Information Operations: Wisdom Warfare For 2025

A Research Paper
Presented To

Air Force ***2025***

by

Lt Col Edward F. Murphy
Maj Gary C. Bender
Maj Larry J. Schaefer
Maj Michael M. Shepard
Maj Charles W. Williamson III

April 1996

Disclaimer

2025 is a study designed to comply with a directive from the chief of staff of the Air Force to examine the concepts, capabilities, and technologies the United States will require to remain the dominant air and space force in the future. Presented on 17 June 1996, this report was produced in the Department of Defense school environment of academic freedom and in the interest of advancing concepts related to national defense. The views expressed in this report are those of the authors and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States government.

This report contains fictional representations of future situations/scenarios. Any similarities to real people or events, other than those specifically cited, are unintentional and are for purposes of illustration only.

This publication has been reviewed by security and policy review authorities, is unclassified, and is cleared for public release.

Contents

Illustrations

Tables

Executive Summary

A robust information operations architecture can provide leaders dominant battlespace knowledge and tools for improved decision making. US armed forces in 2025 need an information operations system that generates products and services that are timely, reliable, relevant, and tailored to each user's needs. The products must come from systems that are secure, redundant, survivable, transportable, adaptable, deception resistant, capable of fusing vast amount of data, and capable of forecasting.

The information operations architecture of 2025 this paper proposes consists of thousands of widely distributed nodes performing the full range of collection, data fusion, analysis, and command functions—all linked together through a robust networking system. Data will be collected, organized into usable information, analyzed and assimilated, and displayed in a form that enhances the military decision maker's understanding of the situation. The architecture will also apply modeling, simulation, and forecasting tools to help commanders make sound choices for employing military force. This architecture allows the United States (US) armed forces to conduct Wisdom Warfare.

The system can be used by the commander in chief, unit commander, supervisor, or technician. Somewhere in the workplace, in a vehicle, or on the person there will be a link to the sensors, transmitters, receivers, storage devices, and transformation systems that will provide, in push or pull fashion, all the synthesized information needed to accomplish the mission or task. Information will be presented in a variety of forms selected by the user.

To realize this capability in 2025, America's armed forces will have to alter the way they do business. Doctrinal and organizational changes will have to overcome institutional biases and orchestrate the development of an open architecture. The commercial market's lead in information technology development must be leveraged. New approaches to computing, as well as advancements in processing speeds and capacity, artificial intelligence (AI), software development, and networking must be investigated. In addition, research on human decision-making processes, human system integration, and display technology must be fostered.

To win in 2025, the armed forces of the United States will require an information operations architecture that uses information better and faster than its adversaries. This architecture must be effective across the spectrum of military operations and in any alternate future. To achieve this feasible system by 2025, America must begin to commit its time and money.

Chapter 1

Introduction

In 2025, it is likely the United States will have fewer forces.[1] Most of these forces will be based in the continental US (CONUS). They will be responsible for a variety of missions that will require much greater speed and flexibility than exists today. To meet these requirements, US armed forces of 2025 will have to use information better and faster than their opponents.

"Information operations", a subset of information warfare, deals exclusively with the use of military information functions. It is how data is gathered, manipulated, and fused. It includes such functions as intelligence, surveillance, reconnaissance, command and control, communications, precision navigation, and weather. Information operations does not include actions to deny, corrupt, or destroy the enemy's information or efforts to protect ourselves against those actions.[2] Figure 1-1 shows where information operations fits within the realm of information warfare.[3]

INFORMATION WARFARE

Roles and Missions of Aerospace Power

Aerospace Control	Force Application	Force Enhancement	Force Support
Counterair	Strategic Attack	Airlift	Base Ops & Def
Counterspace	Interdiction	Air Refueling	Logistics
Counterinformation	Close Air Support	Spacelift	Combat Support
	C^2 Attack	Special Operations	On-Orbit Support
		Information Operations	

Figure 1-1. The Role of Information Operations in Aerospace Power

Information operations involve the acquisition, transmission, storage, or transformation of information that enhances the employment of military forces.[4] Information operations devices and systems must be properly applied to give the warrior information superiority. To be useful, the information, a combination of data and instructions, must reduce uncertainty.[5] Acquiring information and putting it in a useful form will help achieve knowledge. “Knowledge and control of information is necessary for all missions, whether in peace or war, logistics or combat.”[6] More is needed to achieve true information superiority. The next step required is wisdom.[7] In this paper, wisdom is defined as knowledge coupled with good judgment.[8] The Wisdom Warfare architecture can dramatically improve a warrior’s good judgment by synthesizing information and modeling and simulating scenarios to provide advice, options, and probabilities of occurrence.

To better understand *wisdom operations*, the process must first be defined. The fundamental principles for acquiring intelligence information against an adversary remain valid over time. Figure 1-2 illustrates the flow from observable event to wisdom. First, some observable event must occur. That event must be observed by a sensor or sensors. The sensors collect the observable phenomena of the event and produce data. The data are processed and forwarded as information. Analysis of the information produces intelligence. The fusion, correlation, and association of relevant archival information lead to an understanding of the event and how it plays a part in the *big picture*. This understanding of the event results in knowledge. Building on that base of knowledge, the decision maker can apply automated decision aids and forecasting

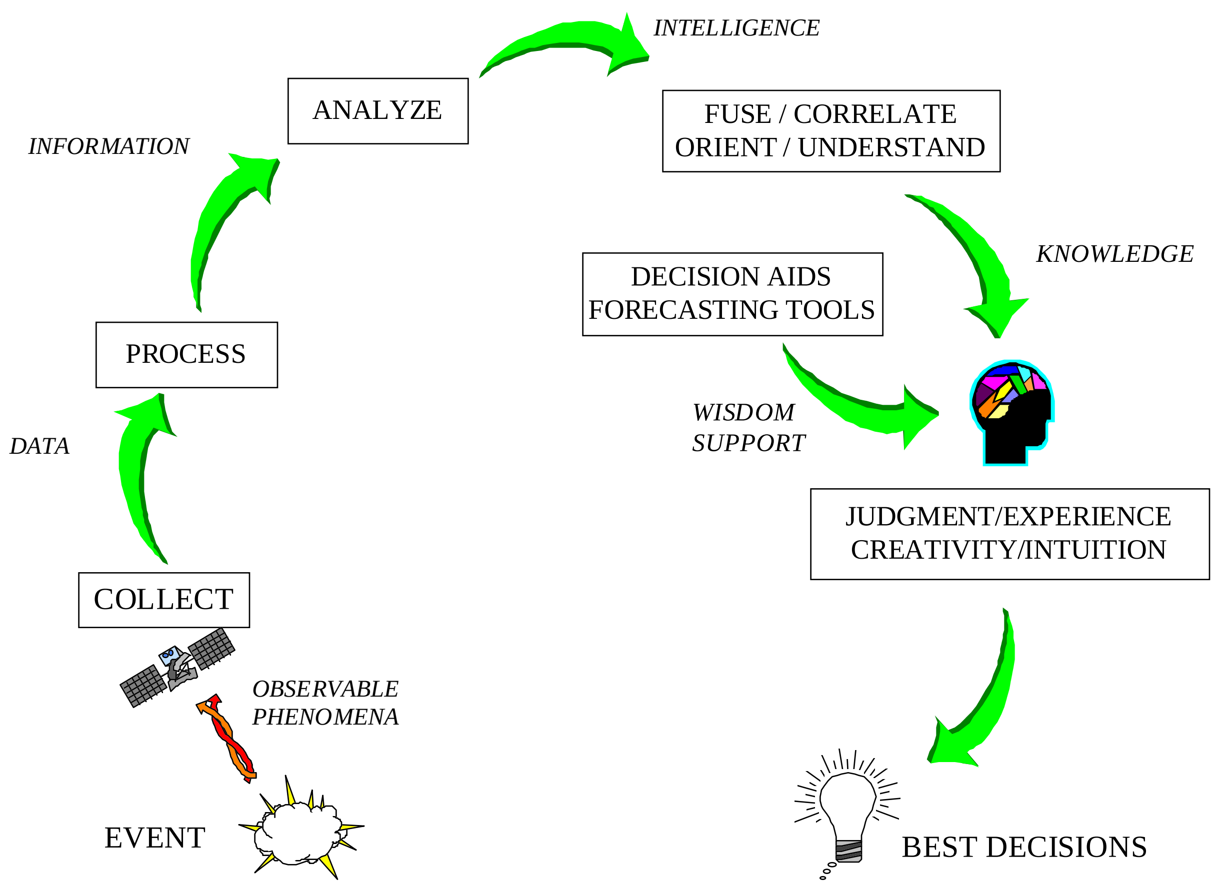

Figure 1-2. The Wisdom Process

tools (*wisdom support*) coupled with his own personal judgment, experience, creativity, and intuition to make the best decisions. This is Wisdom Warfare. "It is the association of well-known principles in an innovative way that produces the revolutionary result."[9] Making the leap from intelligence to wisdom will require innovative approaches for analyzing, fusing, associating, and handling information.

The Wisdom Warfare architecture proposed in this paper has three main components: the *knowledge* component, the *wisdom* component, and the *human system integration* (HSI) component. The *knowledge* component includes systems that collect raw data, organize it into useful information, analyze it to create intelligence, and assimilate it to gain knowledge. The *wisdom* component contains those systems that allow humans to interact with the knowledge to exercise wisdom. This component includes modeling and simulation tools. The final component of the architecture is HSI. The HSI component contains all of the systems necessary to assist decision makers in getting the information needed in the form desired. Once the decision makers understand the information, they can apply experience to make the best decisions.

A properly developed information system will let the warrior observe the battlespace, analyze events, make wiser decisions, and distribute information effectively. What is the aim of such an information system? Sun Tzu said it best. "Know your enemy and know yourself; in a hundred battles you will never be in peril."[10]

Notes

[1] Lt Gen Jay W. Kelley, "Brilliant Warrior" (Unpublished paper, March 1996), 4 (prepared for publication in the *Joint Forces Quarterly*, Summer 1996).

[2] Department of the Air Force, *Cornerstones of Information Warfare*, 1995, 3.

[3] Ibid., 11.

[4] Ibid.

[5] Bill Gates, *The Road Ahead* (New York: Viking Penguin, 1995), 30.

[6] USAF Scientific Advisory Board, *New World Vistas: Air and Space Power for the 21st Century*, summary volume (Washington, D.C.: USAF Scientific Advisory Board, 15 December 1995), 4.

[7] ***2025*** Concept, No. 900339, "Understanding Information Hierarchy," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

[8] Philip B. Gove, editor in chief, *Webster's Third New International Dictionary, Unabridged* (Springfield, Mass.: Merriam-Webster, 1986), 2624, (definition 2 of "wise": "WISE indicates discernment based not only on factual knowledge but on judgment and insight <wise men . . . anticipate possible difficulties, and decide beforehand what they will do if occasions arise—J. A. Froude>).

[9] *New World Vistas*, summary volume, 13.

[10] Sun Tzu, *The Art of War*, translated by Samuel B. Griffith (London: Oxford University Press, 1971), 84.

Chapter 2

Required Capabilities

US armed forces face an array of uncertain futures. They could be called on to perform missions in a variety of environments: deterrence, operations other than war, minor regional conflicts, major regional conflicts, or full-scale war. In addition, those missions will likely be accomplished with a smaller force than today. To accomplish these missions, US armed forces must take advantage of the most significant force multiplier: information.

The proliferation of sensors is creating a flood of information and the flood will likely grow stronger in the future.[1] Tools to handle that flood are insufficient today, and major changes are needed to manage the deluge in 2025.

In the future, information systems must generate products that are timely, current, reliable, relevant, and tailored to the user's needs. These products will come from systems that are secure, redundant, survivable, transportable, adaptable, deception resistant, capable of fusing a vast amount of data, and capable of forecasting.

The challenge in 2025 is to create an adaptive information *architecture* to provide decision makers and operators with superior battlespace awareness by consistently supplying the right information, in sufficient detail, in enough time, to make the best decisions at all levels of command. However, superior battlespace awareness is not enough. The decision makers must not only be aware of what is happening within their area of interest, they must also understand why it is taking place and what to do about it.

Required Knowledge Capabilities

Achieving superior knowledge over the adversary will require the right mix of multispectral sensors, advanced automated processors, analysis and correlation tools, and dynamic storage devices. These devices must be logically integrated to orient enormous quantities of information in a manner that will impart knowledge to a variety of decision makers.

