REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED	
2. Security Classification Authority:	
3. Declassification/Downgrading Schedule:	
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.	
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT	

6. Office Symbol: C	**7. Address**: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207

8. Title (Include Security Classification): Al Qaeda: An Example of Network-Centric Operations

9. Personal Authors: Clayton D. Saunders, CDR, USN

10.Type of Report: FINAL	**11. Date of Report**: 04 February 2002
12.Page Count: 22	**12A Paper Advisor (if any)**: Dr. Elizabeth McIntyre

13.Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. Ten key words that relate to your paper: Al Qaeda, network-centric warfare, Osama Bin Laden, Operational Art, Operational Factors, terrorism, network-centric operations, knowledge superiority

15.Abstract: On 11 September 2001, Al Qaeda used information and knowledge advantage, access, and the ability to support forward-based teams, to conduct effects-based operations against the United States. Although obviously not employing the theory, in practice these operations appear to have been network-centric in nature, with Al Qaeda reaping the benefits inherent in this organizational and operational structure to conduct its attacks. Since VADM Cebrowski and John Garstka's January 1998 article, "Network Centric Warfare: Its Origin and Future," many defense related professional journals have continued the discussion, defining network-centric operations, describing their benefit to the fighting force and explaining how to develop the capability. But the discussion goes far beyond the military. In recent years there has been a change in the structure of information and technology that makes more information available more rapidly. Al Qaeda, by the way it uses information technology has, in effect, become a network-centric organization. Although it is a very different organization than the U.S. military, or more specifically, the Commander-in-Chief (CINC) of a regional unified military command, an examination of Al Qaeda's structure and operations may yield useful examples of network-centric theory put into practice.

16.Distribution / Availability of Abstract:	Unclassified X	Same As Rpt	DTIC Users

17.Abstract Security Classification: UNCLASSIFIED

18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT	
19.Telephone: 841-3556	20.Office Symbol: C

Abstract of

AL QAEDA: AN EXAMPLE OF NETWORK-CENTRIC OPERATIONS

On 11 September 2001, Al Qaeda used information and knowledge advantage, access, and the ability to support forward-based teams, to conduct effects-based operations against the United States. Although obviously not employing the theory, in practice these operations appear to have been network-centric in nature, with Al Qaeda reaping the benefits inherent in this organizational and operational structure to conduct its attacks. Since VADM Cebrowski and John Garstka's January 1998 article, "Network Centric Warfare: Its Origin and Future," many defense related professional journals have continued the discussion, defining network-centric operations, describing their benefit to the fighting force and explaining how to develop the capability. But the discussion goes far beyond the military. In recent years there has been a change in the structure of information and technology that makes more information available more rapidly. Al Qaeda, by the way it uses information technology has, in effect, become a network-centric organization. Although it is a very different organization than the U.S. military, or more specifically, the Commander-in-Chief (CINC) of a regional unified military command, an examination of Al Qaeda's structure and operations may yield useful examples of network-centric theory put into practice.

NAVAL WAR COLLEGE
Newport, R.I.

AL QAEDA: AN EXAMPLE OF NETWORK-CENTRIC OPERATIONS

by

Clayton D. Saunders
Commander, USN

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the
requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the
Naval War College or the Department of the Navy.

Signature: _____

04 February 2002

_____
Dr. Elizabeth McIntyre
Professor, JMO Department

AL QAEDA: AN EXAMPLE OF NETWORK-CENTRIC OPERATIONS

On 11 September 2001, Al Qaeda used information and knowledge advantage, access, and the ability to support forward-based teams, to conduct effects-based operations against the United States. Although obviously not employing the theory, in practice these operations appear to have been network-centric in nature, with Al Qaeda reaping the benefits inherent in this organizational and operational structure to conduct its attacks. Since VADM Cebrowski and John Garstka's January 1998 article, "Network Centric Warfare: Its Origin and Future," many defense related professional journals have continued the discussion, defining network-centric operations, describing their benefit to the fighting force and explaining how to develop the capability. But the discussion goes far beyond the military. In recent years there has been a change in the structure of information and technology that makes more information available more rapidly. "The underlying economics and technologies have changed. American business has changed. We should be surprised and shocked if America's military did not."[1] At the same time, we should also be surprised if terrorism did not change. By the way it uses information technology, Al Qaeda has, in effect, become a network-centric organization. Although it is a very different organization than the U.S. military, or more specifically, the Commander-in-Chief (CINC) of a regional unified military command, an examination of Al Qaeda's structure and operations may yield useful examples of network-centric theory put into practice.

