked warfare's command and control processes.

The third essential enabler for networked warfare is the ability of the people who participate in the network, and key to this is their training. Although the network provides them with the means to interact, "The basic building block of a network-centric enterprise is the entity. Entities work both individually and collectively to create the value generated by network-centric operations."[26] Whilst the entities this statement describes are both people and platforms, it is the people that operate the platforms and make the decisions in the cognitive domain. The US Department of Defense underlines the core role of personnel, identifying that its ability to exploit the shared situational awareness created by networks will depend on individuals being prepared to tackle information age problems with information technologies.[27] In other words, in addition to developing a functioning network that is supported by the necessary shift in policy and doctrine, networking will not succeed without qualified and committed personnel who will "need to adopt new attitudes, accept more responsibility, learn new skills, master new approaches, and operate new systems—all in a faster-paced environment."[28] It is therefore essential that people who are able to understand and develop networked warfare are either recruited or trained, and then retained against the lure of an external environment where their skills will continue to be a valuable commodity.

PRINCIPAL CHALLENGES AND ISSUES

In addition to meeting the conditions highlighted above, there a number of challenges that must be overcome in order to conduct networked warfare, the most immediate being the complexity and cost of the network itself. From the technological perspective alone, the rate of increase of hardware capability[29] means that equipment

---

[25] DND/CF, *Network Enabled Operations Working Paper*, 12/46.

[26] Alberts, Garstka & Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 245.

[27] US DoD, *Network Centric Warfare - Report to Congress*, 10-1.

[28] Alberts, Garstka & Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 229.

[29] For example, according to Moore's law, the performance of computer chips doubles every 18 months, and technological advances in optical cable technology are doubling the transmission capacity of networks every 12 months. *ibid*., 247.

becomes out-dated almost as soon as it is purchased. When considering the need to be interoperable with other national governmental agencies, let alone potential allies, the difficulty of standardizing equipment and procedures multiplies many times. The cost of rolling out a network therefore presents a significant obstacle to developing a networked warfare capability, which most aspiring nations (including the US) are seeking to overcome through a staged implementation process.

Once a network has effectively been developed within a force, it becomes an attractive target to an enemy, not least because of the potential to influence events in the cognitive domain highlighted above. The solution to this problem lies in effective Information Assurance and the associated function of Computer Network Defence, which require robust security measures and procedures, both physical and software enabled. However, the need for effective security is in direct conflict with another of the key principles of networked warfare, which requires information to be shared freely across the network wherever possible. The resulting tension must therefore be carefully managed to achieve the optimum balance between protection and shared awareness. At the same time, the natural tendency of entities within the network to hoard information must be overcome if true shared situational awareness is to be achieved.

The final significant obstacle to effective sharing of information is acquiring the ability to handle the large quantities of data that will be exchanged over an operational network. The distinction between data, information and knowledge represents the transformation of measured data into information as it is put into context and made meaningful, followed by the assimilation of that information in the cognitive domain to create useful knowledge.[30] The need to forge vast quantities of system data into knowledge that is available to enhance understanding (in the cognitive domain) is a challenge that will continue to grow as networked warfare matures and larger networks are formed.

SUMMARY OF NETWORKED WARFARE

Networked warfare in the military context is an enabling concept. It seeks to improve the combat effectiveness of a force by using modern technology to connect individual elements and commanders so that information can be shared more effectively across the entire organization. By sharing information, both the quality of that information and the level of common understanding within the force are increased. When this shared situational awareness includes an understanding of the commander's intent and details of friendly and enemy dispositions, force elements are able to self-synchronize in order to achieve massed effects in time and space from geographically dispersed locations. The fact that this activity can take place without the need for direct intervention by the commander reduces decision cycles within the force, increasing its speed of command, its survivability, and therefore its overall effectiveness.

[30] Although knowledge can also exist in the information domain, it is only of use when it creates understanding in the cognitive domain. Alberts, Garstka, Hayes, & Signori, *Understanding Information Age Warfare*, 16-17.

Implementation of networked warfare concepts requires the military to change its approach to operations. Organizationally, flatter management structures are needed to reduce the obstacles to information flow, whilst adoption of the mission command philosophy is essential to maximize the capability of units to self-synchronize. A commitment to networked operations, supported by policies and doctrine that enable the transition to a fully networked approach must underpin these changes. Specifically, command mechanisms that delegate the maximum amount of authority whilst retaining the ability to exercise control where necessary must be developed. From the equipment perspective, a key enabler is the network itself, which must be deployable and interoperable to achieve maximum access, but also secure enough to carry sensitive information to those that require it. Furthermore, the systems within the network must enable the information it contains to be used effectively, rather than overwhelming the operators.

The challenges that are faced by a military seeking to practise networked warfare begin with the 'entry fee' of physically constructing a suitable network, which then has ongoing costs of maintenance and upgrade. The next group of challenges is associated with operating that network. The most significant of these are the need to share information as freely as possible whilst securing the network and the information it contains, and the ability to achieve interoperability with all likely co-operating agencies. Lastly, establishing the necessary enabling policies and attitudes within an organization, along with educating and training personnel, is essential if the implementation and continued evolution of networked operations are to be successful. Notwithstanding these issues, the benefits of networked warfare outweigh the disadvantages. Once the challenges of implementing and sustaining the networked approach to warfare are overcome, effective information exchange and the shared situational awareness this generates provide the means to significantly enhance the survivability, speed of command, and as a result the overall operational effectiveness of a military force.

UNDERSTANDING AL QAEDA

> Al Qaeda remains such a poorly understood phenomenon….. Is it a monolithic, international terrorist organization with an identifiable command and control apparatus or is it a broader, more amorphous movement tenuously held together by a loosely networked transnational constituency?[31]

Whilst Al Qaeda undoubtedly conducts networked warfare, it is not a military organization. The impact its unique characteristics have on its operational techniques must therefore be assessed before its use of networking can be analyzed in the military context. In conducting its 'war' against the West, Al Qaeda draws strength from its own specific ideology and value systems, both of which govern the evolution of the organization's structure and procedures. These organizational characteristics place specific demands and restrictions on its operational methods, and in particular its use of networks. Consequently, whilst Al Qaeda's continued survival demonstrates that its techniques and procedures should be studied for ways to improve networked capability, some of its methods will simply not translate to the military environment. The following analysis of Al Qaeda's origin, radical views, aims, and structure will provide the context within which its approach to networked warfare can be understood.

THE ORIGIN OF AL QAEDA

The seventeenth of twenty sons of a Saudi construction magnate, Osama Bin Laden was one of a large number of Muslims who travelled to Afghanistan to fight with the Afghan people against the Soviet Union in the 1980s. During this period, Bin Laden used his personal wealth, the contributions of wealthy Arab donors, and considerable American funding to facilitate the flow of resistance fighters into Afghanistan. In support of this task, he built a recruiting and supply network that operated throughout the Middle East, South East Asia, Europe and the United States. That network, known simply as the Maktab al Khidmat (MAK) or 'Bureau of Services,' provided guesthouses, training, weapons, food supplies, and funding for the Afghan fighters.[32] In developing this support network, Bin Laden worked with Dr Abdullah Azzam, a major figure in the Muslim Brotherhood (which was the origin of many radical Islamist groups, including Hamas), and Umar Adb al-Rahman (known as the 'blind shaykh'), who was the spiritual leader of the Islamist group Al Jihad. These two figures were Bin Laden's principal early

---

[31] Bruce Hoffman, *Al Qaeda, Trends in Terrorism, and Future Potentialities: An Assessment* (Santa Monica, CA: Rand Corporation, 2003), 3; available from http://www.rand.org/pubs/papers/P8078/P8078.pdf; Internet; accessed 1 March 2007.

[32] United States, National Commission on Terrorist Attacks upon the United States, *Overview of the Enemy – Staff Statement No. 15* (Washington DC: US Government Printing Office, 2004), 1; available from http://www.9-11commission.gov/staff_statements/staff_statement_15.pdf; Internet; accessed 5 February 2007.

influences, along with Muhammad Qutb, his Islamic studies mentor at the University of Jeddah. Muhammad Qutb's brother, Sayyid, was also a central ideological figure in the early Islamist movement, and it is his writings that form the basis of the justification for violent jihad.[33] Qutb's concept of jihad was first used by Azzam to strengthen resistance in Afghanistan when he portrayed the Soviet occupation as an invasion of sacred Muslim territory by a non-Muslim power,[34] and it remains at the centre of Al Qaeda's strategy today.

In 1988, as victory over the Soviet forces in Afghanistan began to be achieved, Bin Laden and Azzam started to disagree over the future of their organization. At this time, the volunteer force and its associated support network were estimated by the US intelligence services to number between 10,000 and 20,000.[35] The dispute was resolved in November 1989, when Azzam was assassinated by Egyptian elements of the MAK. As a result, Bin Laden gained full control of the organization, and was able to pursue a more radical agenda using his newly acquired army.[36] Between the end of 1989 and 1991, Bin Laden moved from Afghanistan to Saudi Arabia and then to Sudan, using his business skills to develop the MAK into the entity that became known as Al Qaeda. During this period, he also reached out to other Islamic terrorist groups whilst developing and maintaining financial support through legitimate commercial investments.[37] At this early stage, Al Qaeda's structure was based on a series of functional committees that oversaw individual aspects of its operations. As the head of the organization, Bin Laden was supported by a *Shura* or inner advisory council that presided over four operational committees: a military committee, a finance committee, an Islamic law and political committee, and a media and publicity committee. The leaders of these groups were responsible for the smooth day-to-day running of the network, and for providing support in specific areas of the organization's operations through the formation of working groups that were compartmented to maintain security.[38]

Although Al Qaeda's early structure would appear to be a chain of command for terrorist operations, it should not be viewed in this way. Rather, the committee structure performed a co-ordinating function that provided support to individual operations which,

---

[33] For a more detailed explanation of Sayyid Qutb's views and influence on Al Qaeda, see: Peta Tarlington, "Understanding the Adversary, Sayyid Qutb and the Roots of Radical Islam," *Australian Army Journal* Vol 2, No. 2 (Autumn 2005), 173-180.

[34] Kenneth Katzman, *Al Qaeda: Profile and Threat Assessment*, Report Prepared for the United States Congress (Washington DC: Congressional Research Service, 2005), 1-2; available from http://www.fas.org/irp/crs/RS22049.pdf; Internet; accessed 1 March 2007.

[35] *ibid*., 2.

[36] Although Bin Laden never publicly criticized Azzam and was not directly linked to this attack, he was closely involved with the group responsible. Rohan Gunaratna, *Inside Al Qaeda – Global Network of Terror* (New York, NY: Columbia University Press, 2002), 22-23.

[37] 9/11 Commission, *Staff Statement No. 15*, 2.

[38] Gunaratna, *Inside Al Qaeda*, 57.

once conceived, would be entrusted to a dedicated leader who reported directly to Bin Laden.[39] In the military sense, therefore, Bin Laden represents the strategic commander supported by committees that correspond to a central staff within his headquarters. The individual mission leader equates to the tactical commander who receives direct support from above according to his specific needs, but without the need for an intermediate (operational) level. Further detail of this structure is provided by documents captured in operations during the Global War on Terror, which underline the use of a 'central staff' that guided policy, strategy and objectives under Bin Laden's leadership.[40] However, although helpful in providing initial context, this structure does not fully describe Al Qaeda in its current form, as it has as changed significantly in recent years as a result of its conflict with the West.

IDEOLOGICAL ROOTS

Before following Al Qaeda's evolution into its modern form, it is important to understand the ideology that has shaped that development. Most significantly, although it is a Muslim organization, Al Qaeda does not represent the whole of that community. Although Islam has historically been portrayed as a monolithic religion with a single identity, simply watching the television news demonstrates that this is not the case. The Islamic tradition is divided into two broad constituencies: Sunnis who follow the example of the Prophet Muhammad, and Shias who follow the Prophet and his descendants through the example of his son-in-law, Ali. Al Qaeda only accepts members from the four varieties of Sunni Islam, regarding Shia Islam as being founded on "falsehood."[41] Notwithstanding this division, it takes care to avoid confrontation with the other Islamic faiths in an attempt to maintain Muslim unity whilst concentrating on Jihad.[42]

However, to simply say that Al Qaeda is a Sunni group is to fail completely to capture its ideology, as it is most accurately described as a Salafist organization.[43] Salafism is a sub-community of the Islamist tradition that in turn is a part of Sunni Islam. The distinction between Salafists and Islamists can best be understood in terms of the

---

[39] 9/11 Commission, *Staff Statement No. 15*, 2.

[40] United States, United States Military Academy Combating Terrorism Center, *Harmony and Disharmony – Exploiting Al Qa'ida's Organizational Vulnerabilities* (West Point, NY: Combating Terrorism Center, 2006), 61; available from http://www.ctc.usma.edu/aq/Harmony%20and%20Disharmony%20--%20CTC.pdf; Internet; accessed 2 March 2007.

[41] Brian Whitaker, "Revealed: Al-Qaida Plan to Seize Control of Iraq," *The Guardian*, 13 October 2005; available from http://www.guardian.co.uk/Iraq/Story/0,2763,1590979,00.html; Internet; accessed 15 April 2007.

[42] Interview of Saad Al Faqih published in Mahan Abedin, "New Security Realities and al-Qaeda's Changing Tactics: An Interview with Saad al-Faqih," *Spotlight on Terror* Vol III, Issue 12 (December 2005) [journal online]; available from http://www.jamestown.org/terrorism/news/article.php?issue_id=3566; Internet; accessed 4 March 2007.

[43] Abedin, *Interview of Saad Al Faqih*.

place of Puritanism within the Christian movement. Whilst both are firmly religiously oriented, Islamists believe that the culture and law of nation states should be based on the whole of Islamic law; Salafists, on the other hand, require states to apply stricter rules that are based solely on the Qur'an. To complete this ideological analysis, jihadis (or 'holy warriors') are the militant strain of Salafism from which most terrorists are drawn.[44]

As a result of its narrow religious base, Al Qaeda is a relatively pure organization from the ideological perspective. This serves to align its members' views on aims and policy more closely than a broader-based organization, providing a common starting point for achieving the shared purpose that is essential to effective execution of networked warfare. Nonetheless, whilst its members' basic views might be the same, the contents of captured Al Qaeda documents, and analysis of online discussions between its members indicate that there can be significant internal discord and conflict.[45] Consequently, in addition to being a source of unity within Al Qaeda, its ideology is also a vulnerability that could be exploited, as its focused religious foundations present an identifiable means to divide it from the more moderate Muslim majority.[46]

AL QAEDA'S 'MISSION'

Whilst Al Qaeda's ideology has placed it in conflict with a number of different "enemies" throughout its existence, its central aim has not changed. Essentially, it sees itself as defending Islam against the threat of extinction that is a direct consequence of the spread of Western liberalism.[47] As a result, Al Qaeda seeks to follow its Salafist convictions wherever it can by replacing secular regimes with Islamic states based on the Qur'an. This translates into its long-term goal of creating a (potentially) global *Caliphate*, starting in the Arabian Peninsula and expanding through the Maghreb, Pakistan and beyond. This strategy is laid out in more detail in the online jihadi text *The Management of Barbarism*.[48] Al Qaeda's core approach to its struggle is evident from its online propaganda, whose central themes are that the West is implacably hostile to Islam, that the only way to address this threat is through violence, and that Jihad is therefore the only option.[49]

---

[44] For a more thorough description of Islamic communities, see United States, United States Military Academy Combating Terrorism Center, *Militant Ideology Atlas, Executive Report* (West Point, NY: Combating Terrorism Center, 2006), 6; available from http://www.ctc.usma.edu/atlas/Atlas-ExecutiveReport.pdf; Internet; accessed 2 March 2007.

