USAWC STRATEGY RESEARCH PROJECT

INTELLLIGENCE STRATEGY FOR FOURTH GENERATION WARFARE

by

Mr. Edward P. Jamison
Department of Defense

Colonel John Rovegno
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
15 MAR 2006		**00-00-2005 to 00-00-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Intelligence Strategy for Fourth Generation Warfare	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Edward Jamison	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**22**	

ABSTRACT

AUTHOR: Mr. Edward P. Jamison

TITLE: Intelligence Strategy for Fourth Generation Warfare

FORMAT: Strategy Research Project

DATE: 31 January 2006 WORD COUNT: 5,228 PAGES: 21

KEY TERMS: Fourth Generation Warfare, Intelligence, Human Intelligence, Open Source Intelligence, Cultural Intelligence, Intelligence Indicators, Intelligence Processing, Intelligence Analysis, Intelligence Dissemination

CLASSIFICATION: Unclassified

War theorists believe we have entered into a new generation of warfare where an "evolved form of insurgency uses all available networks – political, economic, social, military – to convince the enemy's decision makers that their strategic goals are either unachievable or too costly for the perceived benefit." They have named this new era of war "fourth generation warfare." Currently, the Department of Defense's intelligence strategy is designed to defeat conventional adversaries vise a fourth generation warfare opponent. To be successful against a fourth generation warfare opponent, the Department of Defense must transform its intelligence efforts. It must shift collection efforts from high-technology to low-technology solutions; redefine intelligence indicators; increase processing and analysis capabilities; and develop more agile dissemination systems. In addition, the Department must develop a holistic strategy to fight and win a fourth generation war. This project will discuss the theory of fourth generation warfare and highlight its distinct characteristics. The study then identifies the challenges faced by the intelligence community as a result of this new form a war. Finally, recommendations will be provided to enhance intelligence support to the military in their effort to win a fourth generation war.

INTELLIGENCE STRATEGY FOR FOURTH GENERATION WARFARE

War in the 21st Century is evolving into a new kind of battle, one that many states are ill prepared to fight. Over the last decade, military reformers have been wrestling with what future war will look like and the implications it will have on the military. By examining past wars, they believe a new generation of warfare has emerged - a fourth generation. Fourth generation warfare is defined as an "evolved form of insurgency that uses all available networks – political, economic, social, military – to convince the enemy's decision makers that their strategic goals are either unachievable or too costly for the perceived benefit."[1] Unlike past wars, it does not win by defeating an enemy's military forces, but by defeating their political will.[2]

Fourth generation warfare is not new, but has been evolving for over seventy years. It is the only type of warfare known to have defeated major military powers. It defeated America in Vietnam, Lebanon, and Somalia; the French in Vietnam and Algeria; and the Soviet Union in Afghanistan.[3] Currently, it is being used by Chechnya against the Russians, and in Iraq and Afghanistan against the United States.[4] The defeat of major powers by weaker opponents makes it essential to understand this form of warfare and adapt accordingly. [5]

Success against a fourth generation opponent is contingent on the willingness and ability of a state to adapt to this fundamentally different type of war. Military reformers believe that fourth generation warfare is an intelligence war and that intelligence is the key to success. Major General Martin Dempsey, the Commander of the US Army's 1st Armored Division in Iraq, states "Fundamentally, here in Baghdad we do two things: we are either fighting for intelligence, or we are fighting based on intelligence."[6] The role of intelligence is to define the type of war we face and help defeat those that wish to do us harm. It must provide the clearest possible insight into situations, events, players, and hidden agendas, so our leaders can decide how to act.[7]

To ensure success against a fourth generation warfare opponent, the Department of Defense must transform its intelligence strategy. It must shift its collection efforts from high-technology to low-technology solutions; redefine its intelligence indicators; increase its processing and analysis capabilities; and develop more agile dissemination systems. In addition, the Department must develop a holistic strategy to fight and win a fourth generation war. This paper will discuss the characteristics of fourth generation warfare; analyze the Department of Defense's current intelligence strategy; and provide recommendations to transform that strategy in order to defeat a fourth generation warfare opponent.