Created in the late 1980s by Osama Bin Laden and others, Al Qaeda ties together many separate Sunni extremist organizations.[2] While Al Qaeda has conducted successful operations in

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
04 Feb 2002	N/A	-

Title and Subtitle Al Qaeda: An Example of Network-Centric Operations	**Contract Number**
	Grant Number
	Program Element Number
Author(s)	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Joint Military Operations Department Naval War College 686 Cushing Road Newport, RI 02841-1207	**Performing Organization Report Number**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)

Distribution/Availability Statement
Approved for public release, distribution unlimited

Supplementary Notes

Abstract
On 11 September 2001, Al Qaeda used information and knowledge advantage, access, and the ability to support forward-based teams, to conduct effects-based operations against the United States. Although obviously not employing the theory, in practice these operations appear to have been network-centric in nature, with Al Qaeda reaping the benefits inherent in this organizational and operational structure to conduct its attacks. Since VADM Cebrowski and John Garstka's January 1998 article, "Network Centric Warfare: Its Origin and Future," many defense related professional journals have continued the discussion, defining network-centric operations, describing their benefit to the fighting force and explaining how to develop the capability. But the discussion goes far beyond the military. In recent years there has been a change in the structure of information and technology that makes more information available more rapidly. Al Qaeda, by the way it uses information technology has, in effect, become a network-centric organization. Although it is a very different organization than the U.S. military, or more specifically, the Commander-in-Chief (CINC) of a regional unified military command, an examination of Al Qaeda's structure and operations may yield useful examples of network-centric theory put into practice.

Subject Terms

Report Classification	Classification of this page
unclassified	unclassified

Classification of Abstract	Limitation of Abstract
unclassified	UU
Number of Pages	
24	

the past, the thousands of people killed in the attacks on the World Trade Center towers set a new standard for terrorism. Since 11 September, many in the press have focused their questions on how the attack was possible, pointing fingers at the Clinton Administration and the reduction in Intelligence funding. Others, including those in the current administration, have investigated ways to prevent future terrorist actions in America. The creation of the new Homeland Defense secretariat and the military efforts in Afghanistan are but two examples of this effort. However, one area of analysis that has not been so thoroughly studied is what lessons operational level commanders can learn from the successes of Al Qaeda.

<div align="center">

Network-Centric Operations

</div>

Comparing Al Qaeda to the U.S. military?

Some readers will balk at comparing Al Qaeda to the Department of Defense, or better, a Theater CINC staff. There are indeed drastic differences in the two entities, from mission, to technology, to size. The mission of the U.S. military is to support U.S. national policy. As the regional warfighter, the CINC supports national objectives that are controlled and supervised by civilian authority, while Al Qaeda operates with no such supervision or restrictions. Al Qaeda is a non-state actor, a terrorist organization supported with funding and material from individuals and states sympathetic to its cause. Al Qaeda has no means other than violence to impact policy. Technological differences are also apparent. Al Qaeda does not possess the same level of weapons or communications technology as the U.S. military. For example, the 11 September attacks used no advanced weapons or communications. Final coordination was probably conducted by cellular telephone.[3] Finally, the two organizations are vastly different in size. Discounting the Taliban

membership, Al Qaeda is credited with fewer than 10,000 members worldwide.[4] Its organizational networks are also smaller and probably have little of the staff support found in U.S. military organizations. While this has implications for Al Qaeda's ability to quickly plan and mount operations and for the robustness of its structure, success and failure are to a large degree dependent on its ability to self-synchronize, gain access, and maintain a knowledge advantage.

Do differences in scale necessarily invalidate potential lessons? No, in fact the comparison is not between Al Qaeda and the current U.S. operational structure. The intent here is to analyze Al Qaeda's successes and failures in order to better understand how future U.S. network-centric force would work.

A Working Definition for Network-Centric Operations.

