

**NEW WORLD VISTAS**  
**AIR AND SPACE POWER FOR THE**  
**21ST CENTURY**

*INFORMATION APPLICATIONS VOLUME*

*This report is a forecast of a potential future for the Air Force. This forecast does not necessarily imply future officially sanctioned programs, planning or policy.*

# Executive Summary

## Air Force Information Applications in the 21st Century

**Dr. Charles L. Morefield**

Chairman, Information Applications Panel

USAF Scientific Advisory Board

New World Vistas Study

Victory in war goes to those forces with the most accurate *knowledge*, strongest *protection*, most robust *communication*, best *coordination*, *dominant* force structure, and most *dynamic* operations. In the thoughts that follow, we expand upon these facets of military power by describing information applications<sup>1</sup> that will be important to the Air Force in the years to come. This short summary introduces accompanying monographs written by individual members of the panel. Our monographs contain comments and recommendations that speak to each of the following goals for 21st century aerospace power:

- Get the right *knowledge*, to the right place, at the right time for all aerospace missions
- *Protect* all Air Force computers, software, and data, regardless of platform or location, particularly those involved in warfighting
- Achieve global *communication* between the air, ground, and space assets of the Air Force, as well as those with whom we operate
- Maximize the speed and quality of Air Force *coordination*, planning, and execution
- *Dominate* the information battlespace
- Develop doctrine needed for the use of information in *dynamic* command and control of joint forces

This introductory monograph also provides some comments on information science in the Air Force laboratory system.

### Future War

The US Air Force, a young service, is about to experience its first paradigm shift. The arrival of the information age means that the Air Force has entered a period of great change, one that mirrors the social and economic ferment of the world around it. The causes of this change are rapidly expanding communications bandwidth and computational power, the foremost engines of economic and military competition in the decades to come. Airpower was the deciding factor in the shockingly one-sided United States victory in the Persian Gulf. However, the emerging information age requires new strategies, tasks, and technologies for exercising military power.

---

1. The reader is also referred to the work of the Information Technology Panel for a discussion of technical trends and research issues in the information sciences.

Beginning in 1940, and extending to the fall of the Berlin Wall, powerful currents of military competition drove the technologies most important for today's Air Force. At the edge of the millennium, the equally powerful engines of economic competition are hard at work. They carry us toward a future of ubiquitous computing embedded in a dense global communication grid, technology that will transform the Air Force (see Figure 1).

It appears now that nanofabrication technology will permit computer designers to maintain their hectic pace of greater capability, smaller size, and lower cost. Because of this, computers will disappear into the fabric of everyday life. We will wear computational devices like clothing, glasses and hearing aids. We will soon speak and gesture to them in natural ways, encouraging military reliance upon them to significantly increase. Huge commonsense databases linked to reasoning engines will provide ubiquitous intellectual assistance and entertainment in everyday life. Distributed knowledgebases linked to mobile reasoning engines will dramatically improve the ability of the battlefield team to obtain information, collaborate, and act.

Fiber grids will soon connect all the world's cities, and orbiting cellular overlays may even sooner provide universal access. The information applications inhabiting these global nets will change the economic and social structure of the world. How the Air Force responds to this change will determine its future as a viable military service.

If the Air Force adopts a path that unites aerospace with the infosphere, it will provide the United States with immense new leverage in the world. These two domains share an important characteristic: presence and influence are focused very rapidly on a global scale. An information-based Air Force will retain for the United States its position as the premier global military power into the 21st century.

The Air Force will reengineer its sensors, platforms, weapons, and command centers around the use of new information technologies. Most businesses and elements of the defense establishment are moving in this direction, making it possible to share the development burden of the effort. By

