The Promise of Persistent Surveillance: What are the Implications for the Common Operating Picture?

A Monograph

by

Major David W. Pendall

United States Army

School of Advanced Military Studies

United States Army Command and General Staff College

Fort Leavenworth, Kansas

AY 04-05

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	052605	Monograph

4. TITLE AND SUBTITLE
The Promise of Persistent Surveillance: What are the Implications for the Common Operating Picture?

5. FUNDING NUMBERS

6. AUTHOR(S)
Major David W. Pendall

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

US Army Command and General Staff College
School of Advanced Military Studies
250 Gibbon Ave.
Fort Leavenworth, KS 66027

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army Command and General Staff College
Fort Leavenworth, KS 66027

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

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

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

The defense and intelligence community initiatives to create persistent surveillance capabilities and enable access to the resultant continuous data streams will create significant change in the joint force and partners operating across the domains of war and the levels of war. The joint force must act in qualitatively different ways in order to deal with current and future full spectrum threats, to include the transnational extremist threat we will face for the coming decades. New operational concepts as envisioned by the United States Joint Forces Command guide service transformations, redefine linkages with other elements of national power, and seek full integration of the joint force with all partners- DoD, non-DoD, and multinational. Intelligence transformation from the Cold War Reconnaissance Paradigm to the Persistence Paradigm creates a qualitatively different type of intelligence support and moves actionable intelligence to the lowest levels of our formations in this new operating construct. This new paradigm will enable U.S. DoD, non-DoD, and coalition forces to act coherently through shared understanding and engage in adaptive planning and dynamic execution, overmatching global adversaries in agility and decision speed. The integrating mechanism for delivering persistent surveillance across all domains and levels of war will be the 21st century Common Operating Picture. Enterprise data, collaborative planning, and networked actions will change the command methods and control structures as we conduct the global war against the dispersed and distributed threat. Embedded decision aids, modeling, and an advanced neural network act as a synthetic brain to empower the lowest levels of our formations and mission partners. The granularization of warfare, enabled by persistent surveillance feeds into the Common Operating Picture, will enable U.S. forces and security system partners to win the decision cycle battle in the 21st Century. These changes will also require new leadership attributes, authorities, and operating values.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Intelligence, Common Operating Picture, Surveillance, Operations	75
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
U	U	U	none

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

Major David W. Pendall

Title of Monograph: The Promise of Persistent Surveillance: What are the Implications for the Common Operating Picture?

Approved by:

_____
Colonel Stefan J. Banach, MMAS — Monograph Director

_____
Kevin C.M. Benson, COL, AR — Director, School of Advanced Military Studies

_____
Robert F. Baumann, Ph.D. — Director, Graduate Degree Programs

Abstract

The Promise of Persistent Surveillance: What are the Implications for the Common Operating Picture?, by Major David W. Pendall, 76 pages

The defense and intelligence community initiatives to create persistent surveillance capabilities and enable access to the resultant continuous data streams will create significant change in the joint force and partners operating across the domains of war and the levels of war. The joint force must act in qualitatively different ways in order to deal with current and future full spectrum threats, to include the transnational extremist threat we will face for the coming decades.

New operational concepts as envisioned by the United States Joint Forces Command guide service transformations, redefine linkages with other elements of national power, and seek full integration of the joint force with all partners- DoD, non-DoD, and multinational. Intelligence transformation from the Cold War Reconnaissance Paradigm to the Persistence Paradigm creates a qualitatively different type of intelligence support and moves actionable intelligence to the lowest levels of our formations in this new operating construct. This new paradigm will enable U.S. DoD, non-DoD, and coalition forces to act coherently through shared understanding and engage in adaptive planning and dynamic execution, overmatching global adversaries in agility and decision speed.

The integrating mechanism for delivering persistent surveillance across all domains and levels of war will be the 21st century Common Operating Picture. Enterprise data, collaborative planning, and networked actions will change the command methods and control structures as we conduct the global war against the dispersed and distributed threat. Embedded decision aids, modeling, and an advanced neural network act as a synthetic brain to empower the lowest levels of our formations and mission partners. The granularization of warfare, enabled by persistent surveillance feeds into the Common Operating Picture, will enable U.S. forces and security system partners to win the decision cycle battle in the 21st Century. These changes will also require new leadership attributes, authorities, and operating values.

TABLE OF CONTENTS

LIST OF FIGURES

Introduction

The idea of Persistent Surveillance as a transformational capability has circulated within the national Intelligence Community (IC) and the Department of Defense (DoD) for at least three years.[1] Persistent Surveillance- also described as "Persistent ISR," "Persistent Stare," "Pervasive Knowledge of the Adversary,"- is an often-used term to describe the need for, and application of, future Intelligence Surveillance and Reconnaissance (ISR) capabilities to transform intelligence support qualitatively to operational and tactical commands.[2] The idea surfaces in many forms, including defense program reviews and Congressional testimony.[3] Each expression promotes a vision of a system achieving near perfect knowledge and the removal of uncertainty in war.

Persistence means that once global, theater, or local reconnaissance has found something of intelligence or actionable interest, ISR systems- including processing and dissemination systems- will maintain a constant, enduring contact with the target, thus increasing the level of understanding about the target, enabling a faster decision cycle at all levels of command, and support the application of precision force to achieve desired effects.

Persistent Surveillance integrates the human component and various technologies and processes across formerly stove piped domains. It is not a permanent stare from space or from airborne imagery platforms. In essence, the targeted entity will be unable to move, hide, disperse, deceive, or otherwise break contact with the focused intelligence system. Once achieved,

---

[1] "Transformation Study Report: Transforming Military Operational Capabilities," Executive Summary, *Office of the Secretary of Defense*, 2001, 2.

[2] For the purposes of this monograph, descriptive terms such as persistent or pervasive are considered to mean the same basic operational capability. Lieutenant General (LTG) James M. Dubik (former J9 for U.S. Joint Forces Command (JFCOM) and current I Corps Commander) described the concept of pervasive knowledge during a lecture on October 04, 2004 to the U.S. Army School of Advanced Military Studies (SAMS). The concept is consistent with the national and DoD intelligence community concept of Persistent Surveillance.

[3] Donald H. Rumsfeld, "Quadrennial Defense Review Report," *Office of the Secretary of Defense.* 2001, 30. See also Dr. Stephen A. Cambone, "Statement of Dr. Stephen A. Cambone, Under Secretary of Defense for Intelligence, before the Senate Armed Services Committee, Strategic Forces Subcommittee, Intelligence, Surveillance and Reconnaissance," *Office of the Under Secretary of Defense- Intelligence.* April 7, 2004, 4.

"persistent" ISR coverage will, in theory, deny the adversary sanctuary, enabling coherent decision-making and action, to include rapid combat operations, with reduced risk to friendly forces.

Problem and Significance

The problem addressed in this monograph is to identify implications of a persistent surveillance capability upon the joint force's Common Operating Picture (COP). The significance of persistent surveillance is directly related to the qualitative changes likely to result from this integration.[4] How we act is determined by what we know or what we believe to be true.

The audience for this study consists of operational and tactical level commanders of the joint force, allies, force development designers, and leaders within intelligence organizations from the national to tactical level. The study provides insight on the impact of qualitatively different intelligence support available to commands at the lowest levels of our formations and how actions taken may be different as well. The conclusions of this monograph will present the implications of persistent surveillance to commanders and senior leaders as opportunities for change.

Need for the Study

Persistent surveillance, as described, does not exist today. Persistent surveillance is a concept, albeit a promising one.[5] The promise of a persistent ISR system creates transformational conditions for acting against the adversary within the battlespace. Whether "near perfect" knowledge is possible across battlespaces composed of multi-dimensional and multi-variant actors remains largely a contextual and situational question. Even so, persistent surveillance will

[4] As a point of clarification, the integration of persistent surveillance feeds directly into the COP is considered from the practical and functional sense, rather than the technical sense. The COP view provided on current battle command systems such as Global Command and Control System (GCCS), Command Post of the Future (CPOF) and Force XXI Command Brigade and Below (FBCB2) are separate information architectures and systems than the Distributed Common Ground System (DCGS) architecture likely to distribute persistent surveillance data. In the future, the systems should merge under a single system integrated in the Global Information Grid (GIG).

[5] Even so, for readability I will use the present tense describing persistent surveillance.

increase knowledge and improve the speed to which this knowledge is shared and understood at all levels of command, provided the system is developed in a holistic manner that addresses the human, organizational and technological aspects of the strategy.

Persistent surveillance represents a qualitative change in the content and delivery of intelligence to operational and tactical levels of war. This change should increase the speed of the decision-making process across all battle space domains and at all levels of conflict or war. [6] It should also increase the range of options the joint force and our partners have in applying force, both kinetic and non-kinetic.

The Future Operating Environment and Conditions

The United States Joint Forces Command (USJFCOM) document *Major Combat Operations-Joint Operating Concept* (MCO JOC) gets to the point when describing the emerging and future environment:

> Gone are the days when we were relatively sure we should prepare to fight a largely symmetric conventional war, in a defined set of theaters with improved infrastructures, against a doctrinally "template-able" enemy, with fixed alliances, for predetermined political aims. We cannot forecast the type war we will fight, against whom, with whom, where, or for what aims. Our adversaries have adapted and will continue to do so.[7]

Adding to this description, the Chief of Staff of the Army describes the protracted conflict the US faces today:

> The Nation is decisively engaged in a war fought against global terrorist networks…Of primary importance, we must understand the character of the irregular warfare we now face and adapt accordingly…we have arrayed a vast, hierarchical organization against an elusive, adaptive network…to be effective the Army must adapt-and eliminate irrelevant policies, processes, and doctrines. We must move beyond marginal improvements…[8]

---

[6] The battle space includes three competitive domains. There is a physical domain, an informational domain, and a cognitive domain. These domains are also distributed among the three levels of War- Strategic, Operational, and Tactical. See David S. Alberts and others, *Understanding Information Age Warfare* (Washington, D.C.: Command and Control Research Program, 2001), 10-15.

[7] Office of the Chairman of the Joint Chiefs of Staff, *Major Combat Operations-Joint Operating Concept* [MCO-JOC] (Washington, D.C., September 09, 2004), 4.

[8] Office of the Chief of Staff of the Army, "A Game Plan for Advancing Army Objectives in FY05 and Beyond: Thinking Strategically," *Department of the Army*, 2004, 1.

Even with a future operating environment characterized by uncertainty, the overall effect persistent surveillance is envisioned to provide is captured in the following passage:

> A pervasive knowledge capability is the first step in creating the sense of futility and impunity in the mind of our adversary…**this pervasive knowledge system creates the impression that we can "observe" even an adversary's very intent. The adversary, aware of this system, is constantly looking over his shoulder, sure he is being watched, followed, tracked, and heard** [emphasis added]. This is not to say that we will be all knowing. The complexity of warfare will still involve uncertainty and conditions where we will have to fight with incomplete information.[9]

As incredible as this may seem, to create a pervasive knowledge system, the demand placed on the humans, technologies, and organizations by designers of the joint force to achieve future operating capabilities seems just as incredible. The *Joint Operating Concept* (JOpsC) states that the concept of Full Spectrum Dominance "is based on the ability to sense, understand, decide, and act faster than any adversary in any situation... emphasizes adaptability, balances capabilities and manages risk within a **global perspective** [emphasis added]."[10] Adding further,

> The central theme of the MCO JOC is to achieve decisive conclusions to combat; use a joint, interdependent force that swiftly applies overmatching power simultaneously and sequentially, in a set of contiguous and noncontiguous operations; employ joint power at all points of action…and create in the mind of our enemy an asynchronous perception of our actions—all to compel the enemy to accede to our will. [11]

> Framed within this approach…an evolving security environment background, a new battlespace perspective emerges for future military operations…globally and operationally distributed…the joint force will be able to apply continuous pressure on an adversary, control the tempo of operation…develop and exploit opportunities faster than the adversary can adapt. This continuum of action will require decentralized execution, where joint capabilities are organized and interdependently applied at increasingly lower echelons.[12]

Continuous pressure, controlled operational tempo and an exploitation mindset are hallmarks of this approach, fueled by increased access to battlespace knowledge and an increased depth of

---

[9] MCO JOC. 17.

[10] Office of the Chairman of the Joint Chiefs of Staff, *Joint Operations Concept* [JOpsC] (Washington, D.C., October 03, 2003), 10. This document is fully endorsed by Joint Chiefs of Staff (JCS) and Joint Requirements Oversight Council (JROC) to drive joint service capability integration.

[11] Ibid., 10. As described in the document's note, "Asynchronous, in this context, refers to our desire to create an indiscernible pattern in time and space in the mind of our enemy. Our operations, however, must retain unity of purpose and coherency of action."

[12] Ibid.

understanding. Coherently nested actions must be taken not just against point targets or discreet sets of targets, but against complex interrelationships of enemy actors, neutrals, and component adaptive systems across a global framework. In recognition of co-evolving sets of internal and external security relationships within a given battlespace for a specific commander, the MCO JOC further explains the enabling attributes and underlying premises:

> These decisive conclusions are enabled by the fluid and coherent application of joint military action in conjunction with interagency and coalition power, using an effects-based approach and **leveraging pervasive knowledge in a networked environment to increase levels of collaboration, precision, unity of purpose and coherency in action** [emphasis added] [13]…these enablers help us move from today's paradigm of applying overwhelming force to applying overmatching power, from deconflicting actions to coherent actions, from mostly sequential to more simultaneous operations, from primarily contiguous to more noncontiguous operations, from reacting to pro-acting, and from being joint only at the operational level to becoming joint at the point of action.[14] Additionally, a profound shift in our warfighting concepts occurs when the US aligns and synchronizes deployment, employment, and sustainment activities to conduct **multiple, simultaneous, distributed, decentralized battles and campaigns** [emphasis added].[15]

This common view of the need for persistent surveillance is clear in joint and Army future concepts. The qualitative change demanded by the future operating constructs co-evolves and leverages the ongoing transformation of intelligence, or "Revolution in Intelligence Affairs."[16]

Transforming the Qualities of Intelligence

Persistent surveillance matters because of the conditions it may create. A large part of the promise is "to gain deeper understanding of the adversary and all his complexity."[17] The current ISR system as a whole is not agile enough, persistent enough, nor integrated enough to support

---

[13] Fluidity, in this context, is the ability to readily adapt, shift forces, and redirect operations; the ability to seek out, create, and exploit opportunities and adversary vulnerabilities; and the ability to engage, or appear to engage, an adversary in every dimension, relentlessly, irrespective of his efforts to disengage or to seek advantage. It is analogous to the tendency of fluid to adapt to the shape of any vessel that contains it; to pour through any crack, hole, or gap; and to engulf any object that is immersed in it. It is the manifestation of the emergent behaviors of adaptability and opportunism. [Original JOC MCO footnote]

[14] "Joint at the point of action" refers to being able to apply the power of any element of the joint force at any point of action the joint commander directs. [Original MCO JOC footnote]

[15] MCO JOC, 11-12.

[16] Vice Admiral Lowell Jacoby, "Revolution in Intelligence Affairs," Presentation, *Armed Forces Communications Association, Spring Intelligence Symposium (AFCEA)*, Langley, VA, April 22, 2004.

[17] Vice Admiral (VADM) Lowell Jacoby, Director, Defense Intelligence Agency, interview by author, Pentagon, Washington D.C., October 06, 2004.

rapid shifts in execution except for the narrow range of sensors that support sensor-shooter linkages.[18] The United States requires significant changes from the "AS IS" intelligence system to the "TO BE" system capable of achieving persistent surveillance. That said, a capability to generate understanding to the depth required for full dimensional understanding in effects based operational constructs remains limited by the ISR Paradigm.

Louis Andre, former Special Forces officer during the Vietnam conflict and now the Chief of Staff for the Defense Intelligence Agency (DIA), challenged the current thinking about intelligence in this way: "What is impossible today to do in your business? But if it could be done, how would it fundamentally change what you do?"[19] Mr. Andre credited this challenge to another- Joel Barker, who was speaking about the nature of "Paradigm Shift."

A paradigm shift occurs when there is a consensus recognition that the current rule sets governing organizational behaviors and strategies for competition in a given environment no longer match emerging requirements in the environment. You go back to zero, where the old rule sets guarantee nothing for your future success. Old successes create cognitive blindness to new challenges and opportunities.[20]

The French fell victim to this blindness during the interwar period when they failed to see new patterns of warfare emerging in the further development of tank and mobile warfare capabilities in the German and Russian Armies. They tried to perfect their past conceptions of war through the construction of the ill-fated Maginot line along with a large reserve based infantry and

---

[18] Carol A. Thompson, "ISR Management to Optimally Satisfy Warfighter Information Requirements," Presentation, *Defense Advanced Research Projects Agency, Tactical Technology Office*.

[19] Mr. Louis Andre, Chief of Staff, Defense Intelligence Agency, interview by author, Pentagon, Washington D.C., October 06, 2004.

[20] Joel Barker, *Future Edge: Discovering the New Paradigms of Success* (New York: William Morrow and Co., Inc., 1992). T.S. Kuhn pioneered the recognition of a dramatic "new idea," an unprecedented break from past orientations, where previous paradigms were unable to explain current phenomenon. This results in a "scientific revolution," ushering in radically new conceptualizations of the phenomena, resulting in major shifts within research strategies to find new solutions to newly recognized problems, rather than discounting new problems merely as "anomalies" or attempting to fit the new problems into old scientific theory constructs. This is known as the Kuhn Paradigm. See Paul Davidson Reynolds, *A Primer in Theory Construction* (Boston: Allyn and Bacon, 1971), 21-22.

artillery defense strategy.[21] The world knows the consequence of that failure. The Swiss, who were the worlds leading watch maker in 1968 with 80% of the international market, invented the quartz movement but failed to adopt it because it didn't fit their conception of what a watch should be; the Japanese nearly destroyed them with the digital watch design. The Swiss now control only 10% of today's market.[22] International Business Machines (IBM), when faced with the introduction of the microchip, focused solely on the potential application to its mainframe business and largely ignored the potential of the PC (Personal Computer) market. They did not recover for two decades.[23] And so it goes.

In a preliminary assessment to Congress about Intelligence, Surveillance, and Reconnaissance and Military Transformation, Judy Chizek states "Operationally, some degree of transformation appears to have occurred as shown by the successful integration of Navy ISR assets, particularly the P-3 and space assets, with Air Force assets to produce persistent surveillance and a common operating picture of the battlefield for all services' combat assets operating in Afghanistan."[24] While this explanation of persistence is necessary, it remains insufficient to reach the depth of understanding required for the globally distributed operating concepts described by the JOpsCs and the Army. It is, however, a *re*-cognition of surveillance and a starting point for continued systemic integration and reassessment of the ISR paradigm. The MCO JOC describes the demands for ISR transformation in this way:

> The ability to predict, to understand intention based on patterns, observed behavior, written or observed doctrine, and basic battlespace forensics – **all require a change in our habits concerning the distribution of peacetime ISR assets** [emphasis added]. ISR must relentlessly focus on the most serious emerging threats worldwide with increased concentration as hostilities evolve. Thus, when hostilities begin, ISR will have produced the advantage of knowledge through

[21] Robert Allen Doughty, *The Breaking Point: Sedan and the Fall of France, 1940* (New Haven, CT: Archon Books, 1990).

[22] Barker, 15-18.

[23] Ibid., 141-144.