Before proceeding, it is necessary to set the terms for discussion. There are many articles, books and papers setting competing requirements for network-centric organizations. Many authors have moved beyond the philosophical tenets of this warfighting theory to focus on how technology can improve our ability to self-synchronize at the tactical level while increasing the speed of command or reducing the decision time from sensor to shooter. But technology is not the heart of network-centric warfare; rather, human and organizational behavior is.[5] While the technology enhances our capabilities, it does not define them. The power of this theory goes back to its underlying principles, namely the distribution of decision-making autonomy through the unified effort of self-synchronized forces. Once achieved, the commander can make more informed decisions, faster.

If network-centric operations can be defined for the purpose of this analysis, it would be "the process of deriving maximum military effect through the rapid and robust networking of diverse, well informed, and geographically dispersed forces."[6] Furthermore, this theory of warfare can achieve success throughout the entire spectrum of operations. To meet the definition, a network-centric organization must be able to **self-synchronize** and maintain a **knowledge advantage**. These two concepts are closely related. Robust networking of dispersed forces allows units to achieve unity of effort without physical collocation. This provides a greater degree of tactical flexibility.

There are several additional issues which flow from the definition of network-centric operations and which are important to any analysis.

- Well-informed commanders have knowledge of their own forces and those of the enemy; in essence they have good situational awareness. Adversaries have always wanted to have more information than their opponent, but this heightened sense of awareness, including both the commander's intent and, when possible, the enemy's intent, leads to a faster **speed of command**.

- The network-centric organization must have **assured access**. The ability to conduct offensive operations has always depended on the surety of access to the area of operations. In the network-centric environment, access is of greater importance because of the use of dispersed forces. Network-centric organizations are looking for greater efficiency in force employment, while forcible entry would require the massing of forces to be effective.

- Finally, the network-centric organization will conduct **effects-based operations**. This ties self-synchronization, knowledge superiority, dispersal, and access together. Network-centric operations stress the massing of capabilities, not platforms. Warfighting effects are achieved through the attack of those targets that are most disruptive to the enemy's strategy, without the resulting vulnerability associated with the massing of all combat power in one location.

Self-synchronization and knowledge superiority enables the dispersed, network-centric force to identify and target the enemy's centers of gravity. This paper does not challenge the assumptions made by Cebrowski, Alberts, Garstka, Stein, and others that network-centric operations provide increased combat power. In fact, analysis of Al Qaeda cells demonstrates the reality of their argument.

Al Qaeda.

Like any successful organization, Al Qaeda has strategic goals that are used to define operations. Before an analysis of the operational structure of the organization, it is important to understand its desired end state. Al Qaeda's expressed goal is to create Islamist states throughout the Middle East.[7] Bin Laden and Al Qaeda are violently against any American presence in the Arabian Peninsula and the Arabian Gulf region, which they see as obstructing this goal. Further, the Western values of the U.S. and the secular nature of its government are not consistent with the version of Islam practiced by Bin Laden and his followers.

Bin Laden also opposes King Fahd's regime in Saudi Arabia. In Bin Laden's view, King Fahd is personally responsible for allowing a continuing U.S. presence in Saudi Arabia following the

Gulf War. This particularly outrages him because he and his followers consider Saudi Arabia to be the Holy Land of Islam, forbidden to non-believers. They believe that the current Middle Eastern monarchies, especially those in the Gulf States, are courting a continued U.S. presence because they require the U.S. military to keep them in power. Instead of being true believers in Islam, they are siding with the idolaters; this makes them apostates, i.e., true believers who have forsaken Allah for the material riches of the West.[8] Removing the U.S. presence would give Al Qaeda the opportunity to spread Islamic fundamentalism throughout the Muslim world.