Fourth Generation Warfare

In October 1989, William S. Lind and his co-authors addressed the meaning of generation warfare in an article written for the *Marine Corps Gazette* titled "The Changing Face of War: Into the Fourth Generation."[8] In an attempt to anticipate what future wars would look like, the authors examined the characteristics of previous wars and identified three periods in which significant events changed the way wars were fought. They termed these periods the three generations of warfare and predicted the characteristics of a fourth generation of warfare.

According to the authors, the first generation of warfare ran approximately from 1648 to 1860. It was "reflective of tactics and technology in the time of smoothbore muskets and Napolean. The tactics were of line, column, and mass armies."[9] Battles of this time were formal, with a focus on the front line and an orderly battlefield.[10] In turn, the battlefield of order created a military culture of order characterized by uniforms, saluting, drills, and ceremonies.[11]

"Second generation warfare was a response to the rifled musket, breechloaders, barbed wire, the machine gun, and indirect fire."[12] Tactics were based on movement and mass firepower, with the goal of attrition through linear warfare.[13] Battles were characterized as "conducted battles," where the commander was the conductor.[14] Second generation warfare preserved the culture of order established in the first generation.[15] "The focus was inward on rules, processes, and procedures. Obedience was more important than initiative, and discipline was top-down and imposed."[16]

Third generation warfare was also in response to an increase in firepower.[17] Tactics, however, were based on non-linear warfare with emphasis on maneuver rather than attrition.[18] Battles focused on collapsing the enemy from the rear forward.[19] Besides changes in tactics, third generation warfare is also characterized by changes in the military culture. "A third generation military focuses outward, on the situation, the enemy, and the results the situation requires; not inward on processes and methods. Initiative is more important than obedience and it all depends on self-discipline, not imposed disciplines."[20]

The authors identified several characteristics of warfare that evolved over these generations and seem likely to take on greater significance in the fourth generation. First, each generation of warfare has seen a greater dispersion on the battlefield.[21] The fourth generation battlefield is likely to include the whole of the enemy's society with reliance on small independent groups to carry out tailored missions.[22] "Second is a decreased dependence on centralized logistics."[23] Dispersion, coupled with the need for speed, will require the small independent groups to be self-sufficient and live off the land and the enemy.[24] Third is an increased emphasis on maneuver.[25] Reliance will be more on small, highly maneuverable, agile

forces instead of masses of men or firepower.[26] "Fourth is a goal of collapsing the enemy internally rather than physically destroying him.[27] Targets will include such things as the population's support for the war and the enemy's culture."[28]

Finally, the authors identify three constructs of fourth generation warfare. First, the state no longer has a monopoly on war.[29] Throughout the world, many states already find themselves at war with non-state actors. Second, fourth generation war is marked by a return to a world of cultures and states in conflict.[30] No longer is war just between two states with conventional armies. Third, internal division along ethnic, religious, and special interest within one's own society can be the cause of a fourth generation war.[31]

It should be noted that fourth generation warfare is not terrorism, though terrorism may use some elements of this approach. Fourth generation wars can result from conflicts such as competition over scarce resources, ethnic cleansing, proliferation of weapons of mass destruction, and international crime.

Current Intelligence Strategy

Before the Department of Defense's current intelligence strategy can be discussed, it is important to understand how it sees the future of war and how it plans to prepare. This can best be accomplished by looking at the possible formats of future war envisioned by military reformers.

Many authors writing on the future of war have contemplated the format that the next generation of warfare will take. As a result, two possible types of future war have emerged - cyberwar and netwar. Cyberwar is defined as a knowledge-related conflict at the military level.[32] It involves conducting military operations according to information-related principals to disrupt or destroy the enemy's information and communications systems.[33] Cyberwar is characterized as a high–technology war, especially in communications and intelligence, requiring the military to function as an interconnected network vice institutional hierarchies.[34] Expressed in simpler terms, "cyberwar is essentially third generation warfare made vastly more lethal through the use of information technology."[35]

Netwar, also known as fourth generation warfare, applies to societal struggles most often associated with low intensity conflict by non-state actors.[36] It attempts to disrupt, damage, or modify what a target population knows or thinks it knows about itself and the world around it.[37] Netwar targets elite and/or public opinion through propaganda and psychological campaigns, political and cultural subversion, deception of or interference with local media, and efforts to promote dissident or opposition movements across computer networks.[38]

The Department of Defense envisions cyberwar as the future format of wars. Since its success in the Gulf War, the military has been consistently preparing to fight a high-technology war.[39] This is evident in the evolution of strategic documents published by the department over the last several years. In each evolution, technology was the driving force of change. In particular, the focus has been on technologically advanced weaponry and increased technical capabilities for command and control.[40] Likewise, the department's intelligence strategy has predominately relied on high-technology solutions to increase its capabilities in intelligence collection. It places emphasis on expanding technical capabilities in the areas of signals intelligence, imagery intelligence, and measurement and signature intelligence.