[45] US CTC, *Harmony and Disharmony*, 14.

[46] Jarret M Brachman and William F McCants, *Stealing Al Qa'ida's Playbook* (West Point, NY: Combating Terrorism Center, 2006), 3; available from http://www.ctc.usma.edu/Stealing%20Al-Qai'da's%20Playbook%20--%20CTC.pdf; Internet; accessed 7 January 2007.

[47] Tarlington, *Sayyid Qutb and the Roots of Radical Islam*, 175.

[48] Stephen Ulph, "New Online Book Lays Out al-Qaeda's Military Strategy," *Terrorism Focus* Vol II, Issue 6 (17 March 2005) [journal online], 4; available from http://www.jamestown.org/images/pdf/tf_002_006.pdf; Internet; accessed 12 March 2007.

[49] Hoffman, *Al Qaeda, Trends in Terrorism*, 10.

CATALYSTS FOR EVOLUTION

With this central aim in mind, Al Qaeda's confrontation with the West, and in particular the United States as the symbol of Western secularism, was inevitable. The critical event which set Bin Laden on the path that changed him (and with him Al Qaeda) from an ally of America into its principal enemy was the deployment of US forces to Saudi Arabia following Iraq's 1990 invasion of Kuwait. In the words of Saad Al-Faqih, head of the Movement for Islamic Reform in Arabia and an acknowledged expert on Al Qaeda, "Bin Laden was shocked. He had fought in Afghanistan to keep the Russians out while now the most sacred Islamic country was being invaded by the Americans."[50] Al Faqih went on to offer the opinion that, in order to be consistent, Bin Laden was effectively obliged to attempt to drive the American "occupiers" out of Saudi Arabia.[51]

Initially, Al Qaeda's strategy was not complex, focussing simply (and unsuccessfully) on trying to bomb the United States' forces out of the Arabian Peninsula. The second key event in Al Qaeda's evolution was the radical change of direction that followed its 1998 merger with Dr Ayman Al Zawahiri's Egyptian Islamic Jihad against their (now) common enemy. Following the union, Al Zawahiri guided Bin Laden towards a new, more global strategy[52] based on provoking a conflict between cultures, which ultimately led to the attack on the World Trade Center in 2001. The period of pressure that resulted from America's subsequent attacks on Al Qaeda's logistics, training and operating bases in Afghanistan forced it to move away from the static posture that allowed it to be located and therefore targeted. Indeed, as early as November 2002, Al Qaeda's consultative council is believed to have recognized that it could no longer exist as a single hierarchy, but would have to become a decentralized global network to survive.[53] By 2005, the capture or elimination of 15 out of the 37 identified members of Al Qaeda's senior leadership[54] had caused Bin Laden to completely re-shape the group's entire structure and operational methods. The fact that a functioning command structure has continued to exist in the face of such attrition is clear evidence of the effectiveness of Bin Laden's changes, and also indicates that a "corporate succession plan" of sorts has been in operation.[55] Furthermore, the 2003 assessment by the head of Germany's

---

[50] Abedin, *Interview of Saad Al Faqih*.

[51] The subject of Bin Laden's 1996 fatwa against the United States, reproduced in Bruce Hoffman, "What Can We Learn from the Terrorists?" *Global Agenda 2004* (January 2004), 32; available from http://www.rand.org/commentary/011604GA/learn_from_al-qaeda.pdf; Internet; accessed 3 March 2007.

[52] Abedin, *Interview of Saad Al Faqih*.

[53] US CTC, *Harmony and Disharmony*, 9.

[54] Katzman, *Al Qaeda: Profile and Threat Assessment*, CRS Report to Congress, 5.

[55] Hoffman, *Al Qaeda, Trends in Terrorism*, 8.

intelligence service that Al Qaeda had grown to number some 70,000 world-wide[56] (from an estimated maximum of 20,000 at the end of the Afghan war) provides an indication of the wider organization's resilience and the appeal of its message.

CURRENT STRUCTURE

According to most counter terrorism analysts, Al Qaeda has indeed "evolved from a centrally directed organization into a worldwide franchiser (sic) of terrorist attacks."[57] This view is supported by the analysis presented by Dr Bruce Hoffman to the United States Armed Services Subcommittee on Terrorism in February 2006, which describes Al Qaeda as having become a "vast enterprise – an international franchise" that consists of four distinct, but overlapping dimensions.[58] Hoffman goes on to state that while the old Al Qaeda continues to exist (Hoffman refers to this first part as "Al Qaeda Central"), it has built an international terrorist network around this inner core. In addition to the "original" portion of Al Qaeda, Hoffman identifies "affiliates and associates" that consist of established terrorist groups that are supported by and relatively closely linked to Al Qaeda Central (such as the late Abu Musab Al Zarqawi's Al Qaeda in Mesopotamia, the South-East Asian Jemaah Islamiya, and the Pakistan based Harakat ul Mujahidin). The next layer of the network is described as "Al Qaeda Local," and consists of ex- jihadis who are likely to have some previous terrorist experience and may have been trained by Al Qaeda prior to 9/11. These "Locals" have tenuous links to the central core that may even be dormant. The final, outermost group is described by Hoffman as the "Al Qaeda Network," into which fall home-grown radicals or groups that are inspired by Al Qaeda and share its enmity towards the West, but have no direct links to its central core.[59]

Importantly, Al Qaeda Central's original committee-based command structure remains essentially unchanged in the midst of this diverse and distributed network. However, in contrast to their direct management of this central core, Bin Laden and Al-Zawahiri's influence over the outer layers of the organization is achieved through the provision of "ideological guidance, while leaving planning and financing of operations to the local commanders of allied but autonomous organizations."[60] In this sense, Al Faqih

---

[56] *ibid*., 9.

[57] US CTC, *Harmony and Disharmony*, 8.

[58] Bruce Hoffman, *Combating Al Qaeda and the Militant Islamic Threat - Testimony to the House Armed Services Committee, Subcommittee on Terrorism – February 16, 2006* (Santa Monica, CA: Rand Corporation, 2006), 3; available from http://www.rand.org/pubs/testimonies/2006/RAND_CT255.pdf; Internet; accessed 5 February 2007.

[59] Hoffman, *Combating Al Qaeda and the Militant Islamic Threat*, 4-5.

[60] US CTC, *Harmony and Disharmony*, 8.

characterizes the functioning of the wider network as "a college where people enrol, graduate and then go their separate ways," an organization where people are "encouraged to establish their own satellite networks."[61]

The lack of direct control within Al Qaeda becomes more pronounced the farther removed from the centre one looks, and there is little (if any) direct feedback from these loosely affiliated groups in the way a military organization would require it. Therefore, whilst any networked warfare techniques used in the command and control of Al Qaeda Central (and perhaps its close associates) are likely to be directly relevant to military operations, those that are employed in its interactions with other elements of the network will present a different picture. In this area, although even random attacks assist in spreading terror, Al Qaeda's leadership has a requirement to exercise some control over its wider network, as striking the wrong target can be counterproductive even for terrorists. Consequently, although command and control is not carried out in the military sense, the methods Al Qaeda employs to achieve shared intent across its wider network are of interest.

CONCLUSIONS

Notwithstanding the need for a detailed examination of operational techniques, some conclusions on Al Qaeda's networked characteristics are readily apparent at this stage. Preservation of the compressed command and control mechanism it used during its early years has allowed Al Qaeda to retain the flatter, more linear, networked structures that the long-term goal of military networked warfare and deliver increased operating success to international businesses that have adopted them.[62] This, along with the specific absence of an operational level of command, is a clear illustration of how the enabling structures identified in the networked warfare concept are built into the core of Al Qaeda, making it well suited to the geographically distributed mode of operation it has been forced to adopt.

From the command and control perspective, the organization is geared towards a mission command concept of operations. The freedom of action Al Qaeda Central gives to its local commanders empowers the "entities" within its network. By giving them the latitude they need to adjust to their circumstances, they are better able to achieve the task in hand, which is another key networked warfare enabler. In the case of Al Qaeda's wider network, the general guidance given by Al Zawahiri and Bin Laden can be viewed as an approximation of the military commander's intent that a force must share effectively in order for the networked approach to succeed. When seeking to achieve unity of purpose, Al Qaeda and its associates also derive a significant advantage from the common ground that already exists between them as a result of the movement's shared Salafist goals and its jihadi approach to achieving them.

---

[61] Abedin, *Interview of Saad Al Faqih*.

[62] Hoffman, *What Can We Learn from the Terrorists?*

The combined effect of Al Qaeda's geographic distribution and its mission command approach is that it retains the ability to operate whilst being significantly more difficult to detect than it was in its previous form. Without this critical benefit of a networked approach to operations, the Global War on Terror might already have succeeded in eliminating any significant threat from Al Qaeda. Notwithstanding these early conclusions, the organizational features so far described are only enablers to the successful practice of networked warfare. Realizing the full advantages of networked warfare requires the provision and use of a suitable network, and the implementation of appropriate operational techniques.

AL QAEDA'S USE OF NETWORKING

The multi-layered nature of Al Qaeda gives rise to different command and control relationships for each level of the organization. Whilst Al Qaeda Central maintains an effectively paramilitary structure, Al Qaeda's leadership committees exert a more general influence over the organization's 'Locals' and wider network. In most other areas, the information requirements of each level are similar, which results in their using the same or similar techniques for networked operations. For instance, whether a terrorist cell is a part of Al Qaeda Central or simply a loosely tied affiliate organization, it must develop high quality information on its targets. Similarly, in order to be effective, the network as a whole must develop shared situational awareness and common intent in order to self-synchronize effectively. The following analysis of Al Qaeda's networked activity will consider the organization as a whole, making distinctions between levels only where these are necessary in the area of command and control.

In the first section of this paper, networked warfare was defined as an enabling concept that serves to enhance the performance of an organization by improving the quality and distribution of information within it. In this traditional sense, Al Qaeda has mastered those portions of networking that it needs to succeed across its entire structure. However, in using the Internet to conduct its form of networked warfare, Al Qaeda has maximized its utility. In addition to maintaining support that is essential to its continued effectiveness, Al Qaeda has moved from a simple 'network enabled' approach to using the network itself as a tool. This section will begin by analyzing the techniques and procedures used by Al Qaeda in networked warfare's 'traditional' areas of information sharing, developing shared situational awareness, exercising command and control, and planning. Thereafter, Al Qaeda's use of modern technology to support its networked approach will be examined. The chapter will conclude with an illustration of Al Qaeda's ability to extend the utility of the Internet to provide sustainment, and for use as a weapon in its own right.

PART 1 – 'CLASSIC' NETWORKING

INFORMATION SHARING

The first requirement of any organization that seeks to conduct networked warfare is information. However, simply possessing information is not sufficient to ensure success. Rather, it is the manner in which this information is used that is most important. By sharing information widely, an organization can improve both the quality and spread of its knowledge, and there is ample evidence that terrorists in general, and Al Qaeda in particular, do this on a large scale. By pooling information both internally and with other terrorist organizations, Al Qaeda is able to learn from and adapt to the ever-changing environment within which it seeks to operate. Exchanging information on new tactics or weapons improves members' individual tactical skills and enhances the capability of the organization as a whole. In parallel, improvements in both performance and survivability result from sharing intelligence on potential or planned targets, and on techniques employed by opposing (security) organizations. Pooling information also serves to preserve an organization's collective knowledge should key experts be lost or captured.

Consequently, the ability of a terrorist group to learn and share information is a primary indicator of the level of threat it poses.[63]

There are many examples of how Al Qaeda pools its knowledge, all of which illustrate its proficiency in this area of networked warfare, and information sharing over the Internet will be a recurring theme throughout this analysis. Although e-mail and other one-to-one forms of communication (such as Internet telephony) are used for directing specific operations, the use of discussion fora and virtual message boards on the Internet are more efficient methods of information sharing across a large organization. Not only do these methods allow large numbers of individuals simultaneous access to the information, they also permit discussion and feedback on the data posted, adding detail or eliminating errors in order to improve the overall quality of the information itself. This process is summed up in an article on Internet Jihad by Stephen Ulph, a senior fellow with the Jamestown foundation and the Islamic affairs editor and analyst for Jane's Information Group. Ulph outlines how the Internet is used by jihadis to exchange highly detailed experiences and information, specifically highlighting how groups compare techniques and exchange warnings of the actions of security services.[64]

Although this process would be useful even if it were carried out solely within Al Qaeda, it gains additional value by enabling terrorist groups to access information from outside of their own organizations. An illustration of how knowledge is gathered from external sources is provided by an Al Qaeda laptop captured in Afghanistan that contained data downloaded from the French organization Société Anonyme, which offers a two volume sabotage handbook with sections on assassination and anti-surveillance techniques.[65] With online bulletin boards serving as a conduit for the passage of information, data can be transferred not just within regions, but between terrorists on different continents. An example of the proliferation of capability this can achieve is the case of a request for information on bomb making techniques made by an African group that was answered from within Iraq.[66]

---

[63] Brian A Jackson, John C Baker, Kim Cragin, John Parachini, Horacio R Trujillo, and Peter Chalk, *Aptitude for Destruction Volume 1 - Organizational Learning in Terrorist Groups and Its Implications for Combating Terrorism* (Santa Monica, CA: Rand Corporation, 2005), ix; available from http://www.rand.org/pubs/monographs/2005/RAND_MG331.pdf; Internet; accessed 5 February 2007.

[64] Stephen Ulph, "A guide to Jihad on the Web," *Terrorism Focus* Vol II, Issue 7 (31 March 2005) [journal online]; available from http://www.jamestown.org/publications_details.php?volume_id=410&issue_id=3285&article_id=2369531; Internet; accessed 18 March 2007.

[65] Gabriel Weimann, *United States Institute of Peace Special Report "www.Terror.net" How Modern Terrorism Uses the Internet* (Washington, DC: US Institute of Peace, 2004), 9; available from www.usip.org/pubs/specialreports/sr116.pdf; Internet; accessed 2 February 2007.

[66] Steve Coll and Susan Glasser, "Zarqawi Intertwines Acts on Ground in Iraq With Propaganda Campaign on the Internet," *The Washington Post*, 9 August 2005, A01; available from http://www.washingtonpost.com/wp-dyn/content/article/2005/08/08/AR2005080801018.html; Internet; accessed 16 March 2007.