Al Qaeda has developed an operational concept to achieve its strategic goal of evicting the U.S. from the region. Al Qaeda cannot realistically establish a military force capable of doing this, but it can work to create the political conditions to do so. The conduct of terrorist attacks around the world is designed to undermine U.S. resolve in the region. Bin Laden believes that America is incapable of stomaching the death of its citizens at home or abroad. If it becomes painful enough, the U.S. will leave. The events in Somalia seemed to support this conclusion; the attack on U.S. Special Forces in Mogadishu in October 1993 led directly to the withdrawal of all U.S. forces in 1994. While it can be argued that the U.S. was looking for a way out of Somalia in 1993 and the Special Forces ambush was not the reason for the U.S. withdrawal, Bin Laden found causality. Like the fight against the Soviets in Afghanistan a decade earlier, the Arabs could fight the superpower and win.[9]

Al Qaeda's organizational structure is not military in nature. It more closely resembles a multinational corporate model, a structure with which Bin Laden is familiar.[10] By way of comparison, it is interesting to note that Cebrowski uses business models to identify the changing information technologies that have enabled the increasing value of network-centric principles. In

order to understand how the principles are applied within Al Qaeda, the organization will be

analyzed through the pillars that support the concept of network-centric operations.

Self-synchronization of Dispersed Forces.

The success of the attacks on the American Embassies in Dar es Salaam and Nairobi and

the attacks of 11 September 2001 indicate either that the terrorists had a high degree of

coordination or that they were able to self-synchronize their efforts across several continents. While

some might argue that the coordination would be an easy achievement for a small group of

individuals, if that were the case, Bin Laden would not be the first terrorist to successfully conduct

near simultaneous attacks. Perhaps his success is a result of the proliferation of information

technology or his organization's religious credo instead of the political agenda of other terrorist

organizations. The analysis begins with an understanding of self-synchronization.

To set the terms of discussion, self-synchronization is comprised of three elements, (1) unity

of effort, (2) commander's intent, and (3) rules of engagement. Superior knowledge of one's own

force, the enemy force, and the operating environment enhances self-synchronization. Knowledge

superiority can allow one to "organize and synchronize complex warfare activities from the bottom

up."[11] Self-synchronization then enables the organization to exploit this shared situational awareness

to increase the tempo of operations, increase the responsiveness, lower the costs and risks, and

increase effectiveness.[12] In discussing the importance of self-synchronization, some have focused on

combat units, operations, and effectiveness, stressing the need for technological connectivity, an

information backplane that provides the shared awareness that is the basis of self-synchronization.[13]

Technology alone is not the solution; people are a key part of the system. Starting with the elements listed above, how did Al Qaeda achieve self-synchronization in its operations? A shared fundamentalist Sunni Muslim faith provides Al Qaeda with unity of effort. All members have the same religious background. This provides a very strong identification with the organization and its work. New members are selected from mosques around the world, where clerics sympathetic to Al Qaeda can recommend further indoctrination for promising individuals. Many of the key members of Al Qaeda received religious instruction at the madrassas, or religious schools, in Pakistan. This structure provides a sorting mechanism and allows a high degree of selectivity for the team members.

The second element, commander's intent, is obvious in the case of Bin Laden. The overarching message to his various terrorist cells around the world is to kill American citizens, wherever they are. He made this part of the training and indoctrination programs at the various training sites in Afghanistan. It is also a fundamental part of the fatwas, or religious decrees, he issued in the late 1990s. According to Bin Laden's first fatwa, issued on 23 February 1998:

> For over seven years the United States has been occupying the lands of Islam in the holiest of places, the Arabian peninsula, plundering its riches, dictating to its rulers, humiliating its people, terrorizing its neighbors, and turning its bases in the peninsula into a spearhead through which to fight the neighboring Muslim peoples. . . . On that basis, and in compliance with God's order, we issue the following fatwa to all Muslims. The ruling to kill the Americans and their allies -- civilians and military -- is an individual duty for every Muslim who can do it in any country in which it is possible to do it, in order to liberate the al-Aqsa Mosque and the holy mosque [Mecca] from their grip, and in order for their armies to move out of all the lands of Islam, defeated and unable to threaten any Muslim. This is in accordance with the words of Almighty God.[14]

The third element, rules of engagement, is also fairly straightforward for the various Al Qaeda cells. In the conduct of their attacks, collateral damage is not only acceptable, but

encouraged. Bin Laden is counting on America's inability to suffer the deaths of her people, especially civilians. Therefore, spectacular attacks that embarrass the host nation security services and kill people in the hundreds are the types of engagements desired.

Knowledge Superiority.