Fourth generation warfare is not defined as a high-technology war, but that of a netwar. It requires a low-technology, networked, real-time approach to defeat the enemy. Our current intelligence systems and organizations are not designed to support such an approach. They are designed to collect information against states with large conventional forces, not against small groups and individuals that characterize netwar opponents. In addition, our intelligence systems and organizations are still structured to fight the Cold War – a centralized and hierarchical organization that slows the dissemination of information.

Our country's inability to collect and analyze intelligence in fourth generation wars is evident in the wars currently being waged in both Iraq and Afghanistan. Despite the United States' and its coalition partners' sophisticated technical intelligence capabilities, the wars have yet to be won. One reason is that the capabilities of technical collection systems are too well known by the opponents, thus hampering their effectiveness. They know in advance when satellites will pass overhead and have learned to circumvent them. They are quick to learn about communications collection capabilities and even quicker to adapt low-technology to counter them. When actionable intelligence is collected, it is slow to get to the warfighters, resulting in missed opportunities.

Intelligence Strategy for Fourth Generation Warfare

Success in fourth generation warfare will be driven by intelligence. This will require much more intelligence collection, processing, analysis, and dissemination capabilities than are currently available. While high-technology solutions are still necessary, especially in the area of signals intelligence, they should not be the predominant approach. Emphasis must be placed on low-technology collection capabilities, including a robust human intelligence capability, more reliance on open source intelligence, and improved cultural intelligence capability. Additionally, intelligence indicators need to be redefined, processing and analysis capabilities must be

increased, and flat networks must be developed allowing information to flow not just up the chain, but down and horizontally. More importantly, the Department of Defense must develop a holistic strategy, focusing all components of the military on the common goal of defeating a fourth generation opponent.

Human Intelligence

Since the Cold War, the intelligence community has allocated most of its resources to developing and sustaining sophisticated technical intelligence capabilities at the detriment of human intelligence. While technical capabilities provide substantial benefits against conventional opponents, human intelligence offers the best chance to succeed against a netwar opponent. As noted earlier, fourth generation warfare involves non-state actors, organized in decentralized networks, instead of the traditional hierarchical networks of nation states. Human intelligence is the only intelligence discipline capable of penetrating these networks to learn the true plans and intentions of an adversary. This is evident in recent failures of technical intelligence capabilities. Many believe that had the United States maintained a vigorous human intelligence capability, the events of September 11, 2001 could have been averted. In addition, the failure to win the war in both Iraq and Afghanistan has also been blamed on inadequate human intelligence collection capabilities.

The Department of Defense has recognized the significant role that human intelligence can play in its fight against current opponents, and has recently begun to aggressively enhance its human intelligence capabilities. To develop a robust and reliable human intelligence capability, the department must ensure adherence to the principles of the human intelligence discipline. "These principles are that collectors must have [the right] personal characteristics and a good degree of area knowledge; that they ought to be as closely matched to their potential sources as possible; that they need a decent familiarity with the subject matter upon which they are collecting; that their leaders must be extremely skillful in the basics of human intelligence collection; and that they need independent support from Counterintelligence."[41]

In the past, the Department of Defense's human intelligence efforts were predominately focused on counterintelligence. Today, the department is transforming its human intelligence soldiers into full-spectrum human collection operators.[42] Soldiers will be engaged in conducting human source operations, interrogating noncooperative sources, debriefing cooperative sources, and exploiting documents, hardware, and other media devices.[43] To prepare soldiers for their expanded role in human intelligence, the department must provide them with the proper training, emphasizing foreign area studies and language skills development.