NETWORKED TRAINING

The sharing of information for security and recruiting will be covered later in this chapter; however, the passage of information for training purposes is a central feature of Al Qaeda's use of networking to improve its overall effectiveness. By sharing its accumulated knowledge with less experienced members (whether they be recruits to Al Qaeda Central or simply new affiliates or local radicals), Al Qaeda can spread its influence geographically without the need to operate vulnerable training camps, greatly reducing the likelihood of compromise and subsequent attack or capture of its members. Al Qaeda's approach to the use of the Internet for training is laid down in doctrine written by Abu Musab Al Suri, a central figure within the organization's training system. Al Suri states that jihadi training materials should receive the widest possible distribution, and highlights the centrality of the Internet to achieving this.[67] The presence online of training manuals that include the 700 MB *mawsu'at al-i'dad* (Encyclopaedia of Preparation for Jihad), Al Qaeda's online military magazine *Mu'askar Al-Battar* (The Al-Battar Training Camp),[68] and a variety of separate audio-visual jihadi manuals is clear evidence that Al Suri's policy is being implemented. The encyclopaedia itself is a comprehensive document that includes text and pictures, along with high quality video instructional materials, and all have been available for download from the Internet since January 2005.[69]

Knowledge sharing between Al Qaeda and its associates has been a feature of its operations over recent years. Evidence offered to the 9/11 Commission describes two disrupted attacks that were planned to have taken place at the end of 1999 against Los Angeles Airport and tourist sites in Jordan. Although the operations were to be conducted by independent groups, both had received training and assistance from Al Qaeda affiliated figures.[70] In July 2005, the attacks on the London Underground and on hotels at Sharm el Sheikh in Egypt graphically demonstrated how online advice can contribute to the success of terrorist attacks. In both cases, the perpetrators managed to research, plan and execute their operations under the noses of competent security services without detection. This success has been directly linked to training on how to plan and conduct an urban attack that was offered in Al Qaeda's online journal in September 2004.[71] The benefits to Al Qaeda of making its tactics and techniques available online are

---

[67] Bryjar Lia, "Al-Suri's Doctrines for Decentralized Jihadi Training - Part 2," *Terrorism Monitor* Vol V, Issue 2 (1 February 2007) [journal online], 3; available from http://www.jamestown.org/terrorism/news/uploads/TM_005_002.pdf; Internet; accessed 3 March 2007.

[68] Y Yehoshua, "Islamist Websites as an Integral Part of Jihad: A General Overview," *Middle East Media Research Institute - Inquiry and Analysis Series* No 328 (21 February 2007) [article online]; available from http://memri.org/bin/articles.cgi?Page=archives&Area=ia&ID=IA32807; Internet; accessed 10 March 2007.

[69] Lia, *Al-Suri's Doctrines for Decentralized Jihadi Training - Part 2*, 3.

[70] 9/11 Commission, *Staff Statement No 15*, 9.

[71] Michael Scheuer, "Assessing London and Sharm al-Sheikh: The Role of Internet Intelligence and Urban Warfare Training," *Terrorism Focus* Vol II, Issue 15 (5 August 2005) [journal online], 7;

therefore twofold. Not only does this process improve the quality and currency of knowledge within the core of the organization, it also serves to enhance the capability of its associates and more loosely affiliated groups. By enabling its wider network to succeed against targets that Al Qaeda Central may not have the resources to strike of its own accord, Al Qaeda enhances its overall capability.

DEVELOPING SHARED INTENT

In order to maximize the effect of this extended pool of terrorists, Al Qaeda must develop shared intent to ensure their combined effort remains focussed. In addition to being a resource for sharing information, the Internet is used by jihadis to discuss and debate issues. This often involves open arguments between organizations, the airing of personal disputes, or the publication and debate of religious justification for their attacks. One example of such activity is the events surrounding a division that appeared within Al Qaeda in 2002 when a group of younger Saudi Islamists wished to play a more important role in the organization. The disruptive effect of their unauthorized use of violence and issuing of online pamphlets was responded to by the publication on influential Salafist websites of a 460 page book *Osama Bin Laden: Mujaddid al-Zaman Wa-Qahir al-Amrikan (Osama Bin Laden: The Reformer of Our Times and Defeater of the Americans)*. The book sought to re-establish Bin Laden's primacy by raising him to the level of a major reformer, a status normally reserved for a select few scholars,[72] thereby preventing a split in the organization. In the same way that maintaining Osama Bin Laden's authority serves to reinforce the authority of Al Qaeda's central command structure, the various religious debates attempt to ensure that the organization's view of its collective purpose remains essentially pure. Whilst the former is required to sustain Al Qaeda's direct command and control mechanisms, the latter is an essential component of its mission command philosophy, and both assist in maintaining influence over its wider network. By achieving a common understanding of the targets that are (or are not) acceptable to the leadership, its associates and proxies can work in a more synchronized manner with less direction, a core principle of networked warfare.

As before, the Internet is central to this global debate. As well as maintaining focus and unity within Al Qaeda, the Internet is used to extend its influence. For example, on 8 February 2006, the Information Department of the Mujahideen Shura Council (an umbrella organization set up by Al Qaeda in Iraq[73]) posted an online message calling for other groups to join its ranks. By mid-2006, there were seven insurgency

---

available from http://www.jamestown.org/terrorism/news/article.php?articleid=2369764; Internet; accessed 18 March 2007.

[72] Gabriel Weimann, "Virtual Disputes: The Use of the Internet for Terrorist Debates," *Studies in Conflict & Terrorism* Vol 29, No. 7 (October – November 2006), 625; available through http://www.ebsco.com; Internet; accessed 24 February 2007.

[73] Lydia Khalil, "Mujahideen Shura Council in Iraq Expands Ranks, Continues Attacks," *Terrorism Focus* Vol III, Issue 8 (28 February 2006) [journal online]; available from http://www.jamestown.org/terrorism/news/article.php?articleid=2369913; Internet; accessed 30 March 2007.

groups co-ordinating their efforts in Iraq through the Shura Council.[74] The addition of Abu Musab Al Zarqawi's organization in October 2004 was a particularly significant achievement for Al Qaeda, with negotiations for the alliance having been conducted and announced online. What was even more significant from the perspective of achieving shared intent was that Zarqawi was only allowed to join Al Qaeda after he conformed to its policies by ceasing his attacks on Iraqi Shiites. Thus, in addition to using the Internet to create the conditions for both tied and affiliated organizations to achieve independent operational success, Al Qaeda uses the network to extend its influence to control or consume other organizations.

CENTRAL CONTROL – DISPERSED GUIDANCE

Notwithstanding Al Qaeda's ability to achieve a common view of its overall purpose, co-operating elements must be able to self-synchronize for distributed mission command to function effectively. This requires some form of unified command to provide a common view of targeting and timing, and this is exactly what jihadi leaders are able to achieve using the Internet.[75] At the strategic level, direction of Al Qaeda as a whole is provided by its central leadership structures that include Bin Laden and Al Zawahiri. However, as previously indicated, the organization's diffuse structure results in the use of two broad categories of command and control. Whilst the 9/11 attacks and those on the East African embassies in 1998 and the *USS Cole* in 2000 were centrally co-ordinated, and while events on the ground in Somalia were locally controlled by Al Qaeda deputies,[76] such direct control does not exist for the wider network. Although Al Qaeda has established relationships with several Islamist groups to inspire and assist it in attacking a range of targets,[77] control in the military sense can only be considered to exist when these organizations are working with Al Qaeda Central or are receiving its direct support to achieve a specific task. Accordingly, this analysis will first examine traditional command mechanisms, followed by a study of Al Qaeda's techniques for influencing its wider network.

The most documented operation conducted by what is now known as Al Qaeda Central was its attack on the World Trade Center on 11 September 2001. This operation also provides the "most illustrative example of the medium the internet provides for those… who desire to plan, coordinate (sic) and carry out attacks in Western democracies."[78] Evidence of the central command and control exercised through the Internet was discovered by US federal officials in the form of encrypted messages on the

---

[74] Weimann, *Virtual Disputes: The Use of the Internet for Terrorist Debates*, 633.

[75] Brachman and McCants, *Stealing Al Qa'ida's Playbook*.

[76] Gunaratna, *Inside Al Qaeda*, 77.

[77] *ibid*., 5-6.

[78] Canada. Canadian Security Intelligence Service Integrated Threat Assessment Centre, *Trends in Terrorism Series, A Framework for Understanding Terrorist Use of the Internet* Vol 2006-2, 8-9; available from http://www.csis-scrs.gc.ca/en/itac/itacdocs/2006-2.pdf; Internet; accessed 9 March 2007.

computer of Abu Zubaydah, a convicted Al Qaeda operative who is reputed to have masterminded the attacks. These messages had been exchanged between May 2001 and 9 September 2001 with the highest number of messages having been passed in August of that year.[79] Detail of the contents of those messages is reported to have been revealed by laptops captured in Afghanistan that demonstrated Al Qaeda was collecting intelligence and passing it in encrypted form over the Internet to locations in the United States.[80] In addition to such covert communication, the 9/11 teams also used the Internet to pass messages in clear speech, and Mohammed Atta's method for initiating the attacks is believed to have been a simple statement that employed code words to confirm the intended targets.[81] Although the Internet was used both to initiate actions and to provide feedback between the commander and his team early in the operation, it could not provide it in its latter stages of a suicide attack. Nevertheless, Bin Laden was still able to follow the operation's progress from Afghanistan, receiving detailed assessments of the damage it had caused in the form of radio and satellite television broadcasts.[82] The attack is therefore a clear demonstration of how the Internet, supplemented by the international media where necessary, provides Al Qaeda with the means to execute traditional military command and control from a distance.

More generally, the investigation that followed the attacks on the London Underground in 2005 has illustrated that the Internet has become the indispensable instrument through which Al Qaeda encourages strikes against Western targets by its wider network.[83] At the centre of Al Qaeda's influence over its affiliates and imitators are 'in-house' websites such as alneda.com, which, along with numerous other sites, have provided it with the ability to deliver strategic guidance and moral inspiration to its dispersed membership.[84] In addition to the theological content of these sites, specific guidance on target selection is provided to good effect. In 2004, Abdul Azziz Al Moqrin, the reputed Al Qaeda commander in the Arabian Peninsula at the time, issued instructions to his followers in an online publication regarding the preferred hierarchy of targets that they should attack, advocating most strongly strikes against economic targets related to the oil industry. The spate of kidnappings and killings amongst foreign oil workers that followed indicated that the instructions were closely followed.[85] In a less successful

---

[79] Weimann, *"www.Terror.net" How Modern Terrorism Uses the Internet*, 9.

[80] Timothy L Thomas, "Al Qaeda and the Internet: The Danger of "Cyberplanning"," *Parameters* Vol 33, Issue 1 (Spring 2003) [journal online], 112; available from http://www.carlisle.army.mil/usawc/Parameters/03spring/thomas.pdf; Internet; accessed 20 March 2007.

[81] Thomas, *Al Qaeda and the Internet: The Danger of "Cyberplanning"*, 119.

[82] Gunaratna, *Inside Al Qaeda*, 103.

[83] Shawn Brimley and Aidan Kirby, "Al Qaeda's Virtual Sanctuary," *Toronto Star*, August 23, 2005, A18; http://www.ebscohost.com/; Internet; accessed 13 January 2007.

[84] Thomas, *Al Qaeda and the Internet: The Danger of "Cyberplanning"*, 113.

[85] Bruce Hoffman, *The Use of the Internet by Islamic Extremists Testimony to the House Permanent Select Committee on Intelligence – May 4, 2006* (Santa Monica, CA: Rand Corporation, 2006),

example in 2006, an online posting directed jihadists to attack the trans-Alaska oil pipeline and Port of Valdez, providing links to other websites that contained useful information about the pipeline to assist in the planning of attacks.[86]

As stated above, in addition to providing specific tactical direction, the Al Qaeda leadership assists its wider network in maintaining a common direction by providing more generalized strategic guidance. In an online posting in October 2005, Al Zawahiri urged Al Qaeda associates to conduct attacks against oil installations throughout the Gulf States, explaining that Al Qaeda's anti-American strategy was an economic, not a military battle. The guidance went on to highlight the potential vulnerabilities of the West, detailing how best to strike at economic centres of gravity and stating that targets in Kuwait, Saudi Arabia and Venezuela should be considered.[87] The Internet therefore allows Al Qaeda's leadership to control a widely dispersed network of core operatives and willing supporters through a combination of specific direction and more general influence. By regularly issuing statements or speeches, the central leadership can maintain the ideological and strategic coherence of both its inner core and its looser affiliates, thereby maintaining the focus of the network's activity on Al Qaeda's ultimate aim of spreading radical Islam. By appealing to their common Islamist ideology, Bin Laden also seeks to enhance his influence over the thinking and behaviour of these latter, less closely controlled groups.[88]

OPERATIONAL PLANNING AND RESEARCH

Having developed shared intent and succeeded in providing broad direction for operations, Al Qaeda must lastly conduct detailed planning. Although its ability to share and enhance information has already been demonstrated, the capability to acquire high quality information and then to plan whilst remaining dispersed is the final component required for success in networked warfare. In this area, one of the hallmarks of an Al Qaeda attack is the huge investment in planning and preparation that is made. Before executing any operation, planning and rehearsal is preceded by the careful gathering and analysis of essential intelligence.[89] Although not strictly within the classic definition of

---

10-11; available from http://www.rand.org/pubs/testimonies/2006/RAND_CT262-1.pdf; Internet; accessed 5 February 2007.

[86] James Forrest, "The Internet and Global Terrorism," Family Security Matters website, http://www.familysecuritymatters.org/terrorism.php?id=244620; Internet; accessed 6 January 2007.

[87] Stephen Ulph, "Internet Mujahideen Intensify Research on US Economic Targets," *Terrorism Focus* Volume III, Issue 2 (January 18, 2006) [journal online], 3-4; available from http://www.jamestown.org/terrorism/news/uploads/tf_003_002.pdf; Internet; accessed 18 March 2007.

[88] Gunaratna, *Inside Al Qaeda*, 56-7.

[89] Gunaratna, *Inside Al Qaeda*, 8.

networked warfare, Al Qaeda's ability to use the Internet to acquire the information it needs to function effectively is a key feature of its operations, and the danger this ability to learn from its environment indicates was highlighted previously. Of particular interest is Al Qaeda's ability to meet one of networked warfare's particular challenges by developing operationally useful information out of the vast quantity of data that is available online. Once this information is in the hands of any part of its network, the ability to exchange, refine and then employ it described at the beginning of this section enables the planning process, which can be further assisted and directed from within Al Qaeda Central as necessary.

Acquiring what would appear to be sensitive information from open sources is not as difficult as one might expect, particularly since the advent of the Internet. However, such is the huge quantity of data available on the Internet that the use of open source intelligence (OSINT) is not easy. John E. Pike (who follows American intelligence agencies at the Web site, GlobalSecurity.org) summarized the use of OSINT as being "like drinking from Niagara Falls," stating that the greatest challenge to a user was the ability to "select what is most revealing."[90] Despite these challenges, the benefits available from OSINT are worth overcoming. As a result of the West's desire to place large quantities of information online, and a combination of poor security and laws that require governments to be demonstrably transparent, there is a significant amount of sensitive information available on the Internet. For example, by searching through online newspapers and journals, a terrorist can often develop a good idea of measures that may obstruct a planned operation. This was ably demonstrated in a 2002 media report that compromised the methods US law enforcement agencies were using to track Al Qaeda's telephone and online communications.[91] Al Qaeda does not ignore such reports. In evidence given to the 12th public hearing of the 9/11 Commission, the United States Attorney for the Northern District of Illinois stated that an Al Qaeda operative involved in the 1998 East African embassy bombings had been discovered in possession of sensitive official court documents. The fact that this information was earmarked for delivery to Bin Laden highlights the (understandable) interest within Al Qaeda in any anti-terrorism efforts that should appear in the open media.[92] Of equal value to terrorists is that OSINT is not limited to official information. In 2004, the *London Times* described information released by the US Government that terrorists had been accumulating intelligence on such

---

[90] John E. Pike, quoted in Scott Shane, "A T-Shirt-and-Dagger Operation," *The New York Times*, 13 November 2005; available from http://www.nytimes.com/2005/11/13/weekinreview/13shane.html?ex=1289538000&en=78e4e508a2e006a7&ei=5090&partner=rssuserland&emc=rss; Internet; accessed 19 March 2007.