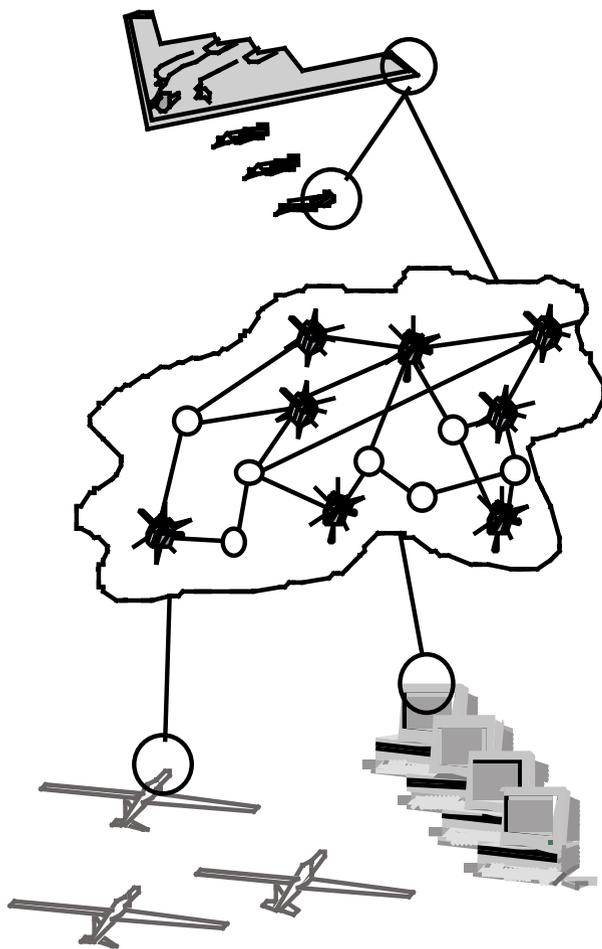


Figure 1. Telecommunications and computer technology will transform the Air Force

2025 (the notional end of this monograph), even the smallest artifacts of everyday life and cheapest weapons can have powerful embedded computers and sensors. The integration of such weapons, and the wide scale adoption of trusted automatic systems for information fusion and coordination, will change the face and pace of warfare.

## Information Warfare<sup>2</sup>

Today's computer systems are a limited and sometimes frustrating portal into a patchwork of databases of varying integrity. In the 21st century, the infosphere will evolve into a much more powerful and useful information utility. As computers emerge that respond coherently to speech and gestures, the infosphere will become a pervasive tool of everyday life. It will become a meeting place for teleconferences, real time global situation assessment, automated decision support, and for management of the global battlespace. The infosphere will encourage new relationships:

- Pseudo-intelligent agents will interact in complex ways with human beings and with each other
- Manned aircraft will interact with smart weapons, smart sensors, smart spacecraft, and smart unmanned aircraft, as well as command and fusion centers
- Commercial knowledgebases for weather, intelligence, and surveillance information will become available within the infosphere
- Military users will come to rely ever more extensively on the global grid, commercial information providers, and commercial information technologies

For these reasons, *information warfare* will radically alter the tasks associated with putting energy on targets. Early in the next century, however, information warfare will also take place *within* the infosphere. Such warfare will extend beyond the military domain, and will couple to it in ways that we cannot now predict. Computer networks will tie the economies of the world together in critical ways. This will present attractive opportunities for competing global interests to develop automated information fusion and planning systems for both military and commercial purposes. The leading edge of this pattern is visible now as electronic trading of financial instruments, the commercial use of GPS, and automated transportation and tracking systems.

The degree to which the Air Force develops the professional expertise to engage in national policy debates, allocates research and development expenditures, and encourages a military doctrinal evolution will determine its future. Information objects contained solely within the infosphere will become as important as real objects in the 21st century. Digital cash, a powerful target recognition algorithm, a predicted drop in the S&P 500, or the current position of a military leader may only exist as objects in some computer's memory. However, they would be knowledge of great commercial and military importance.

---

2. We use the term *information warfare* in the following way: protecting and using to best advantage our own information operations, while attacking and exploiting opposing information systems. In this definition, information warfare includes command and control, surveillance, electronic warfare, protection, and other technical information operations. The term is also applicable to the protection of national and global infrastructure, including networks for electric power, telecommunication, finance, and transportation.

We require a clearer understanding of how software munitions will affect future wars. A rapidly increasing population of valuable information objects requires the United States to develop the tools to protect its commercial and military information systems. We should prepare ourselves for sophisticated software weapons operating solely within the infosphere, directed against our economic, social, and military institutions. The Air Force should prepare itself through its research programs for a key role in dealing with protection issues. Since it is first a military service, it must also have the means to respond to attack in a destructive way (or at least pose the threat of destruction).

Mutual assured disruption (MAD) within the infosphere will become a key point of policy debate. Because of the increased integration of the world economy, and the complexity of its information linkages, side effects of war within the information domain will be unpredictable. Even “restricted” attacks against one part of the infosphere may lead to unpredictable collateral disruption of money flows, transportation links, or other facets of 21st century life.