Fourth generation warfare opponents are characterized as agile, decentralized forces capable of operating inside their adversary's Observe-Orient-Decide-Act decision loop.[44] To counter this ability, the department must teach its human collectors to conduct all-source analysis capable of examining and interpreting a broad range of information to include raw data from the various intelligence disciplines, as well as products from single source analysts. They can then combine all the information to produce finished intelligence reports or assessments. As all-source analysts, human intelligence soldiers will be capable of consolidating all available information regarding a requirement from across the intelligence community, identifying what information still needs to be collected, and then efficiently focusing collection assets to produce that information. This will not only save valuable collection resources, but also decrease the time it takes to answer intelligence requirements, thus allowing the commander to make faster decisions.

Finally, the department must provide human intelligence soldiers with the latest technology. To support all-source analysis, the department must develop advanced analytic tools, flat networks, and distributed databases. Currently, the department is employing the Biometric Automated Toolset that identifies people by their fingerprints, facial features, iris patterns, hand measurements, and voice. This has significantly reduced the time required to identify individuals of interest. The department has also given their soldiers handheld personal digital assistants to make receiving and reporting of information quick and simple.

Human intelligence is vital to defeating a fourth generation warfare opponent, but it has several limitations. The biggest limitation of human intelligence is that collection success can not be predicted with certainty. As the name implies, human intelligence depends on interactions between people to be successful, and human nature is most unpredictable. Additionally, the amount of time it takes to collect, report, and verify information can be so long that it renders that information useless. Implementing a flat network and distributed databases can help improve the processing time of intelligence. Certain information can also be politically sensitive, thus difficult to use without causing potential repercussions for the United States government. Finally, human intelligence collection is highly susceptible to deception. Determining the reliability of the source and verifying the information is often very difficult.

Open Source Intelligence

Stronger reliance upon open source intelligence can provide an advantage over, or at least match, a fourth generation warfare adversary. Open source intelligence provides support in terms of indications and warnings, contingency planning, security assistance, and tactical

operations. Open source intelligence is information collected from publicly available sources, including media reports, professional journals, and the Internet. The technology and information revolutions have made access to this information extremely easy. Some open source enthusiasts believe that open source intelligence can provide up to eighty percent of the intelligence needed for unconventional and low intensity missions against non-state actors.[45] In addition, "open sources often equal or surpass classified information in monitoring and analyzing such pressing problems as terrorism, proliferation of weapons of mass destruction, and counterintelligence."[46] Like most intelligence, there are both advantages and disadvantages to open source intelligence.

The biggest advantage of open source intelligence is that it is unclassified information: "secrets that don't have to be stolen."[47] Therefore, the information can be collected, analyzed, and disseminated by people who do not have security clearances. Unclassified information can also be shared with everyone and easily disseminated across all modes of communication. Another major advantage is that open sources enhance secret collection programs by providing substantiating information and freeing up resources to be applied to the more difficult problems.[48] Other advantages include the ease of gathering information and its low cost.

The biggest disadvantage of open source intelligence is its' lack of reliability. Adversaries may intentionally release false information as part of a deception program. Additionally, information from the Internet may be biased or simply inaccurate. Quality control programs should be set up to validate information obtained from open sources. Other disadvantages are that the information needed may not be available through open sources, or state censorship can deny the collection of desired information. Finally, just the act of collecting certain types of information can reveal intentions and plans to adversaries.

Currently, the Department of Defense has some open source intelligence capabilities scattered throughout the Department, but no holistic approach. Congress has recognized the importance of open source intelligence and directed the Department to establish a 'Strategy for Open-Source Intelligence.' There are several important areas the Department must address when implementing this strategy. First, the Department must consider developing a network to disseminate open source intelligence. Information must flow freely in all directions. Ideally, open source intelligence should traverse the same platforms as classified intelligence to enable fusion of data, but due to security concerns, this is not currently possible. The Department must continue to push for research in multi-level security platforms to realize this capability. Second, the Department must hire people who have knowledge of foreign languages and countries to gather and analyze open sources. Without such capabilities, open source information has the

potential to be degraded through improper translation. Finally, the Department must work closely with the Intelligence Community's new Open Source Center at the Central Intelligence Agency to leverage efforts and reduce redundancy.