[91] Thomas, *Al Qaeda and the Internet: The Danger of "Cyberplanning"*, 114.

[92] United States, National Commission on Terrorist Attacks upon the United States, 12th Public Hearing, 16 June 2004, *Statement of Patrick J Fitzgerald, United States Attorney, Northern District of Illinois*, 4; available from http://www.9-11commission.gov/hearings/hearing12/pfitzgerald_statement.pdf; Internet; accessed 12 March 2007.

diverse subjects as the flow of pedestrians outside target buildings, factors that might prevent a building from collapsing and the location of nearby emergency services.[93]

Despite its presence, the ability to glean useful drops of information from the ocean of data that the Internet contains does not come without effort. Modern terrorists rely on the support of a network of co-operating cells that aggregate intelligence into large databases to assist in attack planning and co-ordination. The power of this technique is illustrated by the words of an Al Qaeda training manual recovered in Afghanistan in 2003, which states that public sources can be used openly and legally to gather at least 80 percent of all information required about the enemy.[94] The fact that terrorists can access academic research data and sensitive details of potential targets, including threat and vulnerability assessments of these facilities, underlines the breadth of information available.[95] A preview of the potential applications of this combination of data and analysis tools comes from another captured Al Qaeda computer, which contained downloaded engineering features of a dam that would enable Al Qaeda planners to simulate catastrophic failures. Similar searches of other electronic media captured from Al Qaeda revealed evidence of research into the software and programming instructions for the digital switches that run power, water, transportation, and communications grids.[96] As a result of resources openly available online, Al Qaeda operatives are therefore able not only to improve their ability to conduct a successful attack, but also to refine the methods they employ to achieve maximum effect. While there is no suggestion that Al Qaeda knew it could bring down the twin towers, the far-reaching economic, political and social effects of the 9/11 attack demonstrate the impact that can be achieved by such 'spectaculars'. The effectiveness of 'cyberplanning' is a classic example of how networked warfare's principles of distributed collection, wide distribution and focussed utilization of information can help Al Qaeda continue to be "the most destructive international terrorist group in history."[97]

COMPARISON WITH MILITARY CONCEPT

The first section of this paper described the basic concepts upon which networked warfare is founded, detailing the benefits and problems that arise from its implementation. The preceding analysis demonstrates how Al Qaeda has employed the networked warfare concepts to its significant advantage. Through its mastery of information distribution both within and outside of its network, Al Qaeda has been able to refine and improve the quality of information it possesses, and at the same time to raise the general level of

---

[93] Zahid Hussain, "Confessions of a Computer Expert Gave US Vital Clues," *The Times*, 3 August 2004, 4; available through http://www.ebsco.com; Internet; accessed 5 February 2007.

[94] Canadian Security Intelligence Service ITAC, *A Framework for Understanding Terrorist Use of the Internet*, 7.

[95] Ulph, *Internet Mujahideen Intensify Research on US Economic Targets*.

[96] Weimann, *"www.Terror.net" How Modern Terrorism Uses the Internet*, 7.

[97] Gunaratna, *Inside Al Qaeda*, 13.

knowledge within its network as a whole. A core part of the information that is shared is directed at training its members in operational techniques and procedures. This shared training is supplemented by a steady diet of ideological dogma that is designed to justify and support the organization's cause. By simultaneously maintaining its shared ideology and developing common procedures, Al Qaeda lays the foundations for the mission command approach to operations that is at the core of its success. Having established the basis for shared intent, Al Qaeda's organizational unity and wider influence are enhanced through dialogue both internally and with other terrorist organizations. Whilst professional journals act as the forum for the airing of ideas within the Western militaries, it is the Internet that performs this function for Al Qaeda. Once achieved, shared intent is then extended by exercising distributed command and control, either directly (as in the Case of Al Qaeda Central) or through the strategic influence exerted by Bin Laden and Zawahiri over the wider network. This is designed to maintain Al Qaeda's operational coherence by ensuring that the actions of all parts of the organization contribute to its long-term aim, rather than achieving the damaging negative results of Zarqawi's indiscriminate attack on an Arab wedding in Egypt in 2005.[98]

As a result of its complex structure, Al Qaeda's basic use of networked warfare diverges from the military version in the area of command and control. Whilst networked principles are followed closely within its central core, Al Qaeda relies on publishing strategic guidance in its online magazines to achieve influence over its wider network. The apparent success of this approach is most likely due to the common ideological view Al Qaeda strives to maintain amongst its members, along with the fact that (unlike the military) there are few 'no-strike' targets in a terrorist campaign. Having issued direction, Al Qaeda again makes significant use of networking to research and plan its operations. Information is collected and then shared across the organization by the successful application of open source data mining. The overall effect of Al Qaeda's dispersed, networked approach is that it is extremely difficult to locate and therefore to target, and that it is able to mass effect in time and space from dispersed operating locations.[99] The resulting increase in survivability of the Al Qaeda network, the speed with which the organization responds to changes in its environment, and its demonstrable operational success in a hostile environment[100] are all key indicators of its status as an effectively networked organization. Al Qaeda achieves this success through its use of networked warfare over a 'Global Information Grid' which, ironically, the West has provided in the form of the Internet. The next section will demonstrate how Al Qaeda's

---

[98] Kathleen Ridolfo, "No Escape from Al Qaeda for Jordan," *Asia Times Online*, 15 November 2005; available from http://www.atimes.com/atimes/Middle_East/GK15Ak01.html; Internet; accessed 20 February 2007.

[99] For example "To launch the 9/11 operation AQ used Germany, the UAE, and Malaysia as launchpads to enter the United States. Cells in each country were established independently of each other…a few select members were permitted to liase between the compartmentalised cells." Gunaratna, *Inside Al Qaeda*, 104.

[100] Al Qaeda is capable of changing its messages within hours or days, and can reach its followers very quickly in comparison to its Western opposition. Information from Tom Quiggin, Senior Fellow at the Nanyang Technological University, Singapore, who is recognized by the Ontario Superior court as an expert on Al Qaeda and global jihad.

use of the Internet both solves problems inherent in the practise of networked warfare and exposes it to challenges that it must overcome to remain effective.

PART 2 – USING THE INTERNET AS AN ENABLER

Despite its somewhat puritanical ideology, Al Qaeda is a modern organization that is both proficient and adept at exploiting new technology to achieve truly global reach.[101] The expansion of the Internet that has accompanied Al Qaeda's evolution has been a major factor in its continued success, a fact that is supported by the rapid proliferation of terrorist websites from only 12 in 1997 to more than 4,500 by the middle of 2005.[102] However, whilst the Internet provides Al Qaeda with the "efficient and interoperable information grid" required by the networked warfare concept, the hardware, software and operating demands of the Internet provide a mixture of benefits and challenges. As a result of the Global War on Terror, Al Qaeda has adapted its doctrine and methods to best suit the online environment, taking advantage of existing opportunities whilst reducing or eliminating the associated risks as far as it is able.

THE INTERNET AS A 'GLOBAL GRID'

Although the concept of networked warfare did not exist at the birth of the Internet, an examination of the requirements of networking reveals that the Internet is well suited to supporting networked operations. From an infrastructure perspective, the Internet is capable of rapidly distributing large amounts of information to multiple users very efficiently, and at little or no additional cost to the owner of a laptop with access to a telephone line. Furthermore, using the Internet immediately solves the 'entry fee' issue faced by any military seeking to practise networked warfare, as the global infrastructure (both hardware and software) already exists. Commercial provision of online access removes the burden of maintenance and upgrade faced by the user of a bespoke network, whilst business pressures act to ensure the most modern technology is made available as soon as it is economic to do so. In addition to reducing cost, commercial support of the Internet ensures that it meets networked warfare's essential interoperability requirement, as new products must be designed to be compatible with existing infrastructure if they are to succeed in the open market. Moreover, because the Internet is available almost anywhere in the world (the 'almost' in this statement disappears if a laptop is linked to a satellite telephone), the need for a deployable network is removed. Thus, from an infrastructure perspective, the Internet meets the majority of networked warfare's support demands.

ADDITIONAL BENEFITS OF THE INTERNET

[101] Gunaratna, *Inside Al Qaeda*, 11.

[102] Mafoot Simon, "Countering Militant Islam in Cyberspace," *The Straits Times*, 18 October 2005; available from www.asiamedia.ucla.edu/print.asp?parentid=31719; Internet; accessed 19 March 2007.

The advantages gained by Al Qaeda from using the Internet to enable its networked operations are more than simply structural, as the presence of a suitable information grid is not the sole enabler of networked warfare. Without trained operators and a suitable enabling culture and doctrine within the networked organization, the majority of networked warfare's potential advantages cannot be realized. In itself, Al Qaeda's move to reliance on the Internet is clear evidence of its commitment to networking as a core part of its operational make-up, and the relatively flat structures that have developed within it are a result of its adaptation to networked operations. Notwithstanding the fact that Al Qaeda's transition was largely forced upon it, the Darwinian pressure that resulted from the Global War on Terror has undoubtedly combined with the success that has resulted from networked operations to drive Al Qaeda's evolution. Moving on to look at networked warfare's requirement for suitably trained personnel, the spread of standardised commercial technology and the resulting advent of the 'Nintendo generation' has provided Al Qaeda with a pool of ready-trained potential recruits. Whilst militaries are struggling to train their personnel on new operating systems and software, Al Qaeda simply draws on an ever expanding group of young people that have grown up with Internet technology and learned its use through play and (in many countries) as a formal part of their education.

Two very good examples of how readily trained personnel are available to Al Qaeda can be found in the cases of Mohammed Naeem Noor Khan and Babar Ahmad. Khan is characteristic of the young, educated Pakistani men who are targeted for recruitment by Al Qaeda. He holds a degree in computer engineering from a university in Karachi, and received guerrilla training in Afghanistan before being used to relay Al Qaeda messages. Following his arrest in Pakistan in July 2004, information from Khan's computer was used to warn of attacks in both the United Kingdom and America.[103] In a similar case that may have resulted from data recovered from Khan's computer, Babar Ahmed was arrested on a charge of running a network of Al Qaeda websites from the office where he worked as a mechanical engineer at a university in London.[104] Although the level of technical training may not be constant across Al Qaeda's areas of operation, these examples and the proliferation of its online presence illustrate that sufficient qualified recruits are available to support Al Qaeda's networked activity.

OPPORTUNITIES FOR SECURITY FORCES

Despite the apparent advantages offered by the Internet, there is one requirement of networked warfare doctrine that it does not inherently provide. As an open system, data that is passed over the Internet is susceptible to interception and interference, which presents both an opportunity for security forces and a challenge for Al Qaeda. Because it recognizes the problems of conducting its business in full view of the security services, Al Qaeda faces a continuing struggle to balance the demands of tactical control with

[103] Hussain, *Confessions of a Computer Expert Gave US Vital Clues*.

[104] Craig Whitlock, "Briton Used Internet as his Bully Pulpit," *The Washington Post*, 8 August 2005, A01; available from http://www.ebsco.com; Internet; accessed 19 March 2007.

operational security.[105] However, it has already been demonstrated that, in the post-September 11 environment, Al Qaeda has little option but to overcome the security challenges that result from its use of the Internet. In addition to the possibility of compromise through the monitoring of Al Qaeda's communications, security services have the opportunity to hack into, or to shut down its websites.[106] Alternatively, fake websites can be used to collect information on jihadis should they be fooled into using them. In any case, since all electronic communication leaves a trail of evidence that must be concealed or destroyed, Al Qaeda's hardware is vulnerable. The potential value of such computer evidence was illustrated by the 1999 arrest of Khalil Deek on terrorist charges in Pakistan. Details recovered from his home computer by the American National Security Agency enabled the FBI to prevent a bomb attack on New Year celebrations in Jordan in 1999.[107] However, whilst the thought of passing highly classified communications over the Internet might seem to open Al Qaeda to defeat at every turn, there are many factors that conspire to limit the effectiveness of the security services.

The principal challenge security forces face is the sheer difficulty of finding either messages or websites of interest from within an ocean of Internet data that continues to grow from its 2001 level of 28 billion images and 2 billion websites.[108] Having intercepted communications traffic, the problem has only just begun as decrypting messages can take a long time. For example, following the capture of Ramzi Yousef for his involvement in the 1993 World Trade Center bombing, files found on his computer that hid details of further operations took more than a year to decrypt.[109] With regard to the use of fake websites, the challenge is that of counter-detection. Such operations cannot hope to deceive jihadis unless they are designed and run by webmasters that understand both their culture and the obscure dialects that some groups use. In the same way that a member of the British gentry would struggle to pose as a rap artist in New York, Western intelligence agencies can be relatively easily to detect online.[110] Lastly, and in spite of the size of these practical challenges, the most significant obstacles faced by security agencies arise from the limitations liberal Western societies place upon their law enforcement agencies. The restrictions result mainly from free speech and human

---

[105] US CTC, *Harmony and Disharmony*, 12.

[106] Marie-Hélène Boccara, "Islamist Websites and Their Hosts Part I: Islamist Terror Organizations," *Middle East Media Research Institute – Special Report* No 31 (16 July 2004) [article online]; available from http://memri.org/bin/articles.cgi?Page=archives&Area=sr&ID=SR3104; Internet; accessed 20 March 2007.

[107] Jack Kelley, "Terror Groups Hide Behind Web Encryption," *USA Today*, 5 February 2001; available from http://www.usatoday.com:80/tech/news/2001-02-05-binladen.htm; Internet; accessed 16 March 2007.

[108] *ibid*.

[109] *ibid*.

[110] Information from Tom Quiggin, Senior Fellow at the Nanyang Technological University, Singapore.

rights laws, and range from controls on the filtering and blocking of online content to restrictions on the monitoring of communications.[111] The value of the protection afforded by Western societies to the very organizations that seek to undermine them is demonstrated by the servers these organizations chose as hosts. Not only are most Islamist websites located on the servers of companies in the West, many are even registered there.[112]

AL QAEDA'S SECURITY PRECAUTIONS

Despite the difficulties they face, security services still present a very real threat to Al Qaeda's online activity. Terrorist groups in general devote considerable effort to preventing successful information gathering efforts against them,[113] and Al Qaeda is no exception to this rule. In general, the organization maintains a functionally and regionally compartmented structure and places the highest priority on secure communications. Al Qaeda Central also has its own internal security service that vets new members to protect it from infiltration.[114] Whilst the basic system of human couriers and encrypted e-mails that supported its 9/11 operation[115] continues to be a feature of Al Qaeda's central core, its expanding global network has forced it to adopt more general forms of communication that are in turn more susceptible to detection and attack.