Sensors must detect a wide variety of phenomena and be deployable around the globe. To achieve this, the conventional intelligence, surveillance, and reconnaissance methods must be complemented with exotic types of information collectors. These techniques might include seismic, acoustic, magnetic resonance imaging, and atmospheric (aircraft and missile wake) detection.[2] The ability to obtain information directly from an adversary's databases (mapping and penetrating the military and commercial information systems of the enemy) remains a high priority. Also included in this mix of data collectors are weather sensors to provide timely and accurate environmental reports. Finally, a new family of low cost, "leave-behind" sensors must be developed to provide near-real-time poststrike effects assessments.[3]

Needs of the emerging weapon systems will drive specific sensor requirements such as resolution or geolocational accuracy. Precision weapons require precision intelligence. Lasers and other directed energy weapons may require resolutions down to a few centimeters.

The Air Force Scientific Advisory Board recently published *New World Vistas: Air and Space Power for the 21st Century*. In it they stated "the power of the new information systems will lie in their ability to correlate data automatically and rapidly from many sources to form a complete picture of the operational area, whether it be a battlefield or the site of a mobility operation."[4] This represents the heart of any information operations engine. The ability to fuse vast amounts of data from the multitude of sensors, automatically sort it, identify the essential pieces of information, and provide the right information to the right node in near real time is the goal. This represents one of the greatest challenges. The best system will be able to identify the relevant databases across dissimilar networks, search through and filter vast amounts of stored information, and rapidly analyze and correlate data across distributed databases with thousands or millions of variables.[5] The architecture must automatically maintain current information on designated target sets at all times and assist in targeting by presenting vulnerability, aim points, and strike options. This process must remain effective even when incomplete or uncertain data are part of the underlying situation.[6]

The system must also integrate knowledge of the operating environment, especially the terrain over which forces will operate. A world map using a common grid is needed, plus the ability to provide maps expressed in unique coordinates but derived from a common database or grid.[7] The goal of precision mapping is to provide the user with less than one meter accuracy. An onboard map coupled with navigation aids will permit aircraft and unmanned air vehicles to fly anytime, anywhere, on any route.[8]

Well-trained personnel are crucial for the proper analysis and evaluation of information; without them the commander is presented with a "regurgitation of previously reported 'facts' that may or may not be relevant."[9] In 2025, the human element is still the key. However, in the face of the information explosion and high tempo military operations expected in 2025, the analytic tasks performed by those well-trained professionals must be complemented by automated processes wherever possible.

The evolving doctrine in the new information age mandates each commander be empowered to act quickly and decisively to changes taking place on the battlefield. For this empowerment to be successful, the information operations architecture must deliver the essential information relevant to that particular commander. The architecture must do this simultaneously for each command or weapon system node.[10] Once the required knowledge is gained, decision makers will need to use it to increase military effectiveness. In other words, they must use the knowledge wisely.

Required Wisdom Capabilities

The *wisdom* component helps decision makers reach good conclusions quickly. The architecture includes the models, simulations, forecasting aids, decision aids, planning and execution tools, and archival methods that enable information superiority over an adversary.[11] The models and simulations also need to incorporate response mechanisms so outcomes are included in future scenarios.

Campaign planning is a critical role for the *wisdom* component. Forecasting tools or intuitive knowledge and decision support systems are critical to the war fighter.[12] In campaign planning, the system can assist the commander by forecasting possible enemy courses of action (COA). Similarly, the campaign planner would pursue various alternatives for friendly COAs. Each of these friendly COAs could be pursued against each of the enemy COAs. Figure 2-1 illustrates this process for the most likely enemy COAs. An ability to permanently store or archive past forecasts and actual outcomes or decisions is required so they are available as input in new scenarios. Linking simulations to real-world exercises on live ranges verifies whether these simulations represent reality.

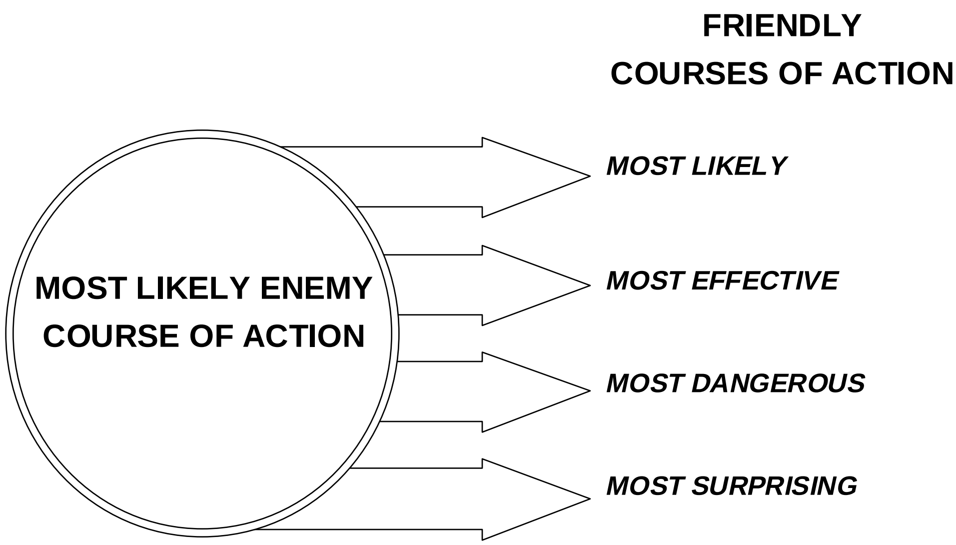

Figure 2-1. Course of Action Development

The *wisdom* component must aid training by allowing friendly forces to perform virtual missions.[13] It must support the modernization of existing systems and development of new systems. This will improve test and evaluation, reduce acquisition cycle times, and reduce costs.[14] It must also model future foreign systems, technologies, and scenarios so the military acquisition system can maintain technical superiority.

Required Human System Integration Capabilities

The human will remain the essential element of the information operation systems of the future. Humans will exercise command and control and apply their unique attributes to information processing and decision making—an integral part of the Wisdom Warfare concept. Humans can process large amounts of information through the five senses; chiefly visual (billions of bits per second) and audient (tens of thousands of bits per second).[15] However, the human as an information channel (usually transmitting information orally) is limited to about 50 bits per second.[16] Gaining and maintaining information superiority in 2025 will require effective integration and interfacing between humans and systems. This effective integration will rely on improved capabilities in three areas: the human, the system, and the way they interact.

The human area consists of improving and enhancing the way people deal with information. This includes human sensing capabilities and human cognitive functions like problem solving and decision making. The system area consists of developing and improving information transformation systems to include artificial intelligence (AI), intelligent software, information filters, and information access systems. The final area consists of improving and enhancing the integration between humans and systems. This integration focuses not only on improving the human-machine interfaces but also includes the larger idea of gaining synergy between humans and systems. This synergy incorporates capabilities like brain activated control of machines.

Obviously, in an environment of exponential growth in information available to humans, capabilities to improve and enhance the ways humans deal with information are required. The first step is to gain a better understanding of how humans work with information. This requires a significant improvement in the understanding of the immensely complex human brain.[17] The capability to understand how the human brain works in different situations will help improve human performance. A required capability for improvement is enhancement of memory since it has been shown excellent memory helps develop proficiency in situational awareness.[18]

Achieving effective integration between humans and systems will require a long-term systems engineering process. The process will begin early in a person's career where evolved portable computers will be used to store information on the methods the decision maker uses in problem solving in all kinds of situations. This process will also require training to improve the human mental dexterity in using the system.[19] The human brain is a great processor, and it should be used to the maximum extent possible.

Another required capability is to design systems that can determine the status of the decision maker's cognitive processes and adjust the information available and the way it is being presented to avoid information overload. Improved information displays will be required to present information to the decision maker in a variety of forms.[20] Systems that take into account the nonverbal methods of communication like gesturing and facial expressions need to be developed.[21] As systems become more intelligent and autonomous, humans must understand what actions are being taken and the potential limitations these actions might create for the decision maker.

So what is really required in 2025? First, the leaders of tomorrow must have an architecture that acquires and transforms a vast amount of information from a wide variety of sources. Second, the architecture must forecast courses of action and provide advice to the war fighter. Finally, the architecture must present information in a form that is timely, reliable, relevant, and tailored to the war fighter's information needs.

Notes

[1] Barry R. Schneider and Lawrence E. Grinter, eds., "Overview: Information Warfare Issues," *Battlefield of the Future: 21st Century Warfare Issues*, Air War College Studies in National Security No. 3 (Maxwell AFB, Ala.: Air University Press, September 1995), 150–151, 189.

[2] *Spacecast 2020*, Surveillance and Reconnaissance Volume (Maxwell AFB, Ala.: Air University, 1994), 3.

[3] ***2025*** Concept, No. 900518, "Electronic Grid—Throwaway Sensors," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

[4] USAF Scientific Advisory Board, *New World Vistas: Air and Space Power for the 21st Century*, summary volume (Washington, D.C.: USAF Scientific Advisory Board, 15 December 1995), 11.

[5] Ibid., 24.

[6] *New World Vistas,* (unpublished draft, the technology application volume), 10.

[7] Ibid., 19.

[8] Ibid., 20.

[9] Lt Col Norman B. Hutcherson, *Command and Control Warfare* (Maxwell AFB, Ala.: Air University Press, 1994), 29.

[10] *New World Vistas*, (unpublished draft, the technology application volume), 24.

[11] ***2025*** Concept, No. 900386, "Computer-Assisted Battle Decision System," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

[12] Department of the Air Force, *Air Force Executive Guidance*, December 1995, 20.

[13] Kelley, "Brilliant Warrior" 9.

[14] *Air Force Executive Guidance*, 21.

[15] Sarnoff Research Center, "Exploiting the Consumer Digital Systems (CDS) Revolution," briefing to Lieutenant General Kelley, Air University commander, Maxwell AFB, Ala., 24 March 1994.

[16] J. R. Pierce and J. E. Karlin, "Reading Rates and the Information Rate of a Human Channel" (Convention Record Part 2, IEEE WESCON, 1957), 60.

[17] *Compton's Interactive Encyclopedia*, 1994 ed., s.v. "human brain." Given that the human brain contains 100–200 billion neurons with each one connected to 1,000 or more other neurons and having more than 60 chemical messengers (neurotransmitters and neuropeptides) to communicate with in any combination, "the number of possible brain states is inconceivably large."

[18] *New World Vistas*, (unpublished draft, the human systems and biotechnology volume), appendix M, 2-4.

[19] Additional required capabilities can be found in 2025 white papers on General Education and Training; Training and Readiness; and Information Technology in Education and Training.

[20] *New World Vistas*, (unpublished draft, the human systems and biotechnology volume), appendix F. Appendix F describes research for improving the design of displays. Though the discussion focuses on improvements for displaying information to pilots of aircraft these concepts can be used in a large variety of situations.

[21] Nicholas Negroponte, *Being Digital* (New York: Vintage Books, 1996), 91–92; Idem, "Affective Computing," *Wired*, April 1996, 184.

Chapter 3

System Description

This section describes an architecture of information systems for use by the US armed forces in 2025. All the capabilities may not be possible by 2025. However, this paper was written to provide the map to near-maximum expected capability. Any stop short of that destination will still have useful features for air power.

The information operations architecture of 2025 consists of thousands of widely distributed nodes, performing the full range of collection, data fusion, analysis, and command functions, all linked through a robust networking system. It is an open architecture allowing modular upgrades without massive redesign. The architecture collects raw data, organizes it into useable information, analyzes and assimilates it, and imparts it in a form that enhances the military decision-maker's understanding of the battlespace. The architecture also applies modeling, simulation, and forecasting tools to help commanders make sound choices for employing military force.

