THE
LAND
WARFARE
PAPERS

No. 36 OCTOBER 2000

The Janus Paradox:
The Army's Preparation for Conflicts of the 21st Century

Wayne M. Hall

A National Security Affairs Paper
published on occasion by
THE INSTITUTE OF
LAND WARFARE
ASSOCIATION OF THE
UNITED STATES ARMY
Arlington, Virginia

The Janus Paradox:
The Army's Preparation
for Conflicts of the 21st Century

by

Wayne M. Hall

The Institute of Land Warfare
ASSOCIATION OF THE UNITED STATES ARMY

AN AUSA INSTITUTE OF LAND WARFARE PAPER

The purpose of the Institute of Land Warfare is to extend the educational work of AUSA by sponsoring scholarly publications, to include books, monographs and essays on key defense issues, as well as workshops and symposia. A work selected for publication as a Land Warfare Paper represents research by the author which, in the opinion of the editorial board, will contribute to a better understanding of a particular defense or national security issue. Publication as an Institute of Land Warfare Paper does not indicate that the Association of the United States Army agrees with everything in the paper, but does suggest that the Association believes the paper will stimulate the thinking of AUSA members and others concerned about important defense issues.

LAND WARFARE PAPER NO. 36, OCTOBER 2000

The Janus Paradox:
The Army's Preparation for Conflicts of the 21st Century

by Wayne M. Hall

Brigadier General Wayne Michael Hall, USA Ret., currently works for Lockheed Martin Energy Systems at Oak Ridge Tennessee, having retired from the Army on 1 October 1999. During his 30-year career, BG Hall served 12 years in four infantry divisions, commanding at the company, battalion and brigade levels of command. He also was a battalion S-2, brigade S-2, division G-2, and J-2 of United States Forces Korea. As his last assignment in the Army, he led a study team in redesigning Army Military Intelligence for the future in the Intel XXI study. A graduate of intelligence officer basic and advanced courses, he also attended the Command and General Staff College School of Advanced Military Studies (SAMS) and the National War College. He holds master's degrees from Kansas State University and the U.S. Army Command and General Staff College, and a doctorate degree from George Washington University.

This paper represents the opinions of the author and should not be taken to represent the views of the Department of the Army, the Department of Defense, the United States Government, the Institute of Land Warfare, or the Association of the United States Army or its members.

Inquiries regarding this and future Land Warfare Papers should be directed to: Association of the United States Army, Institute of Land Warfare, telephone: 1-800-336-4570 or 703-841-4300, extension 229.

Contents

Foreword

The world is changing dramatically and rapidly because of the information revolution and influence of the Internet on all aspects of life. Because of these changes, the Army has chosen to change as well, and has committed itself to the Interim Brigade Combat Team (IBCT) and Objective Force. The Army calls its progress toward change and adaptation to an increasingly complex future the Transformation process. This process is extraordinarily complex. All aspects of complexity, however, pale in comparison to the immensity of the C^4ISR (command, control, communications, computers, intelligence, surveillance and reconnaissance) system's challenges in providing the essential system and intellectual capabilities to enable the Army to seek and find information superiority. Without information superiority, neither the Army's vision of the future, nor the joint vision of the future as depicted in Joint Vision 2020, will be possible. Thus, in the judgment of the author, the Army must think seriously about the meaning of information superiority and determine if its C^4ISR system can satisfy conditions leading to the effects characterized by the words "information superiority."

This paper provides a thoughtful view of the environmental context in which the Army will operate. The context depicts an adapting, changing and coevolving threat using asymmetric strategies and nefarious digital tools of the information age in large urban areas to offset technological advantages held by the U.S. Army. Urban operations have historically been difficult for any army and therefore have been avoided to the greatest extent practicable. Now, the author postulates, foes using asymmetric strategies will purposefully seek to engage the U.S. Army in urban areas to reduce a strong nation's firepower, maneuver, communications and collection, thereby rendering the notion of information superiority problematic. Moreover, it makes sense for any foe using asymmetric strategies to seek engagement with the U.S. Army in urban areas to capitalize on societal and international constraints that a digital, interconnected world brings to any conceivable competitive situation in which the Army will find itself.

The paper provides a multitude of observations and recommendations for improving C^4ISR in urban areas. It also asks senior Army leaders to think through the distinct possibilities that themes interwoven throughout the paper will come into being. Since the environmental context described is so different from what the Army is preparing for, it would be advantageous for senior Army leaders to consider the ideas in the paper very carefully and nurture them into maturity, as appropriate.

GORDON R. SULLIVAN
General, U.S. Army Retired
President

October 2000

The Janus Paradox:
The Army’s Preparation for Conflicts of the 21st Century

Janus, the ancient Roman god of doorways, has two faces—one looking back and one looking forward. The paradox: human beings become so mesmerized with thinking about the past—what was—that when they think about the future—what could be—it is past experience they consider, not future possibilities.

Introduction

This paper poses a serious question about the Army’s future. Has the Army sufficiently thought through the environments the newly devised Interim Brigade Combat Team (IBCT) and its more futuristic Objective Force will face in the future? The conclusion: The Army’s thinkers have done a great job in thinking through traditional combat—after all, open, force-on-force, *symmetrical* combat is precisely what the Army has done magnificently over the years. But the Army hasn’t given sufficient thought to possible environmental variables it will cope with during future operations. If the Army doesn’t reorient its current thinking, it could face serious shortfalls in doctrine, training, logistics, materiel, organizations and soldier systems.

Specifically, the Army’s thinking must expand to include nontraditional environmental variables that could influence its operations. The IBCT and Objective Force won’t habitually face conventional forces in open areas fighting as armies have fought for hundreds of years. No, the Information Revolution has brought upon the Army (and all services) the specter of *asymmetric warfare*—a strategy in which a weak opponent successfully engages a stronger opponent by using a variety of offsets for gaining advantage in hopes of achieving objectives and goals. Asymmetric approaches involve information operations (IO), weapons of mass destruction, and indirect attacks against soldiers, knowledge workers and their families.

Asymmetric warfare is a perfect strategy for operating in the 21st century. That is, asymmetric operations are nonlinear and cellular in an organizational sense. Asymmetric foes will seek and strike weaknesses, attack in areas in which they are strong, count on intelligence and deception, and work the fine lines of psychological operations (PSYOPS) and deception en route and in the objective area, as well as in the continental United States, including soldiers’ home bases.

This paper is in three parts. First, it provides some broad concepts to support its position on what the Army will face in future conflicts. Included in this part is the premise that the Army’s opponents of the future will successfully compete with the

United States military regardless of their conventional military prowess. It also makes an argument that the Army must prepare for kinetic, force-on-force conflict, along with facing foes who use asymmetric strategies and engage in a combination of kinetic combat and invisible, digital struggles. Second, the paper provides some concrete observations about conceptual work the Army's planners have done with the Interim Brigade Combat Team. Third, the paper provides some specific C^4ISR (command, control, communications, computers, intelligence, surveillance and reconnaissance) recommendations for the Army's leaders to consider, as they move the organization into a future whose complexities are difficult to grapple with and perceive.

Rationale

The future Army must prepare to operate in multiple, complex and widely ranging environments against industrial-age foes as well as asymmetric opponents who use a combination of kinetic and invisible, digital methods to compete. While the IBCT and Objective Force concepts deal very well with force-on-force encounters, they don't fare as well when dealing with the invisible, highly related, intangible struggles of asymmetric competition. Regardless of how the Army longs for the days when brute force—tank on tank, ship on ship, and plane on plane—was the clarion call, it must adjust its institutional thinking. Quite simply, the Army has to accommodate the ascendancy of invisible struggles to a coequal and eventually predominant position in the way it competes with others.

The IBCT and the Objective Force are great ideas. Actually, the shift to a lighter, more flexible organization and mind-set could and should have occurred years ago. Army planners took on some very difficult subjects and performed admirably.

This paper has two purposes. First, it provides an alternative, or perhaps an addendum, to conventional thinking, thereby suggesting a need for more thought and debate on the subject of the environmental context the future Army will face. Second, the paper provides a way of viewing the future and preparing the Army writ large for the distinct possibility of a new type of competition.

This is not an argument for the Army to shift too radically and develop a singular approach to the future by locking its thinking on a conflict devoid of violence. That there will be death and dying in national security competition in the future is a given—it's the nature of the business. The Army of the future must have the capability to deal with both environments described herein—the kinetic force-on-force struggle and the invisible asymmetric struggle.