Cultural Intelligence

Although cultural intelligence has been a low priority within the Department of Defense, experiences in Iraq and Afghanistan are quickly changing its perceived value. Soldiers working in these areas say the most useful intelligence is from the indigenous population and that understanding their society, culture, and language is essential toward establishing the relationships needed to foster such communications. Establishing one-on-one relationships with the population is key to both intelligence collection and winning hearts and minds.[49] Cultural intelligence is the study of an adversary's culture – "it requires an understanding of their habits, intentions, beliefs, social organizations, and political symbols."[50] It not only helps establish interpersonal relationships; it can also help determine the form of warfare, organizational structure, and motivations of a fourth generation opponent.[51]

Cultural intelligence is key to ensuring success in humanitarian and peacekeeping efforts. Regardless of the mission, engagement with the populace is crucial and the soldiers' ability to interact with them can greatly effect the outcome. Currently, the Department of Defense has a limited strategy on cultural intelligence. The cultural analysis organizations that do exist are under-funded, marginalized, and dispersed.[52] Cultural training is only provided to soldiers prior to deployment and is often brief and oversimplified. The Department must develop a holistic approach to cultural intelligence to ensure that it is incorporated into plans and operations at all levels. Training and education programs must be developed that focus on foreign areas studies, language, and political and social structures. In addition, soldiers must be provided the opportunity to be immersed in the culture to learn first hand cultural and social knowledge.

Intelligence Indicators

To prevent surprise attacks from a fourth generation warfare opponent, the Department of Defense must redefine its intelligence indicators. Intelligence indicators are intended to detect time-sensitive information on events that could involve a threat to the United States' military, political, or economic interests, or to United States citizens.[53] They include forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; weapons of mass destruction attacks on the United States, its overseas forces, or allied and/or coalition nations; hostile reactions to United States reconnaissance activities; terrorist attacks; and other similar events.[54]

Intelligence indicators can be either ambiguous or unambiguous. Ambiguous intelligence indicators are activities of a potential adversary that raise cause for concern. These activities by themselves do not indicate that a specific event is imminent. There could be multiple reasons for the activities. Intelligence indicators merely provide a tip-off that an adversary might be planning an event that requires a response. Ambiguous warnings allow time to consider what to do: to step up efforts to acquire more specific information about the situation, to rehearse the scenario that could be faced if the warning proves to be correct, to spell out the likely consequences if the warning is genuine, to review their commitments and contingency plans, and last but not least in importance - to seize the opportunity to avert a possible dangerous crisis.[55] In short, ambiguous indicators provide an opportunity to deal with the situation and/or the misperceptions associated with it before it leads to a violent conflict.[56] For example, increased propaganda by an opponent does not indicate an event is about to occur, but does cause one to become alert to the possibility. Whereas, activities identified as unambiguous warning indicators have only one plausible explanation – that a specific event is imminent and immediate action is required.

In order to provide adequate warnings of hostile actions by a fourth generation warfare opponent, the Department of Defense must expand its list of traditional intelligence indicators. The department needs to develop intelligence indicators that are based on fourth generation warfare adversary's capability to conduct warfare against the United States. Intelligence indicators should not be limited to only tactical operations, but also include ancillary indicators that enable tactical operations to be conducted. Ancillary indicators could be in the traditional third generation form, as well as be based in the civilian sector supporting fourth generation warfare adversaries. Military intelligence indicators must be expanded to include military associations with agitators and insurgents, criminal organizations, and money making ventures.

Intelligence Processing and Analysis

Improvements in the collection capabilities discussed above will vastly increase the amount of data to be processed and analyzed, adding to the already overwhelmed intelligence capabilities of the military. To successfully convert large amounts of raw data collected into products that can be readily used by intelligence analysts, the Department of Defense must increase its processing capabilities in the areas of data interpretation, document translation, data conversion, technical analysis of captured adversary material, and decryption.[57] In addition, the department must also increase its ability to manage information to include

indexing, sorting, and organizing raw data into files so that the information can be rapidly retrieved.

To increase its analysis capabilities, the Department of Defense must increase the number of fully qualified all-source analysts. Investments must be made in the development of analytic expertise, field experience, and training in advanced analytical methods. To increase the timeliness of intelligence back to the commander, analysts must be deployed as far forward as possible. The Department of the Army is currently increasing the number of its intelligence analysts and moving them from the brigade level to the battalion level. While this action will increase timeliness of intelligence, better results would occur if the analysts were assigned even further downrange.

