THE CHALLENGES OF INFORMATION MANAGEMENT IN THE NETWORKED BATTLESPACE:

UNMANNED AIRCRAFT SYSTEMS, RAW DATA AND THE WARFIGHTER

GRADUATE RESEARCH PROJECT

Samuel D. Bass, Maj, USAF

AFIT/IC4/ENG/06-01

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright- Patterson Air Force Base, Ohio

The views expressed in this graduate research project are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

AFIT/IC4/ENG/06-01

THE CHALLENGES OF INFORMATION MANAGEMENT
IN THE NETWORKED BATTLESPACE:
UNMANNED AIRCRAFT SYSTEMS, RAW DATA AND THE WARFIGHTER

GRADUATE RESEARCH PROJECT

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in C4I Systems

Samuel D. Bass, M.S.

Major, USAF

June 2006

AFIT/IC4/ENG/06-01

THE CHALLENGES OF INFORMATION MANAGEMENT
IN THE NETWORKED BATTLESPACE:
UNMANNED AIRCRAFT SYSTEMS, RAW DATA AND THE WARFIGHTER

GRADUATE RESEARCH PROJECT

Samuel D. Bass, Major, USAF

Approved:

// signed // 9 June 2006

Guna S. Seetharaman, Ph.D. (Chairman) Date

// signed // 9 June 2006

Robert F. Mills, Ph.D. (Member) Date

AFIT/IC4/ENG/06-01

Abstract

The purpose of this research project was to explore how information is collected and used in the battlefield and identify areas of further research that could help ease the burden of processing, managing and transmitting that information. The research included surveys of the intelligence analysis process and an exploration of some of the sources of data produced and consumed in the battlespace. The findings of this research led to the identification of several areas of research that could help warfighters deal with the problems posed by the DoD's rapidly growing mountain of unorganized and unprocessed data.

The culmination of the research is the development of the Integrity-Relevance-Classification Data Sharing Model developed by the author and Dr. Rusty Baldwin (AFIT Staff), and proposes areas for its future analysis and implementation.

To Julie,

Thanks for putting up with my countless hours behind the computer.

You’re my best buddy!

Acknowledgements

I would like to express my sincere appreciation to my faculty advisor, Dr. Guna Seetharaman, who planted the seeds that became the focus of this paper and for more ideas than I could hope to accomplish in this too-short period of time. I'm not done yet! I would also like to thank Dr. Robert Mills for his help in placing me in the right program here at AFIT; you're right sir: motivation and desire do make a difference. To Dr. Rusty Baldwin I pass on thanks for the brilliantly taught and thought-provoking class on Information Security, and I hope our work isn't done yet.

To the AFIT faculty and staff, I pass on my sincere thanks for putting together such a great program in a tough environment. For me, this was a life-changing opportunity and I am deeply honored that I was chosen to be an AFIT student.

Thanks again to all of you,

Samuel D. Bass

Table of Contents

The Challenges of Information Management in the Networked Battlespace: Unmanned Aircraft Systems, Raw Data and the Warfighter

1 Intelligence – Process and Sources

In current conflicts against terrorists with dynamic or even poorly defined communications lines and chains of command, traditional intelligence analysis might not normally yield effective information during the planning phase of the terrorist's mission. As a result, the first indicator of a terrorist event is in many instances some physical change in an environment like a vehicle evading a barrier or parking in an unusual location, or an object like a bag or suitcase left in a public space. Other indicators might appear completely ordinary and would not trigger any significant intelligence analysis; their utility in the plan might not be discovered until well after the event occurs. Besides visual cues, other sources of information could provide warning of an attack or lead investigators to the source of an attack. Unfortunately, the traditional goal of knowing your enemy before battle cannot be fully achieved against a dynamic population of terrorist actors. In response, new and non-traditional methods of intelligence, surveillance and reconnaissance (ISR) are being researched and field-tested.

Before we can effectively discuss methods for improving information collection and storage, we need to understand the intelligence process that converts raw pieces of data into meaningful intelligence. This section will define some key intelligence terms, summarize the intelligence process and discuss some of the sources that are currently or could potentially provide inputs to this process.

1.1 Definitions

DOD Joint Doctrine provides several definitions, but the primary definition of Intelligence is listed as follows:

> *1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas.*
>
> *2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.* [JP 2-0, pg GL-5]

Likewise, Information is defined as follows:

> *Facts, data, or instructions in any medium or form.* [JP 2-0, pg GL-4]

Since there is a key distinction between raw data and intelligence, it is important to note that data and information can be small atomic pieces of information not necessarily ready for consumption by end users. Raw information will not necessarily become "intelligence" about a particular subject or condition without analysis using the intelligence process and will be referred to as unprocessed data. When data is processed by some portion of the intelligence process, we will refer to it explicitly as processed data or intelligence information.

Intelligence Sources provide information used in the intelligence process and are defined in the Joint Doctrine as follows:

> *The means or system that can be used to observe and record information relating to the condition, situation, or activities of a targeted location, organization, or individual. An intelligence source can be people, documents, equipment, or technical sensors.* [JP 2-0, pg GL-6]

Because we will be focusing our efforts on automated data feeds from multiple sources, the "technical sensor" term of the above definition deserves more discussion. Sensors of various kinds have been used in warfare for centuries, beginning with trip wires and snares used to entangle intruders or pinpoint perimeter breaches. Modern sensors include remote sensing stations that report weather and visibility data for airfield conditions, ground sensors for reporting vibration or acoustic readings, or airborne sensors to report friendly and hostile aircraft locations or ground details such as terrain or troop emplacements. [Correll] To meet the requirements of the DoD's goal for a fully interconnected fighting force, future sensors will need to implement an easily deployable high-speed connectivity system to link to one another for data aggregation and sharing. As defined in JP 2-0, an intelligence source can come from one of seven intelligence disciplines: imagery intelligence (IMINT); human intelligence (HUMINT); signals intelligence (SIGINT); measurement and signature intelligence (MASINT); open-source intelligence (OSINT); technical intelligence (TECHINT); and Counterintelligence (CI). [JP 2-0, pg II-2]

The Infosphere is a term that has emerged to describe all of the information available in the battlespace. Some sources define the infosphere as all *knowledge* about the battlespace, which infers analysis and understanding. (USAF-SAB) Because the author believes that every piece of information—accurate, inaccurate, analyzed or not—will impact the warfighter's decision making efficiency, this paper defines the infosphere as the space that contains all raw information, misinformation, processed data and intelligence relevant to, related to or simply present in the battlespace.

Computer Assisted Detection/Computer Assisted Classification (CAD/CAC): Techniques using image processing, artificial intelligence and statistical analysis to detect and group objects in an image. CAD/CAC techniques have been used to detect cancers, identify manufacturing flaws, and identifying targets in weapon system sensors.

1.2 Intelligence Process

In order to discuss key areas that will be complicated by tomorrow's sensors and data processing systems, we will use the Joint Doctrine definition of the Intelligence Process. The process is composed of six phases: planning and direction; collection; processing and exploitation; analysis and production; dissemination and integration; and evaluation and feedback. The intelligence cycle is focused on the mission, which is a key focus area of the process but not necessarily part of the process. Similarly, each phase does not need to be accomplished sequentially; conversely, each phase can affect other phases, and the other phases can begin and end at any time. The cycle is depicted in Figure 1 below.

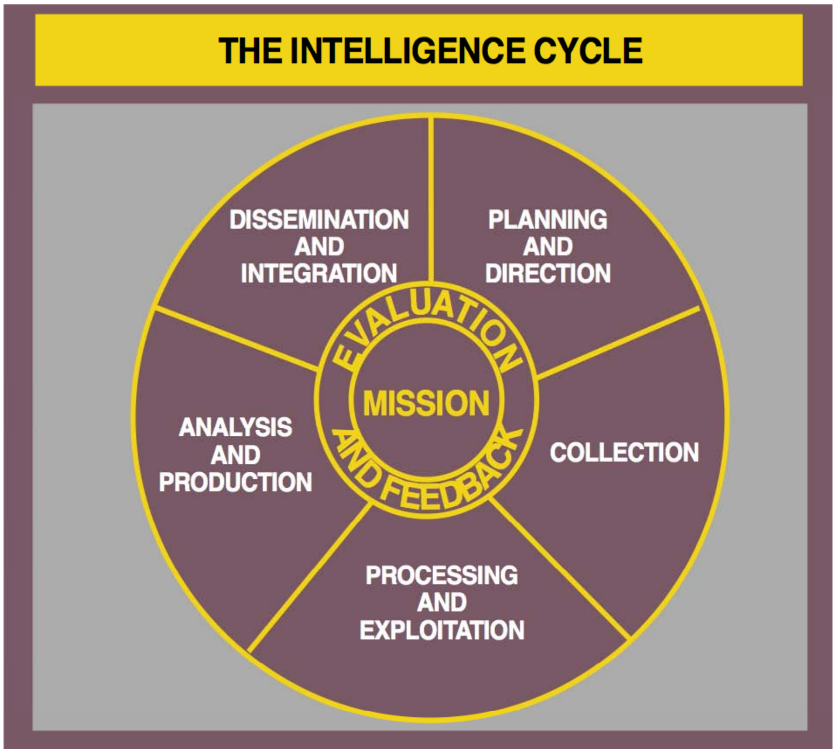


Figure 1: The Intelligence Cycle [JP 2-0, pg II-1]

A quick summary of each phase will ensure that our discussion remains focused on the applicable phases of the intelligence cycle.