With that said, though, kinetic conflict in which the predominant leitmotif is to kill people, break things and overpower people will become more infrequent and less important with the passage of time. Why? Quite simply, the rationale goes like this. It's obviously stupid to take on U.S. military forces—armies are too expensive to develop and throw away in a force-on-force, gun-on-gun and traditional way of competing. Nobody has the capability to enter this realm and have any hope of winning. Yet people, organizations and groups still hate us, covet our riches, and want to supplant our global leadership role.

How do these people so filled with hate hope to compete? If they attack us in a conventional force-on-force competition, they will lose. If they leave the United States alone, our foes of the future won't be striking at the entity they hate. This situation represents a conundrum to foes of the future. Arguably, there is a very good possibility our foes haven't learned enough and developed intellects sufficient to develop viable alternatives to kinetic, violent, force-on-force, attritional engagements. *But it is highly likely they will learn to use asymmetric strategies against the United States military in the very near future*.

The Situation

The Information Revolution has brought with it the Revolution in Military Affairs (RMA). In a general sense, the RMA enables our armed forces to leverage information technology as a significant force multiplier. Because of advances in information technology (IT), U.S. forces have the potential to acquire vast amounts of usable information. Along with the acquisition of information come related capabilities such as sophisticated fusion, visualization, precision weapons, communications anywhere on the earth, collaboration within and among services, and enhanced logistics.

The RMA provides the potential to seek, find and exploit the powerful phenomenon of synergy where the whole is greater than the sum of its parts (e.g., services working together, intelligence collectors working together complementing strengths and overcoming shortfalls.)[1] The RMA has led the military to change its vision and doctrine. *Joint Vision 2020,* for example, extols as its pillars *just-in-time logistics, dominant maneuver, full protection* and *precision engagement*. The vision also says *information superiority*[2] is the principal enhancer of the vision.

The military in general and the Army specifically has "burned the ships," so to speak, and entered the digital age totally. Unfortunately, with this bold leap forward comes a multitude of opponent strategies homing in on vulnerabilities the Army didn't have to deal with before. The Army built its entire power structure, logistics, training (particularly modeling and simulation), materiel development, organizations, doctrine and soldier systems to deal with an industrial-age foe—and it dealt with that foe very well.

Now, with the RMA and ascendancy of asymmetric foes using strategies such as information operations, *the Army has to shift the way it does things. It now must consider both an industrial, kinetic warfare approach and an opponent using asymmetric strategies.* Doctrine has to deal with both, as well as training, logistics, organizations, materiel development and soldier systems.

The Internet is the greatest learning tool for people everywhere since the invention of the printing press. Generally, the learning potential of the Internet is a great step toward progress for the human race. Along with this positive aspect of potentially enlightening the earth's populace comes one of the most ominous and potentially dangerous characteristics of the Internet age. That is, our opponents of the future will use the Internet to learn, orchestrate and coordinate at the speed of light. Additionally, our opponents of the future will use the Internet to empower small groups and individuals around the world to the point that time and distance become irrelevant. They will engage our forces in invisible struggles to affect decisions, and find and strike weaknesses, no matter where, of the technologically advantaged. These weaknesses will be particularly difficult to recognize because they are also strengths.

The Information Revolution has also brought on the age of data overload, and a very different type of competitive struggle. This is an invisible struggle for momentum and initiative. It is a struggle for influence and control of the will of opponents, populace in objective areas, coalition forces and their governments, and people of the United States. These invisible struggles can vault to the forefront of decisionmakers' attention owing to the ubiquity of the media and the digital tools they use to quickly move images and explanations to the television sets and computers of the populace of the United States.

Additionally, the Information Revolution has allowed for the rise of the truly global earth in which all-important systems are becoming increasingly interrelated, e.g., social, political, transportation, ecological, economic and financial. In fact, military planners are working with a tapestry of interwoven relationships. Thus, military strategists and planners cannot deal with the military system without dealing with its relationships with other systems. All of these broad elements form a very powerful operating environment the Army must recognize, analyze and synthesize, and ultimately master.

The Competitive World of the 21st Century

It is painfully obvious that a way exists for opponents to compete with the United States militarily. That is, our opponents of the future will first read our doctrine and then engage us in areas we say will be our pillars and combat multipliers. They will seek ways to manipulate commanders' trust in the veracity of data, information and knowledge. They will attempt to take away the collaboration that leads to situational understanding (a key component of information superiority). They will seek to disrupt just-in-time logistics by attacking knowledge workers, disrupting the time phased force deployment (TPFD) synchronization, affecting the operations of lines of communications (LOCs), aerial ports of debarkation (APODs) and seaports of debarkation (SEAPODs). Our future asymmetric opponent will attempt to affect precision fires by disrupting or manipulating data streams from collectors, jamming up- and downlinks, attacking mission ground stations, and conducting sophisticated denial and deception operations. They will also attack and manipulate knowledge workers (such as system administrators and software engineers) who run and maintain key computer, collection and communications systems in mission ground stations. They will use incapacitating agents and individual-delivered point weapons of mass destruction to affect knowledge workers and people who operate ports. They will attempt to manipulate the will of the people of the United States by creating large numbers of U.S. casualties, both civilian and military. They will drag out in time any competition in hopes that the immediacy phenomenon, so dominant in the United States, will influence public will and national policy.

When we write about asymmetric threats, in most cases our efforts fail to describe the phenomenon sufficient to provide knowledge and understanding. We have a difficult time thinking as asymmetric opponents think because we have been the strongest country in the world for such an extended period of time that we have trouble conceiving viable competition. Failure to think through these issues realistically causes us to grow intellectually "flabby."

Asymmetric opponents will be learning, adaptive and coevolving. They will learn from their own mistakes, the mistakes of others, and the mistakes of the U.S. Army. They will learn from the Internet, access commercial imagery, collaborate, use commercial encryption, and follow news and world events. They will access databases and virtual universities. They will retrieve and use the hacker software that is so plentiful on the Internet.

Asymmetric foes in the context of these comments are weaker than the United States and seek off-sets against our military and technical prowess by using indirect approaches, attacking or manipulating our vulnerabilities, and often making use of low-tech strategies, techniques and procedures to obtain temporary advantages. Asymmetric opponents will search for our vulnerabilities much like hackers reconnoitered and found vulnerabilities in e-commerce computers and websites during the denial-of-service attacks that occurred in February 2000. Foes who use an asymmetric strategy could be terrorists, Chechen-type military forces, information warriors, drug gangs or criminal groups, to name a few.

Asymmetric foes could very well possess goals (and subordinate objectives) alien to what we classify as military goals and objectives. They could, for example, have limited objectives. They could have small objectives that relate to large objectives, with plans for enacting larger goals over several years. They could mask their intentions and goals with traditional and cyberdeception. They could hate to the point that they become suicidal to accomplish some of their objectives. Moreover, their objectives in a city could simply be to continue their criminal activity unimpeded or to delay our mission accomplishment, making our military look inept.

As a strategy, our asymmetric foes of the future will engage and "tar-baby" the United States in *urban areas*. They will attempt to negate our intelligence collection, use the power of information operations stretching around the earth, take advantage of volatile political situations, and use the Internet to orchestrate and coordinate their actions across time and distance. They will attack and manipulate interconnections of the major systems that make up the fabric of the system of systems that bind people as a global earth. Ironically, they will use strengths of the United States (such as the media, openness and proclivity to protect our bill of rights) against us.

Environment

Departure from the past. Historical analogy usually provides some good ways of viewing the future. We go back to the past and search past situations for trends, insights and relationships. We then think through implications and try to devise what the future will be. Basically, we use historical analogy to get our intellects in focus on what the future will be like. This line of reasoning has served us well in the past. We can continue to use the methodology in the future given that we are smart enough to know the methodology's inherent dangers. Thinking through this process helps us understand the Janus paradox.

What are these dangers? First, the description above is a linear, reductionist way of seeking the future and developing implications. Unchecked linear thinking leads to very narrow points of view particularly when we acknowledge that we live in a nonlinear, holistic world comprised of relationships and nonhierarchical activities. Second, we should not rely totally on historical analogy and projection to consider the future owing to stark differences of the new age. People living in the past didn't have the Internet. The Internet is revolutionizing the way we make money, spend leisure time, socialize and compete. Third, historical analogy tends to stifle creative thinking and leads people to conclude that *what was* and *what is* become more important than *what could be*. We must be very careful when we use a straight-line historical projection, in an additive way that depends entirely on what happened in the past to forecast the future. Such a methodology is dangerous owing to the potential to encourage people to prepare for the past and the "last war" instead of using our inherent creativity to prepare for and *shape the future*. Along with historical analogy the Army must learn to use vision development and enactment to "dream" about a future state of being and develop plans that lead along a nonlinear path toward enactment of the vision. In essence the Army must shape the future from the seeds of the environmental context it sees unfolding into an ill-defined future while keeping traditions and ethos appropriate for operating in the envisioned future environmental context.