The doctrine of “mutual assured destruction” became a strategic cornerstone of the Cold War. Similarly, the fragility and importance of the world’s information infrastructure can lead to an equivalent doctrinal impasse. Such a policy event would not diminish the importance of information to other parts of warfare, nor would it relieve us from the need to protect our vital systems. Small interest groups (below the level of nation-states) may choose not to subscribe to MAD. Since information technology is universally available, such groups may use sophisticated software munitions as threats.

We must develop new defense policies that clarify our response to digital events. The dividing line between economic espionage and attacks against our homeland will begin to blur. Taking down a regional power grid by software attack, with its attendant loss of life, is clearly an act of war. Would it be an act of war to destroy the digital financial or technical records of critical semiconductor companies? How can we respond (particularly if we are unable to unambiguously determine the bad actors)?

## **The Revolution in Military Aerospace**

Dealing with information warfare in a fundamental way will cause a profound cultural shift in the Air Force. This shift will begin in earnest over the next decade, and may be wrenching for those imbued with the cultural heritage of manned aircraft. It will come at a time of increasing use of unmanned aerospace vehicles, widespread interest in information warfare issues, and changing roles and missions among the services and agencies of the United States defense establishment. We must integrate aerospace military strategy with the information rich techniques that will dominate future battlefields. We should extend our functional capabilities in situation assessment, battle management and simulation to encompass objects within the information battlespace.

To respond to these changes, the Air Force must expand its traditional role as the leading proponent of airpower to include the infosphere. To the extent the Air Force can effectively unite aerospace power with information based power (networking, sensors, fusion, coordination, protection and other capabilities), it will remain a dominant factor in the defense of our nation. We should establish carefully thought out goals, goals responsive to the evolution of technology

and other commercial and government institutions. We must carry out difficult comparisons among the competing requirements for manned aircraft, space, and the informational components of force structure.

## **Issues Affecting Air Force Battlefield Information Applications**

Military designers increasingly focus on *minimizing* the detection of friendly platforms, while *maximizing* the detection of enemy targets. Ever increasing volumes of multi-source global surveillance data from unmanned aircraft, ground and sea sensors, national, and open commercial sources are available to support the detection function. Since human processing of this magnitude is not possible, the Air Force will need to replace manual information processing with intelligent automation. As a corollary, the high processing load will require the Air Force to use network-based, scaleable computing resources to accomplish fusion.

Among larger nations, aerospace warfare will eventually be dominated by forces possessing the best:

- Stealthy air, ground, and space delivery systems able to prosecute maneuvering and non-maneuvering targets
- Ability to detect and suppress air defense systems, cruise missiles, ballistic missiles, satellite attack, and digital attack
- Ability to attack important ground facilities mixed in with civilian populations, and obscured by camouflage and movement
- Ability to fuse a diverse mix of sensors
- Ability to rapidly coordinate complex missions involving precision attack
- Ability to protect its information assets, while attacking those of its opponents

In a short time every nation (and small interest group) will have access to:

- Orbiting wireless communication switches integrated with the global fiber grid
- Commercial satellite surveillance and navigation
- Public networks of increasingly powerful computers and sophisticated software
- Commercial multimedia knowledgebases

Both micro wars and major regional contingencies have become information intensive conflicts. As a corollary, warfare will emerge *within* the information domain driven by the proliferation of computer technology, low cost of entry, and large numbers of attractive military and civilian targets. Even small interest groups can develop the systems integration skills required to build niche military capabilities. Feasible specialties include information systems, wide area weapons, ground-to-air missile systems, cruise missiles, and unmanned aircraft. They will become adept users of the global telecommunications grid, commercial navigation and surveillance satellites, open source knowledgebases, computers and software, commercially available surveillance components, and exported weapons.

Low cost of entry will encourage the emergence of one or more small nations focused on information warfare. They will carefully shape their legal systems to support this activity. Even small interest groups will find this attractive, given the available cheap infrastructure (for example, satellite data services, global fiber grid, cheap computers, ready availability of highly trained computer scientists). Because of this, others will replicate key parts of the US military advantage.

Within our own military and economic spheres, other changes are taking place. These include integration of our national/airborne/commercial surveillance resources, the emergence of a civilian space surveillance industry, and the increasing reliance of the US military on internationally produced electronics components.