Finally, the enabler, or force multiplier, is the development of knowledge superiority. Ever increasing amounts of information are needed in order to achieve speed of command. Improved knowledge management also leads to shared awareness, the building block that enables self-synchronization. These concepts are the foundation of the ability to conduct effects-based operations.[15] Knowledge superiority is a necessary but not sufficient element in all of the successful attacks conducted by Al Qaeda, including the Dar es Salaam and Nairobi Embassy bombings, the Khobar Towers bombing, the attack on USS COLE, and the 11 September attacks in New York and Washington. Given time, the terrorist cells were able to identify vulnerabilities that could be exploited.

Speed of Command.

Within the theory of network-centric operations, speed of command permits freedom of decision. If one side is able to make command decisions faster than the opponent force based on better knowledge, connectivity, and awareness, the opponent commander is forced to conduct a hasty response rather than take decisive action. Therefore, speed of command is always relative to the adversary's speed of command. Al Qaeda used superior operational knowledge to dictate the terms of battle. The U.S. was forced to respond to Al Qaeda's actions, because the U.S. forces

did not possess adequate knowledge of Al Qaeda's intentions to prosecute a campaign. Speed of command for Bin Laden's forces is not measured in minutes or seconds, but in months and years. Operational security enabled his forces to achieve a knowledge advantage and lock out U.S. courses of action.

Therefore Al Qaeda's attacks demonstrate good self-synchronization of dispersed forces. The cells possessed unity of effort and were provided with commander's intent and clear rules of engagement. Further, the use of information technology, such as the Internet, allowed the cells to develop shared awareness and knowledge superiority. It is a combination of technological development and the common religious belief structure that provides the basis for the self-synchronization of the various Al Qaeda cells.

Assured Access.

For Al Qaeda, access was achieved slowly, often over a period of years. Al Qaeda put agents and cells in place, blending them into the community to limit their exposure to counter-terror operations. While Al Qaeda is not a quick reaction force, its actions highlight the importance of access and presence in the conduct of network-centric operations. The hallmark of its engagement philosophy is to achieve the operational and strategic goals through the massing of effects vice the massing of forces. While the U.S. military retains the ability to respond with far superior force, it seeks more efficient ways to accomplish this through a flexible response capability. Maintaining access and presence becomes critical for any network-centric organization.

Al Qaeda focused on infiltration of the enemy. Its dependence on short-term presence was risky because the failure to gain access at the last moment could have jeopardized mission

execution. Success depends on accurate understanding of the enemy and his response. This is best achieved through surveillance and rehearsal. To disguise agents' presence in enemy territory, they followed the local lifestyles and even married.[16]

In the case of the 11 September attacks, Mohammed Atta and Marwan al-Shehhi, who were on American Airlines flight 11 and United Airlines flight 175 respectively, had lived in the United States for more than a year prior to the attack. Both men attended flight training schools in Florida and received money by wire transfer from an individual in the United Arab Emirates.[17] In this example, time was the ally of Al Qaeda. Time allowed Mohammed Atta's cell to infiltrate the United States, conduct surveillance on airport security, and even conduct a rehearsal on the same flights a week earlier. This Al Qaeda cell had superior knowledge of the enemy capabilities and procedures and of the operating environment. All of this was possible because these individuals had access to the operational theater. A shorter planning timeline risks failure if, as in the case of Ramzi Bin al-Shibh, a visa is denied.[18]

Conduct of Effects-based Operations.

Effects-based operations entail the massing of effects on a target, not the massing of forces, to achieve the objective. For Bin Laden, the strategic objective is the withdrawal of U.S. forces from the region. The most successful example was the October 1993 attack on U.S. forces in Mogadishu. Militarily the Somali ambush was unsuccessful. Although 18 soldiers lost their lives and 84 more were injured, anywhere from 350 to 1000 Somalis were killed by superior American firepower. But the end result was an American withdrawal from Somalia within the year. From Bin Laden's perspective, the ambush had the desired effect without requiring a decisive military blow.