Environmental demands on information. The Army will face significant information challenges in future operations with the IBCT and eventually the Objective Force. Environmental demands seriously affect information in several ways.

- First, information must be "*tailorable*." Information appropriate for one place in the world against a particular set of circumstances will be inappropriate for another mission to another place with another set of circumstances. That is, each situation will require different information in terms of *timeliness, specificity, accuracy* and *relevancy*.
- Second, environments the Army will face in the future demand *adaptable information*. For example, in some situations, soldiers will be conducting humanitarian relief operations in large urban areas. Such activity will dominate their days; these operations will demand distinct information requirements. Then, while in the midst of benign humanitarian relief operations, soldiers in small units will bump or careen into episodic violence in which they will face high-tech, well-armed opponents who could be drug dealers, terrorists or criminal gangs. This episodic violence will be sporadic and will defy prediction owing to the randomness of a chaotic environment. This problem set demands information different from that of the humanitarian relief problem set.
- Third, information must be *adjustable* to how individual human beings think. All people are different and think differently. It follows that they use and process information differently. Thus, they need individually adjusted information to make quick, good decisions.
- Fourth, to find true value, a transformation process must occur. That is, in a purposeful way, data turns into information and information turns into knowledge. Once we have knowledge, we can seek wisdom. To find knowledge, human beings must collaborate and understand, not just be aware.

- Fifth, people have to share information among their own communities of interest, with coalition partners and with media supporting the operation. Information and knowledge must be relevant to the issue at hand. That is, a squad leader leading his troopers in a humanitarian patrol in a large city will require very specific, mission-dependent, instantaneous information. His sphere will be small and focused. His company commander, on the other hand, will need information in a much broader context. He will need to know what is going on all around the squad leader to provide the benefit of a "God's-eye" view of the battlespace. This line of reasoning goes on through a chain of command and represents one of the greatest challenges to information technologists.

- Sixth, owing to the importance of decisionmaking and a deployed force's vulnerability in the objective area, en route to the objective, and in the continental United States to intrusion, cyberdeception, hacking and cracking, *information must be secure and must come from trusted sources.*

- Seventh, new types of information and knowledge will have to ascend in manipulable databases. For example, along with traditional electronic order of battle (EOB) and order of battle (OB), analysts, staff officers and commanders will need resources such as "hacker order of battle" (HOB)—asymmetric preparation of the battlespace (APB) that includes the tapestry of architectures making up the means to seek and gain information superiority for both sides. They will also need adaptive war-gaming in a virtual environment in which the opponent is represented by an avatar programmed to think like the leadership and perhaps even the people in the objective area. What the Army must seek is a way to avoid the intellectual trap of mirror imaging in which we superimpose our minds and our beliefs and our backgrounds into the mind of a foe when the foe's thoughts are antithetical to ours. The idea of the adaptive war-gaming will be for the software to get smarter and become more formidable, thereby helping to identify variables against which friendly leadership manipulate and task intelligence collectors to see if manipulation is or isn't working.

Constraints

In any military situation in the future, there will be an amazing labyrinth of constraints surging forth as rules of engagement (ROE). Other constraints will remain unspoken but involve tacit knowledge embedded in the intellects of commanders and their subordinates. Regardless, constraints will be significant inhibitors of force. Moreover, a wily foe will attempt to manipulate the binding effect of rules of engagement to their advantage. Constraints won't lessen—they will increase with the volatility of political situations and the vagueness of missions that the Army of the future will face. There will be the usual military constraints represented by numbers, time, distance and the laws of physics. Also, there will be social, political, economic and ecological constraints making any operation very complex. As roles and missions blur among departments, organizations and agencies, constitutional guidance, legal mandates and laws will become constraints.

As a related thought, in any situation in which we find ourselves, the operational environment represents a tapestry. The symbols, messages and pictures represented on the tapestry are interconnected. Any tug on one thread of the tapestry results in the rest of the threads moving and changing, too. This analogy works for the military as well. That is, in any conceivable situation, a complex tapestry representing reality will dominate Army operations. Social, political, military, ecological and economic relationships will be so interwoven that activity in one sphere will cause activities in other spheres. This interrelatedness is important. Why? Quite simply, for years soldiers have prided themselves on focusing on the military aspects of operations. Now, though, they must concentrate on the tapestry and realize activity in one sphere relates to other spheres.

The tapestry is an abstract representation of constraints and their relationships with military matters. If the Army is shortsighted in this aspect of future operations, it could conceivably lose in a military competition because what it did in the military thread affected other threads of the tapestry extensively. The tapestry notion has immense implications for the Army's training and education system and is one among many arguments for dramatically changing officers' and noncommissioned officers' (NCOs') thinking capabilities.

Casualties. As another constraint, our people and government are loath to accept high casualties. There is ample evidence of this proclivity. It has been the American way of war since the birth of our country to reduce casualties by using technology to help us win in combat—life is too precious to be squandered. We have ample evidence from the Gulf War, Somalia, Bosnia and Kosovo to cause us to know, without question, that America wants very few casualties. This desire is compounded by our belief in technology and the distinct possibility that it will enable us to wage and win "clean" wars with very little violence for our troops. Unfortunately, we're going to be faced by intelligent, adaptive, learning foes who will understand our aversion to casualties; they will attempt to create those casualties in hopes of influencing public opinion. More of this phenomenon will be addressed later in the paper when the subject of urban operations comes to the forefront.

Collateral damage. As yet another constraint, in any conceivable environment that our Army of the future will operate, soldiers and leaders will be constrained by the absolute need to minimize collateral damage. After all, we have come a long way from the "destroy the village to save the people" syndrome that was stereotypically the Army in Vietnam. Our soldiers can't indiscriminately use military force to accomplish objectives—force has to be tied to potential outcomes, second- and third-order effects, intensity, public will, nature of mission, nature of the environment and so forth. The use of force has to be reasoned and minimized owing to the second- and third-order effects (most of which cannot be determined but could have far-reaching, cascading effects detrimental to any mission) that come from conflict in a chaos-dominated field of competition. Moreover, as previously mentioned, the military thread connects with social, economic, ecological and political threads. So heavy collateral damage that helps accomplish military objectives will invariably cause repercussions in other spheres. This problem is compounded by the formidable and serious role played by the media and their instantaneous, global communications systems. The media can and will cross domain boundaries very quickly, and what have heretofore been military issues can very quickly become political, social, economic issues.

Political volatility. In every conceivable situation, the potential for political volatility will constrain military operations. Several reasons exist to explain this phenomenon.

First, the information revolution has enabled very senior leaders to know instantaneously what is occurring in the military objective area. Moreover, that same technology enables our senior leaders to know how other countries are reacting to actions in an objective area. Second, second- and third-order effects in nonlinear, chaos-ridden operations will quickly affect nonmilitary spheres of influence. The media will help to cause this spreading and affecting of other spheres much as a virus spreads on the Internet. Often, the social sphere will have immense second- and third-order effects owing to the humanness of our country (that is, at once a strength and a weakness), the power of images and symbols, and compassion toward those who suffer. Third, in any operation in the future, the Army will be working with people from other countries in a coalition situation. Sometimes, these people will have very different points of view and reactions to the military use of force. Once again, the constraint grows in magnitude owing to the presence of the media and instantaneous, global communications that reach people no matter where they are.

Threads of continuity. When U.S. forces go anywhere, they require support. The Army's stated desire to travel light and to reduce its footprint forward doesn't obviate the absolute requirement for logistics, intelligence and administrative support. This support stretches across the battlefield operating system (BOS) and straddles the pipeline encompassing time and distance as connecting threads. The connecting threads stretch from the deploying force into the fountainhead of their existence—the United States. Some of the threads are fragile (e.g., logistics). The location of the operation is crucial as well, as distance can affect the strength of the threads. Moreover, once again, depending on location of the operation, weight and volume of supply flow affect the threads. The threads are highly dependent on technology for their continuity, yet technology is in many cases fragile, indeed vulnerable to asymmetric manipulation. To be strong, the threads must connect much as links connect in a cobweb. If a link breaks in a cobweb, the strength of the overarching cobweb dissipates; the same holds true in the threads from a force in the objective area to the fountainhead.