As mentioned above, all-source analysts are responsible for fusing intelligence information from various sources into a single product. To accomplish this goal, analysts must gain access to and traverse multiple databases. This is a time consuming process that can result in analysts missing key information. To resolve these problems, the Department of Defense must develop a distributed database system, where there is a single shared knowledge of information, but the storage of that data resides on multiple computers.[58] In other words, a distributed database acts as a single logical database where analysts can retrieve information through one access point even though that information resides in multiple locations. Because the database is distributed, different users can access it without interfering with one another. The advantages of a distributed database include improved availability of data and performance; lower costs; and easier system modifications; however, caution must be taken to ensure that each transaction maintains database integrity across multiple databases.[59]

To help analysts deal with the overwhelming amount of data collected in a distributed database, the department must procure new analytical tools. Advanced tools are needed in the areas of collaboration, language translation, pattern recognition, and data mining and retrieval techniques to include push/pull capabilities. In particular, advances in automated support to fusion are needed, enabling analysts to rapidly and accurately answer the commander's intelligence requirements.[60]

Intelligence Dissemination

In order for intelligence to be of value, it must be disseminated to the end user in enough time for them to react. To accomplish this, "a low-technology fourth generation actor simply relies on the existing networks created by the information-based economy. These networks provide a cheap, robust, redundant system and allow the information to blend into the trillions of

legitimate transactions that take place every day."[61] They are unconstrained by a top-down hierarchical and compartmented structure that plagues the military's intelligence dissemination systems. This enables them to communicate seamlessly and in real-time, thus allowing them to act on intelligence quickly.

Unfortunately, the Department of Defense's intelligence dissemination systems are not structured to be as fast or flexible as the internet. The top-down hierarchical structure of these networks hinders the speed in which information is disseminated. Information flows easily from the bottom to the top, but is slow to be approved for release back down to the user. The classification system of intelligence further hinders the flow of information by limiting the depth in which intelligence can be disseminated. Most intelligence is provided at such a high classification level that it can only be read by a few personnel. In addition, the variety of disparate computer networks with various operating systems and applications further adds to the difficulty of sharing intelligence. It slows the vertical flow of information and makes sharing information horizontally extremely difficult.

In order to respond to intelligence as quickly as a fourth generation warfare opponent, the Department of Defense must redesign its networks to enable seamless, real-time communications. It must build "flat" networks with a standard architecture to increase the flow of intelligence both vertically and horizontally. The networks must provide ubiquitous access to information; a secure, collaborative information-sharing environment; and the capability for users to pull information from any available source. Challenges of developing flat networks include bandwidth requirements, interoperability, and instant connectivity between any two points on the globe. The department is currently developing the Distributed Common Ground/Surface System that will begin to address some of these concerns. In addition, the department must also push access to special compartmented information down as far as possible, enabling soldiers to quickly access data from and collaborate within the Department of Defense and the rest of the Intelligence Community.

Doctrine

The above intelligence strategy for fourth generation warfare requires the Department of Defense to refocus its efforts from a cyberwar to a netwar. In most instances, the department has already begun to take the initial steps toward enhancing the capabilities discussed in this paper, but only through an uncoordinated and disjointed effort. This has fragmented the overall intelligence capability of the department. Some capabilities are being pursued by one military service or a service component, but not by the military as a whole. For example, the Marine

Corps has invested in cultural training to better understand the enemy they are fighting and the people they are helping, whereas the Army has only provided limited training.[62] As a result, there is a noticeable difference between how the Marines and the Army interact with the indigenous population of Iraq. To ensure a cohesive effort, the Department of Defense must develop a unified intelligence strategy.

As stated earlier, fourth generation warfare is an intelligence war. Intelligence, however, is not the only component of the military that must change. In addition to realigning intelligence, the department must transform its doctrine, organization, training, and education to think about, prepare for, and win a netwar. The department must also coordinate efforts with other government agencies and work with them to develop decentralized networks like those of a fourth generation warfare actor. To properly focus all military components and associated agencies on developing a holistic approach toward fourth generation warfare and defeating a netwar opponent, the military leadership must formally recognize fourth generation warfare as a legitimate threat to the United States.