## **Current Air Force Communications**

The Air Force currently organizes its airborne data links around three paradigms:

- Tactical links: local area multiple user networks, and modems attached to low bandwidth point-to-point voice channels
- Dissemination links: low bandwidth wide area data broadcasts
- Collection links: higher bandwidth point-to-point linkages

Current airborne data links have thin, inflexible airborne service layers<sup>3</sup> focused on encrypted and anti-jam connections. This puts the responsibility on users to provide custom solutions for their needs, and does not provide scaleable bandwidth, user driven network management, or other services. Wide band fiber and satellite links provide near-term ground connections to bitways.

Service layers for ground nodes (and some wide-body aircraft) are beginning to mirror commercial standards. Important strides are being made in adapting commercial open standards to workstation-based applications. New airborne systems represent our first opportunities for airborne open software standards in embedded systems.

Air Force airborne tactical data links have historically been constrained by cost and lack of clear doctrinal necessity. The near future is being largely determined by:

- An Air Force decision to equip many fighters with voice radio modems
- The Air Force experience at Mountain Home Air Force Base, Idaho (and DoD mandates) supporting a standard local area data network for aircraft and other mobile platforms
- Emergence of air warfare doctrine supporting real time information flows into the cockpit, supported by experimental trials of onboard information systems
- DoD interest in wide area data broadcast systems

The bitways connecting ground based systems derive in part from Cold War legacy systems, but are rapidly being supplanted by the commercial global grid and the evolution of government furnished infrastructure. The service layers for ground based systems are a mix of new commercial

---

3. *Service layers* consist of software that provides a standardized means of managing the raw bandwidth provided by a data link.

and custom legacy systems. There is rapid movement toward commercial open system standards, and toward use of commercial network services within a military context.

## **Current Information Applications**

Current military information applications are custom designed for each platform and mission. Legacy hardware substrates are increasingly replaced by workstations or powerful embedded commercial microprocessors. There is little direct coordination of information applications among participating computers and functions. However, merger of information applications across individual programs and missions is beginning to rationalize the overlap among legacy applications (for example, mission support systems for pilots). Fusion systems are hand-tooled and have low levels of automation. Coordination systems are large and unnecessarily complex.

Substantial research has been focused on automated fusion and planning systems, but successful fielded applications are still largely manual. Current automated systems (e.g., for model-based target recognition and multitarget tracking) are fragile devices that will require substantial research investments before trusted implementations become available.

Current and near future Air Force and DoD ground-based information applications are evolving through the merger of numerous legacy command, control and intelligence systems. This will leave in place large, complex analyst-intensive approaches to both fusion and coordination. It will also let stand a confused information architecture.

Lacking integrated bitways, service layers, or integrated applications architectures, today's information applications are isolated, platform centered designs. Even the newest Air Force platforms accept this approach.

## **A Long Term Vision for Air Force Information Applications**

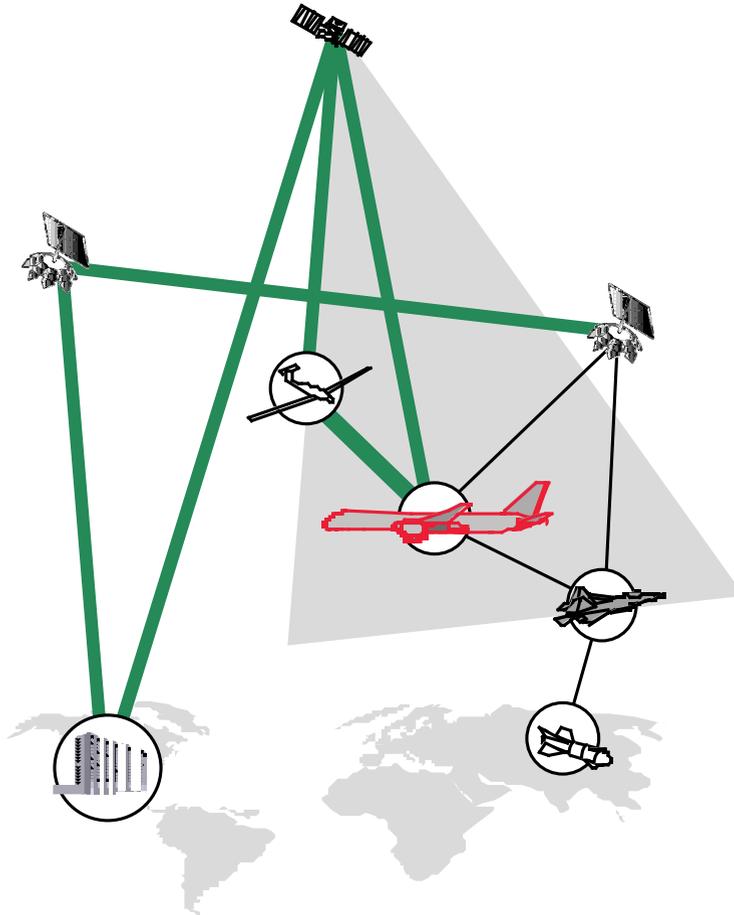
Given this background, what is the appropriate direction for aerospace information applications? The issues split into several parts:

- What are the doctrinal imperatives the applications should serve?
- What communication designs are affordable?
- What protective services are feasible?
- What information applications should operate across the system?

The Air Force has yet to accomplish a careful long term look at the impact that extensive reengineering of its information systems will have on air warfare doctrine. The primary areas now discussed are wide area broadcast and air campaign management. The issues go deeper. For example, will the Air Force need planning and battle management assets in the theater of operations? (Data links could substitute for on-site presence.) How are all assets (aircraft, spacecraft, sensors, communication links, joint and allied resources) managed? (Integrated and joint warfare imply some loss of autonomy.) How quickly can the Air Force employ its tactical air power? Should command and control follow a horizontal model? (It could, when global nets become available.)

The communication pathways of the future Air Force should include a netted airborne information system that supports a wide range of military tasks, available on a global basis for any task or mission. Figure 2 illustrates some of the physical bitways of such systems. Numerous data channels could be available in this network, including:

- Globally available broadcast channels (a wideband satellite downlink with many available channels)
- Globally available two-way data channels (multiple access wireless connections to a worldwide digital network)



Wideband broadcast links are under consideration in a number of government activities, and used daily in commercial digital television broadcasts. This type of channel could provide a “push” or “knowledge by design” or “immediate warning and control” type of link. Replaying constantly the current situation updates, it would provide the ability for a weapons controller to immediately reach an aircraft that is controlling emissions. (In many cases, military aircraft may not want to transmit, yet still receive some type of knowledge flow into the cockpit.) It would, for example, give a controller or other source of critical information the ability to warn a pilot of an impending surface-to-air missile attack. Pilots would adjust their pre-flight filters with access keys to select channels corresponding to their needs.

Figure 2. Future data links between aerospace platforms

Two-way data links to aircraft in flight are harder to develop than the broadcast link discussed above. A flexible, globally available multiple access two-way data channel should be able to do many things. For example, a weapons controller at Langley Air Force Base could open a data link to an aircraft in flight anywhere in the world. The controller could (for example) see a replication of the cockpit instruments, stores, and the onboard situation displays. The

channel would provide a digital connection to any aerospace platform (satellite, aircraft, ground center) maintained in real time between two or more points around the globe. This would provide a “pull” or “collaborative” or “knowledge on demand” type of link. Links of this type, if global, would require some combination of satellite and unmanned air vehicle transponders. An unprotected commercial version of this system will be available for Air Force use if currently proposed satellite systems are built.

The communication pathways will have a layer that includes protection and other services. The communication links will be wrapped in protective walls of software and monitored by software warriors that police the fabric of the net. As part of the service layer, software agents<sup>4</sup> could talk to one another in a coordinated fashion. Software facilitators between the pilot and information agents will manage the flow of knowledge to cockpit displays, thereby avoiding information overload.