Why is this addressed as a constraint? The answer is straightforward: *The competition will see these threads as places to attack and will do so with sound and fury*. They will attack and attempt to sever or weaken these threads in an objective area, en route to an objective area, and in the continental United States. They will use various combinations of weapons of mass destruction (WMD), information operations (IO), terrorism, extortion, threats against both soldier and knowledge-worker families, and more traditional asymmetric attacks. Thus, we have to anticipate these attacks, war-game responses, work on these issues in training, modeling and simulation, and debate in the halls of Leavenworth and Carlisle. These threads will be addressed later in the paper as they relate to tenets such as "just-in-time logistics," "assured communications," "common operating picture," "precision fires," "information superiority" and "synchronization."

Infrastructure. Most places in which military operations occur will have weak infrastructures. That is, there will be minimum communications backbones, limited fiber-optic cable, limited port and air facilities, poor distribution and transportation systems, and limited power grids. These shortfalls will constrain our forces and cause us to make serious adjustments in concepts of operations and activities in the objective area.

Interestingly, weak infrastructure flies in the face of the desire to reduce the footprint of our deployment. While ground and air forces desire to reduce their footprint to enable a more rapid deployment, footprint creep occurs because of the dearth of infrastructure.

Suffice it to say, technology will do much to help overcome this constraint. At this point in the paper, we have to conclude that reduction in footprint is good and we must do everything we can to facilitate rapidly deploying forces who need minimum infrastructure related support in the objective area. A wily foe will want us weighted down by a ponderous infrastructure. With increased infrastructure comes more hierarchy and a more ponderous decisionmaking processes. A hierarchy and ponderous decisionmaking apparatus are antithetical to the absolute need to make rapid decisions and self-synchronize in a nonlinear, amorphous, chaotic environment populated by learning, adaptive, coevolving foes.

Cultures and thought processes. The ways people think, sense and perceive are constraints in future operations. This observation holds true for people we face in competitive endeavors and for people we work with in coalition operations. Army leaders have to work on understanding opponents' thoughts and decisionmaking, as they war-game possible courses of action and act, react and counteract cycles. With the stated importance of multinational and coalition operations, *it's just as important to war-game the act, react and counteract cycles of coalition partners as it is to war-game against the actions of foes*. Of course, the less time you have to learn about the opponent, the more difficult it is to gain understanding sufficient for influencing decisions.

Information operations, for example, deal with perception influence. To work on the psyches of people through deception, psychological operations, and civil affairs, the Army has to know something about the way people think and perceive. Limitations exist —a lack of time to learn about the opponent and to design complex, intricate information operations against a thought process very different from ours. This is a critical constraint, and it is a hard problem to solve. Thus, to live and excel with the rest of the constraints, it stands to reason we must know and understand how our opponent, people in the objective area, and coalition partners think and perceive. Suffice it to say, a virtual, collaborative, cultural and linguistic expert support environment will be fundamental to any Army operation of the future. Quite simply, the IBCT or Objective Force will have to determine the perceptions of people they are trying to help and those with interests inimical to ours. It will be difficult to find such expertise in a no-notice deployment.

Regardless, the goal should be to provide 24-hour-per-day support to deploying Army forces from people expert in the language, culture and decisionmaking processes of potential opponents, civilians and coalition partners in a virtual, collaborative environment. There is a possible solution for this dilemma; it will be offered later in the paper. Suffice it to say, the Army needs to satisfy this requirement by developing an information operations analytic center (IOAC) in which its best and brightest analysts support deploying forces in the realm of IO.

Chaos. Any operational environment of the future will be populated by foes operating in a chaotic environment. Perhaps few of our foes will read and understand chaos theory. But one doesn't need to read the theory to understand how to compete with the United States asymmetrically. People have been doing so successfully for years, the latest being the Chinese Communists operating under the doctrinal influence of Mao and the North

Vietnamese operating under the guidance of Giap and Ho Chi Min. Flat organizations are decentralized and loosely connected—they normally adapt and make decisions quickly because they aren't tethered to a layered chain of command and they operate within the visages of a broad guidance/vision their leader articulates as intent. Moreover, they engage in self-synchronization based on environmental perturbations, and they can self-heal, grow or become extinct quickly. They adapt to their foe's activities and coevolve.

These foes operate at the edge of chaos, taking advantage of the things chaos brings (creativity, adjustment, adaptation, coevolution, disparate relationships, self-synchronization), while maintaining just enough order to be classified as an organized force. Along with being flat and cellular, their organizations will be secretive and loosely connected. Their system will self-heal, grow or self-eliminate. They operate by seeking and understanding patterns and relationships in what they and their opponents do. They will seek to strike at the opponent's relationships owing to the complexity of systems lashed together and the distinct need to deny the absolute state of synergy that can come with knitting relationships into a coherent collage.

Foes operating at the edge of chaos will coevolve with their opponents. That is, they will learn, adapt and change based on what their opponent is doing and how environmental influences affect their goals and missions and those of their foes. If, for example, they see on CNN that people in the United States are unhappy with something U.S. troops are doing, the wise asymmetric foes accentuate that point as a weakness and create situations among their very loose cells or suborganizations to nurture conditions for creating effects to maximize the weakness. Perception, after all, is the key to the door leading to will and morale of the public.

Initial Summary

Environmental context will have a tremendous influence on Army operations. This environment will be very complex, and many constraints will be highly influential. Our soldiers will be operating in a chaotic environment. They cannot be hindered by a lethargic, hierarchical, unadaptive organization serving as the chain of command. Our soldiers will face very formidable, asymmetric foes. These foes will excel in chaos, attack our vulnerabilities, and avoid confrontation except for places and times and goals of their choice. Our soldiers will be constrained by the strong societal need for minimum casualties and very limited collateral damage. The threads, or BOS connections, stretching back to the United States are vulnerable to traditional and asymmetric attacks. These threads, particularly where they connect to cells comprising the cobweb of our enterprises, will be vulnerable to point, individually delivered weapons of mass destruction and incapacitants. Our knowledge workers will be vulnerable to attack, manipulation and threats from extortion. The same will hold true for soldiers' and knowledge workers' families. The social, political, economic, military and ecological spheres or domains will be inextricably woven into a delicate tapestry where activity in one sphere will have a marked influence on activities in other spheres. *Our opponents will recognize the tapestry and will attack the points where key threads come together.* The thoughts, feelings and perceptions of people comprising a coalition or partnership will have more influence than ever.

The environment the Army faces will be far different from anything it has dealt with in the past. The military mind will have to grow, change and adapt to handle the nuance, abstraction, relationships, synthesis and synergy dominating all activities in such environments. Indeed, the Army must prepare for the power and fury of environmental influences our soldiers will face in future operations.

The IBCT Concept

Information operations. Information operations constitute the single most important struggle spelling victory or failure in any future operation. The IBCT and Objective Force need this important tool for the offense and defense alike. Our asymmetric opponents will seize upon IO as a great tool to achieve offset against our technological and kinetic advantages.

IO is a dominant force (or soon will be) for two reasons. First, we depend on information for everything we do. Both the Army and the joint world imply as much in the thoughts and writings that underpin doctrine. Second, our opponents will seize upon our dependence on information technology and attack that state of being. The attacks will come directly and indirectly to achieve momentary advantages in tempo and initiative at the tactical, operational and strategic levels of competition. Indeed, information technology is a great strength. Yet, at the same time, it's a vulnerability. When one depends on something, a window of vulnerability presents itself unless somebody or something closes it. Moreover, IO is the key variable in seeking, achieving and retaining information dominance for any length of time. We should know the truth of this assertion; our opponents surely do.

Conflict of the future will be a combination of kinetic-laden violence with the murky, invisible struggle of digits. Digital and kinetic struggles are different and require different thinking skills, planning and materiel. Thus, the Army must recognize IO as a force to exploit in an offensive sense and as a force to defend against when faced with the adaptive, learning organism constituting our future foes. These foes will attempt to affect a multitude of glaring IT vulnerabilities with great sound and fury.

IO is and will continue to be a theme at least coequal with physical maneuver and fire support. After all, to achieve information dominance, commanders will have to maneuver digits and weight the main effort with information just as surely as they have thought through fire support and close air support (CAS) in the past. IO should become, over time, the most important aspect of environmental contexts, particularly in the difficult realm of urban terrain.

Urban conflicts. Foes of the future who desire to compete with the United States militarily will establish conditions for causing U.S. forces to engage in urban operations. Why? Urban terrain presents the only place opponents can hope to establish conditions to accomplish their goals. This section of the paper briefly discusses the rationale for the premise.

Asymmetric competition. Urban areas are perfect places to unleash asymmetric strategies by a host of foes. Urban areas are conducive to asymmetric operations because our opponents can manipulate casualties, set up conditions that will enable extensive collateral damage, and play to the minds and emotions of Americans watching television or operating their computers. Moreover, competitors using asymmetric strategies can exploit the constraints discussed earlier in the paper.