The National Defense Strategy of the United States identifies some characteristics of fourth generation warfare under the heading of irregular challenges. Under this heading, the military leadership lists terrorism and insurgency as irregular challenges, but military reformers believe that fourth generation warfare is a more advanced form of insurgency. "The strategic concepts, operational executions, and tactical techniques of fourth generation war require major changes in the way we think about defense."[63] Reformers believe that fourth generation warfare will continue to evolve and that the military must prepare for this fight. Some military leaders believe that maintaining a third generation warfare capability to defeat potential adversaries such as China or North Korea is critical. "History, [however,] has repeatedly demonstrated that nations organized and prepared to deal with an emerging generation of war can defeat those of earlier generations."[64] The opposite is not true. In addition, many military reformers anticipate that fourth generation warfare will be the prevalent form of war for the next twenty-five years or more. Not only will insurgent groups employ fourth generation warfare techniques, but nations as well.[65] It is believed that nations such as China will use fourth generation warfare techniques to try and neutralize the conventional forces of the Untied States prior to a conventional attack.[66]

Therefore, it is essential that the military leadership recognizes fourth generation warfare as an emerging challenge in its grand strategy. From that strategy, the services, combatant commanders, and various components of the department can focus on identifying the specific capabilities needed to win a netwar. Those capabilities can then be de-conflicted, prioritized,

and resourced in the Quadrennial Defense Review process. Thereafter, a holistic approach can be developed to defeat a fourth generation warfare opponent.

Conclusion

"Whoever is first to recognize, understand, and implement a generational change [in warfare] can gain a decisive advantage. Conversely, a nation that is slow to adapt to generational change opens itself to catastrophic defeat."[67] Fourth generation warfare is the only type of war that has defeated superpowers. The United States' adversaries in Afghanistan are studying fourth generation warfare, evident by the copies of William Lind and his co-authors' article on fourth generation warfare found by United States' troops in the caves of Tora Bora.[68] It is essential, therefore, that the Department of Defense recognizes this new generation of warfare and adapt accordingly.

Fourth generation warfare opponents are characterized as loose networks that operate in decentralized fashion, moving, planning, and acting in small groups who depend on low-technology.[69] To beat this enemy, one must act like him. The key to victory is intelligence. To ensure access to and proper analysis and dissemination of this intelligence, the department must significantly improve its collection efforts on human intelligence, open source intelligence, and cultural intelligence. It must also redefine its intelligence indicators, increase its intelligence processing and analysis capabilities, and develop flat networks that allow intelligence to flow both vertically and horizontally. For the department's intelligence strategy to be successful, the military leadership must develop a unified grand strategy so that all components of the military and associated agencies are aligned toward achieving the common goal of defeating a fourth generation warfare opponent.

Endnotes

[1] COL Thomas X. Hammes, *The Sling and The Stone* (St. Paul, MN: Zenith Press, 2004), 2.

[2] Ibid.

[3] Ibid., 3.

[4] Ibid.

[5] Ibid.

[6] "Insurgency and Intelligence in Iraq," *Jane's Intelligence Digest*, 21 October 2005; available from http://80-www2.janes.com.650z.carlisle.army.mil/K2/results.jsp; Internet; accessed 20 November 2005.

[7] COL Gary Wilson, USMCR, SGT John P. Sullivan, LA County Sherrif's Dept., LtCOL Hal Kempfer, USMCR, "Fourth-Generation Warfare," *Armed Forces Journal* (October 2002): 60.

[8] William S. Lind, COL Keith Nightengale, USA, Capt John F. Schmitt, USMC, COL Joseph W. Sutton, USA, and LtCol Gary I. Wilson, USMC, "The Changing Face of War: Into the Fourth Generation," *Marine Corps Gazette* (November 2001): 65.

[9] Greg Wilcox and Gary I. Wilson, "Military Response to Fourth Generation Warfare in Afghanistan," 5 May 2002; available from http://www.emergency.com/2004/4gw5may02.htm; Internet; accessed 29 October 2005.

[10] William S. Lind, "Understanding Fourth Generation War," 15 January 2004: available from http://antiwar.com/lind/index.php?articled=1702; Internet; accessed 29 October 2005.

[11] Ibid.

[12] William S. Lind, COL Keith Nightengale et al., 65.

[13] Ibid.

[14] Lind.