Planning and direction: In the context of JP 2-0, intelligence planning and direction happens at one of two times: “well ahead of time as part of a command’s overall, integrated deliberate planning process” or “when a particular crisis situation unfolds” [JP 2-0, pg II-2]. Normally, intelligence is continually gathered for a particular area of responsibility. Combatant commanders use this information to prepare deliberate plans to respond to probable events. If or when a situation occurs, the deliberate plans are used as the basis of a crisis action plan that is built *ad hoc* in reaction to the situation. The intelligence used during the planning phase is a combination of previously collected intelligence and constantly emerging intelligence. As a plan is executed, new intelligence is used in the direction of operations.

Collection: The collection phase is a cycle in itself; in this phase, information requests are matched with collection means, information is collected, and future collection planning is revised based on the success of collection and any emerging requirements for information.

Processing and exploitation: This phase is where raw information is processed, dissected, translated and converted into information usable by intelligence analysts in the production phase. Information is not normally released to the warfighter at this point, but networked sensors could prove to complicate this phase of the intelligence process. As stated in JP 2-0, data from various sources require "different degrees of processing before they can be used." [JP 2-0, pg II-8]

Analysis and production: In this phase, intelligence analysts in units at every echelon of the command structure produce products to meet the commander's requests for information. Depending on the form of the product and the source data, the production tasks can be shared and accomplished around the world. Typically the products fit into one of six categories: indications and warning (I&W); current; general military; target; scientific and technical; and counterintelligence (CI). While an in-depth understanding of each of these product types is not necessary, we will be referring to several of these products, so a brief summary is warranted.

> Indications and Warning: Time-sensitive warnings or indications of foreign threats against the United States, our interests or our allies.
>
> Current Intelligence: Updated all-source intelligence about a particular region or situation.
>
> General Military Intelligence: Information concerning the capabilities and intentions of foreign military or non-uniformed combatant units.
>
> Target Intelligence: Information used in the selection of targets and the apportionment of munitions or tactics to impact those targets
>
> Scientific and Technical Intelligence: Information on foreign activities that may result in military advancements or technologies with warfare potential.
>
> Counterintelligence: Products that summarize the intelligence threats posed by other intelligence agencies or organizations.

In order to be responsive to warfighter needs, the analysis and production phase needs to be efficient and rapid. Since this process could get new data from other sources on the same subject during analysis, it will need to be continually automated and improved to keep up with the increased volume of sensors.

Dissemination and integration: This is where information is delivered to the consumer using whatever means are available for transmission. Care was taken in JP 2-0 to emphasize that the "diversity of dissemination paths reinforces the need for interoperability" [JP 2-0, pg II-13]. This is a key point that we will revisit; the bandwidth requirement of systems that create, produce and share information is a primary concern of this paper.

Evaluation and feedback: Feedback on the quality of products from each phase is a key control mechanism used to determine the quality of every aspect of the intelligence process; the feedback is provided to personnel at all levels of the intelligence community.

1.3 Data Sources

The information used in the intelligence process can come from any number of sources. Recall that doctrine groups sources into seven categories: IMINT; HUMINT; SIGINT; MASINT; OSINT; TECHINT; and CI. To ensure the integrity of derived intelligence, data is sought from multiple sources to avoid bias and susceptibility to misinformation and deception. [JP 2-0, pg II-2] In some cases, sources are sought in other categories to verify the information from another source; for example, a HUMINT source could be verified with MASINT data. The data from sources in any of these categories can come in the form of the following formats.

1.3.1 Text

Data from any source can be communicated in text format, which is a representation using alphanumeric characters. Paper-based information can be read or translated as source material, while electronic transmissions of text can be used to represent other encoded data types. Data in the text format can be used as inputs for automated systems or part of standard file formats like text files, audio, video, or imagery data files. For the purposes of this paper, we will refer to text formatted sources as data readable by a human, so imagery or other data digitized and transmitted as a series of text characters is will not be considered text data. Some sources in text format will be readable by humans *and* used as inputs to automated systems. For example, data in eXtensible Markup Language (XML) is a text format data source that is readable by both humans and automated systems.

1.3.2 Still Imagery

Data representing imagery can be in multiple formats representing various spectrums of electromagnetic radiation, ranging from visible to non-visible imagery (infrared and radar, for example). Imagery can be formatted on film, paper or digitally, and can come from surface, air and space-based sources. Electronic file sizes for still imagery depend on the amount of detail, resolution and compression scheme for the image. Today's basic consumer digital cameras readily produce images compressed using the Joint Photographic Experts Group (JPEG) standard that average 1-megabyte in size. This image quality and size is a useful analogy when describing images taken by sensors for analysis; military-grade sensors with better optics and circuitry could take images that are significantly larger. Imagery data can be transmitted physically or virtually using networks of nearly any type, but transmission speed is very dependent on file size and available bandwidth.

1.3.3 Video Imagery

Data representing video imagery can be collected and transmitted using magnetic tape, film, digital video files or other video formats. Typical file sizes vary with quality, ranging from low quality, grainy resolution movies averaging 5 megabytes per minute to the DVD-quality digital video file size of 200 megabytes per minute. Since file sizes can be very large for television-quality digitized video, available network bandwidth is a critical factor for transmitting video imagery. The adoption of the high definition video standard will significantly increase resolution and file size, placing even more demands on bandwidth for transmission.

1.3.4 Audio

Data representing audio information can be collected and transmitted using magnetic tape, digital audio files or other forms of audio capture. Audio file sizes vary with encoding bit rates and compression schemes, but voice-only audio files can vary in size with high-quality files averaging about 250 kilobytes per minutes. Audio data is typically included with video imagery data.

1.4 Sensor Platforms

The DoD has deployed automated and remotely operated sensors in the battlespace for decades. In Vietnam, US forces deployed remote sensors to track hostile ground forces using seismic and acoustic detectors. [Correll] In our oceans, sonobuoys have been used across the globe to detect, identify, and track surface and subsurface vessels. Platforms orbiting the earth provide valuable intelligence information about our borders and our potential adversaries. Today, technological advancements and the reduced costs of electronics have enabled more advanced sensors to be deployed anywhere in the world and uplink this data for analysis. The proliferation of sources and hunger for data are creating a complicated environment filled with increasing amounts of unprocessed information. Sensors can be placed in the particular environment of interest in nearly any environment; in the ocean, on land, or attached to a vehicle. Sensor pods are prevalent on aircraft, ocean vessels, and are now commonly integrated in military land vehicles. One sensor platform gaining much media and Congressional attention lately is unmanned vehicles. Due to long loiter time requirements or hostile conditions for most Intelligence Surveillance and Reconnaissance (ISR) missions, manned vehicles may not always be a viable option. Unmanned vehicles that operate on land, in or on water, or in the air can be either remotely operated or autonomous. Remotely operated vehicles are controlled by humans connected to the vehicle by some wired or wireless technology, while autonomous vehicles are robotically controlled and can operate without direct human control.

1.4.1 Unmanned Aircraft Systems and Unmanned Aerial Vehicles

Two terms are associated with pilotless aircraft: Unmanned Aircraft Systems (UAS) and Unmanned Aerial Vehicles (UAV). The term UAS is becoming more popular as there are more components than just the vehicle itself that make up the entire system. [GAO-06-610T, pg 1] The DoD defines the UAV as a "powered, aerial vehicle that does not carry a human operator, uses aerodynamic forces to provide vehicle lift, can fly autonomously or be piloted remotely, can be expendable or recoverable, and can carry a lethal or nonlethal payload. Ballistic or semiballistic vehicles, cruise missiles, and artillery projectiles are not considered unmanned aerial vehicles." [DOD Dict] Because only the most recent research utilizes the term UAS, we will refer to individual unmanned aircraft as UAVs and the entire system from the ground control unit to the sensor suite on the vehicle as the UAS. In the most basic sense of the term, UAVs have been used since man realized he could make objects hang in the sky. One of the first documented military applications was invented by Charles Perley in 1863. The balloon-based UAV was designed to be set aloft with a bomb that would be dropped after a timer elapsed, but the lack of control and precision made the platform ineffective. Development of UAS technology for military application continued while powered flight was perfected. The most efficient use of early UAVs by the US and UK military was in the role of target aircraft for anti-aircraft gunner training. By the 1960s, remotely piloted UAVs were in regular use in reconnaissance missions over Vietnam. In 1973, the Israeli Air Force used a flight of 12 Firebee-based UAVs to successfully lead an attack against Egyptian air defenses. Today, UAVs as large as the 25,000 pound Global Hawk highendurance high-altitude ISR platform or as small as the tiny six inch and two ounce Black Widow concept UAV are receiving great attention from the DoD. [Klein]

1.4.2 Unmanned Ground Vehicles

While aerial platforms are of interest to many warfighting or support units, unmanned ground vehicles (UGVs) have proven critical in many tasks. While there is no DoD definition for UGVs, they are analogous to UAVs except that they operate on land and are normally wheeled or tracked. Today, explosive ordinance removal teams use remotely operated UGVs to inspect, dismantle or detonate possible explosive devices. In the near future, UGVs will cross hazardous or mined terrain to clear the way ahead or to deliver supplies through unsecured territory. The US Army is currently using several man-portable UGVs for “around the corner” surveillance in Iraq and Afghanistan, and the Army’s Future Combat System includes plans for Armed Robotic Vehicles (ARVs) and Small Unmanned Ground Vehicles (SUGVs), both of which will be integrated into the next generation of interconnected combat systems. [FCS Website] Current research in the field of UGVs is tested in the annual Defense Advanced Research Projects Agency (DARPA) Grand Challenge, where dozens of autonomous UGVs navigate their way around a desert or urban race track to demonstrate their technology. [DARPA GC website]

1.4.3 Other Existing Sensor Networks

In addition to vehicle-borne sensors, sensors can be deployed in standalone configurations. Sonobuoy sensor networks are currently in use around the globe for submarine detection and anti-submarine warfare. Unattended ground sensors are capable of detecting various emissions and report findings via radio. Along the US-Mexico border, the Tethered Aerostat Radar System (TARS) provides radar coverage along the border and supplies an air picture of aircraft flying as low as 500 feet to Immigration and Customs Enforcement operations centers. (Belz) Future sensors will include small and inexpensive sensors built for scattering throughout the battlespace to provide unprecedented amounts of data about weather, ground vehicle and personnel movement, audio, video and electronic surveillance. Connected by self-healing networks, the sensor nets of the future could provide real-time localized data. [Kadrovach]

1.4.4 Space-based Sensors

It is no surprise that space-based sensors on satellites provide data without which today's military would literally be ineffective. Weather, ISR, terrain and foliage analysis, and bomb damage assessment rely on space-based platforms. Uninterrupted access to space-based sensors is essential, but the data they provide normally requires significant processing.