Collection in urban terrain. Intelligence collection, a complicated business, has improved over time; by the end of the Cold War it worked very well. Yet perplexing shortfalls remained and have carried over into the new operating environment that the IBCT and Objective Force face. For example, collected information doesn't fuse well among military service collectors. Thus, it's difficult to create conditions enhancing synergy. As another example, collectors in the Cold War era concentrated on military communications, moving targets, and attrition ranging from destroyed tanks to the damage inflicted by nuclear weapons. Unfortunately, this issue constitutes only part of the problem that commanders of the future will face. If the situation arises in which a conventional force engages the United States in force-on-force combat situations, the holdover collection system will work well. But if the environment is similar to what has been described above, the collection system will prove inadequate and our IBCT and Objective Force soldiers will suffer the consequences. That is, if our foes using asymmetric strategies engage our forces in urban terrain, existing and planned collectors will have a difficult time providing information sufficient for the demands of the situation. Specifically,

- In an urban area, human intelligence (HUMINT) will be the premier collector. Signals intelligence (SIGINT) will be difficult to collect owing to problems with the rapidly growing cellular phone and wireless phenomena. Imagery intelligence (IMINT) will help in some situations, particularly in precision targeting. Nevertheless, it won't help much with intentions and possible opponent courses of action open to asymmetric foes. Measurement and signature intelligence (MASINT) can help some, but it won't help much with stealthy movement by small groups and individuals. MASINT, though, could very well provide entrée into sophisticated collection for thinking through possible locations of and detection of weapons of mass destruction. Collectors such as unmanned aerial vehicles (UAVs) and miniature UAVs will help some owing to their dwell time, ability to stare at a particular location, and ability to tell commanders about gatherings of people, traffic patterns, and locations of U.S. forces operating in a nonlinear environment. But they are not the answer to all the IBCT's and Objective Force's collection challenges.

- What collection capabilities are needed by people operating in an urban environment? First, U.S. forces need to improve the capability to operate against wireless, cellular phones, computers and personal digital assistants (PDAs). Second, U.S. forces need very fast access to HUMINT-derived information. HUMINT collectors need a way to digitize their thoughts, observations and reflections, and to transmit to a fusion system where the data fuses with all sources of information collection into dynamic, changing, situational awareness visualization. Technology must provide information assurance to the point that veracity is a given, so commanders can believe in HUMINT rather than rejecting, delaying or confirming with other sources prior to accepting the information. Third, collection must get into the rooms where asymmetric foes plot their operations and whisper instructions. Fourth, we must have collectors that are stealthy, miniature and robotic. They must be capable of collecting, processing and transmitting information to satellites or satellite surrogates for gathering into fusion technology and immediate dissemination to people operating on the ground. Fifth, collection must sense the moods of crowds so commanders can anticipate potential crowd-related troubles. Sixth, collection must answer questions about metrics associated with effects of information operations.

- Intelligence activities in urban operations will be very different from intelligence support to traditional force-on-force operations. Actually, this is one of the most important issues the Army, indeed any joint force, will encounter in future operations. If the IBCT and Objective Force depend on information superiority as the force multiplier that enables reduction of footprint, the Army must address collection of information in urban terrain. The Army's combat systems, soldiers and mission accomplishment depend on successful resolution of information collection challenges.

- As was mentioned earlier, asymmetric foes—be they drug cells, terrorists, special forces, criminal gangs, societal gangs or conventional forces—will seek to offset the Army's technological prowess and advantages by luring it into urban terrain. Alternatively, they will take advantage of existing operations, such as humanitarian relief, to engage the Army in urban operations. This strategy makes sense, given that somebody decides to compete with U.S. forces. Once in urban terrain, though, many aspects of the environment change. These changing aspects of environment cause changes in collection operations.

- Let's lay out some of the major differences and put forth some ideas about what to do. First, violence will be episodic. That is, for long periods of time, soldiers will be taking care of other human beings—feeding them, caring for them, guarding their homes, evacuating them. They will have very distinct information requirements to perform this type of operation. Occasionally, though, small, nonlinear, nonhierarchical Army units will careen into small, well-equipped, high-tech and lethal forces waging asymmetric operations. These encounters will be extreme and intense, and could last from a few minutes to several hours**.** *Information requirements will be dramatically different from humanitarian relief information requirements.* In essence, the Army needs flexibility to perform analysis and synthesis, collect, process, visualize and communicate to meet the needs of these two environments or have two separate yet related systems. Second, opponents won't always operate as hierarchical organizations. Instead, they may be flat organizationally, spread throughout a city or under it, and only loosely connected. Moreover, owing to the potential of compromise of intent and personalities, their flat structures will change and relocate frequently, thereby making the information challenges for analysts and commanders all the more immense. For example, using the Internet, diverse organizations may come together to support one activity or protest and then disband (as the opponents of the World Trade Organization did in Seattle during the spring of 2000). Third, future foes operating in urban terrain will perform their activities inside buildings, underground, on the Internet, or in other aspects of cyberspace. Intrabuilding and subterranean operations make sense owing to shortfalls of U.S. collection capabilities to collect, process, fuse and visualize data, information and knowledge in urban terrain. Fourth, because future foes are adaptive and learning, they will avoid use of cellular phones and computers over phone lines without encryption because to use these devices indiscriminately and insecurely could very well lead to compromise and neutralization.

- Human intelligence is and will be critical in urban operations. So what are the problems inhibiting HUMINT?

  - HUMINT is difficult to collect and use because often it isn't timely.

  - Moreover, commanders sometimes don't believe what HUMINT is telling them without verification from other sources unless they believe HUMINT-provided information is valid.

  - As another issue, HUMINT collectors have to transmit their information to other people, by whom the information is analyzed, synthesized and then resubmitted to fusion processors for inclusion with other sources of information.

  To summarize, timely and accurate transmission of HUMINT information and automated fusion with other sources of information is and will be a significant challenge for anybody attempting to seek, find and sustain information superiority.

- Where do these issues leave us? First, in urban environments, and owing to the importance of HUMINT, commanders have to recognize the need for sole-source intelligence and take action quickly because they exist in an incredibly fast-changing environment. Second, HUMINT collectors need reliable, unobtrusive and very light digital communications equipment whose transmission paths bypass the current lengthy processing system. In this respect, HUMINT-derived information has to be highly secure and verifiable for commanders to use. Third, HUMINT must fuse with technical intelligence to provide commanders situational awareness and situational understanding. These are issues dealing with the technical and training areas encompassed by information assurance.

- Intelligence collection must also focus on seeking, finding and interpreting metrics for assessing the effectiveness of information operations. Traditional means of assessing battle damage won't work. Why? Primarily metrics associated with IO focus on perceptions, mood, morale-precluding or -inhibiting behavior—planners and commanders using IO need to know and understand effects their IO efforts bring forth. Indicants of behavior-revealing effectiveness of IO include leadership directives, thinking and planning. Moreover, combatant morale provides a useful way to start judging effectiveness. Civilian populace provides yet another indicant of effectiveness—the local populace, through conversation and actions, provides insights into the effectiveness of IO. Typically, HUMINT has been the only way to ascertain these effectiveness criteria. It seems logical, though, that with a focused collection manager's thought process at the helm, some technical collectors could help with this task. Unmanned aerial vehicles, for example, as currently configured, provide imagery (electro-optical, forward-looking infrared) that can tell commanders that an activity is occurring or not occurring. As an example, UAVs could identify crowd movement or how many individuals are loitering or how many people are in a line waiting for food. What UAVs cannot provide is information pertaining to the mood of people in a crowd, loitering or waiting in line.

- Collection also needs to work on the problem of individuals conferring in rooms or underground. Traditional SIGINT won't be the solution to this challenge—people won't always be talking on the phone, and if they do so, messages and conversations will often be encoded, cryptic or designed to wage cyberdeception. While useful as one aspect of the collection effort, SIGINT will not be a panacea. No, to get at intent of competitor leadership, U.S. Army personnel will need access to some very innovative collectors. What might these collectors be like? First, they must be small and unmanned. Second, these sensors must be unobservable—not only small but also stealthy. Third, they must have the capability to detect sound and must be able to provide images. Fourth, these collectors must be able to smell and sense individual and group moods as sweat or chemical bodily emissions. Fifth, these sensors must be capable of transmitting what they see, hear and smell through windows, through walls, through air shafts and electrical conduits. These transmissions must be broken into packets, wrapped for security (recall the need for information assurance), and processed and correlated by a relay satellite or surrogate satellite; they must then be fused and visualized to assist in quick decisionmaking by commanders in information advantage centers and soldiers operating in small groups throughout a city. Sixth, these sensors need to operate in swarms and they need to be expendable.