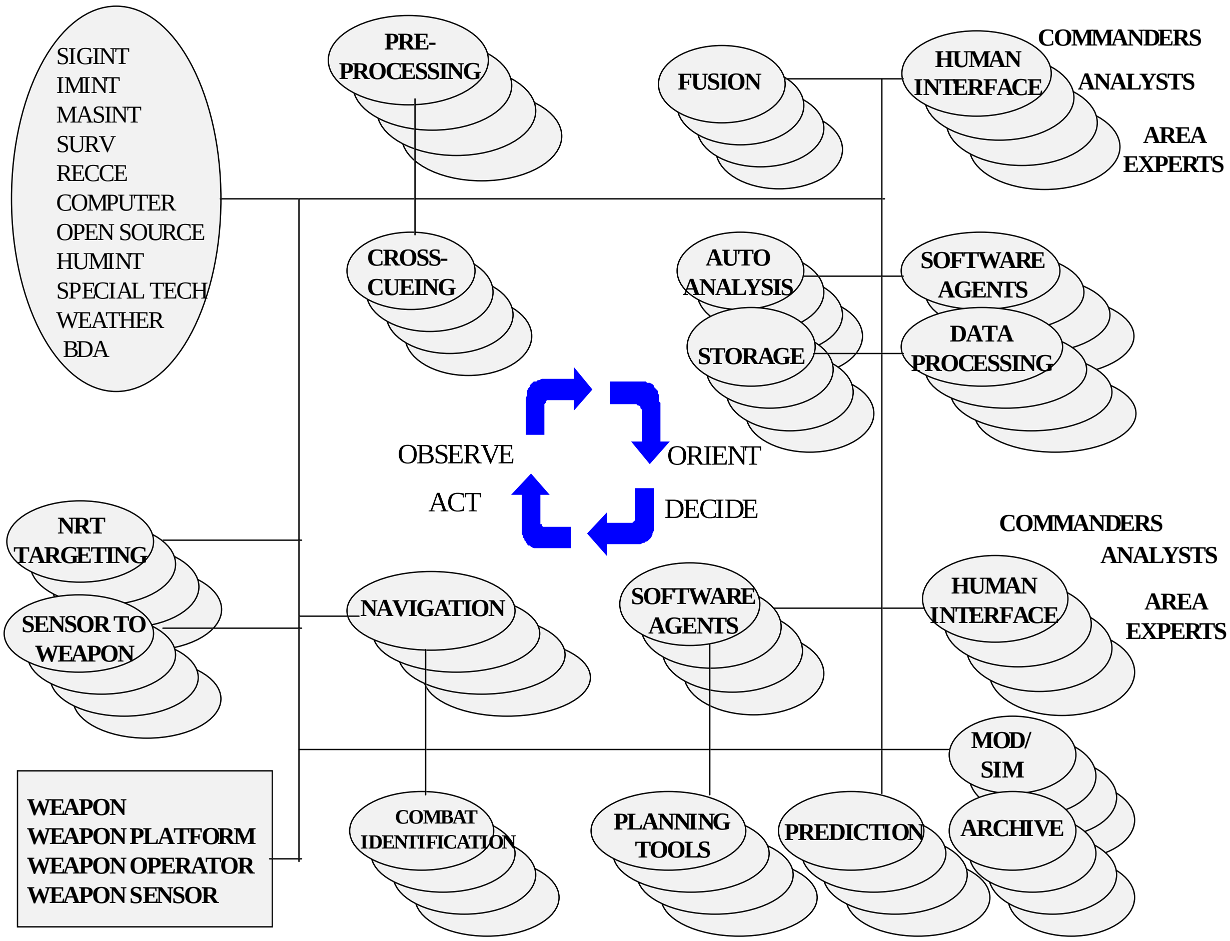

Figure 3-1. Wisdom Warfare Architecture

Figure 3-1 shows one vision of this architecture. (Abbreviations are listed in appendix A.) It is a functional rather than a physical depiction. To understand how this architecture operates, it is helpful to divide it into four functional areas that mirror the Col John R. Boyd OODA loop; that is, *observe*, *orient*, *decide*, and *act*. This division is for illustrative purposes only. In reality, when dealing with information operations, it is difficult to determine exactly where one function ends and another begins. All the nodes are tied together; they exchange information, share processing and storage capacity, and all work together to solve a common problem—superior battlespace knowledge and wisdom. All four elements of the OODA loop are represented in the architecture and are vital to its proper functioning. However, the focus of this paper is on *orient* and *decide*, which can be roughly equated to the *knowledge* and *wisdom* components. The *observe* and *act* functions are the subjects of other white papers and will be addressed here only briefly.

Within the *observe* component of the architecture, most data collection occurs. Included are all the traditional elements of sensing commonly found in intelligence, surveillance, and reconnaissance. Also included are sensors for weather and terrain mapping, as well as new collection techniques such as noninvasive magnetic source imaging, magnetic resonance imaging, and aircraft wake turbulence detection.[1] Sensors process data as far forward as possible, at the point of collection in some cases, to reduce overall observation reporting time. New chip architecture offers the promise of lighter and more efficient hardware, improved power requirements, and reduced failure potential for a host of sensor equipped devices.[2]

Many weapon systems, especially airborne weapon systems, are capable of contributing their observations to the overall architecture, as well as being capable of autonomous operations with their sensor suites to reduce their reliance on any vulnerabilities in C^2 systems.

For Battle Effects Assessment, expendable sensors can deploy with the weapon systems.[3] These sensors could consist of miniature gliding flight vehicles that carry onboard processors, independent navigation capabilities, and various sensing technologies including optical, infrared, radio frequency, and acoustic.

The *observe* component also includes nodes for the correlation and fusion of sensor data from different sources and nodes for sensor cross-cueing to provide automated sensor-to-sensor tip-offs for collection steerage. Additionally, there are nodes for collection management of preplanned and directed search activities. Finally, the *observe* functional area is tightly linked, accessible, and highly responsive to the *act* component.

The elements within the *act* area include those directly supporting a weapon system in accomplishing its task. Of course, the *act* component in 2025 may well include air power actions other than “bombs on target." The system must provide navigation, combat identification, and targeting information. Weapon systems have direct links to the *observe* component. This direct link provides real-time (seconds) sensor-to-shooter and sensor-to-weapon data flow and provides near-real-time (minutes) targeting information to planning cells. These links must be developed in conjunction with the development of the weapon system to ensure full integration rather than an add-on capability. Since specific weapon systems design of 2025 is beyond the scope of this paper, this area of information operations will not be addressed further.[4]

Knowledge Systems

The *orient* component of the architecture performs what this paper describes as the *knowledge* function of information operations. It contains the various nodes for automated data fusion, analysis, storage, and retrieval. It is composed of a mix of old and new technologies in an open architecture that allows incremental upgrades of individual elements as technology continues to advance. The architecture is also networked in a fashion that allows graceful degradation as a result of enemy action or component failure (fig. 5).

As a result of many years of collecting information from a wide variety of sources and methods, the architecture’s databases contain information on virtually every potential target set or system vulnerable to combat power, both lethal and nonlethal. This information includes an up-to-date compendium of physical descriptions, multiple view images, floor plans, material lists, subsystem component descriptions, technical specifications and drawings, operations manuals, and relationships with other systems.[5]

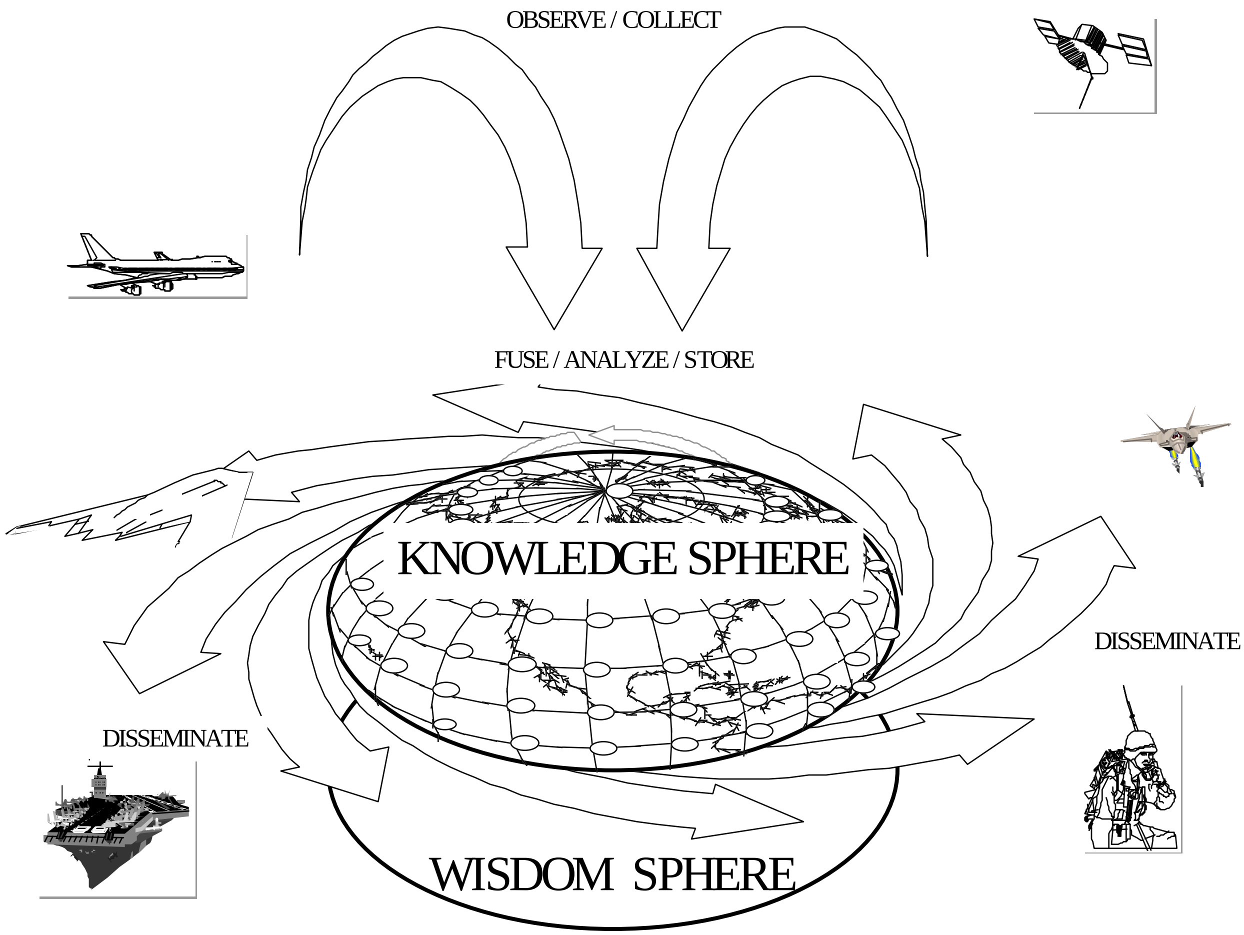

Figure 3-2. The Knowledge and Wisdom Spheres

This massive amount of information is too large for humans to maintain and keep current without the help of automation. The architecture automatically recognizes gaps, deficiencies, or outdated information in the databases and, without human intervention, searches the global information net.[6] It then retrieves the information directly from the various information libraries around the world, or sends a request for collection of the missing or outdated information. The architecture tracks the progress of the response and follows up as necessary. The architecture also reviews numerous satellite images and alerts human analysts of any changes found at potential target areas making obvious exceptions for weather.

Besides information on potential adversaries, the architecture also integrates information on our own and allied forces as reported from the *act* component. This friendly information includes maintenance status, crew health and availability, location, and mission status.[7]

New generations of nonmagnetic media—possibly associated with lasers, optical disks, and other newly emerging technologies—will be used to store data. Client-server and distributed data warehouse models can transfer data from the source to the military users' local storage media.[8] The architecture can take advantage of lower-cost technologies as well. If massive communications bandwidths are relatively inexpensive, then users' storage devices do not have to be unlimited since the users have unlimited access to source servers. The users simply download what is required for a given mission. However, if cost favors large local memory, then the system could use it and only rely on communications for updates.

Algorithms specifically designed for synchronization, truth maintenance, and queuing delays are used to efficiently integrate all this data from very large distributed databases.[9] Every individual data set is tagged with a location indicator to permit immediate and automatic synchronization and alignment of the data or objects of interest.[10]

Data fusion is crucial to taking the massive amount of data available and turning it into useful information without overloading either the human or the information systems themselves. The fusion process takes place across the entire distributed network of sensors, computing servers, and platforms. The architecture integrates fusion applications across multiple nodes using coordination languages to tie together dissimilar operating systems. To do this it employs many separate tools (target models, search, and filtering algorithms) with very large amounts of common sense knowledge. Key fusion functions include automatic target recognition, multi-target tracking, pattern recognition, and object relationship analysis for dynamic situation assessment.[11]

Achieving *knowledge*-level and *wisdom*-level fusion requires information access technology (IAT) for searching across very large distributed databases.[12] One promising approach for IAT is the use of artificial intelligence or intelligent software agents (ISA). ISA are discussed in greater detail in the Key Technologies section.

The next portion of the information architecture is the *decide*, or *wisdom*, component. With much of the correlation, fusion, and basic-level analysis accomplished by automation, the human will spend less time on where the tanks are and more time on which tanks would be the most effective to attack.[13] This is where modeling, simulation, and decision tools come into play.

Wisdom Systems

The *wisdom* component includes the modeling, simulations, software agents, forecasting tools, decision aids, planning and execution tools, and the archival methods that enable US armed forces' information and knowledge to be superior over an adversary. Usually, the commander who has explored the most alternatives before combat emerges victorious. The forecasting tools will present a range of possible enemy COAs based on the current situation as defined by the knowledge process and based on historic precedence as recalled from the archives. The *wisdom* systems also identify potential strengths and weaknesses for each forecasted enemy COA. The campaign planner may try out, through modeling and simulation, various friendly responses to each of the enemy COAs. The system identifies probabilities of success and identifies potential weaknesses in friendly COAs.