As a result of increasingly successful online counter-terrorist operations against its fixed websites such as alneda.com, two complementary lines of operation have emerged. First, Al Qaeda is taking more advantage of the openness of the Internet by regularly moving its sites between service providers that often know nothing of the sites that they support. For example, despite sustained pressure in early 2002, alneda.com remained active by moving between hosts in Malaysia, Texas and Michigan during a period of less than six weeks.[116] Should attacks on fixed sites become too effective, communications can fall back on the use of third party chat rooms and message boards,[117] many of which offer free upload of data and require little or no information on their users. A particularly effective method for communicating sensitive information through these sites is the

---

[111] For further examples of the restrictions faced by law enforcement agencies, see: Organization for Security and Co-operation in Europe, The Office of the Representative on Freedom of the Media, *Expert Workshop on Combating the use of The Internet for Terrorist Purposes* (Vienna: OSCE 2005) [document online]; available from http://www.osce.org/documents/odihr/2005/10/16705_en.pdf; Internet; accessed 19 March 2007.

[112] Yehoshua, *Islamist Websites as an Integral Part of Jihad: A General Overview*.

[113] Jackson, Baker Cragin, Parachini, Trujillo, and Chalk, *Aptitude for Destruction Volume 1 - Organizational Learning in Terrorist Groups*, xiv.

[114] Gunaratna, *Inside Al Qaeda*, 10, 58 & 80.

[115] *ibid*., 105.

[116] Thomas, *Al Qaeda and the Internet: The Danger of "Cyberplanning,"* 115.

[117] Boccara, *Islamist Websites and Their Hosts Part I: Islamist Terror Organizations*.

'virtual dead drop,' which involves the opening of an e-mail account on a free service such as Hotmail where a message is left in draft form. The host account details are then passed in code by other means to the intended recipient, allowing them to access the saved information.[118] If necessary, security can be further improved by transmitting the account identity and password in separate coded messages. By adapting their methods in this manner, Al Qaeda and other Islamist groups have proven themselves to be extremely resilient and resourceful. They demonstrate good awareness of the threat they face as well as the technical ability to react effectively.

Al Qaeda has developed methods to supplement these general procedures by using more complex techniques enabled by software that is readily available online. The simplest security measure available to Al Qaeda is the encryption of messages, which has been outlined in previous examples. Basic encryption software is available from free online sites that can be found by a simple Google search, whilst more advanced applications are available for purchase or can be downloaded for free for a limited period. More significantly, jihadis are also developing their own software. In January 2007, a website linked to Al Qaeda announced the release of a high quality encryption program designed specifically for information exchange over the Internet.[119] Other software (also available for free trial) can be used to pass information by hiding it in picture files in a technique called steganography. Interactive maps, photographs, directions and detailed technical information have all been disguised using this technique.[120] In addition to these more sophisticated encryption techniques, more secure networking services such as 'onion routers' or community groups like MySpace or Google's Orkut are also appearing. An 'onion router' is freely available plug-in for Internet browsers that is designed to prevent online traffic analysis and related forms of Internet surveillance. It works by using multiple encryption and re-routing of data through different locations around the world.[121] Al Qaeda's proven capacity to harness the benefits of new technology, added to the fact that onion router software is available for free download and is already widely used, makes it almost certain that its members are taking advantage of the privacy it offers. Orkut and MySpace, on the other hand, are community-based services that allow users to form private discussion groups. Orkut describes itself on its login page as "an online community that connects people through a network of trusted friends,"[122] whilst

---

[118] Canadian Security Intelligence Service ITAC, *A Framework for Understanding Terrorist Use of the Internet*, 9.

[119] Middle East Media Research Institute, "GIMF Announces Imminent Release of New Software," *Special Dispatch Series* No 1407 (3 January 2007) [article online]; available from http://memri.org/bin/articles.cgi?Page=archives&Area=sd&ID=SP140707; Internet; accessed 7 April 2007.

[120] Canadian Security Intelligence Service ITAC, *A Framework for Understanding Terrorist Use of the Internet*, 9.

[121] Paul Cesarini, "Caught in the Network," *The Chronicle of Higher Education* Vol 53, Issue 23 (9 February 2007), B5; available through http://proquest.com; Internet; accessed 3 April 2007.

[122] Orkut, "Login Page," http://www.orkut.com/GLogin.aspx?done=http%3A%2F%2Fwww.orkut.com%2F; Internet; accessed 25 March 2007.

MySpace states that it enables users to "create a private community" where you can "meet your friend's friends and suggest matches."[123] The attraction of these services is that they allow their members to share information amongst closed groups of like minded people based on the personal profiles they create. An example of their popularity amongst the online jihadis comes from Orkut's own tracking statistics, which reveal at least ten communities devoted to Bin Laden, Al Qaeda or jihad, with the largest Bin Laden community having more than 2000 members.[124]

In addition to hiding behind community based sites with more restricted access, some radical websites require new members to be introduced or simply restrict access to their content by use of an 'admissions committee.' Although this could be seen as limiting the free spread of information, it affords the users a greater degree of protection against unwanted monitoring than would otherwise be available.[125] Finally, as an aid to would-be supporters who might be less technically aware, some sites follow Al Qaeda's doctrine of online training and information sharing, offering specific advice on how to access radical sites and to protect personal data.[126] As a result of these multi-faceted security precautions, the depth and complexity of which has only been covered in broad detail here, Al Qaeda has reduced the security problems it faces from operating online to a manageable level. Protected by the constant chatter of the Internet, it can pass secure information in relative comfort, knowing that unless a security force is very well informed, it will be lucky to detect anything useful.

Although the risk of online compromise is relatively low, the need for security has the potential to reduce the effectiveness of Al Qaeda's network by restricting the flow of information within it. Although not specifically a security precaution, Al Qaeda's approach to information sharing is therefore relevant to this discussion. One of the central organizational qualities identified as an enabler of networked warfare is a commitment to the free flow of information across the network. In light of Al Qaeda's need to avoid detection by anti-terrorist agencies, it might be expected that security precautions might restrict its ability to implement networking principles. However, this is not the case, as Al Qaeda regards the risks involved in electronic communication as an acceptable price to pay for the benefits it brings.[127] The commitment to networked warfare this demonstrates produces a culture of sharing that contrasts with the difficulty militaries often face in achieving the openness that networked warfare requires, even

---

[123] MySpace.com, "About Us," http://www.myspace.com/Modules/Common/Pages/AboutUs.aspx; Internet; accessed 7 April 2007.

[124] Kasie Hunt, "Osama Bin Laden Fan Clubs, Jihad Recruiters Build Online Communities," *USA Today*, 9 March 2006, 04a; available through http://www.ebsco.com; Internet; accessed 29 March 2007.

[125] Yehoshua, *Islamist Websites as an Integral Part of Jihad: A General Overview*.

[126] SITE Institute, "A Guide for Internet Safety and Anonymity Posted to Jihadist Forum," http://siteinstitute.org/bin/articles.cgi?ID=publications160206&Category=publications&Subcategory=0; Internet; accessed 15 March 2007.

[127] Gunaratna, *Inside Al Qaeda*, 80.

when handling routine working data. Whilst Al Qaeda's preference for operational effectiveness over total security may not be appropriate across the spectrum of military operations, it does serve as an indication of the route to achieving more effective networked warfare.

SUMMARY OF ENABLING INTERNET USE

Al Qaeda's use of the Internet is an essential enabler of its current networked approach to operations that solves many of the problems faced by users of a bespoke network. By taking advantage of an in-place, commercially supported network, Al Qaeda faces none of the start-up or maintenance costs that hinder aspiring military practitioners of networked warfare. Similarly, the need to ensure interoperability and deployability are swept away by virtue of the Internet's ubiquity and its use of commercial equipment and software. Although the spread of technology also removes the need for Al Qaeda to conduct lengthy training of its network operators, it is not a panacea as its use of the Internet in support of operations creates a number of significant security challenges. Fortunately for Al Qaeda, the sheer size of the Internet presents an enormous challenge for security services seeking to gather useful intelligence that is made more severe by the law in liberal Western societies. Against this backdrop, Al Qaeda has adopted a number of complementary security measures that are supported (yet again) by the Internet. Having minimized the risks that are inherent in supporting its operations online, Al Qaeda's acceptance of the residual threat through its emphasis on information sharing over security demonstrates its commitment to maximize the benefits of networked operations.

It is clear from the example set by Al Qaeda that the Internet has considerable advantages in terms of speed, efficiency and availability to offer any organization that seeks to engage in networked warfare. The most significant drawback of conducting business on the Internet is its lack of watertight security. However, Al Qaeda's ability to survive against the determined efforts and technical superiority of the combined Western intelligence services demonstrates that this problem is manageable for an organization of Al Qaeda's size using freely available commercial technology. Whether in the form of its flat management structures, its use of mission command, or its commitment to the free flow of information (where appropriate), Al Qaeda has succeeded in establishing the key organizational enablers that underpin in its operational success. For the West, the benefits that Al Qaeda gains from its use of open source intelligence or by hiding behind Western laws are an indication of areas that should be considered when seeking to limit the jihadi threat. Although the imposition of draconian anti-terrorist laws would be handing the terrorists a victory in kind, the cessation of blind adherence to freedom of information legislation would go a long way towards limiting Al Qaeda's access to valuable planning data. Similarly, in the same way that Al Qaeda strives to strike a balance between the benefits of information sharing and security, the publishing of discussions and analyses of the techniques and shortcomings of anti-terrorist measures should be conducted with care.

PART 3 - EXTENDING THE USE OF THE NETWORK

Not only is Al Qaeda extremely effective at harnessing the power of the Internet to enhance its operational capability, it sees the network as much more than a simple enabler for its operations. In addition to its information exchange function, Al Qaeda extends the utility of the Internet by using it as a recruiting tool, as a source of funds, and as an offensive weapon. Alongside mounting traditional Information Operations, the Internet's lack of accountability and regulation has provided Al Qaeda with a method to conduct virtual attacks on its enemies. These cyber attacks offer the potential simply to cause disruption or to achieve more destructive results, either through data destruction, hardware damage, or by interfering with critical safety systems (such as air traffic control systems).[128]

NETWORKED SUPPORT - RECRUITING AND FINANCE

Al Qaeda actively advertises for new members on the open Internet. Whether it needs fighters, support workers, or online warriors for cyber attacks it advertises its 'positions vacant' on sites like those run by its media arm, Al-Jabha Al-I'lamiyya Al-Islamiyya Al-`Alamiyya (known in English as the Global Islamic Media Front (GIMF)). The job specifications in these advertisements often call for "excellent" skills in English and Arabic, or request help producing videos and other media,[129] providing a good indication that those recruited will not simply be used to conduct kinetic attacks. The Internet is invaluable in Al Qaeda's quest for these types of new members, as it is capable of reaching large numbers of potential recruits who would not be online unless they were computer literate. More significantly, Internet tracking software allows Al Qaeda to monitor user demographics and to identify potential sympathisers. These users can then be approached more directly, either as potential recruits or with requests for money.[130] In a March 2007 article on the US Department of Defense's online military news service, US Central Command's head of intelligence confirmed the effectiveness of using the Internet for recruiting, describing it as "the most important venue for the radicalization of Islamic youth."[131] In the same article, Stephen Ulph described how young people's mental views of their religion were first disrupted and then re-aligned towards radical Islam by online recruiters to draw them into jihadi organizations. Evidence of the widespread nature of online recruiting is provided by Saudi Arabia's new online counter-

---

[128] John Arquila and David Ronfeldt, *Networks and Netwars* (Santa Monica, CA: Rand Corporation, 2001), 41-45.

[129] Anton La Guardia, "Al-Qa'eda Places Recruiting Ads," *The Daily Telegraph*, 10 August 2005; available from http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2005/10/08/walq08.xml; Internet; accessed 29 March 2007.

[130] Canadian Security Intelligence Service ITAC, *A Framework for Understanding Terrorist Use of the Internet*, 7.

[131] John J Kruzel, "Jihadists Use Internet as Recruiting, Networking Tool, Intel Official Says," US Department of Defense American Forces Press Service [article online]; available from http://www.defenselink.mil/news/newsarticle.aspx?id=3261; Internet accessed 5 April 2007.

terrorism campaign to combat what it sees as Al Qaeda's main source of terrorist recruitment.[132]

In addition to needing a steady supply of recruits, terrorists cannot operate without funding. Whilst there are no reliable estimates of the demands placed upon Al Qaeda by its current operations, a 2002 estimate placed its annual budget in the region of $50 million.[133] Under Bin Laden, Al Qaeda has developed a sophisticated financial network to sustain its activity across the globe, with the majority of its fundraising is carried out through non-networked sources that include sympathetic donors in the Arab world and infiltrated Islamic charities.[134] Notwithstanding these conventional fundraising efforts, a significant and growing portion of Al Qaeda's income is generated from online activity. At the basic level, Al Qaeda broadcasts appeals on jihadi websites to solicit donations from sympathisers, and directly targets individuals whose potential support has been identified by their online activity in the manner outlined above. One example of such a general appeal is the 2001 broadcast by the Al Qaeda site azzam.com instructing its members to deliver funds to the Taleban in Pakistan, which resulted in criminal charges being brought against it.[135] Of more concern to the general public than soliciting donations from its supporters is Al Qaeda's use of online fraud. As early as 1997, Algerian led gangs were believed to be generating as much as $1 million a month for Al Qaeda through online fraud in Europe,[136] and the rise of Internet commerce that has taken place since is certain to have increased its earning capacity. A more recent example is the 2002 case of Imam Samudra, the Bali bomber who was accused of being a member of an Al Qaeda affiliated group, and was found to have attempted to finance his attack using online fraud.[137]

Once it has obtained its money, Al Qaeda also uses global networks to move it between parts of its organization. Having relied on a series of wire transfers to avoid detection whilst providing funds to the groups involved in the 9/11 attacks,[138] the advent of online banking has provided Al Qaeda with a simple but secure option for remotely

---

[132] Roula Khalaf, "Saudis Go Online to Thwart Would-Be Terrorists," *The Financial Times*, 1 April 2007; available from http://www.ft.com/cms/s/b238a7c6-e075-11db-8b48-000b5df10621.html; Internet; accessed 5 April 2007.

[133] Gunaratna, *Inside Al Qaeda*, 60-61.

[134] For a detailed discussion of Al Qaeda's fundraising, see: Victor Comras**, "**Al Qaeda Finances and Funding to Affiliated Groups," *Strategic Insights* Vol IV, Issue 1 (January 2005) [journal online]; available from http://www.ccc.nps.navy.mil/si/2005/Jan/comrasJan05.asp#references; Internet; accessed 5 April 2007.

[135] Whitlock, *Briton Used Internet as his Bully Pulpit*.

[136] Gunaratna, *Inside Al Qaeda*, 65.

[137] Jon Swartz, "Terrorists' use of Internet spreads," *USA Today*, 20 February 2005; available from http://www.usatoday.com/money/industries/technology/2005-02-20-cyber-terror-usat_x.htm; Internet; accessed 5 April 2007.

[138] Gunaratna, *Inside Al Qaeda*, 107.

managing its finances. Al Qaeda's use of the Internet has therefore allowed it to supplement support from donors and charities (willing or otherwise), whilst also increasing its ability to operate at a distance from the financial institutions that hold its funds.