In the 11 September attack, the long-term effects are not so clear. While the impact of the attack on the American economy appears significant, it is not clear that the extent of that effect could have been accurately predicted. The intent was to kill hundreds or thousands of people and blame their deaths on a continuing U.S. presence in the Middle East and on support for Israel. In the four months since the attack, the U.S. presence in the region has dramatically increased and some Islamic states, notably Pakistan and post-Taliban Afghanistan, are looking for renewed ties with America. However, the increased U.S. presence is a potential irritant to such regional powers as Iran and China. Both countries appear to be trying to minimize American political gains, especially in Pakistan and Afghanistan. While Al Qaeda was able to use terrorism to remove the U.S. from less vital areas of the Middle East, such as Somalia, terrorism alone may be insufficient to remove the U.S. from areas considered vital to our national interests. It is clear that Al Qaeda conducted operations designed to achieve effects in the Middle East, however it failed to appreciate that attacks on the U.S. homeland might galvanize the U.S. public toward demanding a military response.

Al Qaeda as a Model.

While the argument undoubtedly will continue over whether or not the U.S. military can learn from the business sector, Al Qaeda is learning to use information technology in warfare. Its various cells are using information technology to support dispersed, self-synchronized teams that have access to the theater of operations and a knowledge advantage. These teams receive guidance and intent from Al Qaeda, but planning, training, and execution are the responsibility of the team leadership. The cells operating in the U.S. used the advantage of our open society to

coordinate the actions of the independent cells in the conduct of the 11 September attacks. These teams then conducted effects-based operations to achieve Bin Laden's strategic goal of removing the U.S. presence from the Middle East. When the cells have knowledge superiority, access, and can self-synchronize, they can conduct successful missions.

The planned millennium attack on Los Angeles International Airport was foiled with Ahmed Ressam's capture at the Canadian border in Decmber 1999. In this case, Al Qaeda did not have assured access for the conduct of the mission. The failure to get the explosives into the U.S. might have been the result of a poor intelligence estimate of U.S. capabilities at the border. It is clear that the cell operatives did not have knowledge superiority in conducting this phase of the operation and the result was the unraveling of that cell's plan. However, decentralization of the execution teams prevented the discovery of other planning cells operating in America, so the damage to the Al Qaeda network was limited.

Implications

Decentralized Execution.

Although the exact details may never be known, in the 11 September attacks on the World Trade Center, it is unlikely that Bin Laden knew such detail as the actual flight numbers, or maybe even the day targeted for the attack. Based on the press releases that followed, it is clear that he knew of the plan, had likely approved the operational concept for the attack, and empowered his trained subordinates to carry it out. While the operational commander is responsible to higher authority for the conduct of the mission, to be successful in the information age, the same commander must trust his subordinates to successfully execute the tactical mission in support of the

commander's intent. Clearly Bin Laden is not a student of network-centric warfare, but it is equally clear from Al Qaeda's success that it uses information technology to operationalize network-centric principles.

Al Qaeda's success indicates that decentralized execution is essential to the success of a network-centric organization. Commanders must provide clear intent, ensure subordinate commanders have the appropriate skills, and then empower them to carry out the mission. This empowerment appears to be the dilemma for the U.S. military. Experimentation, such as the U.S. Navy Fleet Battle Experiments (FBE), has shown that operational commanders find it very difficult to allow decentralized execution. For example, FBE India's overarching concept was to operationalize network-centric warfare, with a focus on decentralized execution of joint fires at the various execution cells. The theory being tested was that the time required to conduct time critical strike could be reduced through command by negation. However, the command element still retained responsibility for weapon-target pairings for certain high priority targets and where there was a concern over major collateral damage.[19]

Pace of Warfare.

"The art of warfare at all levels is to obtain and maintain freedom of action."[20] That art is practiced by Al Qaeda just as it is practiced by the U.S. military. Both are analyzing the factors of space, time, force and knowledge to develop an operational plan. The format of the process may differ, but the factors considered are the same. While Milan Vego discusses the merits of information as a factor in his book, Operational Warfare, he subordinates it to the other three factors. The analysis of Al Qaeda suggests a change in the balance of these factors in the context of

network-centric operations. The mere presence of information is not a factor, but the ability to analyze the information and change it into useful, complete, timely, and relevant knowledge is of the utmost importance to the operational commander. The ascendancy of information technology and its importance in network-centric operations clearly promotes knowledge to an equal status among the factors of space, time, and force.