1.5 Non-Traditional Sources of Intelligence

In addition to sensors controlled by the military, other non-military sensors could provide valuable data in the intelligence process. News footage, commercial imagery satellites, security camera footage, and amateur or professional photographs could contain some significant information and could therefore be used as sources in the intelligence process. Any source of data providing one of the previously mentioned data types could be considered a viable input to the intelligence process.

2 Platforms and Complications

The development and fielding of inexpensive UAVs and UGVs will provide multiple sources of long-endurance surveillance and live imagery feeds of areas of interest. The addition of these platforms to traditional intelligence imagery sources add tremendous flexibility, but the pre-processed quality of video or still imagery provided by current systems adds to the analysis workload and could potentially increase the chances for missed opportunities or poor decisions. Additionally, most of the resulting imagery lacks detailed context placement or location registration; further processing will be required to properly orient the data in space and time to provide intelligence analysts with the proper frame of reference. Research continues on potential methods to quickly and automatically orient video imagery, catalog the footage and extract pertinent information from flight data. [Brown], [Pyburn], [Page], [Berridge]

Other sensor systems already in place and on the horizon will produce mountains of data that might contain information valuable to mission planning or execution. Additionally, the non-traditional sources defined in section 1.5 could provide valuable intelligence information if sufficient resources or yet-to-be-developed analysis tools could be applied. In total, there is a bulk of information to sort through, but there are not yet any fielded solutions to this problem.

2.1 Simplified Analysis Process

In its most basic definition, the end goal of collecting information from multiple platforms and integrating them into a cohesive understanding of the battlespace is relatively straight-forward. Sensors from ground, air and space-based platforms collect data and add analysis information to present unique perspectives of the battlespace. This collected and analyzed data needs to be available via a common medium so friendly forces can share the unified view. Data could be pulled by units that want the information or it could be pushed to those who have already agreed to receive the information.

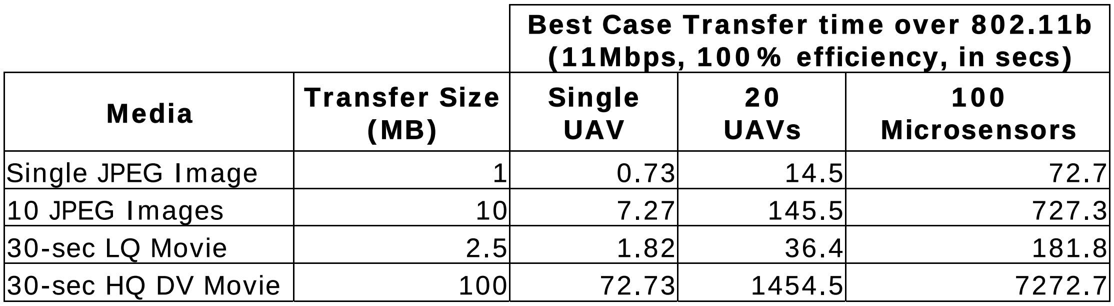
This ability to collect and transmit information in and around the battlespace will create a shared infosphere. Individual units should be able to focus the view of the battlespace on their particular area of responsibility and to limit the displayed information to that which is of interest. Unfortunately, implementing this goal is incredibly complex and severely constrained by limited resources like network bandwidth, radio frequency availability, time for collection and analysis, and external forces like jamming or misinformation. As more sensors are deployed and personnel require more information to understand the complex battlespace, the effects of already limited resources will be magnified.

2.2 Problem Areas

Managing today's battlespace is a difficult and manpower-intensive process. Since new technologies are deployed on the battlefield every day, trying to capture an empirical measurement of the amount of information shared is impractical. Adding more sensors that will feed information into the infosphere will make the challenge even greater. Without sufficient computer assisted detection and classification capabilities built into new sensor platforms, the sensors will need to transmit their data to a central host for analysis and processing. Without on-board CAD/CAC, new solutions will be required to provide bandwidth sufficient enough to handle all communications requirements.

2.2.1 Imagery

Recall that in section 1.3 we defined the file sizes of various data types. Suppose we have a flight of UAVs and a suite of microsensors that can collect and transmit still and movie imagery. Table 1 shows that under optimal conditions, the amount of data sent by multiple sensors sharing a common data link will have a significant impact on the ability to quickly share information.



		Best Case Transfer time over 802.11b (11Mbps, 100% efficiency, in secs)		
Media	**Transfer Size (MB)**	**Single UAV**	**20 UAVs**	**100 Microsensors**
Single JPEG Image	1	0.73	14.5	72.7
10 JPEG Images	10	7.27	145.5	727.3
30-sec LQ Movie	2.5	1.82	36.4	181.8
30-sec HQ DV Movie	100	72.73	1454.5	7272.7

Table 1: Best case file transfer times using commercial-grade wireless network under ideal conditions. A single 11 Mbps link was chosen to mirror the optimal SECNET-11 performance.

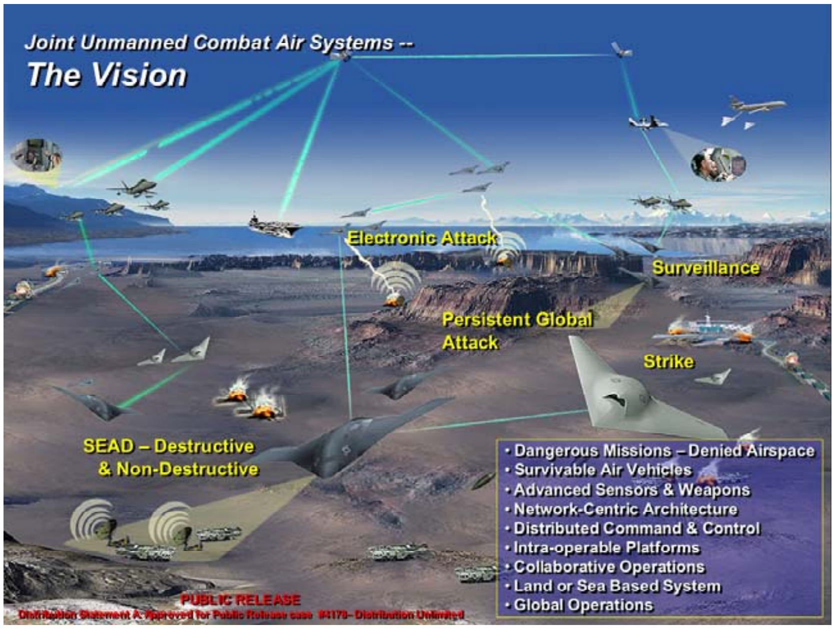
Certainly, if thousands of sensors are deployed to collect data of various types, sensor-based pre-processing and some creative networking will be required to quickly retrieve information at the appropriate level of quality for the intelligence process. Without on-board CAD/CAC technology, ensuring fast response and reliable data retrieval from these sensors will be a major effort in network optimization and modeling.

2.2.2 UAVs/UGVs

UAVs and UGVs deployed on the battlefield will create information that may or may not be analyzed and interpreted before injection into the infosphere. While the USAF's predominant unmanned aircraft systems—the Predator and Global Hawk—require dedicated satellite links to both remotely operate the vehicle and to link to the on-board sensors, tomorrow's UAS will be autonomous and will likely not need the same dedicated bandwidth. To better understand the scope of the information created by UAVs and UGVs on tomorrow's battlefield, we will first explore the Joint Unmanned Combat Air System (J-UCAS).

2.2.2.1 Joint Unmanned Combat Air System

The J-UCAS is a system of Air Force and Navy unmanned strike aircraft that will engage air and ground targets remotely piloted or completely autonomously. The overall system goal is provide a system that is integrated with the battlespace control systems of tomorrow. Figure 2 shows a concept for J-UCAS employment.