[24] Congressional Research Service, Military Transformation: Current Issues in Intelligence, Surveillance, and Reconnaissance, Report prepared by Judy G. Chizek, (Washington, D.C.: Congressional Research Service, 2003, 20.

prediction rather than having to develop knowledge through pure discovery in the course of battle or hostilities.[25]

Old Logic and the Reconnaissance Paradigm

The current set of logic driving most service and joint ISR operations is a continuation of the Cold War Reconnaissance Paradigm- one of periodic, linear snapshots and sampling.[26] The logic of the processes and systemic rules reflect the adaptations and co-evolutions of the past and increasingly demonstrate inadequacies for reaching the adaptations and co-evolutions required for the future.[27] Past investments created the specialized technical systems and human interfaces we have today, which developed predominantly to orient on Cold War adversaries. These systems were designed to detect and characterize large military force signatures. Because of mirrored views of conflict, assumptions formed about conventional formations of Cold War enemies- that they would be easy to find, yet remain hard to kill. The U.S. placed a proportionally small amount of investments in ISR systems and a greater amount in killing systems.[28] Killing required the production of massed force and the ability to engage multiple, massed formations arrayed throughout the depth of the battlefield. As envisioned, ISR supported efforts would decrease the rate of enemy force flow through predetermined engagement zones in order to produce local superiority in killing platforms against a massed, regionally distributed enemy. A corollary rule

---

[25] MCO JOC, 17.

[26] Dr. Cambone, 4.

[27] M. Mitchell Waldrop, *Complexity: The Emerging Science at the Edge of Chaos* (New York: Touchstone Books, 1992), 309. The existence of co-evolution is present in all dynamic systems. It is the adaptation response created when individual actors and clusters of actors change to meet new demands imposed from the environment. Failure to successfully co-evolve with demands from outside influences result in death of the organism. Military history is replete with this phenomenon. The pendulum swings of organizational change and new weapons system developments occurred over time, each successive iteration creates new plateaus to adapt to across the spectrum of warfare. The pace of change varies by level of organization. An infantryman in close combat must adapt and change in real time while new system components and organizational constructs (up-armored HMMWVs, enhanced body armor, and Stryker Brigades) take more time. The real questions become: Are we adapting or mal-adapting and are we changing fast enough?

[28] Michael Nagata, "DoD Intelligence, SOF, and the Global War on Terrorism," Presentation to U.S. Army Command and General Staff College SOF Track, *Office Deputy Undersecretary of Defense for Intelligence and Warning*, December 19, 2003.

in this paradigm is the need to produce overwhelming combat power at distributed, geographic points within a distinctly regional battlefield. Cold War intelligence systems allowed commanders to focus on these points of engagement.

Coverage however, even for "surveillance" assets, remains periodic in this model. Surveillance platforms and supporting processes created a durable yet mass oriented system tied to a "predictable" battlefield framework to engage massed, relatively slow moving enemy forces. "Dwell times" are limited by fuel, maintenance, the environment, aperture setting, human endurance, and targets that do not cooperate or remain within established coverage areas. As war and security requirements shift to compete against an increasingly granular enemy drawing on global and commercial systems and infrastructures, the current ISR construct limits the pace in which the security system can respond and adapt successfully. In other words, ISR is not prepared to cope with the local and global agility of empowered individuals or small groups.

Binary views of the "battlefield" are also a major component of this paradigm: us and the enemy. Most collection systems, particularly technical collection systems, support collection on military targets and related signatures. Military intelligence is military intelligence. Commercial systems and "neutral" populations had often gone unobserved, by design.[29] The binary approach, stemming from our conventional framework of war, created cognitive and systemic blindness to important elements of the larger battlespace and our national security.[30]

---

[29] As U.S. Air Force Lieutenant General (Lt. Gen.) Michael V. Hayden, Director of the National Security Agency (NSA) observed, "Twenty years ago, how many people outside of government or research used a computer—much less had one at home? Forty years ago there were 5,000 stand-alone computers, no fax machines and not one cellular phone. Today, there are over 180 million computers -- most of them networked. There are roughly 14 million fax machines and 40 million cell phones and those numbers continue to grow. The telecommunications industry is making a $1 trillion investment to encircle the world in millions of miles of high bandwidth fiber-optic cable. They are aggressively investing in the future. As private enterprise transitioned from the Industrial Age to the Information Age, so must government. So far, the National Security Agency is lagging behind." Lt. Gen. Michael V. Hayden, USAF, "Address to Kennedy Political Union of American University," *Office of the Director, National Security Agency* February 17, 2000, 2. Lt. Gen. Hayden initiated a transformation of NSA processes and organizational structures in 2000.

[30] Of course some systems and processes were developed to accommodate collection and analytical requirements for "low intensity conflict" and the later term "Military Operations Other than

As the majority of ISR systems developed along service and "INT" specific design paths, the related dissemination systems followed along those same lines. SIGINT systems, for example, from national through tactical levels were designed to operate against a specific enemy emitter and often had sensitivity (antennas and processors) designed to "fit" intended use on the battlefield.[31] Tactical collectors went against tactically deployed enemy systems as national or theater level sensors oriented on target emitters deeper inside the forecasted "linear" battlefield. SIGINT reporting stayed within strict SIGINT channels. Even the HUMINT system divided targets based on the target's position within the adversary's hierarchy and matched reports as they correspond with the organizational level of the related consumer.

The current intelligence process is also a predetermined requirements based system. Once needs are identified through planning and further developed in support of a commander's priorities (Priority Intelligence Requirements), they make their way into a related hierarchical collection management system. Collection management further subdivides by "INT" and aggregates requirements into pools for prioritization and tasking along the hierarchical chain. The rule set for collection and ISR support is governed by the linear and sequential procedure: Task-Process-Exploit-Disseminate. Tasking only occurs once the requirement is "justified" and supported by higher levels of command.[32] This is consistent within a service chain as well as at

---

War," but they remained in the "lesser included and all others category." HUMINT and linguist capability languished, pattern and link analysis only returned to mainstream analysis because of operations in places like Haiti and Bosnia. The ability to do large-scale collection and analysis within commercial and civilian populations and infrastructure remained insufficient. We are now making up for this. See Megan Scully "Social Intel: New Tool For U.S. Military: Intelligence Increasingly Focuses on Relationships Among Individuals," *Defense News*, April 26, 2004, 21.

[31] The artificial and binary views of "tactical" and "national" reflect industrial age, hierarchical and linear thinking. As the levels of war compress, the actor or action is less defined by organization and more by effect achieved, and may be viewed differently by different entities. The "values" assigned as convenient labels are inherently value free.

[32] Of course a dichotomy exists between "Big R" and "little r" requirements. Transitory or temporal requirements, fall into the "little r" bin while an enduring requirement such as "Determine emerging al Qaeda infrastructures" might be a "Big R" requirement and receive new programs investments to close capability gaps.

the joint and national level. Once collection managers input requirements in the form of tasking orders and requests, the tasking is set, and difficult to adjust.

Ground Long Range Surveillance (LRS) is a good example of the lack of agility stemming from strict alignment. During *Operation Iraqi Freedom* (OIF), the V Corps LRS teams, all specially trained infantrymen, "achieved little in return for the risks that they took for them and the effort expended to insert them."[33] Of the 27 potential LRS sites (17 in support of the 3 ID, V Corps Main Effort), V Corps only inserted three teams. The typical planning process for each LRS mission takes 48-72 hours. The collection manager selects LRS coverage areas based on the Corps Commander's Priority Intelligence Requirements (PIR) and his assessment of where the Corps would need the intelligence three to four days into the future. As such, the events unfolded faster than planning and preparation cycles could keep up with, and in a real sense, the LRS teams planned themselves out of the ability to contribute to the mission. "After the initial three insertions, the pace was too fast for anyone to make an educated guess on where the corps would be- and what it would need to know- three to four days out."[34]

Lack of agility does not only apply to LRS. Aerial and space based collection systems may adjust to new reconnaissance or surveillance targets with changes in software based processing, but altering orbit areas or coverage schedules is a completely different matter. Major shifts will only occur with senior leadership decision. In terms of cross-cueing, approval requires multiple organizations and hierarchies of command to authorize reorientation of systems and changes in collection requirements.

Pre-determined requirements made sense in the era of sequential Plan-Then-Execute symmetrical world, where detailed planning- though often a guess from operational and tactical planners about future intelligence needs- drove the collection management process to orient

[33] Gregory Fontenot, E.J. Degan, and David Tohn, *On Point: The United States Army in Operation Iraqi Freedom* (Fort Leavenworth, Kansas: Combat Studies Institute Press, 2004), 162-164.
[34] Ibid., 163.

temporally on anticipated signatures. However, the logic fails to deliver the necessary support to dynamic planning and varied planning horizons. Intelligence must prevent surprise, supporting planning and execution requirements within the dynamic battlespace, at all levels of war, and within each of the domains. Each level and domain has different planning horizons, effects sequencing needs, and effects executors (DoD, non-DoD and non-U.S.). Linear planning and processing models driven by highly structured intelligence need statements are incapable of supporting adaptive planning requirements, which emerge as new conditions unfold in a continuous operations environment.

In the reconnaissance paradigm and related analytical methodologies, anticipated signatures develop from mental and "doctrinal" templates. These models and templates are also the basis for assessments.[35] Filling in missing pieces comes from templates and institutionally oriented understandings of the adversary and historical norms identified through the Cold War intelligence system. If you found the elephant's trunk, you both recognized it as an elephant and could fairly easily determine where the rest of him was. Intelligence assessments are used to fill knowledge gaps. Cold War enemy templates and orders of battle were taught and memorized.

This collection of templates and mental assessment models formed the basis for entire sets of operational plans. Most of the Combat Training Centers and Battle Command Training created Opposing Forces (OPFOR) modeled on projected enemies to reinforce this learning. Deviations from "doctrinal behaviors" were cause for intense controller and commander discussions. During the Cold War period, this was the best way to train and acculturate a large, stable force structure

[35] Anticipating signatures and events enables successful adaptations and is necessary for the survival of dynamic systems; however, the methodology becomes flawed when the anticipation is based primarily on human mental models, doctrinally developed frameworks, and human assessments in the information age. Advanced artificial intelligence tools and working with inference, vice assessments, using large data sets offers alternative methods. Adversarial denial and deception techniques often use the preconceived notions to mask true behaviors, intentions, and capabilities. The Egyptian Army's cross channel attack into Israel in 1973 is an example of the skillful use of Israeli preconceptions, mental models and doctrinal frameworks to achieve surprise. See George W. Gawrych, *The 1973 Arab-Israeli War: The Albatross of Decisive Victory*, Leavenworth Papers Number 21 (Leavenworth, Kansas: Combat Studies Institute, 1996), 20-28.

to anticipate battlefield conditions against our main enemies, ensuring a common language would emerge to facilitate decision and action in a time compressed and de-conflicted battlespace.

A significant event from *Operation Iraqi Freedom* (OIF) serves as an example of flawed assessments and templating. Nearly five brigade sized elements of the Iraqi Republican Guard repositioned just prior to the initiation of the war. A senior ground force commander also relayed another aspect of this event, indicating that the move occurred by small elements, augmented by civilian vehicles, leaving some logistics and artillery in place for deception. "This was not identified by the Intelligence Community."[36] Filling knowledge gaps resulting from reconnaissance and periodic sampling with template based assessments and mental models are insufficient methods for warfare today and in the future. Even with sufficient collection of data, other systemic problems remain.

Horizontally incongruent databases formed because of the INT-centric design process and stove piped "INT" domains. Disparate, nonintegrated data requires interpretation and fusion by humans. All source fusion above tactical levels was difficult; particularly as increased collection capabilities produced huge volumes of data. The volume required filtering even before processing and much of the data never made it into the analytic system. To put the example above about the Republican Guard elements into even more context, Major General John F. Kimmons, J2 for Central Command (CENTCOM) during the war, provides these observations:

> You have to understand this unit was one of CENTCOM's targets, and its movement was completely missed by analysis. We owned the sky [Operation Southern and Northern Watch was ongoing] and had space support. We had repeated, daily coverage on them. Yet, we never had the ability to recognize the change in density and match it to a baseline of data because the collection data resided in non-integrated databases. Thousands of heavy vehicles moved in broad daylight. We just couldn't see it with stove piped data sets; systemic human analyst searches missed it-we didn't have a near real time [machine data search and pattern recognition] capability. We should have had [automated] triggers in place to identify density change and trigger reporting thresholds. A computer could find it [density change] and we could leverage MASINT/EO/Spectral collection

[36] Notes taken during a presentation to SAMS by a senior Army commander speaking on the condition of non-attribution. 2004.

> to compare and confirm. We did not have a baseline or history [digitally stored and easily retrievable] to compare to in this case. People just didn't think about it in this way.[37]

Not only was the data in separate and non-interoperable data sets, successive analysts created serialized reports based on their assessment of the consumers needs, often as reflected in the requirements statement. It led to reporting constrained by user demand and reports formulated to address what an analyst believed the consumer required. If the demand function was inadequate or incomplete, the report often came back inadequate or incomplete. At the analyst level, "data ownership" emerged as a culture and often the release of the "analyst's data" only occurred after an internal review process and the analyst "released it." Latency was cumulative in the system.

Organizational design also hierarchically pairs collection systems with the supported organizations in this rule set. Assets directly support a single, or at best, a few analytical elements that process the collected data before sending finished reports to consumers. Even when multiple consumers would benefit from the reports, or direct feeds, further dissemination is the responsibility of the supported unit. Organic tactical collection supported a single level, or at best, one up and one down in most tactical situations. This could be categorized as "1:1" or "1:few" relationships. Joint Special Operations Command (JSOC) operations in Somalia serves as a clear example of this. Author Mark Bowden, in his book *Black Hawk Down*, provides this perspective about real time surveillance and its inability to directly support elements engaged with Somali irregular forces even though surveillance clearly identified movements and concentrations of forces as the relief convoy proceeded and the battle unfolded:

> Flying about a thousand feet over the C2 helicopter was the navy Orion spy plane, which had surveillance cameras that gave them a clear picture of the convoy's predicament. But the Orion

[37] Major General (MG) John F. Kimmons, Commander, U.S. Army INSCOM, interview by author, Fort Belvoir, VA, August 25, 2004. See also *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, Official Government ed. (Washington, D.C.: U.S. Government Printing Office, 2004), see especially Chapter 8 "*The System was Blinking Red*," 255-277. The inability to share and integrate intelligence, whether due to (perceived) policy or system incompatibility was also a major contributing factor in the failure to prevent al Qaeda terrorists from acting on September 11, 2001.

> pilots were handicapped. They were not allowed to communicate directly with the convoy. There directions were relayed to the commander at the JOC [Joint Operations Center], who would then radio Harrell [Delta Force Squadron Commander] in the command bird. Only then was the plane's advice relayed down to the convoy. This built in a maddening delay.[38]

The current logic also "enslaves" action windows and decision points to the reconnaissance platform timeline.[39] Once a reconnaissance platform cycles through a tasking, commanders had to act while the information is "fresh."[40] Significant change can occur in the battlespace before the next coverage pass on Named Areas of Interest (NAIs). This is as true from satellite reconnaissance through ground patrolling. Gaps in coverage times have to be filled with assessments, often either linear projections based on the template model (doctrinal or situational templates + event templates + time phase lines) or human based fusion of other reports that may or may not match the unfolding reality on the ground.

"Fleeting Targets" or "Time Sensitive Targets" are also products of the reconnaissance platform timeline and static surveillance limitations as much as they are because of the target's own behavior. Action taken against the target depends on the ability to hit the target or create the effect while the target is inside the sensor field of view. Once the target moves outside the field of view, or the reconnaissance platform is unable to continue coverage (local threat increases, aircraft has maintenance or fuel issues, etc.) the opportunity is lost and additional resources must be applied to find the target once again. The larger collection system and reconnaissance paradigm constructs often cannot keep pace or stay in synch to support action. Rather the reconnaissance platform cycles dictates action.[41]

---

[38] Mark Bowden, *Black Hawk Down: A Story of Modern War* (New York: Atlantic Monthly Press, 1999), 112-113.

[39] VADM Jacoby, interview.

[40] Reconnaissance reports normally contain two "time tags", one for time of activity and another indicating the time of report. Sometimes, the two time tags are inadvertently juxtaposed during digital to analog conversion and presentation, usually through human error, or in other cases, reconnaissance reports move separately from any time tags at all, creating even greater user uncertainty about the quality of the information.

[41] VADM Jacoby, interview.

The intelligence system, as a whole, also developed along industrial age organizational network model designs.[42] Process specialization created artificial distinctions in what "intelligence" is and who "does" intelligence, separate from "operations" and who operators "are." The operators receive intelligence and act. Often, no intelligence means no action. Except for cavalry formations and other specialized units designed for reconnaissance, commanders expect the separate intelligence system to provide support to "operations."[43] Another report from OIF also illustrates this paradigm. As the Third Infantry Division began to close on Baghdad, a battalion commander attacked to seize Objective Peach, a key bridge 30 kilometers southwest of Baghdad. The battalion ran headlong into nearly three Iraqi brigades. The objective was key and the unit was not receiving any intelligence from its higher headquarters. The battalion destroyed the Iraqi force and secured the objective.[44] Used as an example of a failure of the intelligence system to provide data to the units who desperately need it, the commander commented "I would argue that I was the intelligence-gathering device for my higher headquarters."[45] Other examples about intelligence never reaching units at the brigade and below level are true, but on balance, these were the exception rather than the rule in OIF. Other reviews of the tactical level intelligence support in OIF paint an entirely different picture.[46] The point here is that

[42] The industrial age model was a hierarchically based network mirroring the information flows to that of the linear, sequential production of goods. Information flows correspond with "command" levels as a means to assert control over subordinate processes.

[43] Nagata, presentation.

[44] Fortunately only eight U.S. soldiers were wounded, none seriously.

[45] David Talbot, "How Technology Failed in Iraq," *Technology Review,* November 2004, 38. The article goes on to review Network Centric Warfare concepts, to include ISR support. The "failure" it describes is a recognized inability to move digital data at the speed and volume required in the twenty-first century to ground forces. This has been described in AARs as the "Digital Divide" and is primarily an indictment of Cold War systems and information backbones in tactical formations. The Digital Divide is a phenomenon of bandwidth inadequacies at the Brigade and Below level.

[46] For a balanced review of the intelligence provided to tactical commanders during "Phase III" of OIF, see Fontenot, Degan and Tohn, 421-422.

commanders expect intelligence to be delivered and do not consider their formations as part of the intelligence system.[47]

New Logic and the Essence of Persistent Surveillance

The essence of persistent surveillance is activity detection in the battle space (activity as characterized as an anomaly or a change against an established baseline), as collected, disseminated and identified through enterprise systems.[48] The recognition of anomalies or change will in turn prompt action from decision makers with the capacity to act. There are three core components of Persistent Surveillance:

> Multi-Mode and Multi-Dimensional continuous collection across all battlespace environments (Sensing).
>
> Near Real Time data and knowledge distribution via Enterprise Systems with tailored, user-defined presentation formats (Delivery)
>
> Horizontal Integration of Data and Advanced, Distributed Analytics (Sense-Making and Understanding)

Persistent surveillance is a component of a broader concept: Network Centric Warfare. This concept demands a process change. Remembering that form follows function, the former linear, sequential process-Task, Process, Exploit, and Disseminate- changes to a networked, distributed user centric process- Task, Post, Process, Use.[49]

---

[47] This can be assessed as a result of fifty-five years of Cold War and Industrial Age imprinting. Prior to the Industrial Age, military forces inherently fought for information as a natural part of combat operations, since separate, robust tactical battlefield intelligence systems did not exist. With the creation and specialization of "military intelligence" units and functions, combat formations perhaps lost this vital orientation.

[48] There is debate about the ability to fully characterize the baseline, meaning the creation of a true change detection system, or a system that provides activity sensing within a given environment, working without an established baseline, but significance is based on inferred behavior patterns as "norms." In either case, sensing detects behaviors, data are dynamically ingested and generate other triggering data, which activate reporting thresholds and are fused into advanced pattern matching and pattern recognition analytic systems. Users receive intelligence in a format sufficient to meet their decision and action requirements.

[49] David S. Alberts and Richard E. Hayes, *Power to the Edge* (Washington, D.C.: Command and Control Research Program, 2003), 82-83.