The broader implication is that through good knowledge management, in the context of network-centric operations, commanders can control the pace of warfare. Tactically, network-centric operations can reduce response time, but operationally, increased operations tempo is not a requirement. Al Qaeda's success on 11 September 2001 indicated that without adequate intelligence, the U.S. could not know where Al Qaeda would strike. The ability to use information technology such as cellular telephones and the Internet, coupled with the openness of American society, forced the U.S. to defend everywhere. This is the nature of terrorism, but in success Al Qaeda has demonstrated the ability to plan and execute coordinated attacks over a large geographic area and use technology to manage knowledge and deny adversaries critical intelligence on potential targets.

Increased Combat Power.

Network-centric warfare advocates stress that the ability to conduct effects-based operations leads to increased levels of combat power. Analysis conducted on one measure of effectiveness, time critical targeting, indicates that a 50-fold increase in the percent of targets destroyed in 100 hours can be achieved given the development of a netted force over the next 20 years. Analysis of other measures of combat effectiveness showed similar improvements with the

introduction of a netted force structure.[21] Returning to FBE India, one of the experiment's

hypotheses was that the time required to conduct time critical strike missions could be reduced

through the application of network-centric principles. The results of FBE India suggest that the

hypothesis is correct.[22]

　　　　Moving beyond the theoretical, Al Qaeda's successes in the East African U.S. Embassy

bombings and the 11 September 2001 terrorist attacks indicate that network-centric operations can

increase combat power. Historically, terrorists have conducted individual attacks, limiting the

potential damage. By self-synchronizing separate, dispersed teams, Bin Laden achieved greater

combat power. The number of people killed and wounded in the Dar es Salaam and Nairobi

bombings was only exceeded by the thousands killed on 11 September 2001.

Conclusion.

　　　　To prove that Al Qaeda is operationally and organizationally network-centric, network-

centric operations were defined and the definition broken into the supporting components, self-

synchronization, knowledge superiority, access, speed of command, and effects-based operations.

Based on the preceding analysis, Al Qaeda's organization is clearly network-centric in nature. This

is not to imply that Bin Laden is a student of network-centric warfare, the analysis merely shows the

impact of information technology proliferation on various organizations. Information technology is

changing the business world, the military, and the face of terrorism.

　　　　While Al Qaeda is a very different organization from the U.S. military, the differences in

size, mission, and technology do not impact the lessons drawn from the analysis. Those lessons are:

- The operational commander must trust his subordinates to successfully execute the mission.

- Balancing knowledge management with the operational factors space, time, and force in operational planning may allow the commander to dictate the pace of warfare.

- Network-centric operations can increase combat power.

Al Qaeda achieved strategic effects through tactical actions despite technological and numerical inferiority. By focusing on operational planning tasks and establishing a decentralized execution structure of coordinated forces, the regional CINC can achieve far greater success given the technological superiority of the U.S. military.

---

[1] Arthur K. Cebrowski and John J. Garstka, "Network Centric Warfare: Its Origin and Future," U.S. Naval Institute Proceedings, 124, no. 1 (January 1998), 29.

[2] Department of State, Patterns of Global Terrorism (Washington D.C.: Department of State Publication 10822, April 2001), 68. Al Qaeda has attempted to globalize terrorism by maintaining connections with other Sunni terrorist organizations, such as Egyptian Islamic Jihad, al-Gama'at al-Islamiyya, the Islamic Movement of

Uzbekistan, Algeria's Armed Islamic Group (GIA), Abu Sayyaf in the Philippines, and the Harakat ul-Mujahidin. Bin Laden's second in command, Ayman Al-Zawahiri, was a former leader of Egyptian Islamic Jihad.

[3] James F. Hoge and Gideon Rose, ed., How Did This Happen? Terrorism and the New War, Council on Foreign Relations, Inc. (New York: PublicAffairs, 2001), 4.

[4] Department of State, 69.

[5] David S. Alberts, John J. Garstka, and Frederick P. Stein, Network Centric Warfare: Developing and Leveraging Information Superiority, 2d ed (rev) (Washington D.C.: C4ISR Cooperative Research Program Publication Series, August 1999), 88.

[6] Arthur K.Cebrowski, "President's Forum," Naval War College Review, vol. 54, no.2 (Spring 2001), 9.

[7] United States of America v. Zacarias Moussaoui, Indictment, U.S. District Court, Eastern District of Virginia (December 2001), 2.