A powerful new tool in the *wisdom* component is genius ghosting (fig. 6). Genius ghosting uses the concepts of historic figures, factors in the current context, provides COAs, then simulates the results to provide probabilities of various outcomes. Academic institutions could provide the historical framework. The *knowledge* component provides the current context. Models provide the COAs. Simulations provide the probabilities of outcomes.[14] For instance, the Wisdom Warfare system could apply a principle of Sun Tzu: "The doctrine of war is to follow the enemy situation in order to decide on battle. Therefore at first be shy as a maiden. When the enemy gives you an opening be swift as a hare and he will be unable to withstand you."[15]

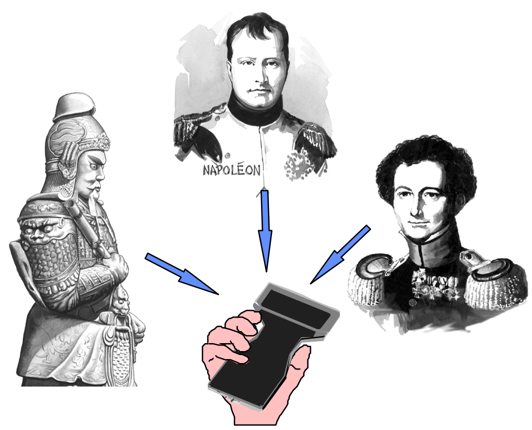

Figure 3-3. Genius Ghosting: Sun Tzu, Napoleon, and Clausewitz

The COAs would include a reactive strike rather than a preemptive strike. They would include forces in defensive positions until the time is right to strike. The Wisdom Warfare system then "wargames" those COAs to provide probabilities of outcomes. By comparing the COAs provided by many different "genius ghosts," a commander will have a broader range to choose from. For instance, a commander could ask how Doolittle, Kenney, or Horner might design a particular campaign, then pick the elements that work best. In addition, the commander can avoid the dangers of dogma by selecting an unexpected COA, for instance, Doolittle's raid on Tokyo. The goal of genius ghosting is not to rigorously predict how a particular figure would fight a campaign. Instead, it is to give the commander a wider variety of creative options than he would have without Wisdom Warfare.

The Wisdom Warfare system also has a feedback mechanism allowing for course corrections (continuous updates and suggested corrections) based on pitfall predictors (after analyzing decisions and potential outcomes) and way point and metric analysis (indications of what to look for). The system learns from actual outcomes and advises the warrior.

The distinctive advantage of the 2025 *wisdom* system is that it is nearly autonomous and produces output just as fast as information is added or subtracted. It can be used during modeling, simulation, acquisition, planning, conflict execution, and conflict termination. In addition, this system applies not just to the strategic and operational levels of military operations but to the tactical as well.

A note of caution is appropriate at this point. There are two areas that may cause concern. First, the architecture design needs to recognize that each decision maker has bias in dealing with information. Second, as the architecture becomes human-like, there may be a tendency for the decision makers to become over-reliant on the architecture. This architecture realizes these two concerns and addresses them through the *human system integration* (HSI) component.

Human System Integration

To make the cycle complete, the system and the decision maker must interact to do something useful with that knowledge and wisdom. Given the proliferation of data and the exponentially expanding capabilities to gather data, a major challenge is to extract only the required data and transform it into a useable format for each specific decision maker when and where it is needed. Links for the information operations architecture maximize the use of the national information infrastructure, both government and commercial.

Using ISAs, the network automatically forwards to each node the essential knowledge that is most relevant for that particular node at any given moment. This requires each node to identify the most essential pieces of knowledge by type, level of detail, and timeliness for it to accomplish its mission. Over time, ISAs help users by learning information desired in a given situation. Each node, of course, retains the ability to pull additional information from the system or each information pushed from a superior node to a subordinate node as required.

The objective of HSI is to make it easier, faster, and more efficient for decision makers to adapt to the environment quickly, gain situational awareness, and apply their wisdom to make the best decisions possible. The architecture incorporates the continued advances in areas like time-critical decision making,[16] reducing information overload,[17] and human computer interaction.[18]

To allow quick adaptation to the environment, the human sensory and cognitive capabilities will be improved through a combination of technologies and training. The human senses can be enhanced through technology aids and drugs. "Smart" eyeglasses or contact lenses can present more than just the visible portion of the electromagnetic spectrum. Hearing aids can translate a wider range of sounds. Other aids will improve smell or incorporate scents into various tasks like memory recall or heightened sensitivity to help focus decision makers on the task at hand.[19] The technology aids also augment other senses to allow recognition of emotions to aid in other decision-making environments such as negotiations. Training is provided to teach the decision makers how to use these enhanced sensory powers. This leads to focusing human cognitive functions so they can make the best use of this information.

With a good understanding of how the human brain works, integration of the human and the system is achieved. It consists of improving the presentation of information to the decision maker given a preference for displays, problem-solving methods, current state of mind, and the situation at hand. The majority of this information will be stored in a personal digital assistant (PDA). The PDA can include training, exercises, and real event data.

Additional tools enhance the human's ability to be trained.[20] The goal is to provide a robust training system that takes advantage of the enhancing technologies described above. Through modeling and simulations, decision makers will be presented with the experiences they need to develop the lessons learned that lead to wisdom. These techniques can be used to speed up the training process—similar to accelerated life-cycle testing of hardware.

Displays are adaptive and flexible to account for each individual's preferences. They provide information through all the senses and include text, graphic, virtual, and holographic methods. They are tailored to optimize each user's learning and absorption capabilities. Additional technologies will be developed to allow human interaction with the displays. These technologies allow the displays to work with the human to adjust to each situation. The displays are scalar to allow zooming to the desired level of detail.[21] In this way the commander in chief can see the big picture of the battlespace or zoom to see the situation at the local level.

As mentioned above, the PDA learns the profiles of the items the decision maker believes are important and creates information filters to assist in avoiding information overload. The displays, in conjunction with modeling and simulations, also provide the capability of presenting the *ghosting* of geniuses as desired. In addition, the display is flexible enough to allow several people to view at the same time and through connections make collective inputs to aid the decision maker. This could be done at the same location or remotely using video teleconferencing for a common view of the battlespace.

Displaying a common picture of the battlespace is critical in ensuring the decision maker's intent is clearly communicated to all levels. Three-dimensional holographic displays are useful, particularly for users working in groups. Another example is "smart" glasses or contact lenses enabling the new concept of "eyes-up display."[22] The systems are completely interoperable and are able to tie into the network wherever users are located. The architecture takes advantage of secure, reliable, high capacity communications systems advanced by the commercial world. Through the combined use of these systems the decision makers are able to communicate their intent to all necessary levels and the advantage of having a common view of the battlespace is realized. Figure 3-4 is an example of this common picture of the battlespace.

Figure 3-4. Common View of the Battlespace

Key Technologies

This section describes some of the key technologies that apply across the entire architecture, including computational power and software.

The computational power contained in this architecture comes from a mix of old (traditional parallel processors, digital signal processors) and new models. One promising new computational approach is based on deoxyribonucleic acid (DNA) molecules. Computer designs based on DNA promise an extraordinary processing capability that operate at billions of tera-operations per second.[23] While the operations per second rate is very high, it can take hours to complete an entire DNA reaction. Therefore, DNA computing is best suited for complex problems with many variables, such as long-term surveillance and planning, which do not require response times that are measured in seconds.[24] In addition, pipelined, superscalar, and parallel processors show promise for computing power near six billion operations per second.[25]

The use of ISAs is vital to the proper functioning of both the *knowledge* and *wisdom* components. These agents are software modules that act independently and have a range of capabilities including directed-action, reasoned-action, and learned-action.[26] Directed-action agents have fixed goals and limited ability to deal with the environment and data encountered. Reasoned-action agents have fixed goals and an ability to sense both environment and data and take a reasoned action. Learned-action agents can do all the above. Additionally, they can accept high-level tasking and are capable of anticipating user needs based on general guidelines. Armed with this information, learned-action agents can issue new goals.

Intelligent software agents demonstrate reasoning and persistence in performing tasks. These *agents* work with their users to determine information needs, navigate the information world to locate appropriate data sources—and appropriate people—from which to extract relevant information. They also act as intelligent, long-term team members by helping to preserve knowledge about tasks, record the reasons for decisions, and retrieve information relevant to new problems.[27]

Neural network software provides another capability. Programmers give the system training data with known conclusions. The system then takes a great amount of information and draws a conclusion.[28] In a future where vast amounts of data are expected, systems that feed on data will be valuable.

Hardware and software must be coupled with advanced automated logic methods. For instance, the statistics of Markov chains can be used to predict the highest probability outcome of COAs.[29] Markov chains could be used to evaluate enemy and friendly COAs.

Another modeling tool is the fuzzy cognitive map (FCM).[30] The FCM draws a causal picture to predict how complex events interact and play. It can even handle imprecise rules like: "Bombing an electrical generator *usually* decreases generator output." The FCM relies heavily on feedback that allows it to be dynamic until it reaches an equilibrium point where a hidden pattern will emerge. This allows predictions of nonlinear system operations, including social systems. FCMs would also be useful in evaluating enemy and friendly COAs.

Chaos theory, a branch of mathematics, provides another modeling tool. Chaos theory deals with the behavior of bounded, nonlinear systems that are sensitive to small perturbations. Chaotic systems often appear to behave randomly but operate within defined bounds. There is reason to believe chaotic behavior occurs in human and organizational decision making and in combat operations.[31] Several features of chaos theory should prove useful. First, techniques like "embedding" make short-term forecasting possible and "attractors" describe the boundaries of the long-term behavior of chaotic systems.[32] These would be useful for forecasting enemy COAs, and the outcome of enemy and friendly COAs. Unlike Markov chains and FCMs, chaos attractors can describe the bounds of a number of outcomes rather than just the most likely one. Second, "Lyapunov exponents" help quantify sensitivities to small disturbances. These would be useful in determining what COAs may result in the greatest gains for the smallest additional inputs of military power. Third, calculations of the "information dimension" indicate the minimum number of variables needed to model a system.[33] The information dimension may indicate that a few variables drive a seemingly random system. Additionally, it makes modeling the system from actual data easier and faster. Overall, chaos theory holds great promise in a wide variety of areas.

Human system integration relies on an integrated use of technologies like: electroencephalograph (EEG),[34] ISAs, information displays, and training programs. EEGs will determine the mental state of the decision maker and tailor displays as appropriate. They will also assist the decision maker in performing computer-related tasks by brain activated control.

Countermeasures and Countercountermeasures

The force-multiplying effect of the Wisdom Warfare architecture on the effective employment of US forces presents a potential center of gravity no adversary can ignore. The attack methods expected to be directed against the architecture include the full range of countermeasures designed to disrupt, degrade, deny, and/or destroy, either locally or globally, the information functions provided to US forces.

In an attempt to disrupt the flow of information to decision makers, physical attacks against key nodes using conventional high explosives or electronic signal jamming are expected. These traditional methods of attack are easily countered through hardening (both the electronics and the physical facilities), dispersal, and redundancy. Indeed, the very nature of the architecture, with its multiple nodes and distributed processing, eliminates any "critical node" target or possibility of a single point of failure. Even if individual nodes or decision makers are effectively cut off from the architecture due to enemy action, the immediate effect is felt only at those isolated points and not across the entire architecture. The information flow is automatically rerouted around the disrupted node, allowing a seamless, continual flow of information.

The distributed nature of the architecture coupled with multiple forecasting models also aids its resistance to deception. The numerous observation nodes using a wide variety of sensing phenomenology, correlation tools, and historic databases greatly reduce the probability a battlefield deception effort by an enemy will be successful. By using multiple forecasting models, the Wisdom Warfare architecture is self-defending since the enemy would have to deceive multiple systems simultaneously.

The most dangerous forms of attack are those designed to corrupt, distort, or implant false information into the databases. These types of attacks may occur without any indications the system is under attack. Included in this form of attack are malicious software, computer viruses, chipping (manufacture of computer chips with malicious design flaws), spoofing, video morphing, and surreptitiously gaining local control of the flow of information on the network.[35] Advances in intelligent software, cryptography, and user-recognition techniques offer some degree of protection against these attacks.

The interface software at each node can provide the first level of protection by ensuring the data message that is attempting to gain access to that node is from whom it purports to be. Using message authentication, each node will verify the data message's origin and whether the data has been altered.[36]

Intelligent software agents can also be employed to monitor the network for the presence of malicious software and computer viruses. The agents can then attack and eliminate the viruses, or isolate them from the rest of the architecture to prevent their spreading, and notify the human operator for further corrective action.