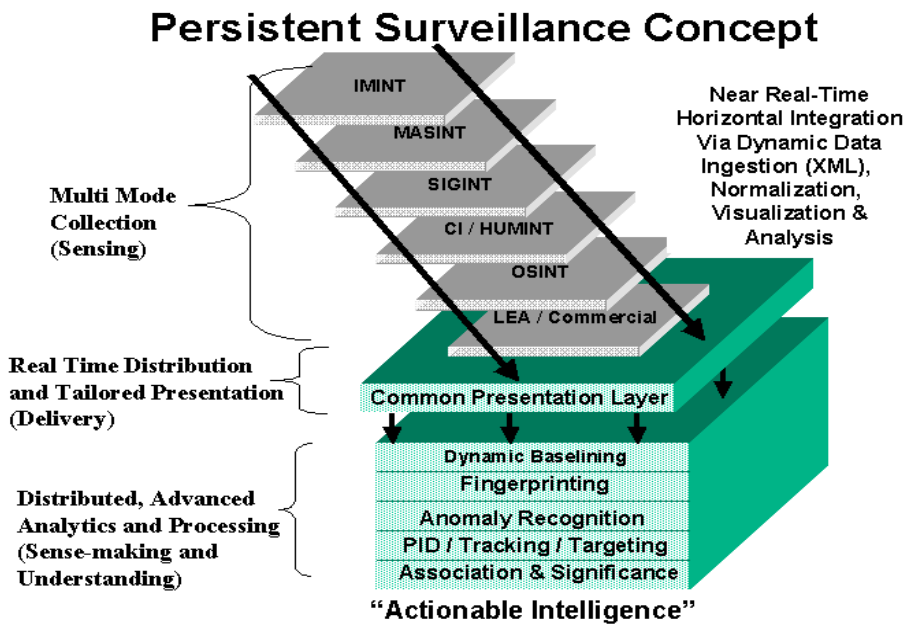

Figure 1. An integrated concept of the core components of persistent surveillance. Processing occurs within Knowledge Advantage Centers. Virtual or "physical" collaboration with analysts or automated processors or preprocessors support edge users with real time intelligence and allow users to access "raw data" or data at the earliest point of consumability. (Concept slide adapted from U.S. Army INSCOM briefing).[50]

Persistent surveillance creates Enterprise (intelligence) Data and Understanding to support an Extended Operational Enterprise. Enterprise Data, Enterprise Systems and Extended Enterprise are Information Management Concepts emerging from the increased capacity of digitized information and distribution networks, namely the World Wide Web, Virtual Private Networks, and Industry Intranets.[51] These concepts allow a simultaneous access and use of enterprise-data generated from internal and external organizational environments, enabling a friendly networked element to leverage knowledge rapidly at the point of competition or interaction with the environment.

[50] MG John F. Kimmons, U.S. Army INSCOM presentation at the Global Intelligence, Surveillance, and Reconnaissance Conference, sponsored by United States Strategic Command (STRATCOM), Denver, Colorado, September 29, 2004.

[51] Laudon, Kenneth C., and Jane P. Laudon, *Management of Information Systems: Managing the Digital Firm*, 7th ed. (Upper Saddle River, NJ: Prentice Hall, 2002), 50-59.

Examples of enterprise systems include mobile, networked sales representatives leveraging dynamic sales and inventory data to make key pricing decisions when negotiating with current or future customers; Air Traffic Controllers collaboratively assessing severe weather patterns on regional airports then making rerouting decisions and impact assessments in near real time; and point of sale transaction systems with above the norm sales levels generating an appropriate supply chain response to ensure shelves are restocked quickly at the local store without requiring unnecessary human intervention, thus reducing latency within the system by alerting suppliers with actionable data.

Many of the difficulties in moving to the intelligence enterprise model, beyond sharing and classification policies, are largely data structure and data mobility problems.[52] As outlined above under old logic, stove piped information systems and non-standard data formats prevented coherent sharing and integrated analysis. Humans have to sort and read through "INT" specific serialized reports and create new "all source" reports, all of which takes time and will likely miss relevant information due to the sheer volume of the task. Much of the data collected never reaches the analyst, much less the end user.

Re-engineered data structures, "Extensible Markup Language (XML) tagging," and data ingestion at the point of collection all work to allow automated processing systems to sort, classify, compare, and detect anomaly from norms and assist the human to gain understanding rapidly, whether the human is an analyst or an end user. Presentation in customized formats allow for improved visualization of data, to include network views of the adversary, streaming video, graphic comparisons and geo-spatially accurate digitized overlays.[53]

[52] MG Kimmons reinforced this point during the interview.

[53] Ibid., summary of the interview with Major General Kimmons, specifically the portion discussing the technical components of the Persistent Surveillance Concept. This summary is consistent with descriptions advanced by John P. Stenbit, former Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD C3I), Dr. Stephen A. Cambone, current Under-Secretary of Defense for Intelligence (USD-I), Vice Admiral Lowell Jacoby, current Director Defense Intelligence

The new rule set firmly acknowledges the requirement to maintain persistent coverage capability against all threats, be they a nation state, non-nation state actor or a trans-national adversary. This represents a capabilities based approach versus the Cold War threat based approach to designing defense systems. It also recognizes the requirement for a capability to wage war and peace at the individual human or "entity level." This re-conception represents a complete systemic transformation from the reconnaissance paradigm that can only generate snapshot views and periodic sampling. Persistent surveillance means longer-term collection on a target to completely understand the problem. This change will provide more data and continuity on a problem to analysts and war fighters.[54]

Just as the ISR logic developed from co-evolution with Cold War adversaries, the new logic represents the paradigm shift occurring after 9/11. It is a purposeful adaptation and recognition of the capabilities and "new rule set" for success against a massively distributed and decentralized global adversary.

Analysis and Synthesis

I have described the essence of persistent surveillance as the continuous process of monitoring and assessing activity and detecting change within the battlespace environment. Persistent surveillance is an emergent capability from the combination of three core components: Sensing, Delivery, and Sense-Making (Understanding). The term *emergent* is chosen for a specific reason, as related to complexity theory.[55]

Agency (DIA), and Lieutenant General Keith B. Alexander, current U.S. Army G2 and others as relayed in journal articles and concept briefings.

[54] VADM Jacoby, interview.

[55] Waldrop, 152. Emergence is a property or condition resulting from component parts but cannot be found to exist within any single part. An eye, or a collection of cones and rods, doesn't "see." Sight is the emergent condition from the complex interaction of the eye, nerves, and brain cells functioning as a system. Complexity theory is the science of emergent behaviors and properties in complex systems.

A review of the core components of persistent surveillance reveals a fundamental change for the intelligence system, adapting to the demands of new security requirements. The new process change overturns the sequential analytic and distribution rules. Higher echelon analysts will *no longer get the data first, but in parallel with users,* including those at the lowest levels of organizations and formations. Analysts will not simply send reports to those *they believe* require the information; rather, the *end user defines the information* required, *on demand* and has the capacity to *create the knowledge directly*. Users will define the information requirements based on *specific decision-making needs and planning horizons.* The creation of serialized reports become of secondary importance, with collaboration and a focus on user real-time support becoming primary. Networking tools connect analysts with other analysts, analysts with end users, and end users with other end users. Because of this network, the creation of physical and virtual communities of interests and communities of practice becomes possible.[56] All entities on the network are supported by a "smart" pull system, with lower level users accessing relevant data in real time, as it is generated.[57] Advanced pre-processing tools support the user immediately in a variety of *user-defined, immediately usable formats.* All of this is done *in parallel to other networked users.*

A persistent surveillance capability will support tighter sensor-shooter linkages and "shorten the kill chain."[58] As collected data is ingested and distributed in near real time to end users with the capacity to act, decision cycles turn faster and allow "shooters" to maintain distinct

[56] Communities of interest and communities of practice are dynamic, collaborative relationships of autonomous actors relying on mission or common purposes to unite and solve complex problems. The collaboration can be physical or virtual, as supported by a distributed enterprise system and parallel operations.

[57] Alberts and Hayes, 120.

[58] The shortened kill chain means that each actor or step in the process must add value to the engagement process or it is eliminated. The decision authority between detection and delivery of effects has often been the step that incorporates the greatest time delays. Legal reviews and imprecise, unclear intent can also lengthen the time between detecting and acting in dynamic environments. A shortened kill chain may mean the same sensor that acquires the target immediately engages the target, such as with the Unmanned Combat Aerial Vehicle, air assets, or other automated, detection and delivery systems. Controls are indirect through ROE, engagement thresholds, and decision logic embedded within the system itself. This logic extends to the empowered soldier as well.

advantage over "the detected." In such a collection rich and distributed delivery environment, the detection battle becomes the key element for action and decisive effect. In terms of automated response systems such as computer defense systems, air and missile defense systems, and other automated fire control systems, the "rules of engagement" and electronic safeguards, must be pre-set. Human decision "in the loop" may be too slow in many circumstances. For manned or unmanned systems with a human "in the loop," such as direct actions, raids, and air strikes, sensor-shooter response is enhanced with streamlined authorities and direct, actionable data feeds with tailored, immediately intelligible presentation to the executor. This also reduces the amount of cognitive loading required on the part of human decision makers.[59] Sensor-Shooter enhancement is only one aspect of the persistent surveillance capability.

Persistent surveillance also provides the instrument "to deeply understand an adversary in all his complexity," to get inside the adversary's entire system, to view the adversary as a Complex Adaptive System (CAS), and discern the system's dynamic evolution.[60] Understanding moves from simply gaining additional awareness about a "thing" or "facts." While reconnaissance and periodic surveillance can create insight about details, or detail complexity, it has a difficult time creating an understanding of dynamic complexity. Detail complexity allows understanding of

[59] Cognitive loading is the required time for a human to interpret and assimilate new information in dynamic environments. In Afghanistan, ranger companies would execute raids and find information at one site, leading immediately to a second site, then perhaps a third. Follow on raids occurred because of acting. The ranger battalion commander rolled the same company from raid site to raid site rather than using different companies because of the cognitive loading issue. Once a company had the situational understanding, the exchange of information to another unit would have resulted in time delays, reducing the ranger unit's ability to stay ahead in the decision cycle battle. This is also a good example of adaptive planning and the merging of intelligence and operations. With persistent surveillance and an enhanced COP, cognitive loading may be substantially reduced and create broader options and greater exploitation opportunities. Monograph discussions with COL Stefan Banach.

[60] A Complex Adaptive System is one that demonstrates complex behaviors, rather than merely complicated processes, capable of adaptation and anticipation of change rather than merely responding to environmental change. All natural living systems are Complex Adaptive Systems. Autonomous agents form building blocks of complexity and emergent characteristics form from interaction of the complex parts. Autonomous agents are capable of perpetually novel actions and thrive on dynamism. Autonomous agents are also capable of spontaneous self-organization. There are no independent variables in a complex system, each of the variables and agents are affected by information flowing from positive and negative feedback loops and continuously adapt to each other. See Waldrop, 11-12.

simple, often explicit variables in a system.[61] A relationship between time distance factors, rates of fire to volumes of fire, and communications interfaces with an observer are one example. A terror operations cell interacting with a finance cell is another example.[62] Dynamic complexity means the ability to sense and understand all the related and often subtle variables within the system, such as intentions, reasons for timing, and influence networks providing goals, driving behaviors and creating coherent strategy.

A persistent surveillance capability envisioned with merely sensor-shooter applications in mind is necessary but remains insufficient to generate the understanding that is necessary to commit and sustain ground forces. Because of the logistical and physical realities of moving and sustaining committed units, understanding must begin before the political and operational decisions are made. Whereas air and sea based forces can maintain operational reach from outside a given territory and remain outside sovereign borders, Army forces must enter that same territory and interact in a much more complex operational environment composed of multivariate actors and rapidly changing human conditions, creating constant flux in the system.[63] The sensor-shooter model appropriate for engaging physical targets with clear, distinct signatures does not work as well in a culturally and values diverse human centric battlespace, particularly if the adversaries increasingly mask themselves within the populations, operate using commercial infrastructure, and look for dual use technologies to remain ambiguous. Precision force requires precise intelligence with situational understanding, including the cultural and ideological components of the battlespace. Recent testimony from Major General (retired) Robert Scales highlights this fact. In citing an example from *Operation Iraqi Freedom*, Scales reflects:

---

[61] Peter M. Senge, *The Fifth Discipline: The Art and Practice of the Learning Organization* (New York: Doubleday, 1990), 71-72.

[62] Detail complexity and Sensor-Shooter support is still required even with the most "exquisite" intelligence from CAS views. Agents and actors carrying out attacks are exponents of a larger CAS but are not a system, in and of themselves. Because they are capable of spontaneous self-organization, have internal rule sets, and independent "will," they must be addressed as individual entities, much like an independent "organism." See James J. Schneider, "Blacklights: Chaos, Complexity, and the Promise of Information Warfare," *Joint Forces Quarterly*, Spring 1997, 21-28.

[63] Controlling people and terrain are the fundamental aspects of the Army's battlespace roles.

> I asked a returning commander from the Third Infantry Division about how well situational awareness (read aerial and ground intelligence technology) worked during the march to Baghdad. "I knew where every enemy tank was dug in on the outskirts of Tallil," he replied. Only problem was my soldiers had to fight fanatics charging on foot or in pickups and firing AK 47s and RPGs. I had perfect situational awareness. What I lacked was cultural awareness. Great technical intelligence…wrong enemy."[64]

Given this perspective, a deeper understanding goes well beyond a targeting or "sensor-shooter" level of situational awareness. Generation of insight and complete understanding comes from "loitering on the target long enough to discern behaviors, relationships and leverage points needed to take decisive action."[65] The capability goes beyond staring at a single point target and is about discovering all the variables that cause the adversary's system and the components to act the way the do. This approach also rejects a binary view of the battlefield and considers the actors and the environment in a more holistic context. The underlying theoretical maps for uncovering these relationships do not come from traditionally held notions of enemy templates and orders of battle. They come from complexity theory and dynamic systems thinking.

The Joint Forces Command is developing the Operational Net Assessment methodology (ONA) for use in the joint force. Operational Net Assessment takes a full systems view of the enemy as a CAS, in context with the friendly and the battlespace environment.[66] Persistent

---

[64] Robert Scales, "Army Transformation: Implications for the Future," *Prepared Statement of Testimony, U.S. House of Representatives, Armed Services Committee*, July 15, 2004, 2. The presence of "fanatics," is indicative of the nature of a complex system generating behaviors that are acted out by autonomous agents. These agents are "cells" which adapt and self organize within the environment. Once in action, they may continue to rely on the larger system, but are capable of operating independently from the system. Cells are not a system, but organisms.

[65] VADM Jacoby, interview. Leverage points are the fundamental focus areas in systems thinking. Leverage follows the principle of economy of means. By understanding leverage points within the system, better results can come from small, precise actions. Often leverage lies at a distance from the observed, explicit behavior and is often found in the balancing feedback "loop" of a given system's structures. Systemic structures influence behaviors, the structures within human systems are subtle, and leverage often comes from new ways of thinking and acting on the problem set. See Senge, 40, 101, 114-115.

[66] Jeremy Biggie, "Operational Net Assessment," Presentation, *USJFCOM*, November 19, 2003. In order for the ONA and PMESII analysis to achieve the desired usability, as broad a range of inputs as possible should enter the analysis, including data and expertise from civil organizations, the military, academia, social and behavioral scientists, multinational organizations such as PVOs and NGOs, just to name a few. Multinational partners, cultural experts and technical experts should also be leveraged, to include their existing databases.

surveillance creates a dynamic, synthetic reality capable of continuously updating the CAS models, allowing planners, analysts, and commanders to overlay, compare and update predictions of enemy behavior. Subordinate analytical structures under ONA combine the adversary's Political, Military, Economic, Social, Infrastructure and Information structures (PMESII) into a coherent view of the adversary. Effects modeling can be run in real time with advanced simulation and generate a broader set of options for commanders, interagency and other partners to predict effects and behaviors, understand and assess the results of their previous effects on the adversary as a CAS. A dynamic analytic and planning capability underpins the capability to achieve coherent Effects Based Operations and leverage all forms of force.[67] This real time assessment and continuous understanding comes from the persistent surveillance. Persistent surveillance, however, does not mean that sensing occurs apart from acting.

Taking action against components of the adversary's system is done purposely to generate further understanding. A persistent capability creates new opportunities to act and shape the target through purposeful stimulations, making collection more valuable. Aircraft purposely entering a radar coverage zone in order to stimulate an air defense network as collection operations collect the environmental data is one example. Consider that the SOF airborne raid into a remote compound in Afghanistan in October 2001 "were primarily aimed at gaining intelligence from captured documents or equipment; the SOF troops remained in the area only a few hours and then were extracted."[68] The series of raids and interrogations of suspected associates of Saddam Hussein prior to his capture are other examples.[69] Each of these actions, as examples, made or forced changes within the enemy as a CAS and the effects of our actions

[67] The physics equation for force is *force equals mass times acceleration* (f=ma). Since information can substitute for, or achieve qualities of mass, a new definition may be "force is any factor used or leveraged in the environment to cause change in the environment." In the case of acting, information enables precision and is embedded within the actor and agent logic sets. For a complete discussion on the duality of information and its character as mass and energy, see Schneider, 24-25.

[68] Glenn W. Goodman, Jr., "Made to Order: U.S. Special Operations Forces Display their Strengths in Afghanistan War," *Armed Forces Journal International*, December 2001.

[69] Evan Thomas and Rod Nordland, "How We Got Saddam," *Newsweek*, December 22, 2003.

created additional intelligence and understanding. In Complexity Theory, this phenomenon is described as the law of increasing returns.[70] The symbiotic relationship between acting and generating intelligence will create greater returns. [71] Operations and Intelligence will further merge as a result.

The overall collection component includes systems of sensors established in the battlespace. In much the same way a combined arms and joint fires approach creates a synergistic effect on the enemy and create complex problems for the target to adapt to, the same strategy is becoming the norm in the sensing realm. Cross-cueing will be dynamic and computer controlled in many cases. This is not new in itself. We have always attempted to use multiple collection methods on high priority targets and some sensor sets were capable of cross-cueing within very specific systems. What is new is the massively distributed and integrated nature of the sensor grid and the "seeding" we are increasingly capable of leveraging.[72] The "1:1 or 1:few" relationship between sensors and levels of organization is overturned as the system generates flexible "many:many" dynamic relationships in the networked battlespace environment. The senior leaders driving persistence as a concept place emphasis on long-dwell sensors; however achieving persistence is not solely dependent on technological collection. As Vice Admiral Jacoby states, "A HUMINT asset may prove to be the best way to dwell on a particular problem. It is about an integrated

[70] Waldrop, 34-38. Increasing returns is an emergent characteristic resulting from positive feedback within an open system. Because stimulation from external elements from the systems environment causes change, the changes cascade across the system in effort to balance and diffuse the energy. This involves a transfer across multiple components of the system and generates increased interaction of the component parts to compensate. The "increasing" element is a function the elements closest to effects to make stronger connection with local "neighbors" in the network or system. This also explains why popular brands in the market place attract more new customers and why "mass" movements start off slowly but peak rapidly. It is a natural system behavior. In military terms, it is why units in contact get more response from support structures than units out of contact.

[71] Consider the police or drug enforcement model of collecting and acting against crime and drug networks. The networked actors are identified and systemic collection is applied. Undercover agents, wire taps, surveillance teams and financial tracking tools all work to form a comprehensive understanding of the network and its infrastructure. Low-level "street dealers" are often allowed to continue to operate as the mid- and upper-level tiers are identified and further collection is applied. Once a network understanding is achieved, law enforcement agents act coherently with district attorneys and judges (warrants issued, agreements form, etc) to take down entire structures rather than simply individual actors.