- Intelligence preparation of cyberspace will be critical. Preparation of collection activities and confirming or denying hypotheses will become the most important aspects of collection operations in urban terrain. Some major differences from past intelligence preparation of the battlefield (IPB) activities that the Army so superbly developed and used include the ideas that follow. First, analysts will have to know and understand how opponents collaborate, coordinate, instruct and synchronize in cyberspace using computers, cellular phones and personal digital assistants. Second, analysts need to think through the fused picture of friendly activities in the machinery of opponent computers. This aspect of cyber-IPB will be important for the initiation of cyberdeception. Third, analysts will have to use cyber-IPB to focus their collection efforts. Miniaturized robots will have to be present at key spots where enemy leaders meet, conduct operations, and fuse information. This activity will have to occur in a physical sense and at ghost nodes in cyberspace somewhere around the world or in space. Fourth, analysts will have to anticipate where weapons of mass destruction could possibly create the most dramatic effect. These analysts will have to know, themselves, what is important, and possible second- and third-order effects far greater than analysts have known and understood in the past. Fifth, analysts have to work with individual opponent minds and perceptions and those of aggregate intellects coming together to solve problems through the use of opponent collaborative tools. Sixth, analysts and commanders must always be on the lookout for chicanery and deception. This challenge is particularly disturbing because so much of IO lies in the invisible realm of digits and perception manipulation.

Jointness. Any Army concept of the future must emphasize jointness. The Army's IBCT concept needs a greater emphasis on jointness—a much broader discussion will be important to the validity of the concept and its acceptance by other services and by Congress. This force will always operate in a joint environment. Indeed, its existence and capability to survive and accomplish its mission rely totally on joint support. As an example, when discussing the reachback needs for the brigade, the IBCT or Objective Force connects to the Army Force (ARFOR) analysis and control element (ACE). But an ARFOR ACE is but one part of a collaborative environment in which the brigade will operate. More importantly, the brigade will connect to the supporting Joint Intelligence Center (JIC) and even the national intelligence community for the best information and knowledge available. Precision for conducting surgical operations and minimizing collateral damage in volatile political environments won't come from organic collectors. Organic collectors will help in the process, but precise information and knowledge will come primarily from the joint intelligence collection system. Thus, jointness is an imperative for achieving and sustaining information superiority.

Information Centers of Gravity (Info-COGs). The Army can't proceed in the future with its focus solely on traditional centers of gravity. IO is about enhancing friendly decision cycles while degrading the opponent's. Thus, the question must be asked: How, where and with what processes will friendly and enemy commanders seek to protect their decisions and affect their opponents'? IO will be an invisible struggle whose outcome will be immense given the importance to decisionmaking of communications, visualization, collaboration and information superiority. Thus, while traditional thoughts of Centers of Gravity focused on material things and kinetic effects, Army planners have to recognize the fundamental shift from kinetic, physical things to include invisible, digital things. Information Centers of Gravity are real or in virtual cyberspace, where a confluence of collection, automation, communications, thinking and planning, and decisionmaking occurs. These places are so important that their demise or sustainment will go far in determining the outcome of competition. This notion is so important that it needs to be at the forefront of the Army's doctrine so it can drive the DTLOMS (Doctrine, Training, Leader development, Organization, Materiel, Soldiers) system.

Logistics and maintenance considerations. Army planners must recognize the tenuousness of "just-in-time logistics," and the fragility of depending on synchronization of the flow of personnel, materiel and supplies. Moreover, planners have to recognize the Achilles heel of the information age—that is, our dependence on purveyors of information or knowledge workers (civilian contractors and military technicians alike) for maintaining our information and other electronically-driven equipment. Clearly, the ideas of just-in-time logistics and synchronization of logistics are great concepts and need to be a part of any concept of the future. But once the Army goes down this path, it must wake up and cope with attendant vulnerabilities; there is no vulnerability potentially more damaging than to attack the knowledge workers who maintain our equipment, run our digital systems, and make our limited parts. A worthy opponent of the future will surely attack these "purveyors of knowledge" in and away from the continental United States. The Army must recognize this possibility and determine ways to overcome the vulnerability. Quite simply, attacking purveyors of knowledge is a great asymmetric tool that any intelligent competitor won't ignore. We rely too heavily on these purveyors to assume otherwise.

Information operations and cultural, geographical and language expertise. Given the basic IBCT and Objective Force premise of rapid deployment anywhere in the world, linguists and country experts must be readily available to assist in the operation. Finding these people and ensuring their competence, though, is problematic at best, especially when thinking through what the brigade touts as its modus operandi—deployment anywhere in 96 hours. How will Army leaders ever find sufficient expertise and language capabilities given a short-notice deployment? This issue is closely related to IO. The Army needs to address and resolve the issue by sponsoring a Joint Virtual IO Analytic Center that has at its disposal a database populated with the location of country experts and proficient linguists inside and outside the military. Moreover, the center must have the capability to perform fine-grained analysis and synthesis that the brigade will demand and will be unable to perform itself. On one hand, a few of these experts need to be capable of deploying with the brigade, which will, of course, require a high degree of professional competence along with country and language expertise. On the other hand, experts scattered around the world need to collaborate virtually using multimedia with deployed troops so as to "blow knowledge and wisdom in the ears of analysts and leaders," when forward-deployed people need help.

Information superiority. Writings on the IBCT discuss information superiority without explaining the thinking that underpins the words. The words "information superiority" are ambiguous. They mean different things to different people. The Army needs to identify what the words mean and what implications come forth in a DTLOMS evaluation. This all-important effect (information superiority) cannot be all the time and everywhere. Quite simply, we can't afford such an effort. Moreover, to think we could create superiority in the information realm all the time and everywhere makes arrogant and degrading assumptions about our opponents or competitors—it makes them seem incompetent when the opposite could very well be true. Instead, the Army should deal with the notion of information superiority by precisely defining the two words. *Information superiority means seizing advantages of initiative and momentum at a time and place of the brigade's choosing with the notion of creating the conditions that lead to effects conducive to the commander's mission.* Planners need to make the bold assertion that such an advantage will be temporary owing to learning, adapting organisms constituting our opponents of the future chaotic environments. Information superiority will be difficult to achieve; its ascendancy and any degree of sustainment will require great intellectual and technological travail.

Common operating picture. It's ludicrous to assert anytime the presence of a near-complete common operating picture (COP) providing the wherewithal for information superiority. Why? First, all the technology available won't provide the "God's-eye" picture people get at the National Training Center. There are too many soldier-induced errors, equipment failures, weather variables and uncooperative, adapting, non-predictable foes to approach a state or metric of "near complete." "Near-complete COP" is a dangerous phrase that leeches the strength and viability from ideas and concepts worthy of more attention. It is a concept more akin to "fairy dust" than reality. Instead, Army planners need to place more emphasis on visualization, collaboration and fusion in their discussions. A fairly robust common operating picture could evolve. But without such technological capabilities, the notions of information superiority and situational understanding will be empty words signifying nothing.

Precision fires. When discussing the IBCT, Army planners put much credence in the importance of precision fires. Yet, even with the most sophisticated technology, there will be great difficulty collecting, processing and sharing information quickly, particularly in an urban environment. Quite simply, the environment isn't conducive to technical collection, particularly against low-tech opponents. That's not to say that technical collection, e.g., UAVs, won't be helpful. It will be quite helpful, especially when the UAV-produced data and information synthesizes with other sources of information expeditiously.

- As was mentioned earlier, the best intelligence collector in urban terrain will often be HUMINT. Suffice it to say, HUMINT is slow to develop, difficult to synthesize, susceptible to deception, and difficult to fuse rapidly with technical collection. There are technological solutions on the horizon to help HUMINT, e.g., speech recognition and turning speech into digits that automation can process, but they aren't available yet.
- Thus, we have to recognize that some of our information won't be accurate enough to ensure that our soldiers meet the constraint standards of collateral damage explicit in rules of engagement. Moreover, many of our technical collectors don't have sufficiently precise information to serve as "laser designators" for precision-guided munitions. Collectors that go after crowd influences and moods won't be precise either. Army planners need to acknowledge these shortfalls to ensure that the concept doesn't sound like empty platitudes and that the Army's technologists and materiel developers have a good idea of what they need to develop to put the "p" in precision.

Collaboration. There hasn't been enough thinking on collaboration and how it remains an absolute must for situational understanding. This shortfall of thinking and discussion becomes particularly acute once we get into the digital "tower of Babel" that seems to exist in the joint world. How will the Army's collaborative tools interact with other joint services' collaborative tools? Joint fusion, data integration and interoperability are absolute requirements for operating in a joint collaborative environment. These important elements of collaboration constitute a vexing contextual issue that the Army, indeed the Joint Staff, must address; otherwise, information superiority will remain as it is—without meaning. Army planners need to acknowledge the existence of the digital tower of Babel and set forth the requirements such a concept will require.