Preventing computer viruses or malicious software from entering the architecture is a high priority. Cryptographic technology provides very high levels of security against unauthorized, surreptitious access to the information network. Encryption techniques can develop keys that may take eons to break (even using the computational power available in 2025), ensuring secure data at individual nodes and throughout the net.[37]

Unauthorized access can also be partially controlled by breakthroughs in biometric identification technologies. These technologies use physiological traits such as voice, fingerprint, eye, or face recognition to provide a continuous identity check of all operators who are using the system's HSI devices to retrieve information from, or input information into, the architecture. If these techniques fail, the system can disconnect any node believed to be compromised or captured.

Finally, unbreakable codes and biometric identification technologies offer no protection against the threat of compromised personnel. Renewed efforts are required to ensure national security policies monitor those individuals who are authorized access to the network and identify potential lapses in architecture integrity. Because technology is constantly evolving, countermeasures and concomitant countercountermeasures will similarly be changing. The operators and maintainers of the *wisdom* architecture must remain vigilant and continue to make changes to the security structure to stay ahead of advances and changes by an adversary.

In 2025, the system described in this chapter can be used by anyone: the commander in chief, unit commander, supervisor, or technician. Somewhere in the workplace, in a vehicle, or on the person will be a link to the sensors, transmitters, receivers, storage devices, and transformation systems that will provide, in push or pull fashion, all the synthesized information needed to accomplish the mission or task. Information will be presented in a variety of forms selected by the user. Key technologies like advanced processing, intelligent software agents, neural network software, automated logic methods, improved modeling techniques, and improved human system integration will make this system a reality. Certainly, there are countermeasures to such a system and one of the challenges in 2025 will be to protect the architecture both with physical and software security measures.

Notes

[1] *SPACECAST 2020*, Surveillance and Reconnaissance Volume (Maxwell AFB, Ala.: Air University, 1994), 3.

[2] "Chip Architecture Removes Signal Processing Bottleneck," *Signal*, February 1996, 58.

[3] ***2025*** Concept, No. 900404, "Built-in Battle Damage Assessment," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996); ***2025*** Concept, No. 900578, "Bulls Eye," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996); Department of the Army, *Force XXI*, 15 January 1995, 15–17.

[4] For additional information see white papers on counterair, counterinformation, strategic and C^2 attack, close air support, surveillance and reconnaissance (S&R) real-time integration, S & R information operations, and space S & R fusion.

[5] ***2025*** Concept, No. 900374, "Living World-wide Intelligence Base, ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

[6] ***2025*** Concept, No. 900446, "Automated Enemy Analysis Software," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

[7] USAF Scientific Advisory Board, *New World Vistas: Air and Space Power for the 21st Century*, summary volume (Washington, D.C.: USAF Scientific Advisory Board, 15 December 1995), 24.

[8] Andrew C. Braunberg, "Data Warehouses Migrate Toward World Wide Web," *Signal*, February 1996, 35.

[9] *New World Vistas*, (unpublished draft, the information applications volume), 13.

[10] Ibid., 57.

[11] Ibid., 8.

[12] Ibid., 45.

[13] Majors Kevin N. Dunleavy and Lester C. Ferguson, "Command and Control and the Doctrinal Basis of the Theater Air Control System," in Lt Col Albert, ed., *Concepts in Airpower for the Campaign Planner* (Maxwell AFB, Ala.: Air University Press, 1993), 135.

[14] *Force XXI*, 16–17.

[15] Sun Tzu, 140.

[16] Eric Horvitz and Matthew Barry, *Proceeding of the Eleventh Conference on Uncertainty in Artificial Intelligence*, Montreal, August 1995. This paper describes methods for managing the complexity of information displayed to people responsible for making high-stakes, time-critical decisions. The area of focus is time-critical applications at NASA's Mission Control Center during Space Shuttle flights.

[17] Pattie Maes, Massachusetts Institute of Technology Media Laboratory, "Agents that Reduce Work and Information Overload," Internet address: http://pattie.www.media.mit.edu/people/pattie/CACM-94/CACM-94.pl.html, 1 February 1996. This paper describes a new style human-computer interaction, where the computer becomes an intelligent, active and personalized collaborator using interface agents that employ artificial intelligence and learn from the user as well as other agents.

[18] Allen Sears and Robert Neches, Advanced Research Projects Agency, Information Technology Office, "Human Computer Interaction," Internet address: http://www.ito.arpa.mil/ResearchAreas/HCI.html, 10 April 1996. This program will support effective and efficient communication between human users and computer-based systems. A key focus is on interactive agents that focus the attention of the user and the software components on critical issues for specific tasks.

[19] Richard Axel, "Mammals Can Recognize Thousands of Odors, Some of Which Prompt Powerful Response," *Scientific American* 273, no. 4 (October 1995): 154–159.

[20] Advanced Research Projects Agency, "Computer Aided Education and Training," Internet address: http://www.ito.arpa.mil/ ResearchAreas/CAETI.html, 31 January 1996.

[21] ***2025*** Concept, No. 900667, "Real-time War Status Board," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

[22] ***2025*** Concept, No. 900385, "3-D Holographic Battlefield Display," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996); ***2025*** Concept, No. 900417, "Battlespace Awareness Holosphere," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996); ***2025*** Concept, No. 900206, "Commander's Universal [order of] Battle Display," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996); ***2025*** Concept, No. 900161, "Holographic C^2 Sandbox," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996); ***2025*** Concept, No. 900115, "Don't Blink," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

[23] *New World Vistas*, (unpublished draft, the information applications volume), 14.

[24] Ibid., 16; Kristin Leutwyler, "Calculating with DNA," *Scientific American* 273, no. 3 (September 1995):18.

[25] David A. Patterson, "Microprocessors in 2020," *Scientific American* 273, no. 3 (September 1995): 48.

[26] Pattie Maes, "Intelligent Software," *Scientific American* 273, no. 3 (September 1995): 66.

[27] *New World Vistas*, (unpublished draft, the information technology volume), 38–41.

[28] E. B. Baatz, "Making Brain Waves," *CIO*, 15 January 1996, 24.

[29] Lt Col Robert J. Wood, "Information Engineering: The Foundation of Information Warfare," research report (Maxwell AFB, Ala.: Air War College, April 1995), 39; John G. Kemeny and J. Laurie Snell, *Finite Markov Chains* (Princeton, N. J.: Van Nostrand, 1960), 24–25, 182–184.

[30] Bart Kosko, *Fuzzy Thinking* (New York: Hyperion, 1993), 222–235.

[31] Maj Glenn E. James, United States Air Force Phillips Laboratory, Edwards AFB, Calif., interviewed during visit to Air Command and Staff College, Maxwell AFB, Ala., 8 March 1996;

J. A. Dewar et al., "Non-Monotonicity, Chaos, and Combat Models," RAND Library Collection, Santa Monica, Calif.: RAND, 1991.

[32] Maj Glenn E. James, "Chaos Theory: The Essentials for Military Applications," in *Theater Air Campaign Studies*, (Maxwell AFB, Ala.: Air Command and Staff College, 1996): 38.

[33] Ibid., 45.

[34] *New World Vistas*, (unpublished draft, the human systems and biotechnology volume), Appendix M. Using EEGs to determine the state of the operator/user to determine workload and cognitive effort; *Airman Magazine* interview with Dr. Grant McMillan, Air Force Armstrong Laboratory, Internet address: http://www.dtic.mil/airforcelink/pa/airman/0296/look.htm, 10 February 1996. The article describes Dr. McMillan's use of EEGs to allow pilots to command a flight simulator to roll to the left or right by thinking about it.

[35] Daniel Magsig, "Information Warfare in the Information Age," Internet address: http://www.seas.gwu.edu/student/dmagsig/infowar.html, 7 February 1996, 7.

[36] "Public Networks Require Tailored Security Action, "*Signal*, March 1996, 23–26.

[37] *New World Vistas*, (unpublished draft, the information technology volume), 92; Gates, 109–110.

Chapter 4

Concept of Operations

The chapters on required capabilities and system description detail the Wisdom Warfare architecture. It is a collection of robust, highly interconnected, smart nodes providing information flow and advice tailored by each user. Nodes and the system learn from their experience and the experience of nodes used by people in analogous situations. These features make the architecture useful throughout the spectrum of conflict and in a variety of alternate futures.

Air power must prepare to face everything from peace to full-scale war in 2025. The Wisdom Warfare architecture helps achieve that broad capability. At the operational level, the architecture provides fully fused intelligence, coordinated logistics, and a variety of courses of action. At the tactical level, it can even provide instructions to technicians. The Wisdom Warfare architecture particularly helps staffs perform their roles in support of commanders.

Personnel staffs can track the status of each person involved in a battle through computers woven into each warrior's clothing.[1] This includes information on name, rank, unit, specialty, health status, and location. Commanders can see the information at any level of organization. In addition, staffs can communicate with troops to educate them on the mission and the cultures involved.

Intelligence staffs will conduct operations in a dramatically different way when compared to today. During peacetime, the system will collect global information and intelligence staffs will construct models to forecast COAs of potential enemies. Intelligence, surveillance, and reconnaissance data are fused with a variety of digitized maps, political factors, cultural guides, opinions from area experts, industrial data, current and forecasted weather, enemy doctrine, and objectives. As hostilities become imminent or erupt, the system will use intelligent software agents to get fused intelligence to the proper nodes that will minimize human delays during conflict. Each user will then use his forecasting and decision-making tools to turn knowledge into good decisions. Forecasting tools will also help determine where collection assets will find the most useful information so they collect data in the most efficient way.

Operations staffs also benefit from the architecture. Before conflicts, the architecture uses several models to determine the most likely enemy centers of gravity.[2] It allows operations staffs to run dozens of friendly COAs against the enemy. Plans can include a variety of force packages to respond to the scenarios. In evaluating the plans, the commander determines the criteria and weights. The architecture then evaluates the plans. For instance, criteria could include

- ability to achieve national objectives
- ability to achieve theater objectives
- contribution to a better state of peace
- casualties to our side
- casualties to the enemy
- estimate of collateral damage
- time to complete the campaign
- logistics feasibility
- cost

The architecture's speed will allow staffs to generate many more plans than today. This method means they can more easily pull a plan off the shelf that is analogous to a crisis when it erupts. All this helps guard against the chance of surprise and maximizes preparedness. However, air power planners should not forget the axiom of Helmuth von Moltke the elder: "No plan of operations survives the first collision with the main body of the enemy."[3]

When conflict erupts, the architecture also provides fast adjustment of existing plans. Its ability to rapidly develop a variety of new COAs will be useful. Once the plans are adjusted, the architecture can automatically issue orders to deploy force packages as directed by the commander. The orders can include situation briefs, cultural briefs, and logistics instructions. The Wisdom Warfare architecture's forecasting tools and decision-making aids help manage the large amounts of information flowing in the twenty-first century battlespace.

Logistics staffs will also benefit. Like the intelligence staffs, logistics planners will spend time before conflict in building forecasting and decision-making tools. As operations plans are developed, they will automatically be fed to the logistics staffs. The decision-making tools will then help them construct the best logistics plans. In addition, materiel status-like location and serviceability will be immediately available.

Once plans are made, they will be used by all warriors. The architecture enhances war fighting by putting forecasting and decision-making tools in the warriors' hands. However, it will be just as important to have full integration of the warrior with the system. For instance, every warrior could access information by smart glasses or contact lenses and control his equipment with advanced EEGs.

The architecture provides tools to enhance knowledge and wisdom at all levels. It is best developed in peacetime by honing its operation through feedback from exercises and day-to-day operations. This is how decision makers will build confidence in the system. The architecture also aids in training and military education.[4] This is not a system that will be born in 2025. It is a system that must grow to maturity by 2025.

The US military can use the Wisdom Warfare architecture in a variety of futures and in the entire spectrum of military operations. A short story in appendix C illustrates a scenario in a low-intensity conflict in 2025. It helps create a picture of what Wisdom Warfare can do in 2025.

Notes

[1] ***2025*** Concept, No. 900572, "Plastic Computing," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996); ***2025*** Concept, No. 900490, "Crewman's Data Vest," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996); Nicholas Negroponte, "Wearable Computing," *Wired*, December 1995, 256.

[2] See, for example, John Warden, "The Enemy as a System," *Strategic Studies Course Book*, vol. 2 (Maxwell AFB, Ala.: Air Command and Staff College, 1995), 437–452; Paul Moscarelli, "Operational Analysis: An Overview," in *Strategic Studies Course Book,* vol. 2, 522–530; Jason Barlow, "Strategic Paralysis: An Airpower Theory for the Present," in *Strategic Studies Course Book,* vol. 2, 453.