Joint Unmanned Combat Air Systems --

The Vision

- Dangerous Missions – Denied Airspace
- Survivable Air Vehicles
- Advanced Sensors & Weapons
- Network-Centric Architecture
- Distributed Command & Control
- Intra-operable Platforms
- Collaborative Operations
- Land or Sea Based System
- Global Operations

Electronic Attack
Surveillance
Persistent Global Attack
Strike
SEAD – Destructive & Non-Destructive
PUBLIC RELEASE
Distribution Statement A: Approved for Public Release case #4170– Distribution Unlimited

Figure 2: J-UCAS Concept of Employment [Alderson]

Figure 2 shows that the J-UCAS will enhance the battlespace with autonomous aircraft loaded with advanced sensors and weapons. J-UCAS aircraft will communicate with other unmanned and manned aircraft in the airspace and are capable of ad hoc planning while airborne. There are currently two platforms in development and testing: the Air Force X-45 and the Navy X-47. The X-45 first flew in May 2002 and has already completed Spiral 0 development. The X-47 is scheduled for its first flight in 2008. Figure 3 shows the relative sizes of the J-UCAS aircraft in comparison with other aircraft. [Alderson]

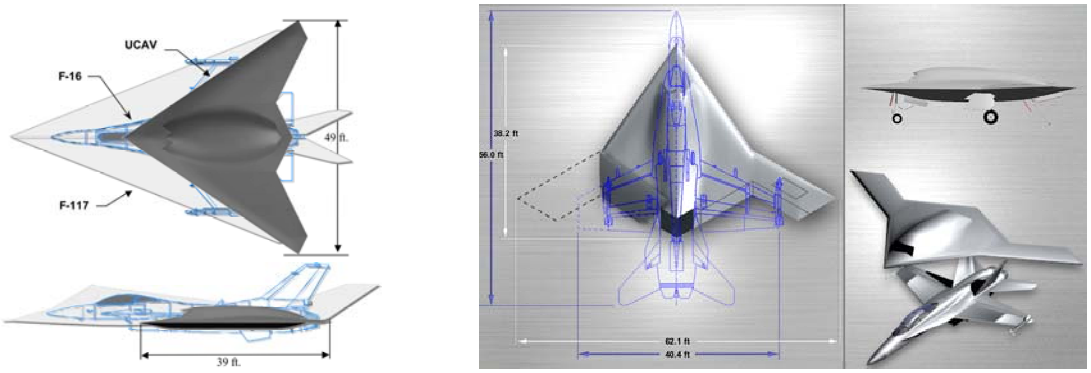


Figure 3: On the left, the X-45 Compared to F-16 and F-117 airframes. On the right, the X-47 Compared to F-18 airframe. [Alderson]

Before we can understand the impact that the J-UCAS will have on the infosphere, we need to explore the autonomous operating modes. Both the X-45 and the X-47 share a common operating system (COS) developed by a consortium brokered by Johns Hopkins University's Applied Physics Lab, with members from industry including, among others, Boeing and Northrop Grumman. The COS is capable of providing four levels of autonomy, as shown in Table 2 below. [Caltabellotta]

Level	Abilities
1	Autonomous flight from waypoint to waypoint
2	Autonomous flight direct to destination
3	Autonomous flight with human approvals
4	Fully autonomous flight and attack

Table 2: J-UCAS Four Levels of Autonomy

Onboard, the J-UCAS is equipped with Link 16 for battlespace management and utilizes UHF and Wideband SATCOM for communications and control. The X-47B will use electro-optical links to other J-UCAS aircraft for mission planning and target hand-off communications.

The J-UCAS program oversight and management recently shifted from the Air Force to the Navy and like many revolutionary projects, funding is always a concern. A 2004 U.S. Senate report suggested “the J-UCAS program has not been properly coordinated with the Services, is overly ambitious with regards to planned technologies and is potentially unaffordable.” [SR 108-284] In March of 2006, the Government Accounting Office submitted a report on the status of the Global Hawk and J-UCAS programs and stated that “since its inception, the J-UCAS program has been in flux. Program management and goals have changed several times, and the recent Quadrennial Defense Review has directed another restructuring into a Navy program to demonstrate a carrier-based, air-refuelable unmanned combat air system.” [Sullivan]

In spite of the concerns, by April 2004, the J-UCAS X-45A Block 2 aircraft accurately delivered munitions, and by August 2005, Block 4 aircraft successfully demonstrated all levels of autonomy including an attack on multiple targets in coordination with a second autonomous X-45. [Alderson]

While there are certainly challenges ahead for the development of the J-UCAS program, the capabilities and performance achieved so far present solid evidence that similar projects will deliver systems that can process most of the data on-board, injecting less unprocessed data into the infosphere. However, other classes of UAVs—particularly Small and Micro-UAVs—will be built to be cheap and expendable. As such, they will not be equipped to do significant on-board pre-processing and so their injects into the infosphere will likely be much greater.

2.2.2.2 Small and Micro-UAVs

The general concept behind small and micro-UAVs is that while large and expensive UAVs provide great capabilities to the DoD, ground forces and forces not normally associated with air operations could gain tremendous benefits by having an eye in the sky or a scout over the horizon. Security forces units deployed in Iraq are using small UAVs to provide a view of the perimeter using a simple laptop interface. Similarly, Marine ground units are equipped with backpack-transported UAVs that can fly above the unit to provide a forward view. While these types of aircraft typically won't provide data that will be analyzed or used as intelligence sources, they could be adapted to do so in the near future. Other concepts for small and micro-UAVs include use in urban environments, indoors, or in close proximity to enemy personnel. [Baldwin, P.] These applications will most certainly be used as inputs to the intelligence process, so the data collected will need to be transmitted and analyzed. If these types of UAVs are as cheap and as ubiquitous as some have suggested, the increase in data injected into the infosphere could be significant.

2.2.3 Stockpiling Data

At the time this article was written, low-end business-class desktop computers ship with 80GB hard drives and can be cheaply upgraded to several hundred gigabytes. Desktop storage now costs about 50 cents a gigabyte, and costs will continue to drop rapidly—some estimate as cheap as 2 cents per gigabyte in the next five years—which will enable users to store *more* information and further complicate the problems of data retrieval. [Gilheany] Easy ways to transport large amounts of data in key-size devices like USB drives means that users will likely hang on to some data for longer periods of time.

As users continue to create information, collect information from other sources, or analyze data and create composite information sources, retrieving any useful information from the hundreds of thousands of computers in the DoD inventory might seem to be a nearly impossible task. Simply finding the subject matter expert on a given topic from among the personnel in a single unit can sometimes be extremely difficult, and larger organizations will only have more problems collecting information from known experts.

As the number of information sources increase and our inventory of collected data grows, the challenge of keeping up with this data will also grow. An automated solution must be developed and implemented as soon as practical.

2.3 Magic Blue Lines

Whenever new systems are presented to a military audience on a single overview slide or image, it is common to see lines of communication between platforms and personnel represented by blue “lightning bolts,” as seen in Figure 2. While many representations are meant to simply indicate a dedicated communications link or common radio frequency, there is usually no battlespace-wide plan for assessing the amount of data that is injected into the infosphere and ensuring adequate network bandwidth.

Many estimates of future bandwidth requirements exist, but many of these estimates are based on recent growth and extrapolation to the future. Some estimates use the bandwidth of yet to be fielded platforms and doctrine for their implementation. The following excerpt from the Congressional Budget Office demonstrates the analysis techniques used to conclude that the Army's bandwidth demand to supply shortfall will be significant (in some cases 4 to 1, but for brigade to lower-echelon units as bad as 30 to 1):

> "Operating the Shadow [Tactical UAV] system at the brigade and higher command levels would generate a sizable demand for bandwidth, depending on the degree to which the information those TUAVs collected was shared throughout the battlefield communications network. The Shadow will have three communications channels. One is a large data channel with an engineering throughput of 16 Mbps that, operationally, should deliver from about 1.5 Mbps to 2 Mbps of useful video bandwidth. The other two are redundant command-and-control channels providing 19.6 Kbps of operational throughput. A division will control between four and eight of these TUAV systems (although division commanders will almost certainly make three to six of them subordinate to brigade commanders).
>
> The doctrine underlying use of the Shadows is still evolving, but at this point, the Army wants to share among brigade and higher command levels the information collected from at least four--and possibly as many as eight--of the TUAVs. Currently, data from TUAV downlinks are shared between the operations and intelligence nets of a command. Under the assumptions that there are three brigades per division and that they will be sharing (that is, networking) the information among themselves and also with their division, then information from four to eight TUAVs will be transmitted on each brigade's operations trunk line. If each TUAV requires 1.5 Mbps of bandwidth, each brigade will need from 6 Mbps to 12 Mbps. Divisions typically command those brigades, and a corps commands the divisions. Hence, the demand for TUAV bandwidth for the sharing of such information at those levels will be from three to nine times larger than at the brigade level." [CBO]

A few interesting points are made in these two paragraphs, the first of which is that the doctrine for employing the UAVs is still evolving, which reinforces the fact that UAVs are—at least for the US military—a revolutionary technology that has not yet been fully integrated. The second point is that the downlinks will be shared with both operations and intelligence nets, meaning that both are getting un-processed raw imagery from the UAV. Depending on the technical implementation of the video feeds, orientation data might not yet be added to the feed and target identification and analysis won’t likely be complete; since the feed is shared, it is possible that operational decisions would be made before intelligence analysis is complete.

While limited resources and insufficient bandwidth are indeed major issues, an information management strategy needs to be fully developed into a critical component of the system design. Fortunately, there are opportunities to correct this growing problem.

3. Automation Opportunities

Clearly, because of the volume and the trend that all forms of information are converging to the digital form, a computer-based solution for managing computer-generated and stored data is the only viable option. To ensure that any data management system meets DoD needs, the author suggests that any system considered is examined using the Intelligence Cycle as a base for evaluation. The first phase we will look at in the cycle is the collection phase. Because exponentially increasing amounts of data will be created by each new sensor system, importing and storing this information for quick retrieval will be the first requirement for any solution. Following storage of the data, analysis and classification are required to ensure that if the data is to be used at all, it will be analyzed using the proper tools; this is analogous to the Processing and Exploitation phase. As the relevant information is extracted and prepared for others, the system is emulating the Analysis and Production phase. To get the data to the correct user or organization, the information is Disseminated and Integrated with other pieces of information. Finally, after sharing the information, users in the system will critique the information available and perhaps begin new searches or new projects to create more data, which mirror the Evaluation and Feedback phase and the Planning and Direction phase. Because the end goal of reading any information is to gain an understanding of the message it contains, any system intended for data management should endeavor to fully support the needs of the Intelligence Cycle.