[15] William S. Lind, "The Four Generations of Modern War," June 2004; available from http://www.lewrockwell.com/lind/lind26.html; Internet; accessed 29 October 2005.

[16] Ibid.

[17] Wilcox et al.

[18] Ibid.

[19] William S. Lind, COL Keith Nightengale et al., 66.

[20] Lind.

[21] William S. Lind, COL Keith Nightengale et al., 66.

[22] Ibid.

[23] Ibid.

[24] Ibid.

[25] Ibid.

[26] Ibid.

[27] Ibid.

[28] Ibid.

[29] Wilcox et al.

[30] Ibid.

[31] Ibid.

[32] John Arquilla and David Ronfeldt, "Cyberwar Is Coming," 1993; available from http://www.well.com:70/0/Military/cyberwar; Internet; accessed 16 November 2005.

[33] Ibid.

[34] Ibid.

[35] LtCol Thomas X. Hammes, "The Evolution of War: The Fourth Generation," September 1994; available from http://www.defense-and-society.org/fcs/hammes.htm; Internet; accessed 04 October 2005.

[36] Arquilla et al.

[37] Ibid.

[38] Ibid.

[39] COL Thomas X. Hammes, *The Sling and The Stone* (St. Paul, MN: Zenith Press, 2004), 6.

[40] Ibid.

[41] Maj Robert A. Sayre, Jr., *Some Principles of Human Intelligence and Their Application Monograph* (Fort Leavenworth: U.S. Army Command and General Staff College, Spring 2004): 45.

[42] "Human Intelligence Revitalization," *Torchbearer National Security Report* (June 2005): 7.

[43] Ibid., 8.

[44] Myke Cole, "From the Military: Applying 4GW Theory to The Intelligence Community," June 2004; available from http://www.defense-and-society.org/fcs/cole_lessons_from_the_military.htm; Internet; accessed 04 October 2005.

[45] Congressman Rob Simmons, "SOF OSINT Handbook – Forward," available from http://www.oss.net; Internet; accessed 22 November 2005.

[46] Stephen C. Mercado, "Reexamining the Distinction Between Open Information and Secrets," available from http://www.cia.gov/csi/studies/Vol49no2/reexamining_the_distinction_3.htm; Internet; accessed 21 November 2005.

[47] Katherine Shrader, “New U.S. Intel Center Studies Free Secrets,” 08 November 2005; available from http://seattlepi.nwsource.com/national/1155AP_Open_Secrets_Center.html; Internet; accessed 21 November 2005.

[48] Mercado.

[49] Montogmery McFate, “The Military Utility of Understanding Adversary Culture,” *Joint Forces Quarterly* (3rd Quarter 2005): 44.

[50] Ibid., 43.

[51] Ibid.

[52] Ibid., 46.

[53] *The Free Dictionary*; January 2006; available from http://www.thefreedictionary.com/indications+and+warning; Internet; accessed 12 January 2006.

[54] Ibid.

[55] Alexander L. George and Jane E. Holl, “The Warning-Response Problem and Missed Opportunities in Preventive Diplomacy,” May 1997; available from http://www.carnegie.org/sub/pubs/deadly/0697warning.htm#better; Internet, accessed 12 January 2006.

[56] Ibid.

[57] U.S. Joint Chiefs of Staff, *Doctrine for Intelligence Support to Joint Operations*, Joint Publication 2-0 (Washington D.C.: Joint Chief of Staff, 9 March 2000), III-7.

[58] David Emery of DSCI, interviewed by author, 05 January 2006.

[59] *Wikipedia Encyclopedia*; available from http://en.wikipedia.org/wiki/Distributed_databasel Internet; accessed 22 January 2006.

[60] “Fusion: An Operational Assessment,” U.S. Army Intelligence Center (06 July 2004): 3.

[61] Cole.

[62] Cindy Fisher, “CMC:’Changes in Corps’ Future Will Benefit Marines’ End-Strength, Restructuring to Increase Crucial Capabilities: Big Changes Are in the Horizon for the Marine Corps,” *Marine Magazine* (April-June 2005).

[63] Hammes.

[64] Ibid., 228.

[65] Ibid., 256.

[66] Ibid., 257.

[67] William S. Lind, COL Keith Nightengale et al., 65.

[68] Lind.

[69] Cole.