[72] VADM Jacoby, interview.

collection approach, with the end result being persistence in your ability to stay with the problem as long as it takes to understand it."[73]

The Army's initiative "Every Soldier is a Sensor (ES2)" also moves to capitalize upon the inherent power of human observation, expanding beyond that of the HUMINT or Counter Intelligence soldier. The program aims to enhance the basic observation skills of all soldiers and provide them the means to quickly access and post information gleaned from street patrols and tactical operations into the larger data set of information.[74] Future Combat Systems will also include embedded sensors integrated with the platforms as well as integrating with other system sensing, such as unmanned platforms, Tactical HUMINT, and advanced Measurement and Signatures Intelligence (MASINT) sensing. Units or entities entering the local battle space substantially increase the localized environmental sensing and provide additional real time data back into the larger system for feedback and effects assessment.

In effect, the force has an extended blanket of sensing around them as they engage in close combat or take other actions to effect the enemy. At the same time, sensing continuously across the global environment provides additional sensory input relevant at all levels of war. Not only will the sensing support military operations but will also create knowledge across the range of national security components and support all instruments of power. Homeland security is also integrated into this sensing environment, as a consumer and as a contributor. This dramatically increases the environmental understanding of elements operating on the edge and allows the larger system to "see" systemic effects.

---

[73] Robert K. Ackerman, "Defense Intelligence Seeks Triple Threat Transformation," *Signal Magazine*, October 2003.

[74] Joe Burles, "Actionable Intelligence Relies on Every Soldier," *Army News Service*, April 13, 2004. [Accessed online November, 06 2004 http://www.tradoc.army.mil/pao/Web_specials/FocusAreas/actionableintelligence.htm.] The ES2 program allows soldiers to access and input directly into the digital network. Soldier will receive "PDA" devices to input patrol reporting easily through customized reporting interfaces, such as drop down menus and reporting templates. The culture shift requires every soldier (including officers) to view him or herself as part of the intelligence system, as they interact with their environment. In a three-month period in OIF, over 400,000 patrols occurred, yet only 6,000 reports were generated and fed into the overall system. The initiative is designed to dramatically change that metric.

The ongoing Horizontal Integration efforts are intended to allow full use of all data, regardless of collection source.[75] Expansion of the storage and processing capabilities within the persistent surveillance system creates the capability to dramatically increase the usability of data in pattern recognition and conduct predictive analysis. The processing functions will act as an artificial neural network.[76] Real time data enters distributed processing nodes across the joint force and interagency partners. Some nodes will pre-process for other nodes. In a dynamic system of constant sensing, the processors match inputs to threshold reporting. Data tagging, including Extensible Markup Language (XML) creates a capability to establish Meta Data linkages and increase processing speed.[77] Moreover, the "tagging standards allow the use of sophisticated 'analytic discovery' tools to further refine both queries and answers."[78] Data tagging increases the value of collected data because it provides embedded information such as the data category, sensor, time of collection, and classification level.

Advances in Artificial Intelligence (AI) allow for applications such as Case Based Reasoning tools and Inference Models to compare and match data to algorithms containing historical instances and fill gaps from inference rather than assessment. Case Based Reasoning compares incoming data and information with stored cases containing underlying facts and logic structures. With inference, the data are compared to all other known data for matches first, then gaps are

---

[75] "National Security and Horizontal Integration," White Paper, *AFCEA*, 2004. Horizontal Integration is a formal Intelligence Community (DoD and non-DoD) initiative to allow data integration and overcome the interoperability issues of diverse data structures and database incompatibility. The issue of classification is also addressed through network user access credentials and system authorization interfaces. The intent is to move the relevant content of the data to users and (in some cases) strip the elements of the data that create classification requirements, such as a sensitive source or collection method.

[76] Marakas, George M., *Decision Support Systems in the 21st Century* (Upper Saddle River, NJ: Prentice Hall, 1999), 365. Neural networks attempt to replicate the way the human brain works. This includes pattern matching and recognition and online storage of data in categories and accessed through the meta tags. This allows for discovery and inference. While a single human brain will always be more complex and capable of true reasoning, the enterprise nature of a neural network massively shares and "learns" as more data enters the collections of nodes and processors.

[77] XML is a data structure allowing multiple users to immediately judge or assess the underlying data content within data "packets" for relevance to their specific need or for machines to parse and store into appropriate knowledge bins. Meta-Data is "the data about data," like a table of contents in machine-readable form.

[78] "National Security and Horizontal Integration," 3.

filled with probability or confidence scores. Suggestions combine with these confidence scores as the "answer," enhancing human decision-making based on the data (information).[79]

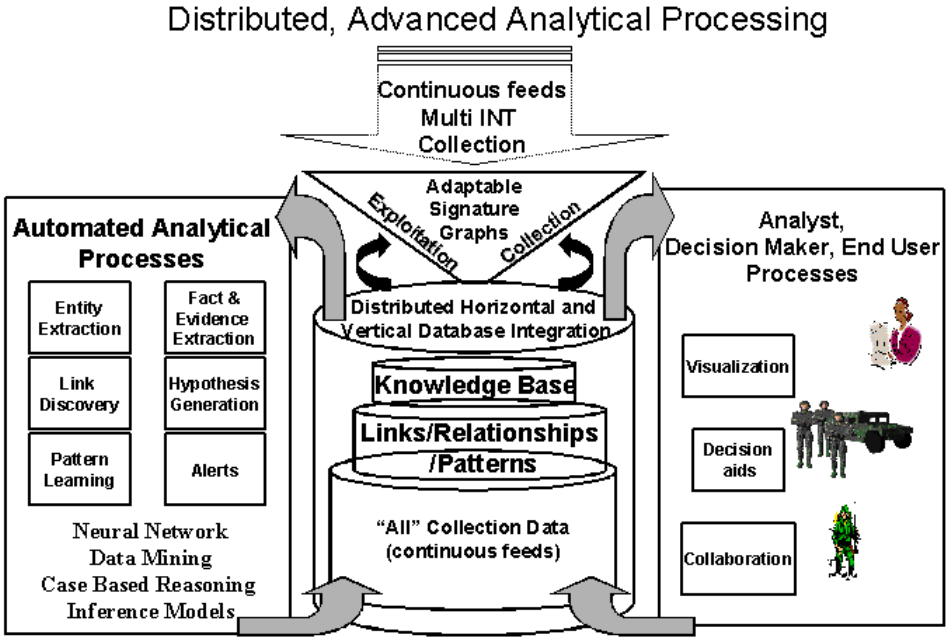

Figure 2. Conceptual depiction of processing nodes (Knowledge Advantage Centers) and User Interfaces. The creation of integrated or virtually unified databases and the continuous data stream analysis creates the conditions for near real time collaboration and support in a networked, collaborative environment. (Slide adapted from U.S. Army INSCOM Presentation).[80]

An example of Case Based Reasoning and Inference comes from interaction with online retailers. When you begin searching for a book, the processors begin creating a template of your demonstrated behaviors and compare it against all other customers exhibiting similar behaviors. When you settle on the item you wish to purchase, the system is in a position to suggest, "what other customers have also purchased" enticing you to associate yourself to this behavior as well

[79] The use of "fuzzy logic" internal to inference algorithms supports better data integration, pattern development, and anomaly or change detection because it allows for data approximation and less than exact input of data fields by users and collection systems. Queries can be done in "natural" language and with a broader range of parameters. Additionally, the "fuzzy" language is more flexible and supportive of exchange with human thought patterns and cognitive frameworks. See Makaras, 289-290.

[80] MG John F. Kimmons, Presentation, Global Intelligence, Surveillance, and Reconnaissance Conference.

and purchase additional items.[81] Because the system "knows" what others have purchased and you *are* purchasing a specific selection, the Case Based Reasoning is updated and "learns" as it updates the stored memory. The overall inference algorithm is also affected and the next iteration has a higher confidence in suggestion when you return to shop online as well as others "like you."

Dynamic Signature Graphs are also part of this neural network, however this is tied to actual individual behaviors that have been "tagged." The credit card industry provides an example of this in their fraud detection systems. With literally billions of worldwide credit transactions occurring every day, the credit card companies can sort through the "noise" to find purchasing transactions which appear as anomalies and present them to humans to take an action. You are tracked as a distinct signature and your card is your "fingerprint." If your credit card is used to purchase something that does not "fit" your recorded buying patterns (your signature), the company calls you to verify this behavior. If you actually did make the purchase, then your individual signature graph is updated (a new baseline is created), as well as the Case Based Reasoning Toolsets and Inference Models. The thresholds for reporting and identifying anomalies become more specific, or in other words, more reliable. These three artificial intelligence tools combine and create a synergy of effect to create usable knowledge.[82] The point is, it is the constant ingestion of *all* collected data and feedback that allows the system as a whole to learn and be more useful to humans in a competitive environment.

This use of all the data is described as "deepening the evidentiary base." [83] Other components of the processing systems will speed data velocity and increase value of the data. Data visualization and data animation will allow humans to rapidly integrate new data and understand

[81] This is also another example of increasing returns.

[82] There are a multitude of additional AI tools that support neural networks. These three tools are used as basic examples to describe the key information age processing components (Sense-Making) of persistent surveillance. The U.S. Army INSCOM's Information Dominance Center (and networked extensions) along with the Pantheon Project seeks to integrate and continuously expand information age toolsets. These efforts support distributed, parallel analytical processing at increasingly lower echelons.

[83] Mr. Louis Andre, interview.

its significance within their localized domain or problem set. Data visualization in the military context may be the creation of network diagrams and individual entity behaviors, such as location, relationships, and component network or "cluster" size. A local cluster is a combination of localized actors and entities, or in some cases virtually connected actors and entities, formed for a specific purpose. This may be a terror or insurgent operations cell, different from the finance or logistics cell, but both acting to achieve a related purpose or outcome. This is not limited to non-state actors. Combined arms units, logistics bases, and air defense nodes combine to form small or local clusters. These are the building blocks for the larger interactions of the complex adaptive system.

In a capability-based system, the target becomes a target based on its individual attributes. It may be because of an association with a known adversary or by conducting an activity we discern as threatening, or even potentially valuable. Activity may be a physical, audible, chemical, behavioral, or a structural characteristic, as dynamically compared to a deepening evidentiary base. This applies to humans as well as material activity signatures. Remember, this logic is based on detecting component granularity, not initially based on mass or groupings. The activities of the target create an anomaly in the global environment or local environment that we are interested in. Artificial intelligence helps to data mine vast data streams, find associations and "score" significance for humans to look at in more depth. From that point on, persistence takes over.

By establishing increased depth in the case based reasoning algorithms and inference models, the system learns and improves as specific actors or entities are captured in the system. The system builds and maintains individualized signature graphs and establishes "fingerprints" with "tags," based on attributes that do not change over time.[84] Baselines are set and then assigned

[84] "Fingerprints" may be biometric, such as voice patterns, facial features, "gait," or non-biometric such as distinctive "computer code" within viruses, discreet auditory or signal parameters, etc. Humans still form a significant component of the system through interaction with other humans and ability to assess

thresholds for alerts to the larger system. This is a complete reverse of the decomposition and analysis approach used in traditional analytical models today. It also allows graphic representation of identified "leverage points" and key nodes of the network. Because of persistent surveillance, the understanding of the whole comes from the observance of the assembly and integration of the parts.

The understanding of behaviors, and potentially prediction of intent, is only possible with a fundamental understanding of the adversary as a CAS. The CAS overall behavior is actually an emergent property composed of thousands of actors demonstrating discreet, intertwined emerging behaviors. The battle space environment is in constant flux, with varied levels of interaction and participation.[85] However, no matter how accurate the CAS approach becomes, the persistent surveillance capability must allow for the identification and tracking of new actors apart from the CAS and support strike operations on point targets, enabling a faster tactical OODA loop and sensor to shooter "kill chain."[86]

As a metaphor, the sensing component of persistent surveillance provides the sight, smell, sound, taste, and touch components, as the processors act as a brain to assemble and make sense of the sensory inputs with both understanding and memory elements. Because of the advances in software, this system also learns and "gets smarter" with greater environmental interaction.

---

anomalies and specific people and behaviors within their environment. The ES2 initiative will dramatically increase the ability for all soldiers to enter their own observances and cues to anomalies into the network with digital interfaces. Soldiers and HUMINT collection will be the most "sentient" sensors because of a combination of training, experience, and the integration of explicit and tacit knowledge about their particular local environment.

[85] The elimination of uncertainty is not possible when dealing with dynamic systems, particularly human systems. Autonomous actors and free will create dynamic uncertainty. Planning horizons are supported, however, with increased depth of knowledge and the ability to predict behaviors and capabilities within a range of probabilities over a given time frame. Once autonomous actors interact with the environment, the unfolding events will create novel behaviors and unpredictable individual actions, particularly at the tactical level of war. Persistent surveillance allows for real time observation of both anticipated and demonstrated novel behaviors as well as the greater systemic adaptations. This creates conditions for precise actions and anticipatory, adaptive planning in each of the domains and levels of war, in support of varied planning horizons.

[86] OODA is the Observe-Orient-Decide-and Act sequence identified by USAF Col (Ret.) John R. Boyd.

The system distributes its "understanding" to the humans in near real time and to the lowest levels, who will combine it with local understanding to create a decision advantage in the battlespace. Continuing with the human body metaphor, dissemination is the central nervous system that transmits brain data to the limbs and other portions of the triune brain. The distribution system for persistent surveillance is through the overarching Global Information Grid (GIG) and components.

The enterprise system leverages network protocols to distribute information smartly, avoiding data overload by incorporating a "post" and "smart pull" system. Essentially, the "post" comes from the posting of the data, or in some cases "productized" information, with the meta-tags. The "smart pull" comes from users knowledgeable of the data sets and categories in the system.[87] The smart network creates a balanced knowledge management distribution system, allowing interaction without overload. Within the Intelligence Community, the Distributed Common Ground System (DCGS) establishes one of the core persistent surveillance distribution networks. The Third Infantry Division will take DCGS-A (the Army's component system of DCGS) into Iraq on its next OIF rotation.[88] Other distribution systems will eventually incorporate the Warfighter Information Network-Tactical (WIN-T) network within the Army. The ability to move relevant and timely data directly to individual soldiers and entities is rapidly increasing. Estimates place DoD's investment in network centric capabilities at over $200B across the next 10 years.[89]

[87] Alberts and Hayes, 82-83. In a "smart push" system, by contrast, the "smart" processor must know all the entities in the network and what their information needs are. In a pull system, the control goes to the authorized user.

[88] "DOD Moving to Link Iraq-Bound Army Units with Fusion Network," *Inside the Pentagon*, September 2, 2004, 1.

[89] Brad Grimes, "OFT: New Defense Opportunities," *Washington Technology*, July 19, 2004, 4.

In terms of content access and delivery, users will self-define relationships and self-register with the system. Access protocols provide and control content distribution.[90] The data visualization and animation tools are decentralized across the processor and pre-processor nodes. In addition to deepening the evidentiary base, the persistent surveillance effort seeks to get more performance from the data by enhancing display applications across the user field. Data can be portrayed in a variety of customized visual formats and user defined displays. The data does not solely reside in an "electronic shoebox," or as a series of website links and text.[91] In this way Army Sergeant Jones receives immediately actionable intelligence in a form he can immediately integrate into his decision cycle, say an identified IED or sniper location, while the same network and persistent processing also supports Police Sergeant Jones on the lookout for a 1993 Ford Escort.[92] If you wish to see reporting in a link diagram, you can. Formal reports, when required, will also contain links with other reports and graphically depict content relationships. If all that is required in real time for units in contact is an icon, then you get an icon, on your screen. Analysts doing broad analysis apply their tools and create the visualization overlays and data fusion they need. Other data will support anticipatory planning requirements for staffs and commanders focused beyond the immediate operations. Analysts can also virtually collaborate and share other insights.

In the current COP, most analog data is converted to digital form to transit the network and then returned to human intelligible form for display and understanding. The point is that the assimilation tools for displaying persistent intelligence significantly increase decision speed because of the human tailored presentation formats. Assimilation means a user compares the local circumstance and tacit knowledge with the persistent surveillance feeds. The user still has to form judgment and act.

---

[90] Users range from analysts to operators and decision makers across the levels of war and include interagency partners, to include homeland security. In some cases, users are machines, rather than human.

[91] MG Kimmons, interview.

[92] VADM Jacoby, interview.

The emergence of persistent surveillance must be considered in context to the overall future combat and national security capability, and as such, should be nested to the higher operational capability it serves. Form follows function. The guiding vision, a globally coherent national security system, creates the goal to develop a coherent operational system for exercising all the elements of national power. The promise of developing a system of persistent surveillance is not found in perfecting the past, but in creating the future.

Persistent Surveillance: Implications for the Common Operating Picture

A persistent surveillance system represents only a portion of the overall national security system. In the previous section of this monograph, I related a persistent surveillance system to the human senses (the sensing functions), a central nervous system (delivery), and cognitive understanding (the sensemaking). While this analogy holds in some contexts, it remains incomplete. For persistent surveillance to achieve full potential, it must combine with other functions to create not only a capacity to know, but also to act. The integrating mechanism to create a complete capability is the Common Operating Picture (COP). The COP is "a single identical display of relevant information shared by more than one command."[93] The COP is also an enterprise information system, supporting an extended operational enterprise, beyond DoD.

In a highly distributed information environment, a singular COP display may remain appropriate if the information distribution moves hierarchically and the information remains static for periods of time. The "single identical display," however, creates its own problems when the future COP becomes a real time enterprise information system, supported by a continuous data environment. Single identical displays are less useful than displays created dynamically to support specific missions and domain views of the battlespace. As the Joint Forces Command study on the Collaborative Information Environment (CIE) finds, collaboration capabilities will

[93] Chairman of the Joint Chiefs of Staff, *Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms, 2003* (Washington, D.C.: U.S. Government Printing Office, 2003).

allow users to tailor their COP displays yet maintain the "common" and "relevant" aspects of the operational picture.[94] The study also finds that a real time environment significantly increases the value of the COP *if they allow the user to define and dynamically tailor the views.*[95] The key word is "if." We must transition to a COP in the twenty-first century with dynamic tailoring capability, supporting both real time operating requirements and varied future planning requirements.

The COP must enable adaptive planning across varied planning horizons to achieve coherent systemic effects. Complex systems survive by anticipating the future. [96] A transparent, but tailored medium such as the integrated COP supports this anticipatory function. Each domain and level of war has associated echelons and sub-organizations, regardless of how "flat" a networked force becomes. Each "level" must operate within the appropriate time horizon. Parallel levels of war and parallel domains must remain nested in purpose, and enterprise behaviors become driven by intent. Because effects can transit multiple domains and levels of war instantaneously in the information age, purposeful adaptations through effects planning must be thoroughly integrated.

Platoons, squads and individual actors are focused on real time execution while the higher level complex organizations focus on setting conditions for the future. Companies and battalions may live in the near future-12-48 hours ahead of the adversary decision cycles, while brigades and divisions may live in the 48-96 hour "future." Joint Task Forces and national decision

[94] "Operational Implications of the Collaborative Information Environment (CIE)," Pamphlet 5, *Joint Warfighting Center,* 11-12. The CIE is "A virtual aggregation of individuals, organizations, systems, infrastructures and processes to create and share the data, information and knowledge needed to plan execute and assess joint force operations and enable a commander to make decisions better and faster than the adversary." Ibid., GL-2.

[95] Ibid., 11-12.

[96] Kevin Kelly, *Out of Control: The New Biology of Machines, Social Systems and the Economic World* (Cambridge, MA: Perseus Books, 1994), 440. Kelly provides the observation that a system stuck in the present is reactive, prone to surprise from change, and will die. A COP only capable of portraying real time conditions creates digitized, myopic views of reality and cognitively handicaps anticipatory actions.

makers must be effective in creating advantageous conditions beyond the 96-hour mark.[97] With a coherent COP enabled view of the planning horizon and persistent surveillance of systemic changes within the adversary, tempo control and effects sequencing provide the desired shaping and battlespace depth required for units executing within the battlespace. Enterprise Planning Systems greatly assist in gaining competitive advantage.