[3] Helmuth Graf von Moltke, *Moltke on the Art of War*, ed. Daniel J. Hughes, trans. Daniel J. Hughes and Harry Bell (Novato, Calif.: Presidio, 1993), viii.

[4] Kelley, 9.

Chapter 5

Investigation Recommendations

The architecture described in this paper cannot be for *air power* only. Realizing the goal of Wisdom Warfare requires the integration of all knowledge sources and core competencies of each service. In a word, it must be *joint*. The architecture must serve the needs of all service components and unified commands. It must be developed and fielded as one common system, providing knowledge and wisdom to the warrior across all levels of war and through the full spectrum of conflict. It must also permit easy integration of coalition or alliance partners, when necessary. This will obviously place a greater burden on the system's security feature, but it should also force reconsideration of the way information is classified and released to foreign military leaders.

The continuing revolution in information technology makes the capabilities described in this architecture possible. However, a revolution in military affairs is not complete until the new technology is applied in combination with new doctrine and organizational changes.[1] They are needed to achieve the synergistic effects of combining intelligence, surveillance, reconnaissance, weather, navigation, communications, and computers. They will also provide the proper environment to train and grow "info-warriors."

New doctrine and organization will have to overcome institutional biases and orchestrate the development of a common architecture across service, government, and commercial sector lines. The DOD must leverage the commercial market's lead in information technology development. The DOD will not need to invest substantial sums to achieve the desired capabilities as the US completes its transition to a Third Wave society.[2] This is not to say the DOD should passively accept whatever information technology the commercial market produces. Rather, the DOD should be an active participant in influencing the direction of certain information technology research and development.

Knowledge and Wisdom Recommendations

The exponential growth of communications and networking technology in the commercial sector will provide the military with cost-effective connectivity around the globe.[3] The military must invest in providing secure, reliable communications links between ground nodes and fast moving platforms. Lightweight, multibeam, broadband, phased-array antennas and small, low-power communications packages are two specific areas requiring further development.

Security must be integrated throughout the architecture. Cryptography and multilevel security operating software can provide high levels of security to individual systems; however, new techniques must be developed to ensure the survivability and assurance of the architecture itself.

New approaches in computing such as DNA-based and optical computing offer the potential of revolutionary advances in processing speed and parallelism.

Advances in storage capacity are required to manage the billions of bits flowing through the architecture. Emerging storage technologies such as holographic memories, vertical block line storage, and data warehousing offer possible alternatives.[4]

Fusion research is important in the infosphere. High-impact artificial intelligence applications require coordinated efforts of research and development across several areas of computer science. Building these systems will require combining AI methods with non-AI approaches and embedding AI technology within larger systems.[5]

DOD should research military applications of AI, intelligent software agents, neural networks, fuzzy cognitive maps, chaos theory, and Markov chains. Additionally, the DOD should concentrate on information technologies that encourage open systems, dual-use defense and commercial technologies, software advances which improve on object-oriented code, adaptive algorithms, pattern recognition, and automatic target recognition.

Human System Integration Recommendations

The technologies needed in the *human system integration* component will require the Air Force to focus research on areas unique to military missions while maximizing its leverage on the advances in the commercial world. Supporting technologies in this area are improvements to human sensory capabilities and technologies that improve the human cognitive capabilities. These technologies will allow the human and system to work with one another to maintain the best situational awareness possible. The Air Force must also pursue an effective training program for humans and systems to achieve good integration and provide the best environment for making decisions. Interactive and learning displays will be a key component of the information operations systems of 2025. To improve the ability of the decision makers to receive the information necessary to make decisions, the Air Force must continue to advance the capabilities of HSI technology.

Cost

The most cost-effective options will likely follow the advances in commercial development and application of technologies in computational, networking, and communications areas. The key technologies in the previous section fall into three general categories.[6] They are depicted in table 1.

The first category includes those technologies developed by the commercial world and not likely to need significant military investment. The second category consists of high-risk technologies with potentially greater long-term payoff but not worth military investment at this stage. The final category contains those with good payoff but which requires military investment at this time.

In addition, the armed forces will need to augment these areas where the military has unique requirements (i.e., multilevel security, high-data-rate encryption, anti-jam, and low probability of intercept communications).

Table 1

Technology Investment Opportunities

Commercial Development	High Risk	Military Investment Areas
• Neural networks • Massively parallel —processors • Superscalar processors • Pipelined processors • Holographic memory • Vertical block line storage • Advanced data —compression • Global fiber networks • High-capacity satellite —communications • Optical interconnects • Image mosaics • Holographic displays • Glasses as displays • Contact lenses as displays • Virtual reality • Software agents to sort, — filter, and distribute — information from a very — large number of sources • Evolving software to —automatically recode —itself to achieve user- —selected goals • Artificial intelligence to —provide predictive tools	• Photonic processors • DNA processors • Atomic level storage —devices • Displays that incorporate —all five human senses	• Military applications for — intelligent software agents • Military applications for — artificial intelligence

The topic of cost for an architecture that is as far-reaching as the one described in this paper is a daunting task even for the experienced cost estimator. The trends in technology improvements show the armed forces can leverage commercial technology for most areas and use scarce research and development dollars on those high-payoff areas that have unique military requirements. The trends are clear. The computational, communications, displays, and software technologies will provide the capability required and at costs that will be affordable for the armed forces.

An often-cited reference on the historic and predicted costs of computational power is Hans Morovec's book, *Mind Children: The Future of Robot and Human Intelligence*. This reference states computers capable of processing 10^{14} bits per second will "be available in a $10 million supercomputer before 2010 and in a $1,000 personal computer by 2030."[7] Even these astounding predictions are shown to be conservative when updated with recent computer advances. This supercomputer is almost a reality today and may be found in a personal computer early next century.[8] The computational power predicted to be available in 2025 will be sufficient to handle the needs of the architecture at extremely reasonable costs.

The advances in communication technology will also allow the architecture to be realized at reasonable costs. Fiber networks are growing exponentially. Over the last 15–20 years the carrying capacity of fiber networks has increased about 10,000 fold and is expected to continue to grow in the future.[9] Similarly, direct broadcast service (DBS) has grown tremendously. The current DBS systems can transmit greater than 64 trillion bits of information per day to large portions of the earth. The military has already recognized the benefits of DBS systems and is pursuing the placement of this technology on military communication satellites by the turn of the next century.

Due to competition and advances in technology, costs of information systems are coming down every year.[10] Besides these reductions, costs savings will be realized through transmission protocols like asynchronous transfer mode which allow users to be charged for only the portion of the communication link they use.

Current programs expect to develop military radios in the next four years that require 60 percent less power, are 3-5 times more capable, are one-third the physical size, and cost less than today's models.[11] Given the continuation of these improvements, it is expected that affordable methods to get needed information or to communicate to anyone will be available anywhere on the globe.[12]

Two other areas that may be cost drivers are display technology and intelligent software development. It is expected both of these areas will be pushed by effort from entertainment and commercial industries. In his book *Being Digital,* Nicholas Negroponte points out: "Games companies are driving display technology so hard that virtual reality will become a reality at very low cost."[13] This statement becomes self-evident when considering the following examples: in 1994 Nintendo announced the $199 virtual reality game called "Virtual Boy" and in 1995 Sony introduced the $200 "Playstation" that has 10 times the computational power of the fastest Intel processor.[14] It is safe to state the necessary display technologies will be available at reasonable costs in the year 2025.

Intelligent software and AI should benefit in a similar fashion. The recent advances in AI provide optimism for the future.[15] An example is a project at the Microelectronics and Computing Corporation where a commonsense knowledge base is being created for computers.[16] The large benefit of this type of system is once the core knowledge base is established it is believed the system can begin to assimilate information on its own—in the ultimate it could reach the point where the system will learn as fast as information is fed to it.[17] Efforts to digitize the Library of Congress have already begun.[18] One can imagine large parts of the library being digitized by 2025 and easily feeding this tremendous amount of information to a commonsense knowledge base at data rates of many trillions of bits per second. Costs will also be reduced through leveraging commercial improvements in systems that create information profiles and "put information at your fingertips."[19]

With an understanding of these advances it can be assumed technology advances in intelligent software will provide the capabilities required by the Wisdom Warfare architecture and will be available at reasonable costs.

Schedule

Given the focus on maximizing leverage of commercial systems, the next few paragraphs describe a three-phase schedule to reaching the Wisdom Warfare architecture.

Planning Phase (present to 2005). Phase I consists of three main tasks. The first task is the systems engineering development of the road map and blueprints for the open architecture that will support Wisdom Warfare. This task includes in the identification and development of the standards for the "open systems" which will allow the architecture to be flexible and capable of rapid change and growth,[20] identification of the unique military requirements that will not be met by commercial practices and ensuring their development does not limit use in the open systems architecture the identification of current and planned systems (military and commercial) that will evolve and migrate into the Wisdom Warfare architecture. This effort will be an extension and continuation of the current DOD and Intelligence Community Intelligence Systems Board migration study.[21]

The second task is the development of forecasting tools, which is expected to be a "long-pole" system.[22] This task also includes the development of the initial databases that will evolve into the learning databases the Wisdom Warfare architecture requires.

The third task involves determination of any organizational and attitude changes necessary for success. This is expected to involve a concerted effort at changing service and personal attitudes to allow the architecture to be effective. The personalities and organizational inertia existing today have already caused significant roadblocks to the achievement of an integrated architecture.[23] This task will also address the training requirements needed to successfully develop the human and system integration requirements for Wisdom Warfare, once review commercial industry lessons learned in the control of cost and the use of commercial software products.[24] The goal of this phase is to establish the foundation for the architecture and create the organizations and technologies that will carry out the road map and blueprints through the next two phases.

Phase II: Initial Ascent (2005 to 2015). The first task is the continued evolution of the prototype programs initiated in Phase I. The modeling and forecasting tools will be enhanced with advances in areas such as chaos theory, fuzzy cognitive maps, and AI. Taking advantage of a new understanding about the human decision-making process, the initial attempts at genius ghosting will be undertaken in this phase. The prototypes of advanced fusion systems will be evolved and continue to improve the timeliness and diversity of data fusing. The databases will continue to evolve and develop additional linkages. New display technologies will be integrated into the systems as holographic and virtual reality displays are improved and reduced in cost due to advances in electronic technologies and the personal entertainment fields.[25] This area will also be enhanced through the improved understanding of human cognitive skills to allow focus on the areas that require HSI.

Initial prototypes will be fielded. Peacetime logistics operations will most likely be the best place to start. Commercial development, such as global package delivery, is likely to continue here because of the advantages of the architecture and technologies. The armed forces can leverage this commercial development. The goal of this phase is to continue evolving the architecture and gain momentum to allow the third phase to carry the architecture to the Wisdom Warfare level.

Phase III: Final Ascent (2015–2025+). The first task of this phase is to complete the *knowledge* level of the architecture. This includes the evolution of the databases and fusion systems to provide the decision makers the ability to understand the information and intelligence that is available. During this phase several things will occur: the architecture will evolve to the point where it truly learns; procedures will be formalized; timelines for planning and execution will be reduced; and the core communications architecture will begin to solidify but will remain flexible for continued change and growth. With this accomplished, the decision makers can successfully employ the decision tools provided at the *wisdom* level of the architecture—the second task of this phase. The decision tools will mature and become part of the training and education system to allow an understanding of the systems, effective HSI, and improved decision-making processes. Once decision makers are comfortable with these tools and the actions and decisions the systems are making they will have achieved a Wisdom Warfare capability.

Is Wisdom Warfare possible in 2025? The answer is most certainly yes. The continuing revolution in information technology will make the capabilities described in this architecture possible. However, the leaders of today must commit to a common system that provides knowledge and wisdom across all levels of war and through the full spectrum of conflict. Such a system is affordable. By leveraging commercial advances in most technologies and using scarce military research and development dollars on others, the war fighters of the future can have the tools to conduct Wisdom Warfare.

Notes

[1] Jeffery McKitrick et al., "The Revolution in Military Affairs," in Barry R. Schneider and Lawrence E. Grinter, eds., *Battlefield of the Future: 21st Century Warfare Issues* (Maxwell AFB, Ala.: Air University Press, September 1995), 65.

[2] Alvin and Heidi Toffler, *War and Anti-War* (New York: Warner Books, Inc., 1993), 64–72.

[3] John L. Peterson, *The Road to 2015: Profiles of the Future* (Corte Madera, Calif.: Waite Group Press, 1994), 33–38.