The bottom line—information superiority depends on situational understanding. Situational understanding depends on collaboration. Collaboration depends on fusion, data integration and interoperability. Neither information superiority nor situational understanding is possible without standard collaborative tools and their integration into joint operations. Without such an approach, collaborative tools won't work among themselves nor will they interact seamlessly with joint collaborative tools. Army "corporate" thinking needs to depict the absolute requirement for integration with joint standards or suggest the need for a common interface/software package that accommodates the myriad collaborative tools floating around in the joint arena.

Communications. Of key importance, this force will need good communications. Army planners, though, make too many assumptions about having assured communications with bandwidth sufficient to collaborate, accomplish telemedicine, perform logistics, correlate information, and visualize to the extent modern operations require. This issue also relates to the lack of infrastructure constraint mentioned earlier. Additionally, it relates to our proclivity to always desire more bandwidth and develop more "bandwidth-hogging" software, as we strive to find the right technical and intellectual conditions for achieving information superiority. The farther away U.S. forces are from the continental United States, the more fragile communications threads become. If communications threads incur perturbation, other threads of support experience volatility as well, as they all relate in one way or another. This is an important issue for footprint reduction and information assurance.

Army planners need to put forth some creative thinking about satellite surrogates, balloons, wireless communications, mobile routers, and use of UAVs for continuous communications support. Satellite surrogates, for example, must connect to an Internet gateway and be capable of staying connected to websites in cyberspace. Even then, there is no such thing as assured communications—too much can go wrong mechanically and environmentally to assume that Army leaders can always plan on assured communications paths with the bandwidth they need. Thus, the Army has to simulate and practice this environmental influence realistically and frequently.

Footprint reduction and technology. The IBCT concept justifiably puts forth the need for footprint reduction owing to operational constraints, lift requirements, and time standards for deployment. This wonderful concept must continue to argue for an austere footprint regardless of institutional pressures arguing contrary. Austerity, however, implies risk—some risks will be present to shrink the footprint sufficiently small to meet rapid mobility requirements. Reachback is a great concept—one that the Army and its concept writers are correct in and must pursue.

Reachback means, however, that the brigade must have more in enclave and less forward. The IBCT intelligence package offers an example that revolves around two notions. First, this brigade will require higher-level thinking in any conceivable scenario of employment. No one, when cold, tired, hungry and afraid, can perform the analysis and synthesis required by future environments. This type of mental work has to be done in enclave where soldiers can think in an environment conducive for thinking, thereby enabling them to think at a higher level than simple IPB requires. Synthesis and holistic thinking and planning are very demanding, but they represent exactly the type of thinking this brigade will require in any conceivable situation. If a heavy analyst team accompanies the commander to the objective area, it is possible that analysts either won't have sufficient expertise or will be mentally engaged with things/activities other than concentrating on the fine-grained analysis and synthesis fueled by country expertise required by the commander. Reachback can leverage analysts assigned to other organizations—such a strategy multiplies commanders' analytic capabilities and brings to bear potentially thousands of minds connecting around the earth via the Internet to work problem sets.

Commanders must be comfortable with analytic support from enclave, and the IBCT and Objective Force concepts need to state this idea in simple, plain terms. Yes, a small amount of analytic support needs to be with the commander to act as an interface and a medium for him to state his information requirements. But the primary functions of fusion, integration and thinking need to be in a relatively benign environment. A deployed IBCT or Objective Force will come to rely on remote joint and Army analytic elements and a smaller footprint.

Training and education. The Army needs to focus its modeling and simulation efforts to replicate the environment soldiers face in future competition. In particular, given that the Army operates in urban terrain, modeling and simulation must depict an environment far different from the typical force-on-force operations that simulations currently represent. The Army must simulate an urban environment, crowds, intelligence collection, IO, communications, fire control, logistics, engineering and air defense in the confines of cities. The Army can draw from experiences of other urban combat situations—Stalingrad, Berlin, Hue, Mogadishu and Panama. But it needs to model asymmetric foes armed with computers, cellular phones, access to the Internet, personal digital assistants, weapons of mass destruction, and lethal, high-tech weapons. Until the Army puts this type of modeling and simulation into its training regimen for the Army officer corps, most of the Army will continue to think about, buy equipment for, and train for the last war instead of preparing for future conflicts.

Development of intellects. The Army's soldiers will operate in a very complex environment characterized by small, decentralized units, movement of information relevant to the situation at hand, nonlinear operations, asymmetric threats, and C^4ISR architectures whose complexities and hidden relationships overwhelm any ordinary mind. Additionally, soldiers will have to maintain their traditional skills owing to the need to engage periodically in kinetic, force-on-force operations. Thus they will need minds sufficiently enlightened to perform traditional intelligence preparation of the battlefield (IPB) along with nontraditional intelligence preparation of cyberspace (IPC). IPC demands people highly capable in technology, information theory and relational thinking along with the traditional leadership capabilities for which the Army has been renowned over the years.

Future leaders have to be comfortable with a dramatically different operational environment in which their units operate in a decentralized, nonlinear way. In this environment, they will make decisions in fluid situations changing literally with the speed of light. Their asymmetric foes will leverage cyberdeception, computer attacks, and PSYOPs aimed at soldiers, their families and the American populace writ large.

The Army must develop purposefully its training and education system to produce minds capable of engaging in this type of competition. For example, the Army needs to analyze its institutional schools and ensure all officer course curricula link and these courses become progressively more difficult, thereby enhancing higher-level thinking skills. Additionally, the Army needs to develop and incorporate realistic simulations to replicate the environment described above. Reading lists should be a combination of traditional value books along with books about the Internet age—commerce, decisionmaking, "dot.com" development and modus operandi, chaos and complexity theory, and books about the future.

Information Superiority Proving Ground. The Army needs an Information Superiority Proving Ground to improve the intellects of its officers for competing in the environment described previously and to determine what information superiority is, and how to seek, achieve and sustain it. Such a proving ground would encompass five major elements. First, this proving ground would be a place for materiel developers to test and evaluate information warfare weapons. Second, the proving ground would be a place where the Army could develop its centers for making decisions (call them information advantage centers, or IACs) and help officers learn how to use new technology to make fast decisions in fluid, nonlinear and information-laden environments. Third, commanders and their staffs would fall in on the IACs and participate in an information superiority battle command training program. They would find themselves engulfed by an environment in which simulations and modeling, driven by National Lab supercomputers, would provide total immersion in situations they will face in invisible struggles of the future—asymmetric conflict, information warfare-dominated environments, weapons of mass destruction, and information warfare (IW) weapons. Fourth, the proving ground would be a place to conduct true experiments the Army needs to determine requirements for seeking, attaining and sustaining information superiority. Fifth, the proving ground would provide a place to evaluate information operations and information superiority doctrine—to determine appropriateness, validity, fragility, and capability to integrate with Army operations writ large.

Recommendations

Information Centers of Gravity (Info-COGs): Cope with a changed environment and deal with Info-COGs along with more traditional Centers of Gravity. Such adjustment will be easy to accomplish, will set the right tenor for evolution of conceptual thinking, and will be suggestive for the "tribal wisdom" of the Army, as it shifts from the current DTLOMS focus to one more attuned to vagaries of the information age.

Information superiority: Carefully define information superiority but also acknowledge the presence of adapting, learning organisms that constitute our future foes. This type of foe and associated technological challenges that become even more complex in the joint world demand that the Army acknowledge the temporary nature of any advantage in the information world. The forces at work in the Army's future competitive environments will cause information superiority to be a short-lived phenomenon, at best.

Focus collection: Cause the Army and joint intelligence communities to focus on future customers in environments the Army faces in future competition. Push a coherent research and development program on *all* materiel developers and labs to produce collectors that will satisfy information requirements of a kinetic conflict, an asymmetric competition, or a combination of the two. Engage commanders and their staffs in sophisticated simulations that account for the intangible, invisible, nuance-laden world of IO and other asymmetric tools.

Information operations: Acknowledge the importance of IO as it affects the operational area and, through the threads leading back to the continental United States, information management facilities, ports and factories that manufacture critical "just-in-time" parts. Recognize the importance of key knowledge workers and take steps to protect them, thereby reducing this potentially, exploitable vulnerability. The concept, in any final analysis, must make the leap from “what is” today to “what could very well be” in the future. Without such acknowledgement, we are in grave danger of surprise and risk of failure.