Current trends in the commercial software sector and the Internet have offered some intriguing potential solutions. Two models have great potential: peer-to-peer file sharing, where the content of peer computers is available for search and retrieval by other computers and convergent search, where information is automatically indexed for later searching as implemented by Google or Apple's Spotlight technology. Peer-to-peer file sharing could provide increased sharing and understanding of the unit's mission, but data classification and security are primary concerns. Convergent searches of large hard drives containing thousands of files—many files blindly migrated from old computers to new—could enable users to abandon the practice of creating hierarchical folders and instead simply store all documents in one location and then quickly search for an item using a few key words. The author calls this "convergent" search because the key words can be a combination of the file's name, text in the file, or text about the file. Another opportunity for automation follows the example set in the Google Earth application. Google Earth presents users with a flight-simulator like view of the earth overlaid with photographic satellite imagery; as the user flies over the terrain, the imagery is updated to provide a realistic effect. The author's "Ogle" concept takes this idea one step further and is discussed in section 3.3.

3.1 Peer-to-Peer File Sharing

Consider a data management model for AF-level peer-to-peer collaboration where every computer in an organization is networked and is running software that allows searches by other users. In this hypothetical organization—say, an Air Control Squadron—several users are communications officers who specialize in network engineering and a dozen enlisted communicators are highly-trained network operators. The unit also has pilots of varying ranks and skill levels, security forces personnel, air traffic control personnel and base support specialists. While in garrison, each user is afforded the use of their own computer, and each office is engaged in individual projects to help improve mission effectiveness. Unfortunately, each office finds it difficult to keep apprised of other office projects in spite of the unit's best efforts to track the projects on the shared network drives.

Using a hypothetical peer-to-peer search program installed on all unit computers, the unit commander performs a unit-wide search on a topic of interest. The commander sees in the results that several projects cover similar areas of interest and discovers opportunities where unit personnel could benefit from cross-project information sharing. Another user searches for the latest version of the deployed site security plan and finds that one of the security forces personnel has a local copy of the plan on his computer, and has made changes to it to reflect work on a new project to integrate wireless cameras. The user making this observation forwards the information on the project to the communications officer known for her knowledge in wireless networks to offer help in the security project. In addition to preparing for their deployable mission, the communications personnel also manage the peer-to-peer system and help train users to better use the system. A well-designed data management system could enable these kinds of discoveries without requiring that individual users be trained on data storage techniques or rules. Meta-data could be added automatically by the system, and if enough information couldn't be determined automatically, the data management system could "interview" the user to determine how this new data should be categorized.

3.2 Convergent Search

Consider a desktop computer in the typical Air Force office. In workcenters with common computers, several users likely share the computer and log on as needed. To make it convenient for the user, system administrators provide shared drives that enable multiple users in an organization to save data in a commonly accessible location. Additionally, roaming profiles allow users to move from computer to computer and their desktop settings and documents move with them. If a convergent search capability was installed in this office, all of the non-personal information could be shared and accessible by other personnel with the proper need to know and security clearance.

Suppose the shared drive was the location where the unit's safety officer saved all of the program's documents and the orderly room published the latest recall roster. When other personnel needed information for their work center safety programs, a convergent search would return links to their safety officer's best practices guides and perhaps links to commonly used forms. A search for the recall roster would return only a link to the orderly room copy and not to a copy that another user made in a folder in their roaming profile. Since the system is intelligent, outdated forms and duplicate copies of documents would not be returned. The result is that users looking for specific or general information wouldn't find links to old and outdated information unless explicitly requested.

3.3 An Optimal Model - Ogle

Today, imagery is collected everywhere around the battlefield. Satellites orbit above and collect thermal and visual imagery for weather, intelligence, or tactical navigation while high altitude UAVs and reconnaissance aircraft provide high-resolution images of targets of interest. Closer to the action, small UAVs and tactical aircraft collect imagery in the form of video feeds or gun camera footage, and on the ground, surveillance cameras watch building exteriors or important traffic intersections, and personnel take digital still images or video. In total, thousands of frames of imagery are collected every minute, making analysis tedious and timely decision-making extremely difficult if not impossible. One concept developed by the author is the Ogle system, which is a combination of a software framework and a collection of rules that help to define how imagery is collected, processed and analyzed.

In accordance with DoD Directive 8320.2 and the DoD CIO policy memo entitled “Net-Centric Data Strategy” and dated 9 May 2003, all data collected by the DoD should be immediately posted before processing to common spaces on the network for use by other users. New data should also be marked with meta-data or information that describes the data for use by others. While this may not be practical due to the space and bandwidth restrictions previously discussed, the Ogle concept could take advantage of this raw data through the use of mass storage media, fast databases, communications and imagery satellites, and advanced analysis methods. The Ogle system would be capable of providing analysts with several modes of operation or simulation: “Geospatial Search Mode” would allow users to search by latitude, longitude and time; “Fly Mode” would allow analysts to fly over a map and imagery information would be superimposed wherever it is available; and “Hover Mode” would allow users to hover over an area in time while images collected from various sources are presented as their relative point in time passes in the simulation. Figure 4 provides one view possible presented by the Ogle concept system.

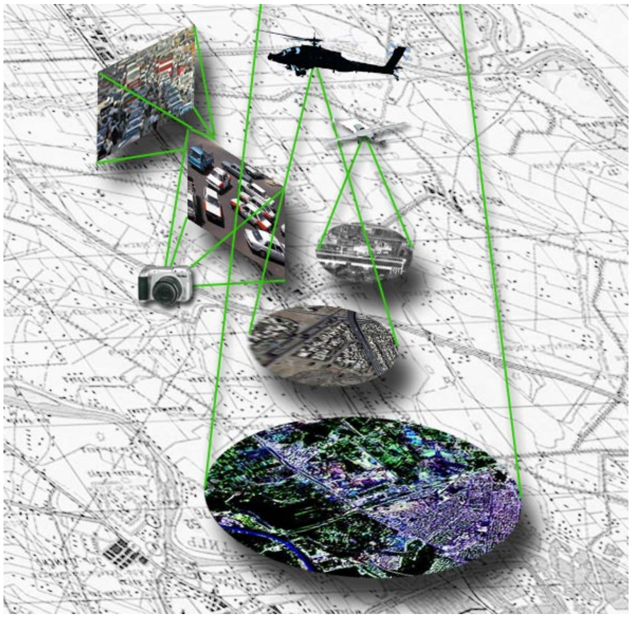


Figure 4: A possible view presented by the author's Ogle concept application, showing current locations of various intelligence sources including handheld cameras, a Hunter UAV, Apache gun camera footage and a space-based platform.

Three examples are provided below to illustrate the concept:

a) <u>IED Factory Location</u>: An improvised explosive device (IED) goes off on a busy road next to a military convoy. Intelligence analysts want to find where the device came from, and use Ogle to pinpoint the factory. Over the past 24 hours, sources of imagery have been loaded into shared imagery storage locations by sources from around the theater. An Air Force Global Hawk was orbiting the city at 60,000 feet and collected imagery and provided data as requested by warplanners and warfighters. An Army Hunter UAV was orbiting 10,000 feet above a neighborhood in the eastern portion of the city to support security forces protecting a water treatment plant rebuilding effort. While on patrol, Army helicopters watched the skies during a routine mission above the city, and on the ground, public affairs officers and combat camera personnel captured dozens of still images of various areas. Following the DoD guidelines, all of the imagery was loaded into databases and all necessary metadata was included with the raw images. Each image or video sequence was automatically or manually time-stamped and marked with GPS coordinates and camera orientation data, as well as any general information describing the scene. As the imagery was uploaded, Ogle indexed the data with minimal processing time, in much the same way that web search engines crawl the web looking for updated content. After the IED incident, intelligence analysts initiate a geospatial search session on Ogle and search for all imagery that covers the location of the IED explosion. Ogle finds that the Hunter UAV might have captured a portion of the area during one of its orbits and the Global Hawk took dozens of still images of the this portion of the city. The analysts ask to see the Hunter footage first, and are able to see the IED explode. In the following moments of the video, they see a blue sedan quickly leaving the area, and note the direction of travel as it leaves the viewing area of the imagery. The analysts ask Ogle for imagery in the vicinity of the departing vehicle, but find none close enough in the time frame to be of help. The analysts then decide to see if they can see the vehicle arriving on the scene before the IED explosion. Several of the Global Hawk images have enough data to determine that the blue sedan came from the west via the main street through the city. The analysts tell Ogle to enter the “Fly Mode,” and are presented with a map of the city with small frames of imagery data highlighted over various areas of the map. The analysts are able to “fly” above the map and click on the various sources of imagery (both still photos and video imagery) that cover the area of interest or are near enough to the area that the camera angle might have captured something of interest. While flying above the map, the analysts are able to piece together enough data to determine that the vehicle came from a specific block in the western part of the city. Armed with an estimated origin and pictures of the vehicle, the analysts pass on the data to friendly forces in the area for further investigation. Several hours later, the vehicle is found outside a warehouse, and the decision is made to raid the facility with law enforcement and military personnel. The warehouse does in fact contain an IED factory, which is carefully dismantled and the terrorists inside are captured.

b) Border Crossings: There are not enough forces to patrol the porous border between a friendly and a hostile country, but cutting the flow of terrorists between the two is critical. Analysts decide to search Ogle for imagery of the border to find any patterns of travel or possible staging locations. Ogle finds only infrared satellite imagery of the area, but the resolution is good enough to see the heat from vehicles. The analysts decide to put Ogle into "hover" mode, and watch all imagery that covers a specific area on the globe and let time fly by. As time speeds by, images from different sources that cover the area are displayed. Several popular staging locations are discovered, as well as a common portion of the route into the friendly country. Analysts pass on this information to mission planners, who step up patrols in the common route and are successful in capturing dozens of inbound terrorists.

c) Amber Alert: In a civilian application, data from sources around the city could be fed in to a system like Ogle for similar analysis. Surveillance cameras, security

> cameras in parking lots and on ATMs, police car dashboard cameras, and helicopter cameras all supply data to the Ogle system. Following an Amber Alert, Ogle could be used to fly through the city near the last known position of the abducted child. Clues from multiple, unconnected sources might catch enough information to pinpoint the origin or destination of the abductor using similar techniques described in the first two examples. Since all inputs are date stamped, assembling a timeline using various sources could help fill in any gaps of missing imagery.