ONLINE INFORMATION WARFARE

Islamists regard information warfare as an integral part of their struggle, employing the concepts of 'propaganda jihad' (*al-jihad al-da'wi*) and 'media jihad' (*al-jihad al-i'lami*), both of which are based on one of the Prophet Muhammad's Hadiths that requires Muslims to take whatever action is within their power to correct wrongs.[139] Al Qaeda's commitment to information warfare is demonstrated by its development of several internal media divisions and production companies, such as the previously mentioned GIMF.[140] These are supported by a range of external organizations such as qa3edoon.com and alsalafyoon.com, both of which provide valuable extra exposure for Al Qaeda's messages. The GIMF's capability was extended in 2005 when it established its Media Jihad Brigade (Katibat Al-Jihad Al-I'lami), whose aim is to fight the 'bias' of the Western media.[141]

Al Qaeda's current propaganda efforts are aimed at three principal target audiences. In addition to the task of maintaining the ideological purity and focus of its current membership described above, Al Qaeda also seeks to influence the wider Muslim community and any neutrals in its battle with the West. By encouraging moderate Muslims and other non-aligned observers to remain aloof, Al Qaeda generates tacit support for its actions amongst these groups; if they do not assist the security services, they help Al Qaeda to hide amongst them. Along with attempting to sway neutrals, widespread propaganda also supports Al Qaeda's recruiting effort through the spread of radicalization (particularly amongst the Muslim youth). Whilst these first two areas can be considered as aspects of Al Qaeda's efforts to sustain and develop itself, its third area of operations concentrates on attacking its enemy in the cognitive domain, a core task that arises from an understanding of the concepts of networked warfare. The area where Al Qaeda's propaganda efforts diverge from the military practise of networked warfare is that in addition to being the subject of the attack, the network and the information it contains also provide the tools for that attack.

Al Qaeda's initial method of publishing official statements, communiqués and videos is through Internet discussion fora, where these items often appear well before being more widely available. Thereafter, material that includes ideological support in the

---

[139] Yehoshua, *Islamist Websites as an Integral Part of Jihad: A General Overview*.

140 Despite its denials of any association with Al Qaeda, the GIMF is widely regarded as one of its websites. See: SITE Institute, "Al Qaeda Front Group Posts Its Spin on Bin Laden Tape to Jihadist Message Boards" [article online]; available from http://siteinstitute.org/bin/articles.cgi?ID=publications9804&Category=publications&Subcategory=0; Internet; accessed 7 April 2007, and: La Guardia, *Al-Qa'eda Places Recruiting Ads*.

[141] Yehoshua, *Islamist Websites as an Integral Part of Jihad: A General Overview*.

form of essays or *fatwas* from supporting religious scholars appears in publications such as Al-Qaeda's online magazine *Sawt Al-Jihad*, and the magazine of the Information Division of Al-Qaeda in Iraq, *Dhurwat Sanam Al-Islam* ('The Crest of the Summit of Islam'). In addition to ideological justifications for terrorist activities, these publications also carry revealing insight into jihadi thinking.[142] In one such article, the author demonstrated Islamists' clear understanding of their need to succeed both in practical operations and the propaganda war, noting that previous campaigns had been lost through media failures.[143] The clearest historical example of Al Qaeda's online ideological activity is the religious defence it mounted of its 2001 attack on the World Trade Center. When the attacks were questioned by several internationally respected Muslims, Al Qaeda used the websites alneda.com and drasat.com to label them as hypocrites with the result that several of them withdrew their criticism.[144]

In addition to its use of the written word, Al Qaeda makes full use of the Internet's multimedia capabilities to spread its messages. Before his death, Zarqawi in particular employed tactics that went far beyond the simple shock videos from which he drew his initial fame, publishing a monthly Internet magazine, *Thurwat al-Sinam* (The Camel's Hump). Zarqawi's approach mixed videos glorifying suicide bombers with an online news service that released details of his exploits several times a day in an attempt to taunt the American military.[145] The success of Al Qaeda's tactics is demonstrated by the celebrity Bin Laden has achieved amongst many Muslim communities. In addition to the spread of his speeches and interviews in these areas, the presence of posters, T-shirts and even pens and sweets bearing his name has become common.[146] Furthermore, by celebrating the actions of suicide bombers, Al Qaeda gives them the 'immortality' they seek, albeit in the online sense rather than the religious variety promised in jihadi propaganda.

Whilst Al Qaeda's self-supporting propaganda is of concern to the West, its use of the Internet for strategic information attack is the more enduring and dangerous threat.[147] To assume that jihadi organizations are simply concerned with conflict in their home territory would be to greatly underestimate their view of the war they are waging. The jihadi handbook *The Management of Barbarism* is quite clear on the need for radical

---

[142] Yehoshua, *Islamist Websites as an Integral Part of Jihad: A General Overview*.

[143] N Al-Kurdi, "The Fronts of Jihad," *Dhuwat Sanam Al-Islam*, Issue No. 3, 25-27, quoted in Yehoshua, "Islamist Websites as an Integral Part of Jihad: A General Overview."

[144] Thomas, *Al Qaeda and the Internet: The Danger of "Cyberplanning,"* 114-5.

[145] Coll and Glasser, *Zarqawi Intertwines Acts on Ground in Iraq With Propaganda Campaign on the Internet*.

[146] Gunaratna, *Inside Al Qaeda*, 52.

[147] Jarret Brachman, "High Tech Terror: Al-Qaeda's Use of Internet Technology," *The Fletcher Forum of World Affairs* Vol 30:2 (Summer 2006), 150; available from http://www.ctc.usma.edu/brachman/brachman-tufts.pdf; Internet; accessed 2 March 07.

Islam to understand how international politics works in relation to its struggle.[148] Bin Laden's suggestion that Al Qaeda would not attack any US state that did not support George Bush in the 2004 US presidential elections was an obvious attempt to influence US politics from afar. By issuing his statement just before the elections took place, he demonstrated his clear understanding of the working of the US political system. In support of its political attacks, Al Qaeda attempts to affect its enemies' public and military commitment to the fight against it by highlighting the collateral damage of military operations, and by showing the treatment received by captured or wounded soldiers.[149] In one specific example aimed at the military in 2005, the GIMF's Media Jihad Brigade claims to have posted threatening messages on websites used by soldiers in Iraq and their families.[150] Al Qaeda also uses the Internet to amplify the results of its operations through the publication of extreme images of terrorist attacks, and by issuing follow-on messages and threats that are designed to enhance the fear and uncertainty those attacks create.[151]

This broad approach to information warfare is completed by Al Qaeda's engagement in the art of deception. Making full use of the awareness it has developed of Western security procedures and of the responses specific threats will produce, Al Qaeda can achieve an effect without placing its members at risk. For example, by simply increasing the level of encrypted Internet messaging in a certain area, Al Qaeda can give the impression of an impending operation, potentially inducing a reaction from local security services.[152] Alternatively, it can issue an overt threat, as illustrated by the string of impending attacks that Al Qaeda has announced since 9/11, all of which received significant media coverage.[153] Thus, Al Qaeda is able to keep pressure applied by maintaining the impression of the threat it poses, and can simultaneously sow the seeds of doubt within the security community in advance of future operations.

By simultaneously seeking to reduce the military effectiveness of a nation's troops, attacking the morale of the general public and directly undermining support for the political leadership, Al Qaeda is conducting a broadly based attack on its enemies' capacity to defeat it. Not only does this approach demonstrate a sophisticated grasp of international politics, it combines the military concepts of manoeuvre warfare and the effects-based approach to operations, which takes a system-of-systems approach to

---

[148] Ulph, *New Online Book Lays Out al-Qaeda's Military Strategy*, 6.

[149] Yehoshua, *Islamist Websites as an Integral Part of Jihad: A General Overview*.

[150] E Alsech, "Cyberspace as a Combat Zone: The Phenomenon of Electronic Jihad," *Middle East Media Research Institute Inquiry and Analysis Series* No 329 (27 February 2007) [article online]; available from; http://memri.org/bin/articles.cgi?Page=archives&Area=ia&ID=IA32907; Internet; accessed 20 March 2007.

[151] Thomas, *Al Qaeda and the Internet: The Danger of "Cyberplanning,"* 115-6.

[152] *ibid*., 122.

[153] Weimann, *"www.Terror.net" How Modern Terrorism Uses the Internet*, 5.

influencing an adversary.[154] The effectiveness of this combined approach can be seen in the changes that are taking place in Western societies in response to the raised profile of radical Islam. In Europe, issues that range from immigration policies in the Netherlands to dress codes in German schools are increasingly high on the public agenda.[155] In North America, the new requirement for Canadians and Americans to carry a passport when crossing their shared border provides further evidence of the terrorists' success in influencing Western societies.

ENHANCING EFFECT – INFLUENCING THE MEDIA

Although Al Qaeda is adept at conducting information warfare through its own websites and those of its supporters, it can significantly enhance the effect of its propaganda by actively courting the international media. Whilst the activities of the GIMF and other online jihadi groups increases Al Qaeda's exposure, they cannot match the reach of organizations like CNN, the BBC or Al Jazeera. By harnessing the access these global news services achieve through both online publication and globally available television and radio programming, its messages can reach the widest possible audience. The techniques employed by terrorists to reach journalists include the provision of detailed online profiles of their organizations, the issuing of direct invitations to journalists to interact by e-mail, and the posting of press releases.[156] This courting of the media is backed by attempts at intimidation through the kidnap and murder of journalists, with videos of their treatment being posted as online warnings to others of the consequences of unfavourable coverage.[157]

The effect of Al Qaeda's use of the media is exemplified by the exposure it receives on the Arabic television station Al Jazeera, much to the annoyance of the United States. Whilst Al Jazeera does provide full coverage to both sides of the conflict, it does not share United States' definition of 'terrorism,' and the resulting suggestion that Al Jazeera be closed has done little to enhance America's claim to support free speech and democracy.[158] By making online material available to the international media, Al Qaeda is therefore able to challenge the West in an environment in which it has difficulty defending itself. The lack of regulation of Internet content allows anyone with a laptop

---

[154] For a detailed discussion of Effects-Based Operations in relation to networked warfare, see: Edward R Smith, *Effects Based Operations - Applying Network Centric Warfare in Peace, Crisis and War* (Washington, DC: US Department of Defense CCRP, 2002); available from http://www.au.af.mil/au/awc/awcgate/ccrp/ebo_smith.pdf; Internet; accessed 7 February 2007.

[155] Information from Tom Quiggin, Senior Fellow at the Nanyang Technological University, Singapore.

[156] Weimann, *"www.Terror.net" How Modern Terrorism Uses the Internet*, 4.

[157] Jacquelyn S Porth, "Terrorists use Cyberspace as an Important Communications Tool," *US Department of State website*, http://usinfo.state.gov/is/Archive/2006/May/08-429418.html; Internet; accessed 9 March 2007.

[158] Center for Defense Information, "Al Jazeera's Unwitting Role in the 'Unrestricted' Afghan War," http://www.cdi.org/terrorism/aljazeera-pr.cfm; Internet; accessed 7 January 2007.

and a telephone line to create their own version of the truth by distortion or selective publication of the facts.[159] When added to the Western media's commercially driven need for controversy and its interest in stories that are seen to 'hold the establishment to account,' terrorists have little difficulty in getting their messages broadcast, making journalists their unwitting assistants. The saturation of cyberspace with messages that are cleverly packaged to appeal to liberal societies' compassion for the underdog and dislike of religious discrimination allows Al Qaeda to create its own online reality. By failing to counter this effect through education of and effective engagement with the media, the West is ceding the high ground in the propaganda war to the terrorists.

CYBER ATTACK

Last in Al Qaeda's arsenal of online offensive weapons is its use of the Internet for conducting cyber attacks, which offer it a range of attractive ways to inflict significant damage on its enemies. Although there is no evidence that a successful attack has yet been made against a government site or one that supports defence interests or financial systems,[160] Bin Laden has been threatening such an event since 2002, and in 2005 the jihadi website al-farouq.com created a forum that called for increased efforts against such targets.[161] According to the FBI, there is substantial circumstantial evidence of attempts to conduct an Internet-based attack against utilities and telephone systems in America at the time of the 9/11 attack, the source of which was traced back to locations in Saudi Arabia, Indonesia and Pakistan. White House and FBI analysts were also quoted in 2002 as believing they had underestimated the time and effort that Al Qaeda had been spending on mapping American vulnerabilities in cyberspace. As a result, they believed that it was more a question of when, rather than if an Al Qaeda cyber attack would take place.[162] Consequently, although it has not yet achieved an 'online 9/11,' the level of interest Al Qaeda has demonstrated in the conduct of online attacks, allied to its capacity for learning, indicates that cyber warfare is a growth area for its struggle against the West.

Alongside its search for high profile targets that are suitable for attack, the online jihadi community continues to refine its skills and procedures against softer targets, and the Internet remains an active area of lower-level confrontation between Islamists and the West. The sophisticated methods employed by online jihadis provide a good indication of their current capability and of the future direction of cyber warfare. Whilst the security services hunt, monitor and occasionally shut down militant Islamist sites, the targets of the 'online mujahideen' can be any group or site that does not conform to Islamist ideals.

---

[159] Porth, *Terrorists use Cyberspace as an Important Communications Tool*.

[160] Alsech, *Cyberspace as a Combat Zone: The Phenomenon of Electronic Jihad*.

[161] Jeffrey Pool, "New Forum Postings Call for Intensified Electronic Jihad against Government Websites," *Spotlight on Terror* Vol III, Issue 8 (29 August 2005) [journal online]; available from http://jamestown.org/terrorism/news/article.php?issue_id=3446; Internet; accessed 22 March 2007.

[162] Barton Gellman, "Cyber-Attacks by Al Qaeda Feared," *The Washington Post*, 27 June 2002, A01; available from http://www.washingtonpost.com/ac2/wp-dyn/A50765-2002Jun26; Internet; accessed 7 April 2007.

In 2005, the Arabic-language site Minbar ahl al-Sunna wal-Jama'a, which has been linked to Al Qaeda, carried a post dividing targets into political, strategic, economic and individual categories. The most popular part of the post discussed attacks designed to disrupt protected systems and the infiltration of private computers, which it claimed was relatively easy.[163] Amongst the websites that are most commonly attacked are those of organizations that oppose hard-line Islamic values (for example answering-islam.org.uk). Alternatively the websites and systems of opposing ideologies such as the Christian, Zionist or Shi'ite faiths are attacked, an illustration of which is the Islamist attempt to penetrate the Vatican website that was detected and repelled in October 2006 following Pope Benedict's comments on Islam at a rally in Regensburg.[164] However, whilst the Vatican attack was conducted in response to a specific event, online jihadis state their general aims to be taking revenge for the death of Muslim 'martyrs' and the 'oppression of Muslims,' damaging the Western economy, and even achieving the total collapse of the West.[165]

In the same way that Al Qaeda uses online training as its backbone for spreading terrorist techniques for real-world operations, online guidance for would-be hackers is in plentiful supply. Sites such as al-farouq.com carry manuals on the destruction of electronic resources, e-mails, data and even computer hardware, and provide supporting links to sites that offer the software necessary to conduct such attacks.[166] The 'jihadi hacker forum' hosted by alghorabaa.net carries similar instructions, the most popular of which details how to penetrate computer devices and Intranet servers.[167] In executing their operations, online attackers favour two main strategies: 'swarming' and the 'ping attack.' Swarm attacks aim to paralyze a site or service by flooding it with inputs that exceed its server's capacity, causing it to reject further inputs or even to crash. Ping attacks aim to achieve the same effect, but employ programs that flood a site with e-mails, some of which may also carry viruses. Although the programs required to conduct ping attacks are widely available online, an indication of the Islamists developing capability is that they also create and distribute their own tailored versions of these attack programmes.[168]

In order to improve the effectiveness of swarm or ping attacks it is necessary to co-ordinate the actions of those involved, and there is extensive evidence of this function being performed by Islamist websites. A series of sites that are operated by 'attack co-

---

[163] Sean O'Neill, "West Faces Attacks from Cyberspace," *The Times*, 17 October 2005; available through http://www.ebsco.com; Internet; accessed 7 April 2007.