[4] "Chip Architecture Removes Signal Processing Bottleneck," *Signal*, February 1996, 31; *SPACECAST 2020*, Surveillance and Reconnaissance Volume (Maxwell AFB, Ala.: Air University, 1994), 15; Andrew C. Braunberg, "Data Warehouses Migrate Toward World Wide Web," *Signal*, February 1996, 35.

[5] USAF Scientific Advisory Board, *New World Vistas: Air and Space Power for the 21st Century* (unpublished draft, the information technology volume, 15 December 1995), 65.

[6] Maj Gregg Gunsch, Air Force Institute of Technology, to Maj Charles Williamson, Air Command and Staff College student, electronic mail, subject: AFIT Assessment of Key Technologies, 22 March 1995.

[7] Hans Morovec, *Mind Children: The Future of Robot and Human Intelligence* (Cambridge, MA: Harvard University Press, 1988), 68.

[8] Sarnoff Research Center, "Exploiting the Consumer Digital Systems (CDS) Revolution," briefing to Lt Gen Jay Kelley, Air University commander, Maxwell AFB, Ala., 24 March, 1994.

[9] Peterson, 35-36; David Voss, "You Say You Want More Bandwidth?" *Wired*, July 1995, 64.

[10] Bill Gates, *The Road Ahead* (New York: Viking Penguin, 1995), 240.

[11] Air Force Rome Laboratory, *Speakeasy Program Briefing* (Internet address: http://woody.c2tc.rl.af. mil:8001/Technology/Demos/SPEAKEASY), March 1996.

[12] George Gilder, "Gilder Meets His Critics," Internet address: http://www.discovery.org/ critics.html, 29 March 1996, 1–13. This article is a portion of Mr Gilder's book *Telecosm* to be published by Simon & Schuster in 1996.

[13] Nicholas Negroponte, *Being Digital* (New York: Vintage Books, 1996), 83.

[14] Ibid.

[15] Edward A. Feigenbaum, chief scientist, US Air Force, "The Intelligent Use of Machine Intelligence," *Crosstalk*, August 1995, 10–13.

[16] Peterson, 41–43; Negroponte, 155–156.

[17] Douglas B. Lenat, "Artificial Intelligence," *Scientific American* 273, no. 3 (September 1995): 64; Peterson, 41–42.

[18] "Library of Congress Opens Digital Library Visitor Center," *Library Journal* 119, no. 19 (15 November, 1994): 21.

[19] Cable News Network, "CNN at Work," Internet address: http://www.intel.com/comm-net/ cnn_work/index.html, 14 February 1996.

[20] Negroponte, 47.

[21] "INTEL04: Integrate Intelligence Community Information Management Systems," Internet address: http://www.odci.gov/ic/npr/intel04.html, 10 April 1996.

[22] Gunsch electronic mail.

[23] Assessor's comment to Information Operations briefing, Air University, Maxwell AFB, Ala., February 1996.

[24] Salvatore Salamone, "Control Software Costs," *Byte*, April 1995, 75–82.

[25] David Pescovitz, "The Future of Holography," *Wired*, July 1995, 60.

Appendix A

Acronyms and Abbreviations

AI	artificial intelligence
BDA	battle damage assessment
C^2	command and control
COA	course of action
DBS	direct broadcast service
DNA	deoxyribonucleic acid
EEG	electroencephalograph
FCM	fuzzy cognitive map
GCCS	global command and control system
HSI	human system integration
HUMINT	human intelligence
IAT	information access technology
IMINT	imagery intelligence
ISA	intelligent software agent
MASINT	measure and signature intelligence
MOD/SIM	modeling and simulation
NCO	non-commissioned officer
NRT	Near Real Time
OODA	observe, orient, decide, and act
OAS	Organization of American States
PDA	personal digital assistant

SIGINT	signals intelligence
SURV	surveillance
UN	United Nations
US	United States
WMD	weapons of mass destruction

Glossary

Architecture: A framework or structure that portrays relationships among all the elements of the subject force, system, or activity.[1]

Battlespace: Area of concentration or concern; typically the workspace. Dependent on the scope of the individual's effort and level in the system hierarchy.

Command and control: The exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission.[2]

Information: Data and instructions.[3]

Information dominance: The state where one adversary possesses almost complete battlespace awareness, while the other adversary is cut off from almost all information sources.[4] Also information superiority.

Information operations: Any action involving the acquisition, transmission, storage, or transformation of information that enhances the employment of military operations.[5]

Information superiority: See information dominance.

Information system: The organized collection, processing, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual. In Information Warfare, this includes the entire infrastructure, organization, and components that collect, process, store, transmit, display, and disseminate information.[6]

Information warfare: Any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions.[7]

Knowledge: The fusion, correlation, and association of related intelligence information leading to understanding.

Offensive counterinformation: Actions against the adversary's information functions.[8]

Wisdom: Discernment based not only on factual knowledge but on judgment and insight.[9]

Notes

[1] Joint Publication 1-02, *DOD Dictionary of Military and Associated Terms*, 23 March 1994, 32.

[2] Joint Publication 1-02, 78.

[3] Department of the Air Force, *Cornerstones of Information Warfare*, 1995, Definitions.

[4] Stewart E. Johnson and Martin C. Libicki, *Dominant Battlespace Knowledge: The Winning Edge* (Washington, D.C.: National Defense University Press, 1995), 27-58.

[5] *Cornerstones*, Definitions.

[6] DoD Directive S-3600.1 [draft]

[7] *Cornerstones*, Definitions.

[8] Ibid.

[9] Philip B. Gove, editor in chief, *Webster's Third New International Dictionary, Unabridged* (Springfield, Massachusetts: Merriam-Webster, 1986), 2624.

Appendix B

Operation Swift Split

On the airplane again. Lt Gen Edward F. Barnes looked at his watch: 0900, 8 September 2025. "We'll be in the middle of the shooting in three hours," he thought. He looked up at the five-tense warriors sitting with him on the modified 797. He was glad to have them as his staff. Each one knew decisions were measured in someone else's blood.

General Barnes couldn't kick his old habit. Their computers knew what his computer knew, but habit made him tell them anyway: "Guyana and Surinam are at it again. Both countries have vacillated between democracy and military juntas since about 2010. Since then, they have argued over the hydropower of the New River.[1] You know the last border dispute ended only two years ago. Secretary of State Hillary Druary told me three days ago she had finished secret negotiations with the UN and OAS to prepare for armed intervention by the US if peace talks failed. Fighting broke out just over four hours ago. Each side has gained territory, and both countries have committed terrorist acts against civilians in Venezuela and Brazil. The situation could easily spin out of control. Our objectives are to separate the armies and reestablish peace based on the last agreement. Let's go to the board."

Col Frank Whorton was the personnel chief: "This is the first time we've used the automatic personnel status reports in a shooting match, but they're working well. The computer woven into each warrior's clothing gives us their name, rank, unit, specialty, health status, and location.[2] You can see the information split out or lumped together at any level of organization. In addition, a random poll of the troops and leaders has assessed morale, understanding of our mission, and understanding of the cultures we're facing."

General Barnes turned to Brig Gen Bill Hladek. "OK, -2, whacha got?" "Well, sir," General Hladek began, "the screen pretty much sums up the intelligence situation. First off, the computer's showing only a 2 percent probability of WMDs in either country. You know the system will almost never give a straight 100 percent or 0 percent answer because it forces us to take responsibility for decisions. My staff and I ran formal reviews of the intelligence synthesis system eight months ago and validated the four decision-making models listed on your screen. Per standard procedures, we've established links with every US embassy in Latin America, the State Department, OAS Headquarters, UN Headquarters, and professors from eight universities in the US and Latin America on contract as consultants. Their recommendations are starting to pour in. They got almost the same briefing as the one you and the National Security Council gave President Stonerock two hours ago. In addition, 14 journals on South American studies were scanned again and their information updated in our databases. Finally, we added 17 reconnaissance platforms to the three already over the area.[3] At this point, we have dispositions on approximately 86 percent of the enemy forces down there, and we expect a 97 percent disposition before our forces touch down. We've pinpointed their command posts down to the company level and located all their armor and mechanized forces. The system identified one hole we're trying to fill. We know your intel plan says you want to know where government leaders are, but we haven't found the Guyanan 'President-for-Life' yet."

Brig Gen Chip Borud was the joint task force operations officer. He spoke next: "Well, folks, here's the ops situation. We started planning three days ago. We set H-hour when the shooting started,, then implemented Joint Operations Plan 14.76 at H+3 after getting the OK from Secretary of Defense Warden. Mission shred-outs for each unit were briefed in mobility holding areas and on the airplanes while flying in. Culture briefings pointed out about 25 percent of the population is Hindu and about 20 percent is Muslim.[4] Cultural and religious taboos were briefed to help enhance legitimacy for peace enforcement after we stop the fighting. Dutch is the official language in Surinam,[5] so every warrior on the ground is wearing his universal language translator in his ear."[6]

General Borud's staff had tested the Wisdom Warrior Advisor System extensively. (The NCOs immediately called the system "the Wiz" and the name stuck.) While putting together the deliberate plan for this theater, General Borud had split his staff into two competing teams. The first team developed courses of action using the now-ancient Global Command and Control System (GCCS) and the second team developed plans using Wiz. Then they ran 400 simulations with the competing plans. For the first hours of the campaign, neither plan had an edge. However, after eight hours, the performance of the Wiz plans pulled way ahead by every measure. First off, Wiz's plans were superior. The plans included factors not considered by the GCCS team and Wiz's team achieved better economy of force. Secondly, information overload killed the GCCS team. The GCCS team discovered human memories and quickly developed gaps, especially under stress. Sometimes those gaps took a long time to fill, even when the whole team worked on them. By contrast, the team with Wiz developed about the same number of memory gaps but could fill them almost instantly just by asking Wiz. Wiz owed a lot to the GCCS concepts but finally put GCCS to rest.

In developing the crisis plan for this campaign, Borud and his team gave Wiz the campaign and national objectives. Then they told Wiz to design campaigns using the philosophies of many commanders and theorists. Sun Tzu in ancient China, Jomini and Clausewitz after Napoleon, MacArthur in World War I, Bradley and Halsey in World War II, Dayan in Israel's fight for Palestine, Giap in Vietnam, Horner in the Gulf War, and Wallman in the Big War of 2013.

Wiz pulled together the information in its databases and all the databases to which it was connected: digitized maps, political maps, cultural guides, industrial data, current weather and forecasts, enemy doctrine, enemy objectives, and the doctrines and capabilities of available US forces. Wiz then used several models to determine the most likely enemy centers of gravity.

Wiz determined the initial center of gravity for both countries was the King Edward VII Falls on the New River. It was the key to exploiting the hydropower potential in the area and was the objective of both countries. Wiz also pointed out our airborne and long-range air assault troops could seize the Falls faster than either Guyana or Surinam. Wiz reasoned that if we held both sides' reason for war, we could gain our initial objective to stop the fighting.

Wiz automatically ran simulations on the planned campaigns and evaluated them against the usual criteria: ability to achieve national objectives, contribution to a long-term better state of peace, casualties to our side, casualties to the enemy, estimate of collateral damage, time to complete the campaign, logistics feasibility, and cost.

General Barnes had given Borud the weights for each factor. Wiz determined Sun Tzu's style would work best overall. However, Wiz pointed out that emulating MacArthur's audacity in World War I would play well in the cultures of Guyana and Surinam and would be useful for establishing legitimacy of UN forces in enforcing the peace.

Borud told all this to Barnes and held his breath. Borud knew this was the point at which Barnes always proved why he was in charge. Barnes was a genius. He trusted Wiz. He appreciated using something much like it when he worked logistics on the joint staff in the Big War just 12 years ago. But Barnes knew no computer could replace him. Barnes could feel the battlefield. He could smell the enemy. Barnes could taste the battle. He knew only a human can run this most human of endeavors. He wanted Wiz's help but he knew the decision was his, and his alone. Barnes closed his eyes and thought silently for several minutes. Finally, he asked, "Roxanne, what about you?"

Col Roxanne Wyant, the J-4, stirred. "General, Wiz is working the logistics just fine. It already projected the minimum and maximum force sets for the most likely scenarios needed to meet the national objectives. It has incorporated the scenarios run by the J-3 and issued orders for the minimum force set to immediately move to staging areas in the theater. It also issued warning orders for units in the maximum force set. We'll send out execution orders to them if you give the word. Wiz alerted our primary suppliers and our "just-in-time" resupply will start flowing this afternoon. Since logistics feasibility was a grading criteria for the ops planning, we have no limiting factors due to logistics in any of the plans in front of you."