While the above scenarios demonstrate the operation of the conceptual Ogle system, it also highlights the scope of the problem and the logistical complexity of collecting thousands of gigabytes of information from multiple disconnected systems. The early adoption of the meta-data marking guidelines set in DoD Net-centric policies will help systems that have yet to be developed like Ogle use old data that might be used to create new information. Following these rules and implementing a system like Ogle could result in raw data stored in multiple locations becoming a part of a searchable network of information stores. Much like the results produced by Google searches of the Internet, Ogle searches of imagery data would produce an interactive 4-dimensional representation in spite of the fact that the source data is spread throughout the theater.

Unfortunately, while increased data sharing will increase intelligence analysis capabilities, indexing multiple computers and peer-to-peer sharing will present major security concerns, particularly when trying to compartmentalize information while maintaining appropriate “need to know” controls.

4 The Integrity-Relevance-Classification Data Sharing Model

While bandwidth restrictions are still major concerns, limiting access to sensitive data will always be a critical control issue. Conversely, if the user is cleared for nearly any kind of information, all of these inbound data streams could be overwhelming. If the flow of information is not somehow controlled, warfighters risk getting inundated by not only too much information, but information at the wrong level of detail.

Military commanders have always needed to fully understand the field of battle. Models ranging in complexity from stick and rock depictions constructed in the field to the craftsmen-built intricate scale models of French fortifications along its seventeenth century border have been successful in conveying points of vulnerability and routes of attack. The development of aircraft and anti-aircraft technology added further requirements for understanding the three-dimensional airspace surrounding the battlefield. In the digital age, commanders are able to watch live video feeds from the cockpit and in many cases, from the weapon itself as it flew into the target. Today, command centers of all levels are built around large data walls that display a constant flow of data. Live video feeds from remotely-piloted Predator aircraft are fed in to Air Operations Centers (AOC), providing commanders and intelligence analysts with what some call “Predator Crack” or “Kill TV” because of the display’s ability to draw the viewer’s full attention away from their primary duties.

While arguments could be made that commanders should be provided every piece of information available and they will decide what to use and what to ignore, technological limitations have already proven risky. Recall how commanders orbiting in BlackHawk helicopters over Somalia tried to relay directions from a reconnaissance aircraft in order to command a rescue convoy through a decaying urban environment. The communications delay between the command post and the trucks on the ground introduced chaos significant enough to confuse the convoy with late instructions and effectively drive it into dead ends. An excerpt from Black Hawk Down describes the chaos:

> "In ordinary circumstances, as close to the first crash as they were, the convoy would have just barreled over to it, running over and shooting through anything in its path. But with all the help overhead, Task Force Ranger was about to demonstrate how too much information can hurt soldiers on a battlefield.
>
> There was an added complication. 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 pilots were handicapped. They were not allowed to communicate directly with the convoy. Their directions were relayed to the commander at the [Joint Operations Center], who would then radio…the command bird. Only then was the plane's advice relayed down to the convoy. This built a maddening delay. The Orion pilots would see a direct line to the crash site. They'd say, "Turn left!" But by the time that instruction reached…the lead Humvee, he had passed the turn. Heeding the belated direction, they'd then turn down the wrong street. High above the fight, commanders watching out their windows or on screens couldn't hear the gunfire and screaming of wounded men, or feel the impact of the explosions. From above, the convoy's progress seemed orderly. The visual image didn't always convey how desperate the situation really was." [Bowden, 137]
>
> "A voice came over the busy command frequency pleading for order. *Stop giving directions!… I think you're talking to the wrong convoy! This is Uniform Six Four, you've got me back in front of the Olympic Hotel. Uniform Six Four, this is Romeo Six Four. You need to turn east.* So the convoy now made a u-turn. They had just driven through a vicious ambush in front of the target house and were now turning around to drive right back through it. Men in the vehicles behind could not understand. It was insane! They seemed to be trying to get killed." [Bowden, 150]

While following the chain of command and control is imperative, the flow of critical information must be flexible enough to prevent situations like the one described above, but at the same time restrictive in the sharing of other possibly misleading information.

Because of the rapidly-increasing volume of collected information, numerous research projects are underway to design virtual environments in which every piece of information could be integrated, analyzed and displayed in an immersive four-dimensional battlespace, where time and perspective can be manipulated to suit the needs of mission planners and commanders. It is not hard to imagine the demands that will be placed on commanders trying to conduct a war from inside a virtual, real-time "sand table" with data from thousands of sources pouring in at incredible data rates. Additionally, the GIG concept could allow soldiers on the ground or in vehicles anywhere in the battlespace to get similar representations streamed to their locations by various data pipes. An obvious hazard to this situation—beyond the critical hazard of information overload—is the possibility that commanders are drawn in to making tactical decisions based on data presented to their strategic perspective, while warfighters on the ground adjust their tactics based on information intended only for strategic planners. Additionally, any communications delays not adequately represented in these distributed models could have devastating results.

4.1 Inverted Perspectives

On 20 Nov 1970, a joint force of more than a hundred aircraft and dozens of Army, Navy and Air Force personnel participated in an operation to rescue American POWs from the Son Tay prison camp near Hanoi, North Vietnam (NVN). The success of the operation relied on the support from many services and included a crucial diversionary movement by nearly sixty carrier-launched sorties to draw attention to the east. On the ground, Air Force C-130s dropped "firefight simulators" (bundles of fireworks intended to sound like engaged ground forces) and inserted Special Forces personnel to conduct the raid on the prison. While the raid was a stunning operational success in that no personnel were lost in the raid, no American POWs were found. This incident provided many situations central to the authors' development of the concept of "Inverted Perspectives" as applied to Information In Warfare. [VietnamWar.com]

Since deception was a key component of the raid on Son Tay, security and secrecy of the plans were also vitally important. When US Navy aircraft appeared on NVN air defense systems, Vietnamese aircraft were diverted and attention was focused on the eastern coast, allowing US aircraft to penetrate from the West unimpeded. On the ground, the deployment of the firefight simulators created noises similar to automatic weapons fire to draw the attention and response of enemy forces. Broadcasting any component of this plan would have drastically altered the responses.

Consider if this identical mission was accomplished using the GIG-enhanced command centers of the future. If so configured, any sensors in the area could have detected key maneuvers and dutifully reported status as they were designed to do. Obviously, limiting access to this data would have to be at the same classification level of the mission, and not all units operating in the area would be briefed on this sensitive and classified operation.

In an ideal environment, we would deploy thousands or perhaps millions of sensors across the battlespace to dutifully collect climate, audio, video or electromagnetic signal data. Additionally, airborne command and control assets would compose an integrated picture of the battlespace. The data reporting the presence of a multi-ship formation of friendly aircraft taking part in the deception maneuver on the Western coast would be visible to those watching the strategic picture. Obviously, sensitive components of the mission would have to be stripped from the display and only the minimum details would be available. In order to de-conflict the airspace, all air operations are planned and coordinated using tools like Air Tasking Orders, but some operations conducted on the ground or on the sea might not be reported and coordinated with all components. A robust sensor net could provide a bridge between these dissimilar components of the battlespace, but the composite picture would likely not be relevant to some warfighters.

From the perspective of ground units, it would take time to analyze reports of audio sensors detecting a firefight before determining which units were in the area and perhaps request air-borne or space-borne surveillance. Other ground units nearby (not involved in or briefed about the sensitive operation) that happen to be monitoring the strategic picture might alter their tactics or maneuver in response to indications of a nearby firefight—particularly if the data indicated activity in the unit's area of responsibility (AOR). Certainly, this data could impact the commander on the ground in a number of ways and in most cases all parties in the AOR would be pre-briefed of the operation. Obviously, there will be times when operations against emerging targets of opportunity must be initiated before there is adequate time to coordinate with regional commanders.

Because strategic commanders could use the GIG-provided display of the battlefield to focus in on details of interest, the hazards of taking too much interest in tactical events and losing sight of the strategic picture increase rapidly. Similarly, tactical commanders might see information intended only for the strategic level that might convince them to alter their tactics, shift their risk assessment, or maneuver to areas that might not achieve the deception intended in strategic plans. The author suggests that either of these conditions is an example of Inverted Perspectives that is enabled (and perhaps encouraged) by the potential capabilities of a truly force-wide, multi-media capable GIG.

An endless number of examples could be presented to demonstrate that data bound for the GIG should have limits to its exposure, which would restrict where the data is transmitted and who is authorized to read the data. Additionally, as Lt. Gen. William T. Hobbins indicated during an interview in Airman magazine, some platforms will produce data at different rates while operators in varying roles will consume data feeds at different rates. Clearly, this paints an amazingly complex picture with fuzzy and continuously evolving operational requirements. Fortunately, some existing controls already exist to limit and protect the flow of information.