Examples of Enterprise Planning Systems integrated with real time enterprise data and anticipated change include the National Weather Service, who uses real time weather data and advanced simulations to anticipate hurricane impacts on specific demographic areas. As a result, local officials can issue localized alerts, conduct highway traffic flow analysis and establish evacuation priorities and instructions. The forest service uses real time weather data and simulation models of forest fires to dynamically adjust firefighters and other assets, planning with far greater insight of the scope and emerging conditions of the problem. Wal-Mart uses environmental data, social data, and local cultural data to forecast and dynamically adjust inventories at the individual store level for items ranging from snow shovels to local football team playoff tee-shirts.[98] Anticipatory planning gets each of these organizations ahead in the decision cycle battle by identifying and generating options.

Developing and supporting proactive, option seeking behaviors and a flexible, exploitation capable framework is difficult under the current ordered, linear, deliberate planning constructs. In today's process and plan centric execution models, commanders often become prescriptive in intent, creating reactive tactical plans because of the perceived need to plan in detail for anticipated conditions. Rapid shifts of enablers in dispersed battlefields become problematic.

[97] The specific temporal orientation is tied to resource allocation and regeneration capacity. The future and associated "times" are used merely to show varied planning, decision-making and action orientations vis a vis adversaries. These will vary. Joint Task Force Commanders and national level decision makers should be future oriented in terms of weeks, months, and perhaps years. Moreover, a new field of computer science deals with the science of "anticipatory computing" in dynamic environments.

[98] In each of these examples, the ability to maintain disciplined focus at the right level and dynamically integrate relevant information and understanding seamlessly with actors across all levels maintains the competitive advantage. A COP view is possible because of the enterprise information systems.

Adaptation is slowed, especially at the operational levels. The ability to capitalize on options and exploit new conditions created at the tactical levels are limited by ordered, mechanistic, linear thinking. It is the deviations from the anticipated and an appreciation of the new, unpredicted and continually emerging circumstances which led Prussian General Helmuth Von Moltke, Senior, to view strategy as the development of a system of expedients [options] and cautioned that plans should only go as far as the first encounter with the enemy.[99]

Commander's Critical Information Requirements (CCIR) reflects deliberate attempts to filter information and allow humans to better synthesize information to support decision in this framework. Decisions themselves are forecasted in advance, often based on assumptions. Where information systems find and report the required elements to support CCIR, other information which could lead to new and improved decisions for superior execution often fall outside the scope of "the plan" and are not seized upon. For all the commander admonishments to "fight the enemy-not the plan," staffs involved in the information management battle often default to presenting only information supporting or denying key elements of "the plan." As retired Army Brigadier General Huba Wass de Czege writes:

> …anticipatory planning and adaptive execution can address the unpredictable will of the enemy and the chance factors which make forecasting the future difficult regardless of how much information we possess...The object is to achieve sound, adaptable, simple and decisive plans based on the best available information, understood and coordinated…so that vigorous teamwork can produce the desired results…Shared understanding and anticipatory planning combine to produce adaptive execution, which is the systemic ability to adapt plans to emerging situations in time to ensure continuous deliberate operations…New planning and execution systems will be needed to implement this process.[100]

---

[99] Martin Van Creveld, *Command in War* (Cambridge, Mass: Harvard University Press, 1985), 145. The literal interpretation of this does not convey the intent of the statement; rather, recognition of the inability to conduct detailed planning for tactical actions from higher headquarters. As Van Creveld relates "the true essence of the Prussian command system was not to try to foresee every move in war as if it were a railway timetable."

[100] Huba Wass de Czege and Jacob D. Biever, **"**Future Battle Command: Where Information Technology, Doctrine and Organization Meet,*" Army Magazine*, August 2001, 10-12.

An execution centric model with real time intelligence to identify changes and predict further changes in the adversaries systems will create new information; reduce operational risk; and enable bold option exploitation.

Army FM 6.0 provides for such information, called "exceptional information." Army Field Manual 6.0 states:

> Exceptional information is specific and immediately vital information that directly affects the success of the current operation. It would have been one of the CCIR if it had been foreseen; it is therefore treated as one of the CCIR. Exceptional information usually results discovering something unanticipated about an enemy. It allows the commander to take advantage of an unexpected opportunity…"[101]

Exceptional information is likely to increase with persistent surveillance capabilities integrated into the COP, particularly as near real time effects-sensing generate feedback to the force. Enemy system adaptations become more clearly identified. An operational paradox emerges, however, since tightly coupled, detailed elements of the plan (usually the basis for synchronization) often make large shifts in execution infeasible.

The "multiple, simultaneous, distributed, decentralized" nature of combat operations described in the JOC requires commander led, execution centric planning at all levels. Collaboration tools in a CIE allow parallel planning to move away from ordered, sequential and time-linear sequenced actions as reflected in JP 5-0.[102] After Action Reviews (AARs) from OIF indicate the

---

[101] U.S. Department of the Army, *FM 6-0, Mission Command: Command and Control of Army Forces* (Washington, D.C.: U. S. Government Printing Office, 2004), 3-13. Properly task organized tactical units (mounted and dismounted maneuver, fires, intelligence, interrogation and translation capability) with seasoned leadership and support (including pulsed sustainment, CASEVAC, joint fires, air and ground quick reaction forces, and robust secure communications) can conduct one tactical engagement after another (roll from target to target) to generate and continue generating exceptional information. Further empowering lower tactical levels with better organization including the addition of unique capabilities creates the ability to roll from target to target under an adaptive execution construct. Special Operations Forces with interagency support do this now. A transformed "conventional" force should also be fully resourced to execute operations under an adaptive execution construct. Monograph discussions with COL Stefan Banach.

[102] Chairman of the Joint Chiefs of Staff, *Joint Publication 5-0, Doctrine for Planning Joint Operations* (Washington, D.C.: U.S. Government Printing Office, 1995).

collaborative capabilities in Force XXI Battle Command System Brigade and Below (FBCB2) are already supporting moves in this direction. Bandwidth and logistics support are a different matter, for the time being. Executing "multiple, simultaneous, distributed, decentralized" actions requires relevant operational information fusion across all levels of command and in presentation formats accessible to all, including multi-agency, civil and coalition partners.

As concepts of "multiple, simultaneous, distributed, decentralized" operations place high adaptive planning and execution demands on the units, it is important to remember why these operational characteristics are important. Self-evident as they may seem, in terms of creating flexibility for the joint commander, these characteristics are inherently required to engage a massively dispersed and complex adaptive enemy system. As the enemy further decentralizes his components into a global framework and increasingly uses global infrastructures to mask, move, consolidate, communicate and act, the options we seek to engage against the components of that system must also expand.

Reordering Information Distributions and Changing the Controls

The fundamental reordering of information pathways, moving information directly to collaborative users (rather than through successive headquarters) empowers all echelons, given the right tailoring of the COP. Integration of persistent intelligence into the joint force empowers all actors and entities with a potentially "insurmountable asymmetric capability against our adversaries."[103] Real time data distribution transforms all previous control mechanisms of information across the joint force and partners.[104] An enterprise COP means "exclusivity of data is not the defining attribute of decision any longer."[105] This notion disrupts the entire command

[103] VADM Jacoby, interview.

[104] Partners may be DoD, non-DoD, or non-US coalition elements. This empowerment through decentralized data distribution requires the relinquishment of expert control to all stakeholders across the enterprise, to even the lowest levels, allowing adaptive planning and execution.

[105] Mr. Louis Andre, interview.

and control process, as it exists today. An extended operational enterprise relies on multiple, decentralized and distributed actors to achieve its overall purpose.

The term "agent" or "actor" simply means any individual, individual element or entity capable of interacting with its environment. Each agent or actor is also capable of creating effects against other actors and the environment.[106] The range of agents incorporates a single rifleman to a Tomahawk missile, a policeman through a Computer Emergency Response Team. The agents are distributed throughout the domains of conflict and the levels of war. Actors and agents interact at the tactical level to create effects across each of the domains and levels of war.[107] The term "warfighter" means many things to many people and often obscures the fact that the real ability to wage war and peace include the multitude of agents, DoD, non-DoD and international partners.[108] An enterprise COP should support them all.

Today, the means of control coexists with levels of command, as exercised under current information dissemination architectures. Information is rationalized and integrated with direct centralized command guidance to actors, as a means to synchronize action at the various levels of war. With an enterprise data generation system, including direct dissemination capabilities, COP control parameters must change. Control mechanisms remain the means of regulating behavior, as they always have in war, but they will move from centralized command nodes to the distributed processing nodes supporting actors across the domains and levels of war in the

---

[106] If the agent or actor cannot act, they cease to be an agent or actor.

[107] Even the most "strategic" actor or agent must take action in the tactical realm. The opening air strike in OIF directed against Saddam Hussein (at his suspected location) was still bound by the tactical, physical employment of the aircraft delivering the precision munitions. Newtonian physics dominate the tactical level of war. There is a tactical component in each domain of war.

[108] "Issue Paper #11. ACS: Knowledge at the Point of Decision and Key to Objective Force Success," *Association of the United States Army*, 2003. A wide range of white papers and concept papers describe the movement of decision quality data and combat information to the "point of decision" or the "point of action." This is one example. These papers seldom make explicit exactly who the decision maker is or at what level the action takes place. Most indicate these "points" are general/flag officer headquarters and may extend down to an Army Brigade/Unit of Action level command. Battalion and below level systems exist and will gain capacity, but are likely to remain outside the scope of the network for "Persistent Surveillance." When the Distributed Common Ground System-Army (DCGS-A) is provided to the battalion level, platoons will remain at least two levels removed from this networked environment as articulated in the program designs.

twenty-first century COP. These distributed processing nodes become Knowledge Advantage Centers (KAC).[109] Knowledge Advantage Centers enhance the capacity for self-organization, self-synchronization, and empowerment to the lowest levels. The Army reflects similar views of providing data and knowledge access to the lowest echelons in the Army Transformation Roadmap, stating,

> A focal point of DOD's thrust to fully exploit network-centric warfare is the development of persistent surveillance. In support to this goal, the Army will develop supporting persistent surveillance capabilities throughout the global battlespace. This provides the commander near continuous access to the priority intelligence targets. The objective is to develop network-sensing suites that tailor their observations to the adversary's rate of activity. The goal is to combine the broad spectrum of current and future sensors into an effective intelligence tool that is geared to the activity of an adversary. The amassed information is input into an Internet protocol where it is universally available to all warfighters. **This approach involves a paradigm shift in how raw data is entered into the network. Instead of analysts processing raw data into information for input into the network, the raw data will be placed on the network for empowered users to exploit for their own particular requirements. The decision on what is important moves from the entity that captures or analyzes the data to the person who uses it.** [emphasis added].[110]

As described earlier, data animation and three-dimensional presentation will allow users to create the understanding needed for specific mission sets and effects generation. Current tools such as Topscene and Falcon View serve as basic examples. These tools allow combined domain views, such as a synthesis of physical attributes of terrain with the infrastructure views of the signal or informational environment. Future tools will greatly increase the value of the enterprise data, creating even greater ability to perceive and understand the dynamic environment within each domain of war. While a complete cognitive domain view is not entirely replicable, the ability to create the social and cognitive influence network views of the adversary is possible.[111] Even with advances in toolsets and the ability to generate dynamic views at the individual level, the COP

---

[109] Wayne Michael Hall, *Stray Voltage: War in the Information Age* (Annapolis, MD: Naval Institute Press, 2003), 158-169. Though I use Brigadier General (Ret.) Hall's terminology, USJFCOM has similar concepts and varied terminology. USJFCOM foresees the creation of distributed knowledge centers for the CIE. Knowledge centers are comprised of humans, information technology and information.

[110] "2003 Army Transformation Roadmap," *Department of the Army*, 7-17.

[111] Julie A. Rosen and Wayne L Smith, "Influence Net Modeling for Strategic Planning: A Structured Approach to Information Operations," Preprint- *Phalanx* (December 2000), available online http://www.inet.saic.com/inet-public/welcome_to_saic.htm. HUMINT and SIGINT operations have historically provided insight into the cognitive domain as well.

must still develop a "synthetic brain" to fully realize coherence of action and unity of purpose across the extended operational enterprise.

From Enterprise Brain to Enterprise Mind

Just as the human brain evolved to establish new structures and an enhanced capacity to learn through evolution, the artificial neural network processing foundation of persistent surveillance forms what could be described as a neocortical brain for the national security system.

> The capstone of the brain, as we know it today, is the *neocortex*…it enables us to think, organize, remember, perceive, speak, choose, create, imagine and cope with or adapt to novelty. Within the neocortex 180 billion neurons or nerve cells interact without any physical connection. The possibilities for interconnections between neurons in one human brain are [infinite]. The [neocortex] also appears to have specialized hemispheres. The left hemisphere of the neocortex or the left-brain is the site of cognition. It processes words and numbers and organizes data in logical and linear sequences. Unlike the left-brain, the right- brain is more adept at registering the images, patterns, sounds and movement discernible in phenomenological perceptions or sensory input. Using holistic processing, the right hemisphere of the brain conceptualizes, hypothesizes and maintains an intuitive sense of the whole.[112]

While an evolved brain created the conditions for advantage in the competition with other mammals and the environment on the planet, the brain's ultimate emergent characteristic is the mind. A single mind works differently than a collective mind. A single brain controlling behavior and supervising correct adaptations of a single body is far different than distributed minds controlling and supervising the coherent actions of many different bodies in a competitive world.

Kevin Kelly, in the book, *Out of Control*, coined the term "Hive Mind," to describe the collective, emergent mind in extended enterprises.[113] A hive mind is a distributed mind that both

---

[112] Richard Szafranski, "Neocortical Warfare? The Acme of Skill," *Military Review*, November 1994, 41–55. Neocortical warfare asserts that, since the purpose of war is to impose will, and will resides within the mind of the adversary, all warfare is ultimately neocortical. Since the decision to "stop fighting" resides within the mind, the mind is the true target for all effects and imposition of will. Some minds require physical destruction, as the indirect approach will be too slow or inadequate for some actors, while combinations of effects may sufficiently influence other minds directly and indirectly. This approach leads to an expansion of force options, including the targeting of values, systemic behaviors, and cognitive frameworks.

[113] Kelly, 5-28.

perceives and remembers.[114] For the remainder of this monograph, I will use the term enterprise mind, rather than "hive mind." The artificial neural networks underlying persistent surveillance create the foundations to achieve an enterprise mind. A *distributed* memory and a *distributed* ability to perceive is the difference between a human mind and an enterprise mind.

Memory is highly reconstructive, involving a selection process to retrieve the right memory from all stored memories in the mind. The selection process comes from current perceptions and interaction with the environment.[115] Artificial memory stems from a reenactment through parallel distributed computing [a neural network, and the COP], which excels in perception, visualization, and simulation.[116] Massively distributed networked entities interact and use artificial memory to achieve advantage in their local competitive environment. As the network of actors tap into the enterprise mind, the number of possible interactions expands exponentially. Distinctly new enterprise behaviors emerge.

Unlike an individual human, however, whose memories and judgment capacity dies when the human body dies, the larger enterprise mind lives on within the man and machine system of the artificial neural network, creating the emergent characteristics of a living and learning being. The system itself is capable of "intelligent behavior." There are four distinct facets to networked, enterprise behaviors:

Absence of imposed centralized control
Autonomous nature of subunits
High connectivity between subunits
Web-like nonlinear causality of peers influencing peers[117]

The Enterprise Mind Enables Enterprise Behavior

The emergence of enterprise behaviors is the result of parallel operating wholes that perform purposely to achieve goals within their environment. Parallel operating wholes are complex

[114] Ibid., 19. Kelly also relates that a honeybee brain has an active memory lasting about six days, whereas the 50 pound beehive retains and operates with a collective memory lasting three months, twice as long as the average bee lives.
[115] Ibid., 18-19.
[116] Ibid., 20.
[117] Ibid., 22-23.

subcomponents interacting through a network, forming a larger complex adaptive system (dynamic system), yet are capable of operating as single unified elements.[118] Each of these operating wholes can contain thousands of autonomous agents.[119] The term "autonomous agents" simply means the agents *follow internal rule sets* and apply those rules based upon the *perception of their local environment*. The advantage of autonomous behavior is that each actor *acts continuously* without looking for centralized control from "higher," or moving in lock step with the larger environment. Autonomous agents are highly interconnected to many other autonomous actors and form peer networks, formally and informally. Novel but purposeful behaviors create complex challenges to an adversary and create the conditions for continuous adaptations in a competitive environment; self-synchronization results. In order to administer the networks, *control is decentralized and distributed within the enterprise system*. A review of the MCO JOC shows that these attributes are desired future operating characteristics.[120] Persistent surveillance and an advanced artificial neocortical brain [a red *and* blue artificial neural network, united within the COP] create the capacity to achieve an enterprise mind and an ability to leverage collective enterprise behaviors emerging from distributed, autonomous friendly actors.

Purpose Drives Behaviors

Command will still provide purpose. Motivation will still come from leadership and shared values. Direction will take a different form.[121] Command over a massively distributed global network of actors cannot be exerted directly to achieve coherent effects. There are too many

---

[118] For example, a Unit of Action is one parallel operating whole, capable of complex internal *and* external interaction, while a single platoon or an individual soldier are comparatively "simple" subcomponents of the UA, and must combine with other external elements to form complex interactions. Each level of actor or clusters of actors contain unique sets of operating logic.

[119] The concept of Swarming, or Battle Swarm has been used throughout history with great effect. Swarming concepts have been associated to Network Centric Warfare concepts. The Hive Behavior, however, is distinctive in that it has a collective memory and perception capability residing externally from individual actors. For a comprehensive review of swarming, see John Arquilla and David Ronfeldt, *Swarming and the Future of Conflict* (Santa Monica, CA: RAND, 2000).

[120] MCO JOC, 55-60.

[121] The Army describes command leadership as the process of providing purpose, direction and motivation to influence behaviors. See *FM 6.0*, 1-4.

autonomous agents with access to actionable information for this command style to work. As Kevin Kelly noted, "[enterprise] behavior is emergent, and "wherever 'emergence' appears, there disappears human control."[122] Command will become much more indirect in the future, through "effects based purpose and intent."[123]

Our assigned mission allows us to derive what those purposeful behaviors are at every level. Control parameters are integral to the processing nodes, with the KACs providing the information inputs into the COP. Some "raw" data feeds are preprocessed in route, within the actors COP itself.[124] With case based reasoning and dynamic signature graphs, the capability exists to create stored mission profiles on the "blue" side of the COP, for each actor and node in the system. By creating a distributed blue memory component, a learning artificial neural network can run in parallel with the persistent surveillance neural network. Interfaces create the potential for a fundamentally new COP for the twenty-first century, integrating autonomous actors across the battlespace, joined by mission set.

For example, a Unit of Action, which has "entered the net", could input mission set parameters and all associated factors such as anticipated duration, location, anticipated target sets, and any other characteristics specific to the mission.[125] Timing of preplanned effects are flexible, since associated actors are capable of collaborating in real time and "see" the adversary on their own COP, along with tailored views of the adversary's component elements targeted for effects.

---

[122] Kelly, 23.

[123] LTG Dubik, presentation notes. LTG Dubik likened command by purpose and effect to his experiences in Haiti and the requirement to deal with multiple agencies and actors in his battlespace. He also compared the need for control in a tank battalion on the attack, where all vehicles generally within sight and radio contact, to that of an infantry battalion on night infiltration at the squad level. Control methods are much different.