[8] Hoge and Rose, 34.

[9] Yossef Bodansky, Bin Laden: The Man Who Declared War on America (Roseville, CA: Prima Publishing, 2001), 89.

[10] Hoge and Rose, 12.

[11] Cebrowski and Garstka, 35.

[12] Alberts, Garstka, and Stein, 89.

[13] Alberts, Garstka, and Stein, 175.

[14] "Saudi Arabia Text of Fatwa Urging Jihad Against Americans London Al-Quds al-'Arabi in Arabic -- 23 Feb 98, Page 3," Summary/Review of Reports Concerning Threats by Osama Bin Laden to Conduct Terrorist Operations Against the United States and/or her Allies - 23 Feb 98 to 16 Jun 98 (includes original February "fatwa"), 23 February 1998. <http://www.emergency.com/bladen98.htm> [05 January 2002].

[15] Cebrowski and Garstka, 32.

[16] Bodansky, 233.

[17] United States v. Moussaoui, 7.

[18] Ibid. In the indictment on Zacarias Moussaoui, Ramzi Bin al-Shibh is identified as an individual known to Moussaoui and the hijackers that was not able to get a visa. That Ziad Jarrah, one of the hijackers on United Airlines flight 93, attempted to get Bin al-Shibh enrolled in a Florida flight school, implicates him in the attack planning. Bin al-Shibh submitted four visa applications for entry to the U.S. between 17 May and 25 October 2000. All were denied.

[19] Joint Military Operations Faculty, Fleet Battle Experiment India (Newport, R.I.: Naval War College, NWC 1004, October 2001), C-1.

[20] Milan Vego, Operational Warfare (Newport, R.I.: Naval War College, 2000), 29.

[21] Chief of Naval Operations Strategic Studies Group XX, <u>FORCEnet and the 21st Century Warrior</u> (Newport, R.I., November 2001), 1-5. Per telephone conversation with Mr. Bill Glenney, Deputy Director, SSG, on 04 February 2002, the analysis data referenced is unclassified.

[22] Joint Military Operations Faculty, 8.

BIBLIOGRAPHY

Alberts, David S., John J. Garstka, and Frederick P. Stein. <u>Network Centric Warfare: Developing and Leveraging Information Superiority</u>, 2d ed (revised). Washington D.C.: C4ISR Cooperative Research Program Publication Series, August 1999.

Bodansky, Yossef. <u>Bin Laden: The Man Who Declared War on America</u>. Roseville, CA: Prima Publishing, 2001.

Cebrowski, Arthur K. and John J. Garstka. "Network Centric Warfare: Its Origin and Future." <u>U.S. Naval Institute Proceedings</u>, 124, no. 1 (January 1998), 28-35.

Cebrowski, Arthur K. "President's Forum." <u>Naval War College Review</u>, vol. 54, no.2 (Spring 2001), 5-11.

Chief of Naval Operations' Strategic Studies Group XX. <u>FORCEnet and the 21st Century Warrior</u>. Newport, R.I., November 2001.

Hoge, James F., and Gideon Rose, ed. <u>How Did This Happen? Terrorism and the New War</u>. Council on Foreign Relations, Inc. New York: PublicAffairs, 2001.

Joint Military Operations Faculty. <u>Fleet Battle Experiment India</u>. Newport, R.I.: Naval War College, NWC 1004, October 2001.

"Saudi Arabia Text of Fatwa Urging Jihad Against Americans London Al-Quds al-'Arabi in Arabic -- 23 Feb 98, Page 3." <u>Summary/Review of Reports Concerning Threats by Osama Bin Laden to Conduct Terrorist Operations Against the United States and/or her Allies - 23 Feb 98 to 16 Jun 98 (includes original February ''fatwa'')</u>. 23 February 1998. <http://www.emergency.com/bladen98.htm> [05 January 2002].

United States of America v. Zacarias Moussaoui. Indictment. U.S. District Court, Eastern District of Virginia. December 2001.

U.S. Department of State. <u>Patterns of Global Terrorism</u>. Washington D.C.: Department of State Publication 10822, April 2001.

Vego, Milan. <u>Operational Warfare</u>. Newport, R.I.: Naval War College, 2000.