4.2 Data Classification

All military personnel are familiar with protecting data at the classification levels defined by the National Security Agency (NSA). Data protected with a higher classification level like "Secret" can be read only by users with Secret or higher clearances. Similarly, readers with a high classification level can read any material at or below their classification level. In the command center described earlier, information specific to a sensitive operation could be classified at a high enough level to prevent those with lower-level classifications from reading the data. Properly implemented, display of data relevant to those classified operations could be reserved for those with the required need to know. Additionally, the data presented on command center displays need to stay at the same clearance levels of all command center personnel.

Using a well-disciplined approach, data from all sources could be properly secured and could eliminate some users from seeing information not cleared for their consumption and would help to avoid instances where lower-level tactical decisions are altered by strategic data sources. But how about data intended for low-level consumption potentially impacting higher-level personnel? Normal data classification techniques will not address the problem of low-level tactical data becoming a distraction to commanders at higher or strategic levels.

4.3 Biba's Integrity Model

While working for MITRE on an Air Force computer security research project in 1977, Biba defined an important policy in what has since become the seminal paper on information integrity. [Bishop, pg 153] Integrity of information is a measure of its trustworthiness; in the military sense, information from a known trustworthy source would have high integrity, while information based on rumor or from unknown sources would have low integrity. Similarly, the integrity state of the reader—the decision maker's confidence in the data—can be influenced by the information consumed. New and startling information provided by a source will affect the user (and the decisions he or she makes in response to that information) to varying degrees based on the integrity of the source. Decision makers might take some risks when the information is from a strong source, while choosing to avoid the same risks when presented the same information from an unreliable source.

In Biba's Integrity Model, three rules apply to the reading, writing and acting upon information from sources of various integrity levels. In the computer security context of Biba's model, once a subject (either a computer program or a user) reads data of a given integrity level, the subject's integrity level might be affected. Another important concept used in comparing security levels or access control is the concept of dominance. One object dominates another when the security level is the same or higher than the other object. For example, a secret clearance dominates secret or unclassified clearances, while top secret dominates top secret, secret and unclassified clearance levels. When a subject dominates an object, the subject can read the object. If the subject does not dominate the object, the subject cannot read the object in the same manner that someone with a secret clearance cannot read a top secret document. Here then are the three rules from Biba's Integrity Model:

1. A subject can read an object if and only if the object's integrity level dominates (is greater or equal to) the subject's integrity level.

2. A subject can write data into an object if and only if the subject's integrity level dominates the object's integrity level.

3. A subject can execute (or direct action of) another subject if and only if the first subject's integrity level dominates the second subject's integrity level. [Bishop, pg 155]

In plain terms, rule 1 means that a subject can only read an object if the data will not have a deceptive or misleading effect on the reader. In a command center, data (the object) would not be presented to the commander (the subject) unless the data was verified as accurate. Rule 2 means that some data source of a lower integrity-level can't inject data that could be interpreted as accurate and valid. Again using the command center analogy, actions of a tactical unit might not be presented to the commander as strategic results until proper bomb-damage assessment or mission debriefing was conducted. Rule 3 would prevent reaction to deceptive acts or pre-processed data from sensors, much like the NVN air defense system drew defensive forces from the area US forces penetrated on the way to Son Tay.

The application of the above Biba Integrity model to a notional command center could solve specific requirements for filtering information, but commander flexibility and the ability to share information would likely be limited. A model that combines the DoD's traditional classification levels with a sense of the data's integrity *and* relevance could be very helpful in the analysis and presentation of data sharing mechanisms being developed for future command centers.

4.4 The Integrity-Relevance-Classification Data Sharing Model

The warfighter's basic need for relevant and accurate information are thoroughly understood and well defined in doctrine and operational art, but defining the scope, sources and format of the data that comprises this information would require continuously updated volumes. Efforts to build systems that provide data in pre-defined formats or follow pre-defined message sharing rules will normally result in products that are hard to integrate or expensive to update. To avoid the problems of updating systems to keep pace with continually evolving technologies, the author and Dr. Rusty Baldwin developed a mechanism to control information flow based on Data Integrity, Relevance and Classification.

In order to better explain this information sharing mechanism, we will explore its application in a notional command center. This command center will be staffed by personnel of varying clearances and areas of functional expertise, similar to other command centers like wing command posts (WCPs), expeditionary operations centers (EOCs), or AOCs. Like Biba's model, personnel and systems that can create and consume data will be referred to as subjects, while the paper or virtual products produced will be referred to as objects. The information sharing mechanism in place will assign three ratings to every subject and object: classification, relevance, and integrity.

The classification rating for subjects and objects can be Unclassified, For Official Use Only, Secret, or Top Secret. We will ignore the complications of clearances for personnel from other countries for the purposes of demonstration. The relevance and integrity ratings of subjects and objects can be Low, Medium or High. Personnel classification ratings normally do not change over time, but their integrity levels can change over time and they will produce objects of varying relevance levels. Similarly, documents and processing systems can take on the same ratings as their content or inputs much in the same way that once a classified disk is accidentally read with an unclassified computer, the computer is then upgraded and protected as secret. All information sharing transactions must occur in accordance with the following rules:

1. Initially, all trusted subjects have a High integrity rating, and all subjects and objects have unique classification ratings. All un-trusted subjects have a Low integrity rating.

2. A subject can read or process an object if and only if the subject's classification level dominates the object's classification level.

3. The integrity level of a subject or object can only be raised through a well-controlled process.

4. The relevance level of a subject or object is determined through another well-controlled process.

5. When a subject creates an object, the created object will have an integrity level equal to the subject that created it. If the newly created object contains information from other subjects or objects, in full or in part, the new object will have the lowest integrity level of the components.

6. If a subject reads an object of a lower integrity level, the subject's integrity level will temporarily take on the object's lower integrity level. The subject will return to its previous integrity level in accordance with Rule 3.

7. A subject can process and manually or automatically forward an object to another subject only if the forwarded object dominates the receiving subject's integrity and relevance levels, and the receiving subject's classification level dominates the object's classification.

4.5 Rule Analysis and Clarification

Rule 1 ensures that personnel and information processing systems will be able to share information following our basic rules. Trusted subjects refer to those sources that are trusted in a wide context, whether that involves coalition partners, our own personnel and information processing systems and equipment, and ISR resources. Untrusted subjects refer to systems and personnel not under our command center's control, and could include subjects like the domestic and international media, informants, or any source of questionable origin.

Rule 2 ensures our most basic requirements of need to know, security and proper access control mechanisms are observed.

Rule 3 dictates that a formal process be established to change the integrity level of a subject or object. The intelligence community uses similar procedures to mark the level of trust in an intelligence resource; multiple sources of lower integrity levels could provide enough corroboration to support raising the integrity level of a subject or object, but the process of doing so should be well understood and accomplished by a delegated entity. This process will obviously be one of the most important components of this model since improperly raising integrity levels of a poor information source could have disastrous effects.

The process suggested by Rule 4 can be somewhat more flexible than that in Rule 3, depending on the role of the receiving subject. For example, a tactical level ground unit would have a much smaller “sphere of relevance” surrounding it than would a C2 aircraft orbiting over an area of responsibility. The ground unit would typically be interested in information about nearby opponent ground forces, in-range artillery units, or re-supply schedules and locations. In contrast, the ground unit would not care to see data sets typically provided for the C2 aircraft, which could include friendly aircraft mission data, enemy air defense threats and air refueling tracks. Some process should be established to ensure that each subject is given an appropriate sphere of relevance. At the operational level, each subject should be able to customize their sphere of relevance to ensure that data of interest could be added or information deemed no longer pertinent could be removed.

Rule 5 ensures that personnel or systems creating information attribute the source accordingly and properly mark the data at the appropriate integrity level. This will ensure that the receiver places the appropriate level of trust or skepticism on the received information. New information compiled from multiple sources will not automatically take on the integrity level of the subject compiling the information; instead, the integrity level of the new object will be the same as the object with the lowest integrity level until the process defined in Rule 3 is applied.

Rule 6 ensures that any low integrity information does not get forwarded as higher-integrity information without proper analysis and consideration. Similarly, personnel that read the low integrity information must be careful not to make decisions or pass on the information without properly putting the information in context. This particular rule would be more difficult to implement on personnel than it would on data processing equipment. A sensor providing erratic and illogical readings could easily be silenced as a malfunction and low-integrity data compiled into a report could be contain the appropriate caveats, but an aggressive individual acting on or up-channeling information based on rumor or conjecture would be hard to monitor.

Rule 7 ensures that information is properly filtered in accordance with previous integrity and relevance rules. A tactical display could become useless if irrelevant or misleading information was displayed at the wrong time, while unprocessed or incomplete data could cause premature and incorrect decisions. The final caveat ensures that sensitive operations are not compromised; data must be sanitized or properly declassified before forwarding to subjects not necessarily involved in the operation.

In combination, Rules 2 and 7 provide the “push and pull rules” that prevent information overload caused by unneeded automatic data pushes, while at the same time preserving flexibility for pulling useful data.

Together, the rules limit low-integrity information from flowing as quickly as high-integrity information, but give commanders the flexibility to change the integrity and relevance rating processes for reduced delays or increased scrutiny. In the field, the system rules filter out information not applicable or destined for lower echelons, but provides controls for feeding tactical data up the chain. Obviously, more research is required to implement this system and test its applicability and resilience in stressful and confusion situations.