General Barnes grunted. It was all being done in accordance with the standard procedures he had issued, but it was still a surprise when the computer thought two steps ahead of him, even when he had told it what steps to take.

The meeting had taken 15 minutes. He needed a cup of coffee and a few minutes to think alone, so he excused the staff. He looked at the holographic battlespace picture on his desk and zoomed in on the King Edward VII Falls. General Barnes knew that every captain in the 82d Airborne could see the same thing through the contact lenses each one wore.[7] "But what do I want those great captains to do?" Barnes paced back and forth in the small cabin. After five minutes, he called the staff in, then called the secretary of defense and the president. "Mr. President, this is what we should do..."

By H+5 hours, the plane carrying Capt "Acid" Raines' airborne company was loitering over the Caribbean along with the six other C-18s carrying the minimum force set. At H+6 hours, everyone there heard and saw President Stonerock give his objectives. Next, General Barnes appeared and briefed his intent and the outline of the campaign plan. The contact lens displays were so vivid, Captain Raines almost came to attention. Five minutes later, the brigade commander appeared and told Captain Raines to secure the northwest side of the top of the King Edward VII Falls. Raines' Raiders had a mission.

Captain Raines asked Wiz for enemy dispositions and estimated arrival times at the falls. He then zoomed in his country display on the falls and asked Wiz for the best drop zone locations. Wiz told Raines to clarify his meaning of "best." After Raines gave Wiz the criteria, Wiz gave Raines a choice. He could land his company together in a clearing on the southeast side of the falls and take boats across to the northwest side. Wiz said this gave him a 90 percent probability he could have his whole company in place one hour before the time Wiz estimated the enemy would arrive. On the other hand, Raines could jump his company into a small drop zone on the northwest side, closer to his final position, but with multiple aircraft passes. That meant he could have men in place three hours before the enemy got there but Wiz said there was a 40 percent chance he would lose 15 men in the hazardous drop into the jungle. Raines would rather have less time to dig in together than have more time with some men dead. He picked the clear zone across the river.

Raines had his platoon sergeants look at the plans. No one suggested changes so Raines sent them to the brigade commander. Wiz noted another company was dropping at the same place so the brigade commander gave Raines priority. Wiz passed the word to both company commanders and used its airspace management routines to vector the transport planes.[8] It would take an hour to fly to the drop zone. Raines decided some practice would help so he had Wiz display the drop, river crossing, and platoon maneuvers in double real time on each man's display, then turned the men over to the platoon sergeants. At H+7 hours, Raines' Raiders started their drop.

It took six days. It really took only four days to separate the armies but it took two more days to convince the Guyanan "President-for-life" to join the peace talks. They fulfilled the prophecy: faster operations mean more effectiveness.[9]

Notes

[1] Central Intelligence Agency, *The World Factbook 1995*, 399.

[2] ***2025*** Concept, No. 900572, "Plastic Computing," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996); ***2025*** Concept, No. 900490, "Crewman's Data Vest," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

[3] ***2025*** Concept, No. 900552, "On-demand Tactical Recce Satellite Constellation," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

[4] Central Intelligence Agency, 399.

[5] Ibid.

[6] ***2025*** Concept, No. 900340, "Universal Language Translator," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

[7] ***2025*** Concept, No. 900263, "The All Seeing Warrior," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

[8] ***2025*** Concept, No. 900526, "Space-Based Airspace Control & Deconfliction System," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

[9] USAF Scientific Advisory Board, *New World Vistas: Air and Space Power for the 21st Century,* summary volume (Washington, D.C.: USAF Scientific Advisory Board, 15 December 1995), 6.

Credits

1. Illustrations of Clausewitz, Sun Tzu, and Napoleon in figure 3-3 courtesy of Daniel M. Armstrong, L. Susan Fair, and Steven C. Garst, artists at Air University Press, Maxwell Air Force Base, Alabama.
2. Globe graphic in figure 3-2 courtesy of Maj Larry Adair, USAF, student at Air Command and Staff College, Maxwell Air Force Base, Alabama.
3. Holographic battlespace in figure 3-7 courtesy of Air Force Institute of Technology.
4. Figures 1-0, 2-3, 3-4, and 3-6 contain clipart from Microsoft Clipart Gallery © 1995 with courtesy from Microsoft Corp.
5. Figure 3-5 contains clipart from Federal Clip Art © 95 with courtesy from One Mile Up, Inc.

Bibliography

2025 Concept Database Maxwell AFB, Ala.: Air War College/***2025***, 1996.

Advanced Research Projects Agency. "Computer Aided Education and Training." Internet address: http://www.ito.arpa.mil/ResearchAreas /CAETI.html, 31 January 1996.

Air Force Rome Laboratory. "Speakeasy Program Briefing." Internet address: http:// woody.c2tc. rl.af.mil:8001/Technology /Demos/SPEAKEASY, March 1996.

Axel, Richard. "Mammals Can Recognize Thousands of Odors, Some of Which Prompt Powerful Response." *Scientific American* 273, no. 4, October 1995.

Baatz, E. B. "Making Brain Waves." *CIO*, 15 January 1996.

Barlow, Jason. "Strategic Paralysis: An Airpower Theory for the Present." *Strategic Studies Course Book* 2 Maxwell AFB, Ala.: Air Command and Staff College, 1995.

Braunberg, Andrew C. "Data Warehouses Migrate Toward World Wide Web." *Signal*, February 1996.

Cable News Network. "CNN at Work." Internet address: http://www.intel.com/comm-net/cnn_ work/index.html, 14 February 1996.

Central Intelligence Agency. *The World Factbook 1995*.

The Chicago Manual of Style. 14th ed. Chicago: The University of Chicago Press, 1993.

"Chip Architecture Removes Signal Processing Bottleneck." *Signal*, February 1996.

College of Aerospace Doctrine, Research, and Education. *AU Press Author Guide*. Maxwell AFB, Ala.: Air University Press, March 1995.

AU Press Style Guide for Writers & Editors. Maxwell AFB, Ala.: Air University Press, December 1994.

Compton's Interactive Encyclopedia, 1994 ed., s.v. "human brain."

Department of the Air Force. *Air Force Executive Guidance*. December 1995.

_____. *Cornerstones of Information Warfare*. 1995.

Department of the Army. *Force XXI*. 15 January 1995.

Dewar, J. A., et al. "Non-Monotonicity, Chaos, and Combat Models." RAND Library Collection, Santa Monica, Calif.: RAND 1991.

DOD Directive S-3600.1 [draft].

Dunleavy, Maj Kevin N., and Maj Lester C. Ferguson. "Command and Control and the Doctrinal Basis of the Theater Air Control System." *Concepts in Airpower for the Campaign Planner*, Maxwell AFB, Ala.: Air University Press, 1993.

Feigenbaum, Edward A. Chief Scientist, US Air Force, "The Intelligent Use of Machine Intelligence." *Crosstalk*, August 1995.

Gates, Bill. *The Road Ahead.* New York: Viking Penguin, 1995.

Gilder, George. "Gilder Meets His Critics." Internet address: http://www.discovery.org/critics.html, 29 March 1996.

Gove, Phillip B., editor in chief. *Webster's Third New International Dictionary, Unabridged.* Springfield, Mass.: Merriam-Webster, 1986.

Gunsch, Maj Gregg, Air Force Institute of Technology. Electronic mail to Maj Charles Williamson, Air Command and Staff College student. Subject: "AFIT Assessment of Key Technologies." (22 March 1995).

Horvitz, Eric, and Matthew Barry. Proceeding of the Eleventh Conference on Uncertainty in Artificial Intelligence, Montreal, August 1995.

Hutcherson, Lt Col Norman B. *Command and Control Warfare*. Maxwell AFB, Ala.: Air University Press, September 1994.

"INTEL04: Integrate Intelligence Community Information Management Systems." Internet address: http://www.odci.gov/ic/npr/intel04.html, 10 April 1996.

James, Maj Glenn E. "Chaos Theory: The Essentials for Military Applications." *Theater Air Campaign Studies Coursebook.* Maxwell AFB, Ala., Air Command and Staff College, 1996.

Johnson, Stewart E., and Martin C. Libicki. *Dominant Battlespace Knowledge: The Winning Edge*. Washington, D. C.: National Defense University Press, 1995.

Joint Publication 1-02. *DOD Dictionary of Military and Associated Terms*, 23 March 1994.

Kelley, Lt Gen Jay W. "Brilliant Warrior." Unpublished paper, March 1996.

Kosko, Bart. *Fuzzy Thinking.* New York: Hyperion, 1993.

Lenat, Douglas B. "Artificial Intelligence." *Scientific American* 273, no. 3 (September 1995).

Leutwyler, Kristin. "Calculating with DNA." *Scientific American*, 273, no. 3 (September 1995).

"Library of Congress Opens Digital Library Visitor Center." *Library Journal* 119, no. 19 (15 November 1994).

Maes, Pattie. "Intelligent Software." *Scientific American* 273, no. 3 (September 1995).

———. Massachusetts Institute of Technology Media Laboratory. "Agents that Reduce Work and Information Overload." Internet address: http://pattie.www.media.mit.edu/people/pattie/CACM-94, 1 February 1996.

Magsig, Daniel. "Information Warfare in the Information Age." Internet address: http://www.seas. gwu.edu/student/dmagsig/infowar.html, 7 February 1996.

McKenna, Pat, TSgt. "Researchers harness brain power to control jets." Internet address: http://www.dtic.mil/airforcelink/pa/airman/0296/look.htm, 10 February 1996.

McKitrick, Jeffery. "The Revolution in Military Affairs," in Barry R. Schneider and Lawrence E. Grinter, eds. *Battlefield of the Future: 21st Century Warfare Issues.* Maxwell AFB, Ala.: Air University Press, September 1995.

Moltke, Helmuth Graf von. *Moltke on the Art of War,* ed. Daniel J. Hughes, trans. Daniel J. Hughes and Harry Bell. Novato, Calif.: Presidio, 1993.

Morovec, Hans. *Mind Children: The Future of Robot and Human Intelligence.* Cambridge, Mass.:, Harvard University Press, 1988.

Moscarelli, Paul. "Operational Analysis: An Overview." *Strategic Studies Course Book* 2. Maxwell AFB, Ala.:, Air Command and Staff College, 1995.

Negroponte, Nicholas. *Being Digital.* New York: Vintage Books, 1996.

Nicholas Negroponte. "Affective Computing." *Wired*, April 1996.

Patterson, David A. "Microprocessors in 2020." *Scientific American* 273, no. 3 (September 1995).

Pescovitz, David. "The Future of Holography." *Wired*, July 1995.

Pierce, J. R. and J. E. Karlin. "Reading Rates and the Information Rate of a Human Channel." Convention Record, IEEE WESCON, 1957.

"Public Networks Require Tailored Security Action. *Signal*, March 1996.

Salamone, Salvatore. "Control Software Costs." *Byte,* April 1995.

Sarnoff Research Center. "Exploiting the Consumer Digital Systems (CDS) Revolution." Briefing to Lt Gen Jay W. Kelley, Air University commander, Maxwell AFB, Ala., 24 March 1994.

Schwartau, Winn. *Information Warfare*. New York: Thunder's Mouth Press, 1994.

Sears, Allen, and Robert Neches, Advanced Research Projects Agency, Information Technology Office. "Human Computer Interaction." Internet address: http://www.ito.arpa.mil/ResearchAreas/HCI.html, 10 April 1996.

Spacecast 2020. "Surveillance and Reconnaissance." Maxwell AFB, Ala.: Air University, 1994.

Sun Tzu. *The Art of War*. Translated by Samuel B. Griffith. London: Oxford University Press, 1971.

Toffler, Alvin and Heidi. *War and Anti-War*. New York: Warner Books, Inc., 1993.

USAF Scientific Advisory Board. *New World Vistas: Air and Space Power for the 21st Century*. Unpublished draft, the Human Systems and Biotechnology Volume. 15 December 1995.

———. *New World Vistas: Air and Space Power for the 21st Century*. Unpublished draft, the Information Applications Volume. 15 December 1995.

———. *New World Vistas: Air and Space Power for the 21st Century*. Unpublished draft, the Information Technology Volume. 15 December 1995.

———. *New World Vistas: Air and Space Power for the 21st Century*, Summary Volume. Washington, D.C.: USAF Scientific Advisory Board, 15 December 1995.

Voss, David. "You Say You Want More Bandwidth?" *Wired*, July 1995.

Warden, John. "The Enemy as a System." *Strategic Studies Course Book* 2. Maxwell AFB, Ala., Air Command and Staff College, 1995.

Wood, Lt Col Robert J. "Information Engineering: The Foundation of Information Warfare." Research Report, Maxwell AFB, Ala.: Air War College, April 1995.