[124] Electronic Intelligence (ELINT) architectures serve as an example of networked preprocessing and smart distribution. F-16s for example, are supported by a variety of sensors in the battlespace as well as onboard sensors. If threat radar turns on, all pilots in the mission set are immediately warned with actionable specifics-location, speed, type, etc. The system knows the radar, presents in immediately usable formats, and understands who needs to know. The actual sensor is transparent.

[125] Unit locations are not necessary since the COP is receiving real time feeds on friendly locations.

Let's say a Unit of Action is preparing for a mission in Country X. By activating its mission set, Artificial Intelligence tools such as Expert Information Systems and related Decision Support Systems of the new COP's integrated neural networks provide intelligence and all other information to every actor in the enterprise COP, including joint, coalition and interagency partners. The Artificial Intelligence tools recall associated "scripts" from past cases and additional information stored in Blue and Red memories. Because the intelligence is continuous, globally related intelligence automatically integrates current and projected knowledge of the enemy's systemic adaptations. Dynamic views form across each COP, fully enabling coherent understanding by each of the mission linked actors.

Globally positioned actors capable of effects against the adversary will act based on mission and purposeful intent. Memory and perceptions combine within the enterprise mind to create knowledge and decision advantage. This creates what the JOC calls Unity of Purpose and Coherence of Action through "sequential, parallel and simultaneous actions distributed throughout the physical, information and cognitive domains of the global battlespace."[126] Novel and non-linear operations are inherently created since empowered, decentralized actors generate effects asynchronously in each domain of war and at all levels of war. As the MCO JOC says, the behavior "creates an indiscernible pattern in time and space in the mind of our enemy."[127] These are the emergent behaviors. The enterprise system would also assess effects in real time and update red and blue memories and Artificial Intelligence profile tools.

Enterprise Behaviors Create Distributed Effects Over Time

Because of the decision distribution, operational art would become a fully collaborative exchange with leadership and planning staffs primarily focused on operational tempo, setting conditions through anticipation, and describing desired effects. In the past, effects ran

[126] JOpsC, 18.
[127] MCO JOC, 10.

concurrently with battlefield actions. As outlined above, distributed, decentralized operations create inherently asynchronous effects. Through tempo control and effects linkages across the levels and domains of war, spatial and temporal capabilities of the adversary are affected. For example, logistics and movement of actors are often the indicators and precursors of action.[128] With persistent surveillance, precursors can be identified and acted upon in a greater variety of methods. It may mean delaying or preventing a collusion of necessary components for a given mission, the seizure of identified key assets, finances, or the denial of supporting commercial transportation means. Each action serves to increase the friction and reduces the operational capacity of the adversary, creating an inward or internal focus, forcing continuous re-planning and adjustments. By creating "deep" systemic effects, the result becomes a temporal advantage to the blue force. Tempo control becomes the most important element of twenty-first century operational art.

Commanders enabled by an integrated COP environment supported by persistent surveillance create tempo through effects planning. Control becomes an indirect method by dynamically directing KACs to alter mission parameters and effects sequencing. Mission formation would take less time as key players, in each domain and level of war, collaborate to construct the effect elements. Collaboration begins with a shared understanding of the commander's effects based intent. It will continue to be purpose and the commander's effects based intent that drives the formulation of the twenty-first century operational art design process.[129] The objective must be clearly defined. Lack of purpose and effects based intent results in incoherence.

---

[128] Remember, actions are bounded by the physics in the tactical realm.

[129] Vision is a function of articulating the linkage between the guiding purpose and the Effects Based Intent (EBI). The use of Tasks (specified tasks in operations orders) in execution centric, decentralized operations can inhibit initiative and create incoherence. The creation of task lists from centralized planning activities is increasingly too slow and too limiting in scope to address emerging conditions and can constrain actors from seeking and exploiting opportunities because finite resources are prioritized and committed to fulfilling a pre-specified task from "higher." Some of these insights come from a SAMS presentation on Marine Corps Operational Planning Observations from OIF. Planners from 1st Marine Expeditionary Force addressed SAMS on December 06, 2004. Tightly coupled task lists for operations resulted in continuous streams of Fragmentary Orders (FRAGOs) when situations changed.

The Enterprise Mind Empowers Enterprise Actors

Mission command at lower levels is established through self-regulating behaviors and self-organization, all related to mission purpose and clear purposeful intent. Rule sets outline a "MAXI-MIN" behavior set to follow.[130] In the current centralized COP environment, a commander's role is to take in information, form judgments and direct changes to subordinates as the situation changes. Conversely, in a distributed enterprise COP, the requirement for a commander's direct intervention is greatly reduced as subordinate actors and systems operate collaboratively to generate the desired effects. Commanders lead "from the center" of the network and provide the overarching umbrella of enabling resources and ensure freedom of action.[131] The commander also fights to extend the view deeper into the battlespace, in order to determine how to shape the environment and create options for tactical execution. Acting occurs continuously through self-synchronizing in parallel, distributed operations, within each domain and at each level of war. In execution centric environments, purpose remains the most important element.[132]

From purpose, the distributed control nodes within the KACs establish the controlling logic for the actors. This is where the autonomous agents receive their rule sets. The processor nodes are integrated systems of humans and system tools supporting a range of actors in the virtually

---

Many of the FRAGO's were irrelevant by the time they reached lower level units. In other cases, units were already engaged in the actions that the FRAGO had specified. Had the units waited for the order (even verbal), the action may have been too slow to produce the required effect. Since the units perceived the need to act, and did so without orders, one can question the validity, or at least the necessity, of the higher headquarters' order which followed. This places the debate about Effects and Tasks firmly in the "Decision Cycle Battle" forum. Task and Purpose may be replaced by Effect and Purpose. To be sure, tasks to subordinate units/elements will not be wholly replaced but the default behavior of specifying discreet actions to subordinates vice articulating effect-based intent may require more thoughtful investigation and doctrinal discussion.

[130] The rule sets for authority in taking action should clearly reflect the maximum latitude an actor has and a minimum level of control logic to accomplish the mission. Thresholds should be identified within the mission set, along with purpose and effects based intent.

[131] "From the center" of the network clusters rather than "from the top" as in a hierarchic organizational structure.

[132] Purpose drives behavior. Commanders describe effects to modify and shape organizational actions to achieve an overarching purpose. Nested purpose and effects create coherence across the domains and levels of war.

connected, collaborative environment. Control parameters form the basis of establishing what we understand as Industrial Age Rules of Engagement.[133]

As a metaphor, think of a dealer (the KACs) in a card game. He is constantly shuffling the cards (information) and distributing them to the players. He is also aware of the specific cards he is dealing to exactly what players. In the case of human actors he is dealing in analog presentation formats. For machines he is dealing in strictly machine-to-machine formats. This is a card deck with multiples of the same cards, blank cards, and unique cards. By controlling the unique cards he is empowering some players over the others to act differently and with varied levels of risk. By dealing blank cards, the dealer introduces sufficient ambiguity and uncertainty to red players.[134] Imagine that he is shaping the outcome in this game for purposeful effect. In this game, the dealer is affecting red, blue, and neutrals. By dealing certain cards to red, he controls information (information warfare) and assembles broader capabilities in the blue hands. The "tables" (COP views) and associated dealers are varied according to the level of play, such as the casino providing $5 games, $100 games and $1,000 games for the variety of players. However, all games are integrated and the "house" (the coherent national security system controlling behavior through the COP) retains operational and strategic *indirect* control.

[133] Industrial Age rules of engagement are still required but can be adjusted dynamically as feedback washes through the system and resets the COPs. Rules of Engagement for machines and robots are exercised through the COP with positive controls and physical and biometric access keys to prevent tampering. Robots and machines are already in war. Patriot Systems, UAVs (including ones armed with Hellfires) and Tomahawk Missiles are robots in the truest sense. Man-Machine interaction will continue to create these systems. The degree of human integrated control is largely a policy issue, not a technical infeasibility issue. In cyberspace, automated response systems act based on predestinated sets of rules and response thresholds. A human in the loop would be too slow. Even the virus protection software of your home computer has the features described, just not a full response capability. Network defenders continuously manage intrusion attacks and counter with response attacks based on "ROE".

[134] The notion of "blank cards" creates uncertainty by displaying actions or behaviors with dual purposes or uncertain purposes to the adversary. This could be in the form of ambiguous press statements, no notice force deployments or redeployments, an exchange of information with new allies and partners, etc. Blank cards also provide sufficient "flux" in the system to retain options for future unanticipated requirements on the blue side.

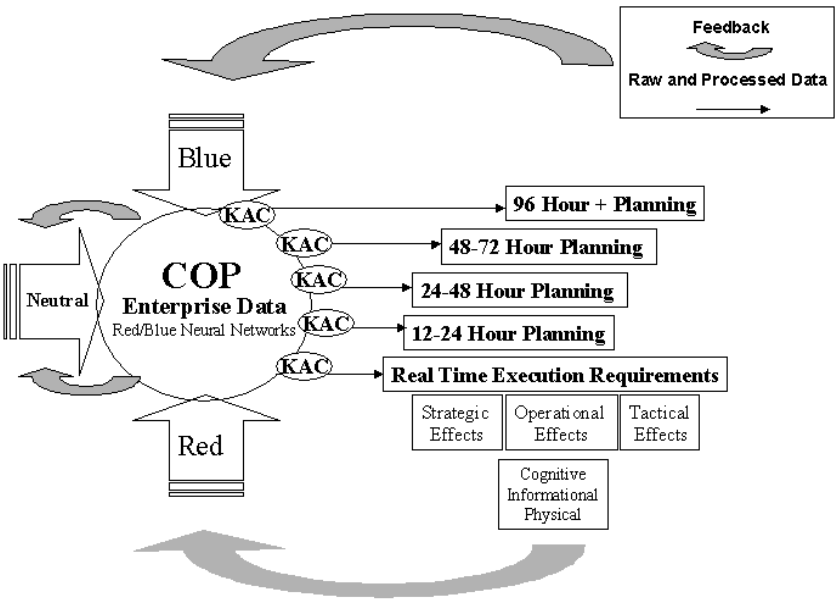

Figure 3. Depiction of the integrated COP with distributed Knowledge Advantage Centers (KACs) and an integrated Blue and Red neural network. Feedback loops from continuous monitoring of the battlespace in each level and domain of war enable coherent adaptation yet remain nested for coherent action.

Achieving Coherence

Coherence of action and continuous operations also require a change from an episodic view of military operations. A move to a "program management" mindset involves a long-term view of creating and maintaining decisive operating advantages and conditions rather than a "project management" mindset focused on producing a single or series of engineered activities of perhaps transitory usefulness and supporting a singularly defined end state. Coherence comes from correct effects design (supporting a larger purpose) and tailored information distribution, not from direct controls over single actors.

Since there is also a lowering of what constitutes the operational level of war, lower level actors are faced with the diverse response requirements as they integrate with broader sets of actors in the battlespace. Battalion commanders often deal directly with non-DoD elements in ways a Corps Commander may have done just 15 years ago. As one senior joint force

commander emphasized, "there are nearly 30 interagency elements operating in Iraq today."[135] Another senior Army commander related a growing appreciation for "shared battlespace" in the context of the current operating environment and that this "creates only the illusion of control. Consider the integrated operations of SOF, Interagency, Coalition and NGOs…you [military commanders] don't really own it [battlespace]- this is real."[136] Exactly *how* to determine what the contributing effects are, or should be, is also left undefined in this notion of coherence, but it must begin with common understanding of the adversary, as a system, across the contributing elements.[137]

Coherent actions may include purposeful combinations of kinetic force, arrests or seizure of material and funds, non-kinetic effects through computer network operations, or the initiation of public diplomacy and other messages intended for dissemination through global media to shape perceptions. Some actions may not be military in nature but may be coordinated and developed by military commanders, then executed by non-military actors to create effects. They may include acting through interagency partners and non-governmental actors, with or without attribution to the military command. Actions will be overt, covert and clandestine, often simultaneously.[138] As the MCO JOC states, joint force commanders will find themselves increasingly engaged in peer leadership outside the organizations that they command and control.[139] This also extends to lower echelon commanders as their forces increasingly act in complex environments around the world as we prosecute the Global War on Terror (GWOT).[140]

---

[135] Notes taken during a presentation to SAMS by a senior joint force commander speaking on the condition of non-attribution. 2004.

[136] Notes taken during a presentation to SAMS by a senior Army commander speaking on the condition of non-attribution. 2004. See also Senge, 290-291. The illusion of control exists when someone has the perception that they can control dynamic and complex interactions "from the top."

[137] The effects design (purpose) describes the "what" with the actors creatively determining the "how" without centralized direct control. Remember that control is maintained through indirect means.

[138] Office of the Chairman o the Joint Chiefs of Staff, *Stability Operations-Joint Operating Concept* [Stability JOC] (Washington, DC., October 03, 2003), 19.

[139] MCO JOC, 7.

[140] Leonard Wong, "Developing Adaptive Leaders: The Crucible Experience of Operation Iraqi Freedom," *U.S. Army Strategic Studies Institute*, 2004, 3-6. Colonel (Ret.) Wong provides a compelling

In short, the need to create unity of purpose and coherence of all effects in the operational environment has expanded. Each effect adds to the overall desired outcome, creates continuous pressure, and changes the decision cycles of the adversary. Moreover, because of an increased ability to identify key relationships and vulnerabilities across an adversary's global operating system, effects may be initiated in many operational areas creating desired effects in others, and vice versa.[141]

Preemption and Prevention

A COP supported by distributed persistent surveillance is also likely to support actions against precursor behaviors, collusion of adversarial actors, and the physical or virtual associations of nodes. Cumulative effects may preempt or diffuse conditions requiring direct lethal force operations. By denying opportunities to the adversary we also deny key conditions for their overall success.[142] Effects based operations are outcome based and are not dependent on a particular organization to generate the input. In the industrial age system, the focus of intelligence was on NAIs. The term is nearly rendered meaningless in a persistent surveillance paradigm. The new term becomes Named Relationships of Interest (NRI). As the enterprise mind gets stronger, CAS analysis becomes increasingly able to predict. With prediction our actions can become more preventative and lethal force is reduced.

---

account describing the range of complex interaction occurring in Iraq today by our junior leaders. Company level leaders and soldiers routinely interact with coalition, multi-agency and non-DoD elements as they transition missions daily (sometimes hourly) from humanitarian and stability support operations, to close combat operations, and back again to non-combat related actions. The demonstrated adaptability, mental agility, and operational flexibility among junior leaders are remarkable.

[141] For example, the persistent surveillance capability may determine linkages among financial transactions in Asia to the transshipment of materials in Africa and the training of an action cell in South America. This is certain to create new methods of developing and executing operational art. We will need new mechanisms to describe, induce and assess coherent effects. If persistent surveillance is a major contributor to generate this understanding for coherent action, it must also include tailored COP as the distribution mechanism for each element taking action. The continuous CAS view of the adversary creates the ability to do this.

[142] Sun Tzu observed, "The highest realization of warfare is to attack the enemy's plans." See Ralph D. Sawyer, *Sun Tzu: The Art of War* (Oxford: Westview Press, 1994), 177.

As an analogy, the Magnetic Resonance Imagery (MRI) created a kind of persistent surveillance in the medical field. As human scanning technologies became more affordable and scanning became more common, scans of individual patients received more frequent imaging. This not only created individual "signature graphs" but improved the evidentiary base (Case Based Reasoning and Inference Models). Doctors could not only review a single patient's results to previous scans, but could also compare anomalies to the base. As the data sets built a greater understanding of the of disease, precursor attributes were identified. With precursors identified, definitive cause and effect linkages were established within the body of medical science. As a result, preventative medicine and alternate treatment options grew tremendously. More and more clinics opened to deal with the increased demands for new treatments. More effective use of medicines and chemotherapy (non-kinetic treatments) resulted in better patient survival rates. With what is called image-guided surgery, doctors also operate with more precision, as *MRI devices scan in real time with during surgery* (kinetic treatments).[143] The capability of the COP should also allow the more precise and effective use of all forms of force across the battlespace.

In the past, cavalry had the role to find and create the next battle and exploit success. Exploitation is an operational term. In the Napoleonic era, there was no deep cavalry because there was no next battle. Industrial age commanders formed cavalry because of the realization that a single "decisive" battle would not end the war. In the twenty-first century, we will see continuous operations and global (small unit) battle. In the information age, cavalry does not exist as much as an organization, but as a sensing system of systems, that being persistent

[143] Ralph J. Begley, Mark Reige, John Rosenblum, and Daniel Tseng, "Adding Intelligence to Medical Devices," *Medical Device and Diagnostic Industry Magazine*, March, 2000, online at http://www.devicelink.com/mddi/archive/00/03/014.html.

surveillance and agents conducting global exploitation operations.[144] Just as cavalry reporting is not perfect, neither is persistent surveillance.

Conclusions and Recommendations

The integration of persistent surveillance with an Information Age Common Operating Picture dramatically increases the potential to transform war fighting and peace management. Continuous sensing of the battlespace environment, a fundamental reordering of the information distribution, and advanced, integrated processing tools for sense making create asymmetric advantages for the United States against all adversaries across the spectrum of war. A coherent national defense system recognizing the global nature of the protracted challenges we face must recognize and support a new means of control due to the reordered information flows, moving actionable intelligence and understanding directly to the individual level.

Persistent surveillance and its associated neural networks create a dynamic and retrievable memory and perception, accessible for all actors capable of leveraging elements of national power. Distributed networked actors are empowered to an unprecedented degree, acting with greater understanding of the adversary and the complex, systemic relationships and influences that drive adversarial behaviors, generate their capabilities, and reveal their intentions. These in turn lead to the distributed ability to act and generate continuous effects on adversaries, their systems, and exponents of these systems- their autonomous agents.

Because of the distributed and parallel nature of the persistent surveillance information distribution through the COP, there will be an expansion of dynamic communities of interest and community of practice, continually redefining operational relationships through complex interaction. Mission packages will form, disband and reform continuously to achieve outcomes.

[144] A key doctrinal component of the cavalry mission is to "Gain and Maintain Contact" with the enemy.

We can leverage a globally distributed capability to wage irregular and "regular" warfare in all battlespace dimensions and at all levels of war. We become the "irregular" force in the protracted Global War on Extremists and move increasingly to preventative and preemptive actions. Decision Support Systems and Expert Information Systems speed the decision cycles and create the ability to anticipate and drive change faster than the adversary can adapt.

Persistent Surveillance will enable the operating attributes as outlined in the Joint Operations Concept and result in new organization, strategy, and authority distribution. With new rule sets, leader and actor/agent behaviors will adapt through training, simulation, experiential learning, creating new operational values and culture.

If the adversary chooses to continue swarming behaviors such as occurred on 9/11, a persistent surveillance capability to find the patterns, relationships and precursors masked in commercial and civil infrastructures is a required capability to defeat them. While the promise of persistent surveillance is transformational when coupled with a broader global security framework and integrated with a twenty-first century COP, we will not be able to fully understand the true potential and emergent qualities of this dynamic system until it is operational.

Perhaps the most significant non-Information Technology (IT) related result from integrating the emergent persistent surveillance capability into a twenty-first century enterprise COP will be on the human capital and the design of security organizations. Rethinking human training models, leadership skills, retention requirements, and better leveraging individual experiential factors are required as an integrated approach to achieve the broader security and operational goals outlined in the Joint Operating Concepts.

Training. Incorporate collaborative problem solving requirements and use simulation to reinforce recognition-primed decision-making at lower levels, such as platoon, squad and teams. Use physical and virtual scenarios with dynamic mission changes, rule set and authority modifications (ROE) as scenarios unfold, and distribute changes to the force through the individualized COPs. Physical skills training for close combat operations should incorporate real time COP feeds and advanced technologies as soon as the spiral insertions allow, practicing the advantages of connecting individual soldiers and entities to the network. Training scenarios should support wide variations to problem solving and encourage innovation at the lowest levels. Training iteration should incorporate the latest experiential data in scenarios. Training

evaluations should specifically reinforce adaptation, virtual and physical collaboration, and mental agility within the mission set. Operational level training should focus on operational design and planning for parallel, distributed actions, using dynamic systems thinking as the basis for a new military science.