[164] Catholic World News, "Islamic Hackers Hit Vatican Website – Unsuccessfully," http://www.cwnews.com/news/viewstory.cfm?recnum=47065; Internet; accessed 7 April 2007.

[165] Alsech, *Cyberspace as a Combat Zone: The Phenomenon of Electronic Jihad*.

[166] Pool, *New Forum Postings Call for Intensified Electronic Jihad against Government Websites*.

[167] Ulph, *Internet Mujahideen Intensify Research on US Economic Targets*, 4.

[168] Alsech, *Cyberspace as a Combat Zone: The Phenomenon of Electronic Jihad*.

ordinators' who use names like 'Hackboy' and 'Majma Al-Hacker Al-Muslim' recruit and organize volunteers for electronic operations. The co-ordinators regularly advertise imminent attacks through posts on multiple websites that instruct participants to look out for details of the planned attack. These include the time the operation is to begin, the Internet address of the target, and the choice of program to be used. Attacks are then initiated by announcements that usually appear about 30 minutes before the appointed start time, a recent example of which targeting a Shi'ite website received 15000 hits and achieved approximately 3000 active responses.[169] The best recent example of a co-ordinated online attack took place in response to the publication of cartoons of the Prophet Muhammad by a Danish paper at the start of 2006. The operation involved a sustained 24-hour effort against both the paper itself and other publications, and was co-ordinated through the al-Ghorabaa site. Al Ghorabaa later publicized its success online, achieving widespread celebrity status amongst jihadi hackers.[170]

SUMMARY OF EXTENDED NETWORK USE

In summary, although each of the areas covered in this part of the paper is a study in itself, Al Qaeda's use of the Internet as more than a simple enabler is not a radical change to the principles of warfare. Indeed, many of the methods it employs and the tasks it completes flow directly from the ideas and concepts of networked warfare, such as the idea of an information attack on the enemy's cognitive domain. Similarly, both the facilitation of cyber attacks through information sharing, and the massing of effect through the exercise of online command and control are excellent examples of the benefits of networked operations. What makes Al Qaeda's activity different in these areas is its use of the Internet not simply as an enabler, but to leverage the access it offers to make it a weapon in its own right. This innovative use of the network is further extended into the areas of financial support and recruiting, both of which are supported by the organization's online propaganda activities. The end result of Al Qaeda's extended online activity is a further enhancement of its effectiveness and reach. Not only is the capability of its core organization increased through better funding and additional recruits, but the latent power of its dispersed supporters (particularly those with home Internet access in the West) can be mobilized to significant effect. Furthermore, by manufacturing propaganda that is attractive to the ratings hungry reporters within the international media, Al Qaeda's propaganda units can greatly enlarge the audience that is exposed to its messages. Finally, as a result of its awareness of the environment within which it operates, and in particular its political and media dimensions, Al Qaeda has succeeded in achieving a network-enabled, effects-based approach to operations that significantly extends the benefits it gains from its use of the network.

---

[169] *ibid*.

[170] Ulph, *Internet Mujahideen Intensify Research on US Economic Targets*, 4.

CONCLUSION

Al Qaeda is not a military organization. Rather, it is a diffuse multi-layered international terrorist network whose outer layers are more akin to an ideological movement than the paramilitary structures within its central core. Notwithstanding these differences, this study of Al Qaeda's methods has demonstrated the proficiency it has achieved in its use of networked warfare techniques, and the enhanced survivability and operational capability this approach has delivered to the organization as a whole. Whilst not all of Al Qaeda's methods are applicable to the military environment, the remainder either demonstrate the value of current networked warfare theory or indicate the direction in which Western militaries should proceed to further develop their networked capability. In addition to assisting us to develop, there are also lessons for our online battle against the asymmetric threat. Whilst the West is well aware of the danger it faces, it must not miss the opportunity to benefit from the lessons that Al Qaeda's techniques reveal simply because they are derived from the actions of terrorists.

LESSONS FOR MILITARY NETWORKING

Looking first from the practical perspective, there are a number of lessons that can be drawn from Al Qaeda's approach to networked warfare. Primarily, its use of the Internet as its information distribution grid solves many of the implementation problems faced by users of a bespoke system. By taking advantage of a commercially supported global network, Al Qaeda avoids prohibitive roll-out and maintenance costs, and faces none of the deployability or interoperability problems that affect many existing military systems. Using a network that operates on standard commercial equipment and software also ensures that a pool of trained personnel is available from within which to recruit. The only significant problem Al Qaeda's reliance on the Internet creates is that of security, which it has reduced to a manageable level through a combination of defensive procedures and heightened threat awareness amongst its members, both of which it promotes through its own online training. The clear functional benefits Al Qaeda derives from its use of the Internet demonstrate that military networks should take advantage of commercial hardware and software wherever possible in order to reduce development and training costs whist simultaneously increasing their interoperability. The utility of the Internet to assist in providing the global network access required to support modern military operations should also be considered. Whilst it is recognized that the volume of data generated by large-scale operations might preclude using the Internet as the sole carrier of data for such an event, Al Qaeda's ability to operate effectively (despite the focussed attention of Western security services) indicates that security concerns should not be a reason to avoid commercial channels completely. Furthermore, as the combination of ordinary laptops with suitable security software already allows remote access to certain systems, there is no clear reason why the military should not also take advantage of an existing global information distribution system that modern youth require little training to operate effectively.

Operationally, Al Qaeda provides a clear demonstration of how networked warfare techniques are capable of enhancing an organization's survivability and effectiveness. At the heart of Al Qaeda's continued success is the commitment it shows

to pursuing a networked approach to warfare. For example, despite its need to balance the maintenance of security with the internal openness required to achieve shared situational awareness, it has prioritized effective information sharing over potentially restrictive security precautions. Furthermore, its use of the mission command approach to operations, although arguably forced on it by the need to limit communications and remain dispersed, is an example of the operational benefit of empowering capable, well informed subordinates. The effort that Al Qaeda puts into maintaining the operational coherence of its wider network through online direction and debate, the great majority of which appears on open websites, demonstrates the value it places on supporting the shared situational awareness of its commanders. The enhanced success Al Qaeda achieves through its employment of networked warfare techniques therefore underlines the validity of the military concepts that they mirror. The most important of these are the need to enable mission command by establishing shared situational awareness that includes a firm grasp of the commander's intent, and the requirement for an organization to commit to sharing information in order for networking to function effectively.

The area where Al Qaeda diverges most from the current military employment of networked warfare is its use of the Internet for offensive operations. Whilst the concept of attacking the cognitive domain flows directly from an understanding of networked warfare, Al Qaeda successfully employs its propaganda machine to both attack its enemies and to underpin its recruiting and fund generation activities. What is more, although it has yet to achieve an online 'spectacular,' Al Qaeda is actively developing the capability to use the Internet as a weapon in its own right to conduct both disruptive and destructive attacks using 'cyber warfare' techniques. Al Qaeda's relative dominance in both cyber warfare and the online information war indicates an area where military operations are weak in comparison to the terrorists. Notwithstanding the fact that there is an awareness of this relative imbalance, and that the US 8th Air Force established a cyber warfare command in November 2006,[171] cyber and offensive information warfare capabilities must be developed by Western militaries. The use of these techniques by terrorists also presents a threat that must not be ignored by the governments they serve.

AL QAEDA'S ONLINE VULNERABILITIES

In addition to presenting examples of effective networked warfare, this analysis also provides an indication of areas where Al Qaeda's use of the Internet could be disrupted. In order to achieve this, measures to reduce the operational benefits Al Qaeda derives from its use of the Internet, and in particular its dominance of the online information war, must be pursued. Although the most effective way to disrupt Al Qaeda's networked operations would be to deny it access to the Internet, not only would this be impossible, it would also have a negative effect on those security services that gain useful information from monitoring its online activity. A more achievable aim would be to counter Al Qaeda's Internet information campaign and to interdict its online

[171] Staff Sgt C Todd Lopez, "8th Air Force to become new Cyber Command," *Official Website of the US Air Force*, http://www.af.mil/news/story.asp?storyID=123030505; Internet; accessed 28 March 2007.

communications, whilst simultaneously attempting to reduce the freedom of action that is provided by the combination of Western privacy laws and the Internet's lack of accountability. For example, by requiring Internet Service Providers (ISPs) to take some responsibility for the content of the sites they host, Western governments could make them more amenable to closing down offending sites once they were reported. Once ISPs were made accountable in this way, they might even take on some of the policing task themselves or be encouraged to maintain (better) records of their users. Although this would certainly not prevent terrorists from accessing the Internet, it would increase the effort devoted to monitoring their activity and may even enhance its effectiveness.

To complement these active methods of disrupting Al Qaeda's online activity, the West can also improve its defences. First, in order to enhance the effectiveness of the security services, a balance between the duty of the state to protect its population and laws that protect individual privacy must be reached. Whilst there is no simple solution to this problem, the advantages currently enjoyed by terrorists must be reduced without losing the very freedoms we seek to protect or handing the terrorists a propaganda victory. Next, the significant benefits Al Qaeda gains from the Internet as a result of our openness and the effect of freedom of information laws must be reduced. Compelling government agencies and critical service providers to place information that is useful to terrorists in the public domain should be reviewed to ensure that it does not do more damage than good. Finally, in the same way that terrorists learn from our activity and behaviour, we should take notice of theirs. There is an enormous quantity of online discussion and debate within and between various terrorist elements, including Al Qaeda. By making use of the access we have to their primary information exchange network, we can increase our understanding of their aims, their methods and their internal divisions in order to counter or exploit them more effectively.

THE FUTURE OF NETWORKED WARFARE

The last, and most significant conclusion that can be drawn from studying Al Qaeda's operational techniques concerns the direction that the future development of networked warfare should take. Al Qaeda's combined operations against the political, military and civilian populations of its enemies demonstrate its firm grasp of the environment within which it is operating, and employ the military concepts of manoeuvre warfare and the effects-based approach to operations. In addition to its own kinetic, cyber and information operations, Al Qaeda enhances its effectiveness by influencing the actions of other terrorist groups, and by using the international media to relay its message to large audiences across the globe. Were it a nation state, its conduct of operations in each of the political, information, military and economic spheres of operation would be considered a 'whole-of-government' approach to conflict. The success achieved by this combination of concepts demonstrates that using manoeuvrist principles and networked warfare techniques in support of an effects-based approach to warfare is an extremely potent combination. Moreover, when Al Qaeda's 'whole of government' approach is extended by its use of other terrorist organizations, its reach and effectiveness are increased still further.

The implication for western militaries is that, in order to succeed in the complicated conflicts in which they are increasingly involved, it is essential that their implementation of networked warfare is extended. Specifically, they must become more closely connected with other government departments and non-governmental agencies along the lines of Canada's Joint Interagency Multinational Public (JIMP) initiative, which seeks to address interoperability issues between these groups.[172] The ability to support a 'Full Spectrum Response' that involves network enabled, effects-based operations in a JIMP environment must be the long-term goal of networked warfare. Whilst achieving such a target is unlikely to be easy (particularly in terms of the command and control issues it raises within governments, let alone wider groups), it nevertheless represents the most complete response to asymmetric threats, and for the conduct of integrated operations in such complex environments as those encountered in the 'three-block war.'

[172] For a short definition of the JIMP concept, see: Canadian Forces Experimentation Centre, "Glossary," http://www.ops.forces.gc.ca/cfec/viewHTML_e.asp?islandid=452; Internet; accessed 20 March 2007.

BIBLIOGRAPHY

Abedin, Mahan. "New Security Realities and al-Qaeda's Changing Tactics: An Interview with Saad al-Faqih." *Spotlight on Terror* Vol III, Issue 12 (December 2005). Journal online; available from http://www.jamestown.org/terrorism/news/article.php?issue_id=3566; Internet; accessed 4 March 2007.

Alberts, David S, John J Garstka, Richard E Hayes, and David A Signori. *Understanding Information Age Warfare 2nd Edition (Revised)*. Washington, DC: Department of Defense Command and Control Research Program, August 2001; available through http://www.dodccrp.org/html3/research_ncw.html; Internet; accessed 15 January 2007.

Alberts, David S, John J Garstka, and Fredrick P Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority*. Washington, DC: Department of Defense C4ISR Cooperative Research Program, August 1999; available through http://www.dodccrp.org/html3/research_ncw.html; Internet; accessed 20 January 2007.

Alsech, E. "Cyberspace as a Combat Zone: The Phenomenon of Electronic Jihad." *Middle East Media Research Institute Inquiry and Analysis Series* No. 329 (27 February 2007). Article online; available from; http://memri.org/bin/articles.cgi?Page=archives&Area=ia&ID=IA32907; Internet; accessed 20 March 2007.

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

Boccara, Marie-Hélène. "Islamist Websites and Their Hosts Part I: Islamist Terror Organizations." *Middle East Media Research Institute – Special Report* No 31 (16 July 2004). Article online; available from http://memri.org/bin/articles.cgi?Page=archives&Area=sr&ID=SR3104; Internet; accessed 20 March 2007.

Brachman, Jarret. "High Tech Terror: Al-Qaeda's Use of Internet Technology." *The Fletcher Forum of World Affairs* Vol 30:2 (Summer 2006): 149-164; available from http://www.ctc.usma.edu/brachman/brachman-tufts.pdf; Internet; accessed 2 March 07.

Brachman, Jarret M and William F McCants. *Stealing Al Qa'ida's Playbook*. West Point, NY: Combating Terrorism Center, 2006; available from http://www.ctc.usma.edu/Stealing%20Al-Qai'da's%20Playbook%20--%20CTC.pdf; Internet; accessed 7 January 2007.

Brimley, Shawn and Aidan Kirby. "Al Qaeda's Virtual Sanctuary." *Toronto Star*, 23 August 2005; available through http://www.ebscohost.com/; Internet; accessed 13 January 2007.

Canada. Canadian Security Intelligence Service Integrated Threat Assessment Centre. *Trends in Terrorism Series, A Framework for Understanding Terrorist Use of the Internet* Vol 2006-2; available from http://www.csis-scrs.gc.ca/en/itac/itacdocs/2006-2.pdf; Internet; accessed 9 March 2007.

Canada. Department of National Defence. *DND/CF Network Enabled Operations Working Paper*. Ottawa: Defence R&D Canada, 31 January 2006; available from http://pubs.drdc.gc.ca/inbasket/dstpol3.060407_0959.p525133.pdf; Internet; accessed 19 February 2007.