5 Recommended Research Areas

This paper summarized the intelligence process and the sources of data feeding this process. We analyzed some new data sources and the potential impacts of our ability to understand the flood of generated information. While some systems like the J-UCAS will conduct a bulk of the information processing and management on their own, several key areas of research remain critical:

1) Peer-to-Peer Sharing: Recommend that the USAF studies ways of cataloging, securing and sharing the information that we already have. To be of use, the peer-to-peer system should have strong security controls and methods for identifying subject matter experts. In order to help automate the identification of subject matter expertise, a system could analyze and publish the user's duty history, resume and interests. Areas of specific concern in this research should include security, the hazards of possible distraction from primary duties, and challenges to the chain of command.
2) Convergent Search: While this is likely more of a commercial research project, the USAF should identify metadata that would be useful to all organizations regardless of the final search solution that is implemented. Information used by the intelligence and civil engineering community could be used to form common metadata for imagery and maps, like camera orientation, altitude, image scale, etc. Some personnel information is used by many organizations; a common description of the metadata, published storage locations and a documented metadata structure would make updates and retrievals by various organizations much easier while at the same time reducing the number of redundant databases.

The metadata could be defined in XML Document Object Models and published in communications instructions for use and subsequent enforcement whenever possible.

3) Integrity-Relevance-Classification Data Sharing: Design a test environment where information could be handled in accordance with the data sharing rules described in Section 4. A system that automatically pushes, pulls or blocks information based on these ratings could have a significant impact on our ability to understand the battlefield by reducing the amount of distracting unprocessed data.

4) Information Bandwidth Estimates and Trends: A common theme in this paper is the difficulty in accurately calculating the required information bandwidth, both now and in the future. We can make rough estimates based on the bandwidth procured for various recent conflicts, but without truly understanding how much necessary data is created by a typical person in a typical unit, any preparations we make in allocating resources are based on hunches and best guesses. While this might seem like an intractable problem, any effort to capture the scope of the problem could help to better define the "magic blue lines" discussed in previous sections. Additionally, an effort to plot the estimated amount of information shared in recent conflicts compared with available commercial technology capabilities growth could provide a valuable forecast of potential requirements.

6 Conclusion

Joint Vision 2020, the latest in the DoD’s efforts to prepare for future conflicts, stressed that we must achieve Full Spectrum Dominance in order “to defeat any adversary and control any situation across the full range of military operations…in all domains – space, sea, land, air, and information.” [JV2020, pg 6] Accomplishing this requires that we fully understand our own information environment, are able to completely capture important data and ignore irrelevant information, and have adequate resources to manage the entire infosphere.

Many efforts are underway to radically increase our military capabilities and effectiveness with advanced, interconnected weapon systems and platforms. If we are to be ready for these new systems, we must be able to fully understand the scope of their data output, handle the increased bandwidth requirements and intelligently manage the information flow.

Bibliography

Alderson, Ralph N, CAPT, Director, J-UCAS Program. J-*UCAS Program Update for the AUVSI Program Review.* Slides from Presentation. 8 February 2006.

Army Center for Military History Website. *The United States Army in Afghanistan: Operation Enduring Freedom*. URL: http://www.army.mil/CMH/brochures/Afghanistan/Operation%20Enduring%20Freedom.htm

Baldwin, Patrick D. *Modeling Information Quality Expectation in Unmanned Aerial Vehicle Swarm Sensor Databases.* Thesis, Air Force Institute of Technology, 2005.

Baldwin, Rusty O. and Samuel D. Bass. *The Networked Battlespace: The Risks of Using Strategic Views to Make Tactical Decisions (and vice versa).* Unpublished, May 2006.

Belz, David S., RAdm, et al. *Statement Before the Select Committee On Homeland Security, U.S. House Of Representatives*. May 5, 2004. URL: http://www.ftp2025.com/security/maritime.pdf

Berridge, Walter T. *Extracting Mission Semantics From Unmanned Aerial Vehicle Telemetry And Flight Plans*. Thesis, Air Force Institute of Technology, 2000.

Bishop, Matt. *Computer Security: Art and Science*. Addison-Wesley, 2003.

Bowden, Mark. *Black Hawk Down: A Story of Modern War.* Penguin Putnam, Inc., New York, NY, 2002.

Brown, Richard K. *Image Registration Using Redundant Wavelet Transforms.* Thesis, Air Force Institute of Technology, 2001.

Caltabellotta, Richard A. and Curtis Jefferson. J-UCAS Group, Aeronautical Systems Center, WPAFB. Personal Interview, 2006.

Congressional Budget Office (CBO). *The Army's Bandwidth Bottleneck.* The Congress of the United States, August 2003.

Correll, John T. *Igloo White*. Air Force Magazine. November 2004, Vol. 87, No. 11. URL: http://www.afa.org/magazine/nov2004/1104igloo.asp

DARPA Grand Challenge Website. URL: http://www.darpa.mil/grandchallenge/

Department of Defense. *Doctrine for Intelligence Support to Joint Operations*. Joint Publication 2-0. Washington: GPO, 9 Mar 2000.

Future Combat Systems Website. URL: http://www.army.mil/fcs/index.html

iRobot Website. URL: http://www.irobot.com/sp.cfm?pageid=109

Joint Chiefs of Staff. *Joint Vision 2020*. URL: http://www.dtic.mil/jointvision/jv2020a.pdf

Kadrovach, Anthony. *A Communications Modeling System for Swarm-based Sensors.* Ph.D. Thesis, Air Force Institute of Technology, 2003.

Klein, L., Producer. *Spies that Fly*. A Nova Production, 2002 WGBH Educational Foundation.

Monument Visitors Site. *Museé des plans-reliefs.* URL: http://www.monum.fr/visitez/decouvrir/fiche.dml?id=102&lang=en

Page, Timothy I. *Incorporating Scene Mosaics As Visual Indexes Into UAV Video Imagery Databases.* Thesis, Air Force Institute of Technology, 1999.

Pane, John F and Leland Joe. *Making Better Use of Bandwidth: Data Compression and Network Management Technologies.* The Rand Corporation, 2005.

Pyburn, Bradley L. *Analysis Of The Applicability Of Video Segmentation To Unmanned Aerial Vehicle Surveillance Video*. Thesis, Air Force Institute of Technology, 1999.

SR 108-284. Senate Report 108-284 - Department Of Defense Appropriations Bill, 2005.

Sullivan, Michael J., Director, Acquisition and Sourcing Management. *Report to the Committee on Armed Services, U.S. Senate*. GAO Report 06-447, March 2006.

Tirpak, John A. *The Network Way of War*. Airman Magazine. Website: http://www.afa.org/magazine/March2005/0305network.asp

United States Department of Defense, *Dictionary of Military and Associated Terms,* Joint Publication 1-02, Apr. 12, 2001, p. 557.

USAF Scientific Advisory Board. *Building the Joint Battlespace Infosphere, Volume 1: Summary*. SAB-TR-99-02, Dec 17, 1999.

VietnamWar.com Website. *The Son Tay Prison Raid*. URL: http://www.vietnamwar.com/sontayprisonraid.htm

Vita

Major Samuel D. Bass graduated from Sarasota High School in Sarasota, Florida. He entered undergraduate studies at the University of Central Florida in Orlando, Florida where he graduated with a Bachelor of Science degree in Liberal Studies and a commission as a Second Lieutenant from the Air Force ROTC program in 1992.

His first assignment was at Vandenberg AFB, California as an Undergraduate Missile Student, where we completed the program as a Distinguished Graduate. For his next assignment, he was sent to be an ICBM crew member at Malmstrom AFB, Montana. While there, he completed a Master of Science degree in Aeronautical Science from Embry-Riddle Aeronautical University. In 1997, he was selected to teach ROTC at the University of Arizona and served as the unit education officer and the Commandant of Cadets. In 2000, he cross-trained to the communications and information career field and was stationed at Scott AFB, Illinois, where he served as the Software Engineering Flight Commander and later as Chief of Air Mobility Command's Network Operations and Security Center. In 2003, he was stationed at Ramstein Air Base, Germany, where he served as the Combat Support Flight commander in the 1st Combat Communications Squadron and later as the Chief of Contingency Plans in the Air Forces Europe Directorate of Communications and Information.

Major Bass completed Squadron Officer School in residence and Air Command and Staff College by correspondence. Upon graduation, he will be assigned to the Defense Information Systems Agency in Alexandria, Virginia.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)* 13-06-2006	**2. REPORT TYPE** Master's Graduate Research Project	**3. DATES COVERED** *(From - To)* January - May 06

4. TITLE AND SUBTITLE

THE CHALLENGES OF INFORMATION MANAGEMENT IN THE NETWORKED BATTLESPACE: UNMANNED AIRCRAFT SYSTEMS, RAW DATA AND THE WARFIGHTER

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Bass, Samuel D., Major, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

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

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way, Building 641
WPAFB, OH 45433-8865

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/IC4/ENG/06-01

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

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The purpose of this research project was to explore how information is collected and used in the battlefield and identify areas of further research would help ease the burden of processing, managing and transmitting that information. The research included surveys of the intelligence analysis process and an exploration of some of the sources of data produced and consumed in the battlespace. The findings of this research led to the identification of several areas of research that could help warfighters deal with the problems posed by the DoD's rapidly growing mountain of unorganized and unprocessed data.
The culmination of the research is the development of the Integrity-Relevance-Classification Data Sharing Model and proposes areas for its future analysis and implementation.

15. SUBJECT TERMS

Sensor networks, distributed processing, mote wireless nodes, Combat Air Force applications

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Seetharaman, Guna S., Ph.D.
U	U	U	U	62	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-3636, x4612