Leadership. Shared persistent surveillance and an integrated COP will require leaders comfortable in exercising indirect control over decentralized missions. Leaders must also develop enhanced skills in peer leadership and informal leadership of non-DoD elements that routinely act within the battlespace. Battlespace visualization and understanding increasingly comes from the COP, not a single commander, as no single commander is likely to have the cognitive ability to understand all the complexities and necessary, tempo sensitive interactions within the battlespace, particularly "on the edge" in tactical operations. Direct leaders at the battalion level and below should receive enhanced training to handle greater authorities. Authorities match increased abilities to achieve effects, coming from enhanced, direct information distribution. Organizational leadership should develop around dynamic systems and enterprise leadership models. Senior leader training should reinforce the need to influence and indirectly control distributed operations through adaptive mission planning and effects design, communicated through the commander's effects based purpose and intent. Leaders should be trained to look for opportunities to enable subordinate operations and create option space rather than seeking direct control of tactical execution.

Retain and Leverage Experience. Improve retention incentives and skillfully manage operational experience. The skill sets required in an enterprise mind enabled force with an integrated COP and persistent surveillance feeds will require enhanced skill sets and increased levels of maturity throughout our formations. We should also leverage the collaborative skills and information technology (IT) savvy soldiers in our formations. Soldiers today are increasingly comfortable with pervasive communications and computing technologies. Junior leaders and soldiers have shown to be tremendously adaptive in OIF and OEF. These soldiers are the bloggers, online gamers, "smart mobsters," and chat room influencers of our world today. Retention of experienced soldiers becomes even more important. In the future, tactical engagements may be primarily at the platoon and below levels, with Unit of Action headquarters serving as the enabler and integrator for dispersed companies and platoons. It is foreseeable that SOF elements may even break into individual and split team operations and work even more closely with interagency partners. We have the most experienced and educated force in our history and our future will require maintaining and leveraging our best in this protracted war.[145]

New organizational constructs should emerge, with authorities following the information flows

and an expanded capacity to act:

Reconsider Organizational Design. Since strategy is reflected through organizational design, force designers should continue to emphasize empowerment at lower level formations, primarily company to team levels, for both conventional and special operations forces. Future force designs should continue to emphasize the soldier and soldier level empowerment. Enablers for integrating force, whether the force is from interagency, multi-national partners or the joint

[145] Wong. We should carefully consider how we can leverage the force who have "been through the crucible" to enhance new force and organizational capabilities. We should not squander the demonstrated mental agility and capacity handle authority with responsibility well beyond what was considered appropriate for them just a decade ago.

force should be the product of coherent operational design and planning at the JTF and UA levels, with particular emphasis on shaping and condition setting. It is unclear with enhanced COP capabilities and the disintermediation resulting from the changed, distributed nature of information enabled by persistent surveillance, what the real role of the UEx G2 will be.[146] Theater and national level planning must establish conditions for deep global operations and long-term success in this protracted war.

Revise the experience levels residing at lower level formations. Increased complexity and authorities will require seasoned leaders and mature supporting staff skills in battalion and below combat formations. Leader to led ratios must increase. Companies should have intelligence sections to fully leverage persistent intelligence distribution and enable tactical planning beyond immediate engagements. Majors should command companies, as in the Special Forces and foreign armies, with captains serving in staff and executive officer roles. Lieutenant colonels should lead UA level staff elements, with majors in all battalion level primary staff roles. Track and manage intangible assets across the force, namely specific experience, specialized skill sets, and demonstrated proficiencies. Each of these suggestions raise the operating capacity of edge organizations and further empowers the lowest levels of the force to act with speed and precision.

Create an integrated force structure combining select special operations elements, rapid strike capable conventional elements and "deep" operations forces, including interagency teams. These forces should engage in Theater Security and Cooperation initiatives and operate with specialized ROE and action authority to create effects, many preemptive or preventative. This force would likely have the agility, fluidity, and judgment to be a primary shaping force for global operations and intervene decisively to prevent larger crisis from forming.

Spiral development and integration of Information Technologies provide asymmetric capability to the force if integrated correctly with the human component. A twenty-first century COP must allow:

> **Access and Assurance.** Ensure all mission elements must have access to real time enterprise data via the tailored COP with assurance in content and reliability.
>
> **Mounted and dismounted support.** The tailored COP views must extend support to individuals, rather than just platforms or command posts. Ensure COPs both reach DoD and non-DoD partners. The family of tailorable COP designs should support dismounted operations in remote areas just as seamlessly as it supports an integrated teammate operating from a hotel room in dial up access mode.
>
> **Robust planning and simulation tools** should reside "online" and allow users to integrate real time data with planning products automatically. Inference models, case-based reasoning tools, persistent intelligence visualizations and data animation should

[146] The INSCOM Overwatch initiative is already supporting units in combat in Afghanistan and Iraq, and will expand its scope of operational support when the XVIII Airborne Corps and the Third Infantry Division move into Iraq. UEx G2s and the ACE will continue to have a purpose, but it may shift emphasis from real time support to a greater emphasis in supporting adaptive planning and effects assessment, allowing the Overwatch to provide real-time "KAC-like" direct support to tactically engaged elements through DCGS-A.

support distributed operational design and planning functions. Tactical planners should be able to integrate the same enterprise data into tactical simulation and visualization tools to create dynamic mission rehearsal and tactical analysis visualizations.

Layered security and smart distribution must allow support users to operate within their mission environment and within the appropriate planning horizon. Assess COP designs or preprocessors for the capacity to parse and mitigate data across varied user access authorizations, as verified by biometrics, and across varied data flow requirements.

Reinvention of display and visualization. One size does not fit all. Allow user groups to design and test new COP designs that work within the anticipated operating environments and continue new technology integrations. With Moore's law as a guideline, there may never be an "end goal" to build to, but a steady move to bring understanding to the individual through technology.

The integration of persistent surveillance with the COP allows a re-conception of security, required when today's threat and threat capabilities are not regionally oriented but globally mobile, intertwined with commercial and civil infrastructures.

Homeland defense and DoD. Leverage persistent intelligence to meet our requirements. through a shared COP, supporting the Army sergeant as well as the police sergeant with actionable data, relevant to their specific local environment.

US Security with partners and allies. Create mechanisms and technologies to allow broader access to non-DoD and non-US elements based on mission and effects contribution. Some allies may be advantageously positioned to provide intelligence feeds into the persistent surveillance system. A multinational capable, tailored COP will further enable global agility and coherent actions. Control and information flows come from the KACs, not twentieth century security procedures.

Expand civil and commercial contributions to persistent surveillance. Create mechanisms for private security and local policing, even neighborhood watch programs to submit data into the persistent surveillance system.

Consider the protection of individual civil liberties and our constitution and balance the need for a persistent, sharable intelligence system.

Appendix A. Recommendations for Further Research

The following recommendations for further research on persistent surveillance flow from insights discovered during the preparation of this monograph and have operational implications for the joint force and future operating concepts.

1. Determine the logistical implications for global continuous operations at the individual or team levels. Consider the basing, commercial and/or military mobility, and sustainment issues for infiltrating and extracting actors in the enterprise behavior framework. Consider the use of commercial and contract sustainment for pulsed operations and immediate response requirements. Will a Special Operations Forces model work? What are the implication of Sea Basing and "Lilly Pad" staging bases for supporting such operations?

2. Determine the network needs to support emerging technologies to bring mission relevant COP views on demand to individual actors and entities, DoD and non-DoD, in a distributed enterprise framework. How should commercial information access and delivery systems, such as the World Wide Web, Virtual Private Networks, commercial cellular systems and optical fiber trunks be used to move COP data and persistent surveillance collection, in addition to the GIG?

3. Determine the security and access controls required to provide mission assured information with "pedigree" to the individual actor. What are the implications for enabling user access to the COP with biometric confirmation, advanced data encryption, remote information purges for COP hardware?

4. Assess current investment strategies for the components of persistent surveillance. An initial review indicates the investment strategies and stakeholder orientation may be imbalanced toward space assets to the detriment of remote ground collection, human collection and advanced artificial intelligence and processing components.

5. Adversaries will attempt to use commercial technologies and old-fashioned HUMINT to establish persistent surveillance of their own. What are the new counterintelligence challenges given new approaches for intelligence?

6. Adversaries will attempt to degrade persistent surveillance into "non-persistence" and perhaps force the system back into the reconnaissance paradigm. What are the vulnerabilities and mitigation required to prevent system failure and data corruption?

Appendix B. Some Potential Features, Expectations, and Insights

The COP should also allow a simulated run through of the varied, sequenced timings of the effects, allowing replays and modifications on demand. Once an operational design is approved, processors are given the program logic and units receive their mission sets. Unit commanders, and even individual actors can run virtual rehearsals and execute playback for AAR purposes. Each level of command would have responsibility to develop the timing internal to the specific mission component set and provide a feasibility analysis back to "higher commanders." The feasibility assessment tools would identify the constraining variable and suggest adjustment to relationships as necessary, in collaborative setting among commanders and necessary actors.[147]

In some cases where an observed adversary promises to generate greater intelligence about the CAS than would an arrest or use of lethal force, a "tag" on the entity could show in the COP alerting actors to the entity but flag it as a "do not engage." The dynamic capabilities of the COP would allow very discriminatory inclusion or modification of adversarial data. For example, say a HUMINT source is inside an adversary element and generating details about the financing structure of a particular network. The cell is located within a larger set of cells in an urban area and a unit has the mission to take down the elements. By flagging, they could remain aware of

[147] Digital-analog conversion interfaces could change as well. For example, a human report of the environment is observed in analog form, digitized into a report or graphic forms, sent, and then the process reverses to print a report, display a slide or other means of communicating to the human. The goal should be immediate machine translation and display, the conversion transparent to users on both ends. With voice recognition software, a proliferation of small camera technology, whiteboard collaboration, and automated reporting of biometrics, locations, vehicle status, etc., the speed of understanding should increase. Speech recognition can allow the production of voice reports just as accurately as typing. Closed Caption technology works on the same principle. Digital speech recognition and machine language conversion is already in use in OIF and OEF in handheld version. It is likely the broader application will also find wider use in the SIGINT realm and allow smarter use of human linguists. Imagine the capacity to capture voice transmissions in the network, as they occur, and search for key words and other attributes. A digital repository could allow other forms of alert and information in near real time. A unit in contact could alert the network by voice alone and the text conversion could be displayed in real time for actors associated to the mission, such as on closed-captioned TV. Machine translation could also provide real time conversion in multiple languages to support multinational operations. Digital speech conversion would at least allow replay and search for recovering historical facts and circumstances.

the existence but not interfere with it. In other cases the existence could be pulled from the COP. Because we have a sensor inside the cell, as the other cells are taken down, the feedback and adaptation could be observed "from the inside" of a specific node of the CAS's network. In a persistent surveillance environment, the notions of "Time Sensitive Targets" or "Fleeting Targets" lose traditional meaning.[148] We either have persistence or we don't.

We continue to granularize the level of actor, down to the individual, through flow of persistent surveillance data in a tailored COP. This is not too far of an extension from current operations.[149] The relationship of effects and levels of war are determined by effect designer's intent for outcomes during the effects targeting process, relative to the understanding of the adversaries CAS, and not by the initiator of the effect. Sub-units will have varied levels of understanding of larger aims, but they must understand the logic and purpose for common interaction with other agents. This is an implicit means of control, flowing from the design, rule sets and purpose. The integrating mechanism is the COP. The future continues in this direction. If it is true that we have entered an era of super-empowered individuals, then the COP should invert the network support capacity and create hyper-empowered individuals.[150]

Granularization exponentially increases operational ability to act. By decreasing the physical mass in the battlespace we increase the overall velocity for war. Mass is a Newtonian science principle and equates to force, but also energy. As mass decreases, the overall velocity increases.

---

[148] There may of course be other reasons that the target becomes time sensitive, such as a predicted hostile action (attack, emplace a car bomb, etc). Other conditions may be the movements into another country where we are politically limited in acting, or in cases where the entity may receive other protections, or where we have added the entity to the effects list as a direct effect to cause other effects. The idea of physically tagging entities comes into the realm of the possible to further reduce "time sensitivity" in the traditional use of the term.

[149] For example, what really distinguishes individual actions of an A-10 pilot from that of a soldier? Speed in battlespace transit? Lethality? Effect on the level of war? Certainly both the A-10 pilot and the forward observer are acting as local sensors and feed information back into the system. A single forward observer is empowered to create a tremendous amount of lethal effect in his battlespace, and sustain it if necessary, often blurring the level of effect as scored against a strict categorization of levels of war.

[150] Thomas L. Friedman, *The Lexus and the Olive Tree* (New York: Random House, 1999), 14-15. Friedman first coined the term "Super Empowered Individuals."

This is a law of physics. As velocity increases, force increases without the reciprocal increase in mass. Units of Action are capable of higher operational velocities than Corps. Special Forces teams are capable of higher velocity than Units of Action. In this case velocity relates to agility and the physical ability to move freely in the battlespace relative to the adversary. The other type of increased velocity stems from decision speed increases, supported by Decision Support Systems and pattern recognition flowing to the distributed entities in near real time. As the number of decentralized entities increase, the overall velocity increases.

Risk in the decentralized battlespace also decreases to the force as a whole, since there is no "mass" to attract a focus of high volume, lethal fires. Thus is the dual nature of concentration, the creation of a mass to be attacked. The move is away from mass to distribution and dispersal.[151] The current anti-access strategies are built upon the risk of introducing combat units in large number through identifiable or likely points of entry and the sustainment base support requirements. With similar changes in the logistics system to support a distributed enterprise, physical mass is greatly reduced. The risk for individual agents remains, but not in greater levels than today. With persistent surveillance and the agents acting as their own sensor, combined with the external COP data, they are greatly empowered and mitigate risk dynamically as they interact with the target. If targets begin to form in aggregation, the thresholds change the ROE and behavior rules to allow additional means of force. Because of enterprise behavior and the increasing returns rule, an agent in contact receives a supportive response from all "neighbors"

[151] The "Theory of the Empty Battlefield," explains that the requirement for dispersion is directly related to the increases in weapons system precision and lethality over time. Unit formations have steadily dispersed and operated in ever increasing frontages since the development of the rifled barrel in small arms and accurate artillery beginning around 1870. See James J. Schneider, "The Theory of the Empty Battlefield," *Journal of the Royal United Services Institute,* September 1987, 37–42. In the precision age, detection means destruction. Dispersion and masking (including stealth) is required. The overall drive is to operate from globally dispersed, small forces to achieve effects and avoid the certain result of losing the detection battle with precision-armed adversaries. The lethality of the individual has also steadily increased over time.

and other agents. Since it is a shared tactical COP, the responses come faster than what occur now. Essentially risk is cross-leveled across the mission set of networked agents.

The shared COP will also create re-conceptions of what maneuver is. In the past, units used maneuver to deploy around the enemy while mitigating risk because of uncertainty. If the situation were certain, there is no need to maneuver, the units would just move. Maneuver slows the force. If the purpose is to "gain positional advantage," the real purpose is advantage. Advantage means an overmatch. With persistent surveillance, the agents have informational advantage and do not need to maneuver, except in contact, which is therefore contact and not maneuver. It is movement under fire. Units under fire were caught in a situation without advantage. The real goal is to generate and maintain options and to reduce the options available for the adversary.[152] The operational and tactical level of war is becoming one of fighting for option generation and option execution while reducing and denying options for the enemy.

An enterprise COP enhances both and accelerates option-creating behaviors. With the ability to reduce the adversary's options, the adversary absorbs more pressure. As we increase options we create the ability to act on his leverage points with multiple directions, creates ambiguity and increases pressure across multiple domains, physical, informational and cognitive. Persistent surveillance allows the continuous identification of leverage points. Option advantage allows us to begin to bind the enemy through option acceleration and to reduce sanctuary in each domain and level of war. By acting coherently, the entire enemy CAS, in theory, is overmatched and must absorb the increased pressure.

---

[152] Robert R. Leonhard, *The Principles of War in the Information Age* (Novato, CA: Presidio Books, 1998), 53-79. Other re-conceptions emerge from a COP view supported by persistent surveillance s well. Surprise and Economy of Force become enhanced through increased decision cycle speeds and higher quality information content. The goal becomes a controlled tempo, with each engagement amounting to the 20th century notion of the "ambush" against unprepared adversaries and component systems in each of the battlespace domains and across all levels of war. See also pages 124-137 and 182-193.

The absorption of effects drives the adversary into chaos, through shock to the overall system. The absorption of effects into the CAS affects the regulation of positive feedback and alters the successful adaptation to the environment. To say we create shock means the enemy system is driven out of control of its functioning component systems. Shock itself is also an emergent condition. The duration of the shock is a function of the amount of energy the CAS is forced to absorb and the rate it can dissipate the effects. We observe the effects across the system, apply effects continuously to maintain decisive conditions, and continue to apply energy to limit the dissipation. A shocked system must realize the shock and sense for itself that it is no longer functional, and as such, defeated. This leads directly to affecting will.

Since all living systems are formed to achieve a purpose, or goal, we can say they have goal seeking behaviors. In a system forced into continuous shocks, the goals will change from the original goal to goals further down the hierarchy of needs. Instead of achieving the group goal, enemy agents find themselves seeking goals related to survival. Until they find a way to rejoin the system, which has also changed its goal, the agents are left with a choice to assimilate or to remain apart from the system. This is a great example of the dissolved Iraqi Army in OIF. Left apart from the system, they were forced to rejoin the resistance or to lead a life apart from it. In the Iraqi Army under Saddam the service was compelled through conscription and brutal reprisals for "opting out." The current enemy in Iraq is one of self-selection to a completely different goal than fighting for Saddam or coerced fighting from repressive regime. In error, perhaps, the creation of a "strange attractor" was not formed to compensate in the vacuum left after the de-Ba'athification and the permanent dissolution of the Iraqi Army.[153] Overall, shocks diffuse will and disassociate the parts. We should identify the fissures in the CAS we are fighting a protracted war with and drive wedges among the agents and collective cells, exploiting varied

[153] Waldrop, 226. A strange attractor is a Chaos theory term that describes the tendency of nonlinear dynamic systems in a state of chaos to stabilize behaviors around a unique attribute of the environment. It is a function of complex interactions and is a spontaneous reorientation to the system components and actors.

levels of will and variance in the sub-system goals. Shocks in systems prevent normal functioning. The parts that remain capable of acting through self-reorganization means retention of will and require precision lethal means to destroy the will. Those also appear in the COP.

Appendix C. List of Acronyms

CI	Counterintelligence
CIA	Central Intelligence Agency
CJCS	Chairman, Joint Chiefs of Staff
COP	Common Operating Picture
CPOF	Command Post of the Future
DCGS	Distributed Common Ground System
DCGS-A	Distributed Common Ground System-Army
DIA	Defense Intelligence Agency
DoD	Department of Defense
FBCB2	Force XXI Battle Command Brigade and Below
GIG	Global Information Grid
GCCS	Global Command and Control System
IMINT	Imagery Intelligence
INSCOM	Intelligence and Security Command
ISR	Intelligence, Surveillance and Reconnaissance
IT	Information Technology
JCS	Joint Chiefs of Staff
JOC	Joint Operating Concept [family of related documents]
JOpsC	Joint Operations Concepts [overarching document]
JROC	Joint Requirements Oversight Council
LRS	Long Range Surveillance
LEA	Law Enforcement Agencies
MASINT	Measurements and Signatures Intelligence
MCO	Major Combat Operations
NSA	National Security Agency
OEF	Operation Enduring Freedom
OIF	Operation Iraqi Freedom
OPFOR	Opposing Forces
OSINT	Open Source Intelligence
PID	Positive Identification
PIR	Priority Intelligence Requirements
SOF	Special Operations Forces
SIGINT	Signals Intelligence
UA	Unit of Action (Army)
UE	Unit of Execution (Army with X and Y designations)
USCENTCOM	United States Central Command
USJFCOM	United States Joint Forces Command
USSTRATCOM	United States Strategic Command
WIN-T	Warfighter Information Network-Tactical

Appendix D. Assumptions

The following assumptions establish a base of relevant factors to begin this study. Further research or qualifications in these areas are not addressed within this monograph.