Canadian Forces' Experimentation Centre. "Glossary." http://www.ops.forces.gc.ca/cfec/viewHTML_e.asp?islandid=452; Internet; accessed 20 March 2007.

Catholic World News. "Islamic Hackers Hit Vatican Website – Unsuccessfully." http://www.cwnews.com/news/viewstory.cfm?recnum=47065; Internet; accessed 7 April 2007.

Cebrowski, Vice Admiral Arthur K, U.S. Navy, and John J Garstka. 'Network-Centric Warfare: Its Origin and Future', *Proceedings* Vol 124, Issue 1 (January 1998), 28-35. Journal online; available through http://www.usni.org/Proceedings/Articles98/PROcebrowski.htm#InfoSuper; Internet; accessed 18 January 2007.

Center for Defense Information. "Al Jazeera's Unwitting Role in the 'Unrestricted' Afghan War." http://www.cdi.org/terrorism/aljazeera-pr.cfm; Internet; accessed 7 January 2007.

Cesarini, Paul. "Caught in the Network." *The Chronicle of Higher Education* Vol 53, Issue 23 (9 February 2007); available through http://proquest.com/; Internet; accessed 3 April 2007.

Coll, Steve and Susan Glasser. "Zarqawi Intertwines Acts on Ground in Iraq With Propaganda Campaign on the Internet," *The Washington Post*, 9 August 2005; available from http://www.washingtonpost.com/wp-dyn/content/article/2005/08/08/AR2005080801018.html; Internet; accessed 16 March 2007.

Comras, Victor. "Al Qaeda Finances and Funding to Affiliated Groups." *Strategic Insights* Vol IV, Issue 1 (January 2005). Journal online; available from http://www.ccc.nps.navy.mil/si/2005/Jan/comrasJan05.asp#references; Internet; accessed 5 April 2007.

Forrest, James. "The Internet and Global Terrorism." Family Security Matters website, http://www.familysecuritymatters.org/terrorism.php?id=244620; Internet; accessed 6 January 2007.

Gellman, Barton. "Cyber-Attacks by Al Qaeda Feared." *The Washington Post*, 27 June 2002; available from http://www.washingtonpost.com/ac2/wp-dyn/A50765-2002Jun26; Internet; accessed 7 April 2007.

Gunaratna, Rohan. *Inside Al Qaeda – Global Network of Terror*. New York, NY: Columbia University Press, 2002.

Hoffman, Bruce. *Al Qaeda, Trends in Terrorism, and Future Potentialities: An Assessment*. Santa Monica, CA: Rand Corporation, 2003; available from http://www.rand.org/pubs/papers/P8078/P8078.pdf; Internet; accessed 1 March 2007.

Hoffman, Bruce. *Combating Al Qaeda and the Militant Islamic Threat - Testimony to the House Armed Services Committee, Subcommittee on Terrorism – February 16, 2006*. Santa Monica, CA: Rand Corporation, 2006; available from http://www.rand.org/pubs/testimonies/2006/RAND_CT255.pdf; Internet; accessed 5 February 2007.

Hoffman, Bruce. *The Use of the Internet by Islamic Extremists Testimony to the House Permanent Select Committee on Intelligence – May 4, 2006*. Santa Monica, CA: Rand Corporation, 2006; available from http://www.rand.org/pubs/testimonies/2006/RAND_CT262-1.pdf; Internet; accessed 5 February 2007.

Hoffman, Bruce. "What Can We Learn from the Terrorists?" *Global Agenda 2004* (January 2004), 32-34; available from http://www.rand.org/commentary/011604GA/learn_from_al-qaeda.pdf; Internet; accessed 3 March 2007.

Hunt, Kasie. "Osama Bin Laden Fan Clubs, Jihad Recruiters Build Online Communities." *USA Today*, 9 March 2006; available through http://www.ebsco.com; Internet; accessed 29 March 2007.

Hussain, Zahid. "Confessions of a Computer Expert Gave US Vital Clues." *The Times*, 3 August 2004; available through http://www.ebsco.com; Internet; accessed 5 February 2007.

Jackson, Brian A, John C Baker, Kim Cragin, John Parachini, Horacio R Trujillo, and Peter Chalk. *Aptitude for Destruction Volume 1 - Organizational Learning in Terrorist Groups and Its Implications for Combating Terrorism*. Santa Monica, CA: Rand Corporation, 2005; available from http://www.rand.org/pubs/monographs/2005/RAND_MG331.pdf; Internet; accessed 5 February 2007.

Katzman, Kenneth. *Al Qaeda: Profile and Threat Assessment*. Report Prepared for the United States Congress. Washington DC: Congressional Research Service, 2005; available from http://www.fas.org/irp/crs/RS22049.pdf; Internet; accessed 1 March 2007.

Kelley, Jack. "Terror Groups Hide Behind Web Encryption." *USA Today*, 5 February 2001; available from http://www.usatoday.com:80/tech/news/2001-02-05-binladen.htm; Internet; accessed 16 March 2007.

Khalaf, Roula. "Saudis Go Online to Thwart Would-Be Terrorists." *The Financial Times*, 1 April 2007; available from http://www.ft.com/cms/s/b238a7c6-e075-11db-8b48-000b5df10621.html; Internet; accessed 5 April 2007.

Khalil, Lydia. "Mujahideen Shura Council in Iraq Expands Ranks, Continues Attacks." *Terrorism Focus* Vol III, Issue 8 (28 February 2006), 2-3. Journal online; available from http://www.jamestown.org/terrorism/news/article.php?articleid=2369913; Internet; accessed 30 March 2007.

Kruzel, John J. "Jihadists Use Internet as Recruiting, Networking Tool, Intel Official Says." US Department of Defense American Forces Press Service. Article online; available from http://www.defenselink.mil/news/newsarticle.aspx?id=3261; Internet accessed 5 April 2007.

La Guardia, Anton. "Al-Qa'eda Places Recruiting Ads." *The Daily Telegraph*, 10 August 2005; available from http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2005/10/08/walq08.xml; Internet; accessed 29 March 2007.

Lia, Bryjar. "Al-Suri's Doctrines for Decentralized Jihadi Training - Part 2," *Terrorism Monitor* Vol V, Issue 2 (1 February 2007), 1-4. Journal online; available from http://www.jamestown.org/terrorism/news/uploads/TM_005_002.pdf; Internet; accessed 3 March 2007.

Lopez, Staff Sgt C Todd. , "8th Air Force to become new Cyber Command." *Official Website of the US Air Force*, http://www.af.mil/news/story.asp?storyID=123030505; Internet; accessed 28 March 2007.

Middle East Media Research Institute. "GIMF Announces Imminent Release of New Software." *Special Dispatch Series* No 1407 (3 January 2007). Article online; available from http://memri.org/bin/articles.cgi?Page=archives&Area=sd&ID=SP140707; Internet; accessed 7 April 2007.

Myspace.com. "About Us." http://www.myspace.com/Modules/Common/Pages/AboutUs.aspx; Internet; accessed 7 April 2007.

O'Neill, Sean. "West Faces Attacks from Cyberspace." *The Times*, 17 October 2005; available through http://www.ebsco.com; Internet; accessed 7 April 2007.

Organization for Security and Co-operation in Europe. The Office of the Representative on Freedom of the Media. *Expert Workshop on Combating the use of The Internet for Terrorist Purposes*. Vienna: OSCE 2005. Document online; available from http://www.osce.org/documents/odihr/2005/10/16705_en.pdf; Internet; accessed 19 March 2007.

Orkut. "Login Page." http://www.orkut.com/GLogin.aspx?done=http%3A%2F%2Fwww.orkut.com%2F; Internet; accessed 25 March 2007.

Pool, Jeffrey. "New Forum Postings Call for Intensified Electronic Jihad against Government Websites." *Spotlight on Terror* Vol III, Issue 8 (29 August 2005). Journal online; available from http://jamestown.org/terrorism/news/article.php?issue_id=3446; Internet; accessed 22 March 2007.

Porth, Jacquelyn S. "Terrorists use Cyberspace as an Important Communications Tool." *US Department of State website*. http://usinfo.state.gov/is/Archive/2006/May/08-429418.html; Internet; accessed 9 March 2007.

Ridolfo, Kathleen. "No Escape from Al Qaeda for Jordan." *Asia Times Online*, 15 November 2005; available from http://www.atimes.com/atimes/Middle_East/GK15Ak01.html; Internet; accessed 20 February 2007.

Scheuer, Michael. "Assessing London and Sharm al-Sheikh: The Role of Internet Intelligence and Urban Warfare Training," *Terrorism Focus* Vol II, Issue 15 (5 August 2005), 6-8. Journal online; available from http://www.jamestown.org/terrorism/news/article.php?articleid=2369764; Internet; accessed 18 March 2007.

Shane, Scott. " A T-Shirt-and-Dagger Operation." *The New York Times*, 13 November 2005; available from http://www.nytimes.com/2005/11/13/weekinreview/13shane.html?ex=1289538000&en=78e4e508a2e006a7&ei=5090&partner=rssuserland&emc=rss; Internet; accessed 19 March 2007.

Simon, Mafoot. "Countering Militant Islam in Cyberspace." *The Straits Times*, 18 October 2005; available from www.asiamedia.ucla.edu/print.asp?parentid=31719; Internet; accessed 19 March 2007.

SITE Institute. "A Guide for Internet Safety and Anonymity Posted to Jihadist Forum." http://siteinstitute.org/bin/articles.cgi?ID=publications160206&Category=publications&Subcategory=0; Internet; accessed 15 March 2007.

SITE Institute. "Al Qaeda Front Group Posts Its Spin on Bin Laden Tape to Jihadist Message Boards." Article online; available from http://siteinstitute.org/bin/articles.cgi?ID=publications9804&Category=publications&Subcategory=0; Internet; accessed 7 April 2007.

Smith, Edward R. *Effects Based Operations - Applying Network Centric Warfare in Peace, Crisis and War*. Washington, DC: US Department of Defense CCRP, 2002; available from http://www.au.af.mil/au/awc/awcgate/ccrp/ebo_smith.pdf; Internet; accessed 7 February 2007.

Swartz, Jon. "Terrorists' use of Internet spreads." *USA Today*, 20 February 2005; available from http://www.usatoday.com/money/industries/technology/2005-02-20-cyber-terror-usat_x.htm; Internet; accessed 5 April 2007.

Tarlington, Peta. "Understanding the Adversary, Sayyid Qutb and the Roots of Radical Islam." *Australian Army Journal* Vol 2, No. 2 (Autumn 2005), 173-180.

Thomas, Timothy L. "Al Qaeda and the Internet: The Danger of "Cyberplanning"." *Parameters* Vol 33, Issue 1 (Spring 2003), 112-123. Journal online; available from http://www.carlisle.army.mil/usawc/Parameters/03spring/thomas.pdf; Internet; accessed 20 March 2007.

Ulph, Stephen. "A guide to Jihad on the Web," *Terrorism Focus* Vol II, Issue 7 (31 March 2005). Journal online; available from http://www.jamestown.org/publications_details.php?volume_id=410&issue_id=3285&article_id=2369531; Internet; accessed 18 March 2007.

Ulph, Stephen. "New Online Book Lays Out al-Qaeda's Military Strategy," *Terrorism Focus* Vol II, Issue 6 (17 March 2005), 4-6. Journal online; available from http://www.jamestown.org/images/pdf/tf_002_006.pdf; Internet; accessed 12 March 2007.

Ulph, Stephen. "Internet Mujahideen Intensify Research on US Economic Targets." *Terrorism Focus* Volume III, Issue 2 (18 January 2006), 3-4. Journal online; available from http://www.jamestown.org/terrorism/news/uploads/tf_003_002.pdf; Internet; accessed 18 March 2007.

United Kingdom. Ministry of Defence. *Network Enabled Capability (JSP 777)*. United Kingdom: Ministry of Defence, January 2005; available from http://www.mod.uk/NR/rdonlyres/E1403E7F-96FA-4550-AE14-4C7FF610FE3E/0/nec_jsp777.pdf; Internet; accessed 19 February 2007.

United States. Department of Defense. *Joint Vision 2020*. Washington, DC: US Government Printing Office, June 2000; available through http://www.dtic.mil/jointvision/jvpub2.htm; Internet; accessed 10 February 2007.

United States. Department of Defense. *Network Centric Warfare – Department of Defense Report to Congress*. Washington DC: Department of Defense, 27 July 2001; available through http://www.dodccrp.org/html3/research_ncw.html; Internet; accessed 22 January 2007.

United States. National Commission on Terrorist Attacks upon the United States, 12th Public Hearing, 16 June 2004. *Statement of Patrick J Fitzgerald, United States Attorney, Northern District of Illinois*; available from http://www.9-11commission.gov/hearings/hearing12/pfitzgerald_statement.pdf; Internet; accessed 12 March 2007.

United States. National Commission on Terrorist Attacks upon the United States. *Overview of the Enemy – Staff Statement No. 15*. Washington DC: US Government Printing Office, 2004; available from http://www.9-11commission.gov/staff_statements/staff_statement_15.pdf; Internet; accessed 5 February 2007.

United States. United States Military Academy Combating Terrorism Center. *Harmony and Disharmony – Exploiting Al Qa'ida's Organizational Vulnerabilities*. West Point, NY: Combating Terrorism Center, 2006; available from http://www.ctc.usma.edu/aq/Harmony%20and%20Disharmony%20--%20CTC.pdf; Internet; accessed 2 March 2007.

United States. United States Military Academy Combating Terrorism Center. *Militant Ideology Atlas, Executive Report*. West Point, NY: Combating Terrorism Center, 2006; available from http://www.ctc.usma.edu/atlas/Atlas-ExecutiveReport.pdf; Internet; accessed 2 March 2007.

United States Command and Control Research Programme. 'Research: Network Centric Warfare.' http://www.dodccrp.org/html3/research_ncw.html; Internet; accessed 30 January 2007.

Weimann, Gabriel. *United States Institute of Peace Special Report "www.Terror.net" How Modern Terrorism Uses the Internet*. Washington, DC: US Institute of Peace, 2004; available from www.usip.org/pubs/specialreports/sr116.pdf; Internet; accessed 2 February 2007.

Weimann, Gabriel. "Virtual Disputes: The Use of the Internet for Terrorist Debates," *Studies in Conflict & Terrorism* Vol 29, No. 7 (October – November 2006), 623-639; available through http://www.ebsco.com; Internet; accessed 24 February 2007.

Whitaker, Brian. "Revealed: Al-Qaida Plan to Seize Control of Iraq." *The Guardian*, 13 October 2005; available from http://www.guardian.co.uk/Iraq/Story/0,2763,1590979,00.html; Internet; accessed 15 April 2007.

Whitlock, Craig. "Briton Used Internet as his Bully Pulpit." *The Washington Post*, 8 August 2005; available from http://www.ebsco.com; Internet; accessed 19 March 2007.

Yehoshua, Y. "Islamist Websites as an Integral Part of Jihad: A General Overview," *Middle East Media Research Institute - Inquiry and Analysis Series* No 328 (21 February 2007). Article online; available from http://memri.org/bin/articles.cgi?Page=archives&Area=ia&ID=IA32807; Internet; accessed 10 March 2007.