Asymmetric strategies: In all concept papers, expand the discussion of and references to asymmetric competition as a strategy of choice for weaker competitors hoping to compete with the United States in the future. Discuss asymmetric competition as a strategy and specific asymmetric threats, (e.g., IO, WMD, attack or manipulation of purveyor of knowledge) in the concept papers. Recognize the pervasiveness, subtleties, relationships and nuances involved in these struggles.

Joint roles/missions and synergy: Think through joint roles and missions relating to the IBCT and Objective Force. The Army will not and cannot operate alone. Thus, thinking behind the IBCT and Objective Force needs to *treat joint operations as an embedded phenomenon*, not as something separate that people call for only when needed. Without this change, materiel developers, trainers and doctrine writers will perpetuate the dearth of joint thinking and references, when they should be emphasizing jointness.

Limits of technology: Rephrase verbiage in IBCT and Objective Force concept papers concerning a “near-complete” common operating procedure. Acknowledge aspects of technology and variables that have to come together and coalesce before any useful COP can come into being. Also, acknowledge reality—the very best COP will provide only a partial view of reality. *The art of battle command, wisdom of the commander, and collective intellects of subordinates tied through collaboration must coalesce to have the best, partial understanding of the battlespace*. We have to remember that soldiers on the ground need access to their relevant information, and commanders need a robust, visualization- and collaboration-dominated COP to lead in an environment requiring clear intent and decentralized execution.

Communications: Ponder and detail the brigade’s communication requirements in an infrastructure-barren operational environment. To seek, find and sustain information superiority, the IBCT and Objective Force must possess good communications paths and bandwidth sufficient to perform their roles and missions. Again, the Army needs to borrow ideas from other services (e.g., Network-Centric Warfare) and from industry (wireless, broadband, storage area networks, application server providers, Internet appliances) to prepare for the operational environment of the 21st century. In this analysis, operators, intelligence people, signal people and logisticians (the biggest users of bandwidth) need to articulate their needs and war-game possibilities to provide adequate communications to support forces in the environment discussed throughout this paper. Discuss variables and their effect on information availability; moreover, plan for failure of primary and secondary paths and acknowledge the need for fast switching along designed alternative routes of information flow.

Collaboration: Expand the discussion of a need for collaboration and explain in detail its direct links with situational understanding and information superiority. Emphasize the absolute imperative for collaborating within the construct of joint task forces—fusion, data integration, interoperability. All collaboration work being done by materiel developers and labs must focus on collaboration within the Army, with other services, and with the entire joint community. Purposefully design a system *transforming data to information to knowledge,* thereby helping commanders achieve wisdom. Collaboration is a key in this transformation process. Collaboration and the art of battle command must occupy a preeminent position in officer training and education of the future. This requirement will exist until computers become smarter than human beings.

Collection: Planners need to articulate their information requirements so the Army and joint intelligence communities can direct their resources to satisfy those needs. If the thinking behind the IBCT and Objective Force continues to emphasize kinetic, force-on-force encounters and ignore asymmetric competition in urban areas, collection will remain oriented on attrition, movement and battle damage assessment. Army planners need to change wording in conceptual documents to acknowledge shortfalls of collection and recognize that stringent requirements for precision will often run counter to just as stringent requirements levied by limitations on collateral damage and rules of engagement.

Reachback: Place more emphasis on clearly articulated enclave functions, capabilities and limitations. Additionally, concept writers need to think about and articulate broad vision thrust points for leveraging the joint intelligence collection system, wireless communications for communicating on the move (whether dismounted or mounted), flexible bandwidth, alternative routes for moving information, and leveraging innovative techniques and procedures for processing, visualizing and communicating. Borrow and experiment with concepts and practices from the commercial world. For example, Army planners need to consider adopting very fast data and information storage inherent to storage area networks (SANs). To reduce weight and transport, the Army again needs to consider borrowing from commercial businesses to provide the conceptual framework for developing Army/joint specific Internet appliances, and rely on application server providers (ASPs) to put much of our data storage and applications in cyberspace, thereby allowing access anytime from anywhere. Additionally, the Army needs true skeletal support forward with the warfighters. In this respect, the Army needs to leverage all of the mental capabilities available on the ground and in cyberspace and focus them on solving the problem at hand.

Information Superiority Proving Ground: Consider the viability of establishing an Information Superiority Proving Ground. In such a proving ground, the Army needs to develop a holistic program for an IO battle command training program; test and evaluate IO weapons against command and control equipment; develop operations centers of the future (information advantage centers); conduct experimentation with functions, forms and equipment that enable information superiority; and conduct an IO doctrinal validation process.

Training and education: Redesign the training and education system for all officers. Create coherency and relationship among the curricula of officer basic, officer advanced, the Command and General Staff College, and the Army War College. Purposefully develop intellects sufficient to become true information warriors fully capable of enacting force-on-force operations and also engaging in asymmetric competition and in information-age struggles for information superiority. Use simulation and modeling to facilitate intellectual development sufficient to understand the power of joint synergy. Simulation and modeling must include kinetic energy force on force and invisible, digital struggles characterizing asymmetric warfare and information operations. Develop in our officers the mental agility to jump rapidly between the two poles of operations, to be adaptive and creative, and to use a holistic, synthesis-laden approach to thinking and planning.[3]

Conclusions

The Army has performed marvelously and accomplished some far-reaching goals over the past few years. None are more important and far-reaching than the dual notions of an Interim Brigade Combat Team (IBCT) and the Objective Force.

With progress, though, comes room for expanding concepts and ideas to include a greater concentration on competing in urban areas and expanding thinking about attendant battlefield operating systems. The Army must first learn to assess the ever-changing *environmental context* in which it will operate. This context needs to be representative of "what is" or "what could be," not "what the Army would like it to be." Moreover, the Army needs to recognize the rise of *asymmetric competition* in which opponents engage in a wide variety of activities to gain offset against our force-on-force and technical prowess. Much of this adjustment must occur in the murky, invisible, digital context of information operations that literally affect every aspect of future Army operations. Continuing with this line of thinking, the Army must think through how it will *operate in urban terrain* in an operational context that could be characterized by humanitarian relief, episodic violence against unconventional enemies and forces, and conventional operations outside of the urban terrain. This wide range of environments requires agile intellects, holistic planning in which relationships are preeminent, inter-operable equipment, and speedy access to specific and relevant information processed, presented and visualized the way individuals think, not how a normed group thinks.

Intelligence collection sensors of the future must be robotic, miniature, stealthy, multisource collectors, innovative transmitters or purveyors of useful information. Designers and system architects must depict swarm, multisource, interrelated, nested webs of collectors in collection and communication architectures. This type of collection activity needs replicating in synthetic environments of war-gaming and simulation so commanders and staffs can better understand the challenges of the urban terrain collection environment. The Army's leaders have to remember that just because a sensor works in the open against moving targets or can take pictures of damaged or destroyed vehicles or intercepts communications among combat vehicles and operations centers doesn't mean these same sensors will provide information sufficient to run competitive operations in cities.

Additionally, the Army's *training and education system* must seek to develop its officers' intellects to learn to cope with the environment and asymmetric threats and to maintain an *intellectual superiority* over foes of the future. Such enlightenment must occur with coherent, related, ascending curricula in institutional learning, at the unit under the tutelage of commanders, and with each individual as he/she engages in distance learning. The Army must immediately change its training system to replicate the environment it faces in the future; leaders and their staffs must develop intellects sufficient to operate in and excel in both environments—the industrial-age force on force *and* the information-age asymmetric, digital struggle.

The Army, in cooperation with the Joint Staff, needs to develop a Virtual IO Analytic Center to help deployed soldiers perform their duties requiring the assistance of country and language experts. The Army needs to write its doctrine and experiment with the concept to ensure that when the IBCT has achieved initial operating capability (IOC) the virtual center is capable of operating as well.

The Army needs to provide distinct guidance and priorities to its research and development labs and their commercial supporters to find the commercial capabilities enabling technological advancements to seek, find, attain and sustain information superiority. *Research and development* needs to constrict and provide maximum financial and intellectual resources on fusion, data integration, joint interoperability, situational awareness, situational understanding, collection, processing, dissemination, and mobile, wireless communications.

Endnotes

1. William Owens, *Lifting the Fog of War* (New York: Farrar, Straus and Giroux, 1999), p. 10.
2. *Joint Vision 2020*, Joint Staff (Washington, D.C.: U.S. Government Printing Office, June 2000), p. 13.
3. BG (Retired) Wayne M. Hall, "Thinking and Planning: Vision 2010," AUSA Landpower Essay Series, AUSA Institute of Land Warfare, No. 98-6, September 1998, p. 13.