1. The Persistent Surveillance Concept is technically feasible. The technologies required to implement major aspects of Persistent Surveillance are feasible and, in some cases, in operation today. Future capabilities are part of DoD acquisition programs and will reach maturity and integration.

2. National level policy decisions supporting major aspects of Persistent Surveillance will be made and are understood in the context of enabling a Persistent Surveillance paradigm. Policy decisions to support horizontal integration of intelligence databases, intelligence sharing, intelligence fusion, and broader dissemination authorities are addressed by both the Intelligence Community (IC) and the DoD.

3. The reorganization of the IC, particularly the Defense Intelligence segments, eliminates the Task-Process-Exploit-Disseminate approaches and explicitly adopts the Task-Post-Process-Use, emphasizing horizontal integration to capitalize on Persistent Surveillance.

4. The DoD's acquisition strategy shift to spiral development and rapid technical insertion will integrate Persistent Surveillance capabilities into the force over time. There will not be a single programmatic milestone for the fielding of "Persistent Surveillance."

5. Persistent Surveillance will not remove "the fog of war." The promise of "near perfect knowledge" is relative to the knowledge generally available today. There will be a qualitative increase in specific types of fused intelligence and combat information available at lower levels of command in near real time.

6. Operational and tactical level commanders will continue to require organic (organizational) ISR capability to reduce knowledge gaps and provide direct support to close combat operations.

Appendix E. Acknowledgements

The following individuals provided great insight and were instrumental in developing this monograph.

Vice Admiral Lowell Jacoby, Major General John F. Kimmons, Mr. Louis Andre, COL Kevin C. Benson, COL Stefan J. Banach, Dr. James J. Schneider, Col (Ret.) Richard Szafranski, COL (Ret.) Neal Vinson, LTC (Ret.) Collin Agee, LTC Stephen Iwicki, and my SAMS classmates.

Bibliography

Books

Alberts, David S. John J. Garstka, Richard E. Hayes, and David A. Signori. *Understanding Information Age Warfare.* Washington, D.C.: Command and Control Research Program, 2001.

Alberts, David S., and Richard E. Hayes. *Power to the Edge.* Washington, D.C.: Command and Control Research Program, 2003.

Arquilla, John, and David Ronfeldt. *Swarming and the Future of Conflict.* Santa Monica, CA: RAND, 2000.

Barker, Joel. *Future Edge: Discovering the New Paradigms of Success.* New York. William Morrow and Company, Inc., 1992.

Berkowitz, Bruce D., and Allen E. Goodman. *Best Truth: Intelligence in the Information Age.* New Haven: Yale University Press, 2000.

Bowden, Mark. *Black Hawk Down: A Story of Modern War*. New York: Atlantic Monthly Press, 1999.

Campen, Alan D. *The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War*. Fairfax, VA: AFCEA International Press, 1992.

Davidson, Paul. *A Primer in Theory Construction*. Boston. Allyn and Bacon. 1971.

Doughty, Robert Allen. *The Breaking Point: Sedan and the Fall of France, 1940*. New Haven, CT. Archon Books, 1990.

Fontenot, Gregory, Degan, A.J., and Tohn, David. *On Point: The United States Army in Operation Iraqi Freedom*. Fort Leavenworth, KS. Combat Studies Institute Press, 2004.

Friedman, Thomas L. *The Lexus and the Olive Tree*. New York: Random House, 1999.

Hall, Wayne Michael. *Stray Voltage: War in the Information Age*. Annapolis, MD: Naval Institute Press, 2003.

Johnson, Stuart E., Martin C. Libicki, (eds.) *Dominant Battlespace Knowledge: The Winning Edge*. Washington, DC: National Defense University Press, 1995.

Keegan, John. *Intelligence in War: Knowledge of the Enemy from Napoleon to Al-Qaeda.* New York: Alfred A Knopf, 2003.

Kelly, Kevin. *Out of Control: The New Biology of Machines, Social Systems and the Economic World.* Cambridge, MA: Perseus Books, 1994.

Klein, Gary. *Sources of Power: How People Make Decisions*. Cambridge, MA: MIT Press, 1999.

Krygiel, Annette J. *Behind the Wizard's Curtain: An Integration Environment for a System of Systems*. Washington, D.C.: Command and Control Research Program, 1999.

Laudon, Kenneth C., and Jane P. Laudon. *Management of Information Systems: Managing the Digital Firm.* 7th ed. Upper Saddle River, NJ: Prentice Hall, 2002.

Leedy, Paul D., and Jeanne Ellis Ormrod. *Practical Research: Planning and Design.* 7th ed. Upper Saddle River: Prentice Hall, 2001.

Leonhard, Robert R. *Fighting By Minutes: Time and the Art of War*. Westport, CT: Praeger Publishers, 1994.

_____. *The Principles of War for the Information Age*. Novato, CA: Presidio Press, 2000.

Marakas, George M. *Decision Support Systems in the 21st Century*. Upper Saddle River, NJ: Prentice Hall, 1999.

Naveh, Shimon. *In Pursuit of Military Excellence: The Evolution of Operational Theory*. Portland, OR: Frank Cass, 1997.

Potts, David (ed). *The Big Issue: Command and Combat in the Information Age (A View from Upavon)*. Washington, D.C.: Command and Control Research Program, 2003.

Reynolds, Paul Davidson. *A Primer in Theory Construction* Boston: Allyn and Bacon, 1971

Sawyer, Ralph D. *Sun Tzu: The Art of War*. Oxford, Westview Press, 1994.

Senge, Peter M. *The Fifth Discipline: The Art and Practice of the Learning Organization*. New York. Doubleday, 1990.

Smith, Edward A. *Effects Based Operations: Applying Network Centric Warfare in Peace, Crisis and War*. Washington, D.C.: Command and Control Research Program, 2002.

Townsend, Elias Carter. *Risks: The Key to Combat Intelligence*. Harrisburg, PA: The Military Service Publishing Company, 1955.

Turabian, Kate L. *A Manual for Writers of Term Papers, Theses, and Dissertations*. 6th ed. Chicago: University of Chicago Press, 1996.

Van Crevald, Martin. *Command in War*. Cambridge, MA.: Harvard University Press, 1985.

Waldrop, M. Mitchell. *Complexity: The Emerging Science at the Edge of Chaos.* New York. Touchstone Books, 1992.

Whitten, Jeffrey L., Lonnie D. Bentley, and Kevin C. Dittman. *Systems Analysis and Design Methods*. 5th ed. New York: Irwin McGraw-Hill, 2000.

Yin, Robert K. *Case Study Research: Design and Methods*. 2nd ed. Thousand Oaks, NJ: Sage Publications, 1994.

U.S. Government Publications

National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. Official Government ed. Washington, D.C.: U.S. Government Printing Office, 2004.

Chairman of the Joint Chiefs of Staff. *Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 2003.*. Washington, D.C.: U.S. Government Printing Office, 2003.

Chairman of the Joint Chiefs of Staff. *Joint Publication 2-0, Doctrine for Intelligence Support to Joint Operations*. Washington, D.C.: U.S. Government Printing Office, 2000.

Chairman of the Joint Chiefs of Staff. *Joint Publication 2-01, Joint and National Intelligence Support to Military Operations*. Revision Final Coordination. Washington, D.C.: U.S. Government Printing Office, 2003.

Chairman of the Joint Chiefs of Staff. *Joint Publication 3-0, Doctrine for Joint Operations*. Washington, D.C.: U.S. Government Printing Office, 2001.

Chairman of the Joint Chiefs of Staff. *Joint Publication 5-0, Doctrine for Joint Planning Operations*. Washington, D.C.: U.S. Government Printing Office, 1995.

Chairman of the Joint Chiefs of Staff. *Joint Publication 6-0, Doctrine for Command, Control, Communications, and Computers (C4) Systems Support to Joint Operations*. Washington, D.C.: U.S. Government Printing Office, 1995.

Congressional Research Service. *Military Transformation: Current Issues in Intelligence, Surveillance, and Reconnaissance*. Report prepared by Judy G. Chizek. Washington, D.C.: Congressional Research Service, 2003.

"Transformation Study Report: Transforming Military Operational Capabilities." Executive Summary. *Office of the Secretary of Defense*. 2001.

Rumsfeld, Donald H. "Quadrennial Defense Review Report." *Office of the Secretary of Defense.* 2001.

U.S. Department of the Army. *FM 2-0, Intelligence*. Washington, D.C.: U.S. Government Printing Office, 2004.

U.S. Department of the Army. *FM 3-0, Operations*. Washington, D.C.: U.S. Government Printing Office, 2001.

U.S. Department of the Army. *FM 34-1, Intelligence and Electronic Warfare Operations*. Washington, D.C.: U.S. Government Printing Office, 1994.

U.S. Department of the Army. *FM 34-2, Collection Management*. Washington, D.C.: U.S. Government Printing Office, 1994.

U.S. Department of the Army. *FM 34-2-1, Tactics, Techniques, and Procedures for Reconnaissance and Surveillance*. Washington, D.C.: U.S. Government Printing Office, 1991.

U.S. Department of the Army. *FM 34-37, Echelon Above Corps Intelligence and Electronic Warfare Operations*. Washington, D.C.: U.S. Government Printing Office, 1991.

U.S. Department of the Army. *FM 6-0, Mission Command: Command and Control of Army Forces.* Washington, D.C.: U.S. Government Printing Office, 2004.

U.S. Marine Corps. *MCWP 2-1 Intelligence Operations.* Washington, D.C.: U.S. Government Printing Office.

Articles

Ackerman, Robert K. "Horizontal Integration Challenges Intelligence Planners: Linking Collection and Dissemination Systems May Be the Key to Winning the War on Terrorism." *Signal Magazine*. (October 2003).

Begley, Ralph J., Reige, Mark, Rosenblum, John, and Tseng, Daniel. "Adding Intelligence to Medical Devices." Medical Device and Diasgnostic Iondustry Magazine. (online) (March 2000), located at http://www.devicelink.com/mddi/archive/00/03/014.html.

Accessed November 02, 2004.

_____. "Persistent Surveillance Comes into View." *Signal Magazine*. (May 2002).

Dunn, Richard J., Price T. Bingham, and Charles A. Fowler. "Unblinking Eye in Space." *Intelligence, Surveillance and Reconnaissance Journal* Vol 3, No. 7 (August 2004): 20-24.

"DoD Moving to Link Iraq Bound Army Units with Fusion Network." *Inside the Pentagon*. 1.

Goodman, Glenn W., Jr. "Intel Internet: U.S. Air Force Pioneers Joint-Services Information Sharing Network." *Intelligence, Surveillance and Reconnaissance Journal* Vol 3, No. 7 (August 2004): 26-30.

_____. "Made to Order: U.S. Special Operations Forces Display their Strengths in Afghanistan War." *Armed Forces Journal International*. (December 2001).

_____. "Nowhere to Hide: Space Based Radar Promises Unprecedented Recon Capabilities." *Intelligence, Surveillance and Reconnaissance Journal* Vol. 3, No. 6 (July 2004): 12-18.

Gormley, Dennis M. "Estimating Ambiguity The Limits of Intelligence: Iraq's Lessons." *Survival The IISS Quarterly*. Vol. 46, No. 3. (Autumn 2004): 7-28.

Kasales, Michael C. "The Reconnaissance Squadron and ISR Operations." *Military Review* (May-June 2002): 52-58.

Kenyon, Henry S. Many Threads Weave the Big Picture." *Signal Magazine* (March 2003).

Matthews, Benjamin M. and A. J. Seidensticker. "3ID COLT Employment in OIF." *Field Artillery* (March-June 2004): 32-33.

Schneider, James J. "Blacklights: Chaos, Complexity, and the Promise of Information Warfare." *Joint Forces Quarterly*. (Spring 1997): 21-28.

_____. "The Theory of the Empty Battlefield." *Journal of the Royal United Services Institute.* (September 1987) 37–42.

Scully, Megan. "Social Intel: New Tool for U.S. Military: Intelligence Increasingly Focuses on Relationships Among Individuals." *Defense News*. (April 26, 2004): 21.

Szafranski, Richard. "Neocortical Warfare? The Acme of Skill." *Military Review*. (November-1994). 41-55.

Talbot, David. "How Technology Failed in Iraq." *Technology Review*. (November 2004): 38.

Thomas, Evan and Nordland, Rod. "How We Got Saddam." *Newsweek*. (December 22, 2003).

Waller, Karen. "A Model of the Future: Multi-Intelligence Tool is on Fast Track." *Intelligence, Surveillance and Reconnaissance Journal* Vol. 3, No. 8 (September 2004): 40-44.

Wass de Czege, Huba, and Biever, Jacob D. "Future Battle Command: Where Information Technology, Doctrine, and Organization Meet." *Army Magazine* (August 2001).

Weslander, Michele. "Multi-INT Collaboration: Geospatial and Signals Intelligence Analysts Lead the Way in Sharing Data," *Intelligence, Surveillance and Reconnaissance Journal* Vol. 3, No. 4 (May 2004): 18.

Wilson, J.R. "Space Assets Transform U.S. Command and Control" *Intelligence, Surveillance and Reconnaissance Journal* Vol. 3, No. 6 (July 2004): 38-40.

Wong, Leonard. "Developing Adaptive Leaders: The Crucible Experience of Operation Iraqi Freedom." Carlisle, PA: *United States Army Strategic Studies Institute*, 2004.

"OFT: New Defense Opportunities." *Washington Technology*. (19 August 2004).

Miscellaneous

"ACS [Airborne Common Sensor]: Knowledge at the Point of Decision and Key to the Objective Force Success." Issue Paper Number 11. *Association of the United States Army*. 2003.

"A Game Plan for Advancing Army Objectives in FY05 and Beyond: Thinking Strategically." *Office of the Chief of Staff of the Army*. Washington, D.C. 2004.

Bowie, Christopher J. "Destroying Mobile Ground Targets In An Anti-Access Environment." *Northrup Grumman Analysis Center Papers.* 2001.

Biggie, Jeremie. "Operational Net Assessment." Presentation. *United States Joint Forces Command.* November 19, 2003.

Burles, Joe. "Actionable Intelligence Relies on Every Soldier." *Army News Service* (online), April 13, 2004, located at http://www.tradoc.army.mil/pao/Web_specials/FocusAreas/actionableintelligence.htm. Accessed November 06, 2004.

Cambone, Stephen A., "Statement of Dr. Stephen A. Cambone, Under Secretary of Defense for Intelligence, Before the Senate Armed Services Committee, Strategic Forces Subcommittee, Intelligence, Surveillance and Reconnaissance." *Office of the Under Secretary of Defense- Intelligence.* April 7, 2004.

Chairman of the Joint Chiefs of Staff. Joint Operations Concepts: JCS Version 1.0. JCS and JROC Endorsed. *Office of the Joint Chiefs of Staff.* Washington, D.C. 2003.

Chairman of the Joint Chiefs of Staff. Major Combat Operations -Joint Operating Concept: *Office of the Joint Chiefs of Staff.* Washington, D.C. 2004.

Chairman of the Joint Chiefs of Staff. Stability Operations-Joint Operating Concept: *Office of the Joint Chiefs of Staff.* Washington, D.C. 2003.

Cordesman, Anthony H. "The Lessons of Afghanistan: Warfighting, Intelligence, Force Transformation, Counterproliferation and Arms Control Executive Summary." *Center for Strategic and International Studies*. 2003.

Cooper, David G. "Context Based Shared Understanding for Situation Awareness." *Lockheed Martin Advanced Technology Laboratories.* 2004.

Dahlstrom, Eric L. "From Reconnaissance to Surveillance: Intelligence Transformation in the New Millennium." *National Defense University.* 2003.

Gawrych, George W. The 1973 Arab-Israeli War: The Albatross of Decisive Victory. Leavenworth Papers Number 21. Leavenworth, KS. Combat Studies Institute, 1996.

Hayden, Michael V., Lieutenant General, USAF. "Address to Kennedy Political Union of American University," *Office of the Director, National Security Agency*, February 17, 2000

Jacoby, Lowell, Vice Admiral, USN. "Revolution in Intelligence Affairs." Presentation. *Armed Forces Communications Association, Spring Intelligence Symposium (AFCEA)*, Langley, VA. April 22, 2004

Kimmons, John F., Major General, USA. "INSCOM: The Army's Operational Intelligence Force." Presentation. *Global Intelligence, Surveillance, and Reconnaissance Conference. Sponsored by the United States Strategic Command (STRATCOM).* Denver, Colorado, September 29, 2004.

Nagata, Michael. "DoD Intelligence, SOF, and the Global War on Terrorism." Presentation. U.S. Army Command and General Staff College, SOF Track. *Office of the Undersecretary of Defense for Intelligence and Warning*. December 19, 2003.

"Operational Implications of the Collaborative Information Environment (CIE)." Pamphlet 5. Suffolf, VA. *Joint Warfighting Center.*

Phister, Paul W., Jr., Timothy Busch and Igor G. Plonisch. "Joint Synthetic Battlespace: Cornerstone for Predictive Battlespace Awareness." *Air Force Research Laboratory/Information Directorate.*

Piccerillo, Robert A. and David A. Brumbaugh, "Predictive Battlespace Awareness: Linking Intelligence, Surveillance and Reconnaissance Operations to Effects Based Operations." *White Paper Presentation, 2004 Command and Control Research and Technology Symposium.* 2004.

Rosen, Julie A., and Smith, Wayne L. "Influence Net Modeling for Strategic Planning: A Structured Approach to Information Operations." Preprint. *Phalanx* (online) (December 2000), located at http://www.inet.saic.com/inet-public/welcome_to_saic.htm. Accessed November 21, 2004.

Scales, Robert H. "Army Transformation: Implications for the Future." *Prepared Statement of Testimony, U.S. House of Representatives, Armed Services Committee.* July 15, 2004.

Thompson, Carol A. "ISR Management to Optimally Satisfy Warfighter Information Requirements." Presentation. *Defense Advanced Research Projects Agency, Tactical Technology Office.* 2003.

"White Paper. National Security and Horizontal Integration." *Armed Forces Communications and Electronics Association. 2004.*

"White Paper. Agent Development Concepts in Support of TCT ISR Operations." *Computer Technology Associates.* 2003.

"White Paper. Time Critical Targeting for Global Strike Task Force: Systems/Software Engineering Considerations." *Computer Technology Associates.* 2003.

"White Paper. Intelligence Reach." *U.S. Army Intelligence Center and School.* 2001.

"White Paper. ISR Integration." *U.S. Army Intelligence Center and School.* 2001.

"White Paper. Overwatch." Draft Version 1. *U.S. Army Intelligence and Security Command.* 2004.

"White Paper. Unit of Action Intelligence Surveillance Reconnaissance." *U.S. Army Program Manager Unit of Action Intelligence Surveillance and Reconnaissance*. 2003.

"2003 Army Transformation Roadmap." *Department of The Army*. 2003.

Interviews

Andre, Louis. Chief of Staff, Defense Intelligence Agency. Pentagon. Washington, D.C. Interview by author. October 06, 2004.

Jacoby, Vice Admiral (VADM) Lowell. Director, Defense Intelligence Agency, Pentagon, Washington D.C. Interview by author. October 06, 2004.

Kimmons, Major General (MG) John. F. Commander, U.S. Army Intelligence and Security Command (INSCOM). Fort Belvoir, VA. Interview by author. August 25, 2004.