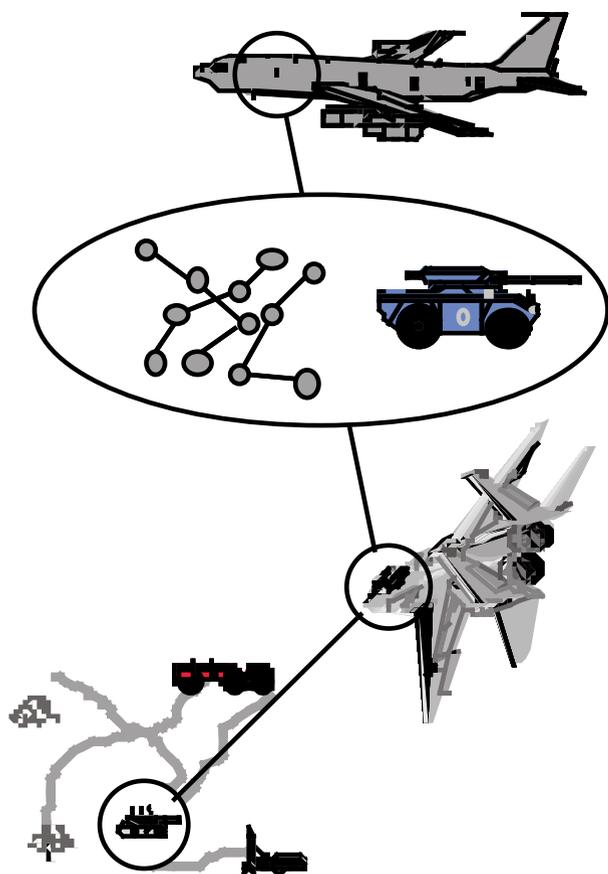


Figure 3. Distributed data fusion

Embedded within the net will be facilities that present a rich and accurate picture of the world. These will be drawn from a global array of sensors, many carried on aerospace platforms. Automated fusion will distill this overwhelming flow of data into a meaningful collection of information. The system will include many automatic fusion engines, distributed to many locations across the net (see Figure 3).

Since speed will be of the essence in future wars, automated coordination assistance will be required. The goal should be an information driven Air Force that relies upon global situation awareness to plan and execute complex missions quickly and accurately, with minimum danger to its personnel.

## The Air Force Research Laboratories

Parts of the research and development goals listed above are already being pursued within numerous research groups, including the laboratories of the US Air Force. How well equipped are these USAF research groups to achieve our suggested long term goals?

4. See the Information Technology Panel’s monograph for a discussion of software agents.

The last few years have seen the fracturing, consolidation, and down-sizing of some of the key research institutions supporting the US military. The Air Force laboratory system has not been exempt from this. Continued down-sizing is inevitable. It is mirrored by a similar trend in allied private research institutions, as their historic business models are called into question by their sponsors. In addition, the major universities that have provided long term ideas in information sciences are being drawn to a shorter term focus through fiscal pressures. This trend will continue for some time, and will shrink significantly the research base under the direct influence of the Air Force.

The Air Force must respond to this with a long term technology strategy for those areas that it will continue to directly support. Not all of these will represent areas of current strength, since the relative importance of individual technologies changes over time. Thus, the Air Force may sometimes face the unenviable task of down-sizing a strong technical group that has become less relevant, to make way for a different research focus.

Regardless of physical location or management format, the Air Force must retain an ability to fund and manage research in the information field. The implication of ubiquitous computing is that information systems will be part of every Air Force research and product development group. It is likely that this distributed approach to the information domain will be continued. This may cause a reallocation of funding among research groups at different locations, depending upon the requirements and decisions of Air Force leadership.

## **Coordination Among Laboratories in Key Research Areas**

It is also important that the research be *coordinated* in key focus areas, such as in the research threads for information fusion discussed in the paragraphs above. Several of these can and should be carried out in coordination with a mix of government, university, and industrial fusion research groups. For example, the fusion systems supporting situation awareness have many common characteristics, whether carried on a ship, helicopter, satellite, fighter, or surveillance aircraft. Common research goals should be established in this area across the numerous groups with a present requirement or capability in fusion. Common goals will draw the government, university, and industrial research base into a more stable long term configuration. Focus groups can be established to support airborne avionics, satellites, weapons, and command and control activities. In fusion research as in aerospace missions, coordinated planning with decentralized execution will prove key to the attainment of difficult goals.

The Air Force needs particular assistance in the development of cheap global mobile communications suitable for use on military aircraft. Government programs, such as those in progress at the Advanced Research Projects Agency, should be pursued aggressively. They provide a unique window for the Air Force into cheaper mobile communication technology (indeed, into many of the key research goals listed above). Much greater use should be made of communications research in institutions aligned closely with the commercial world.

## **Coordination Between Air Force Leaders and the Laboratories**

Research at Air Force labs has not always flourished under Congressional scrutiny in recent years. Part of the reason for this is the natural ebb and flow of opinions of our nation's leaders, and the economic situation in which our nation finds itself. However, the time is ripe

for a careful rethinking of laboratory emphasis. In the information domain, three things would be helpful:

- A more complete strategy for extensive use of commercial information systems technology
- A much longer term viewpoint for the Air Force's internal plans for specific mission areas
- The adoption of a research strategy that matches the long term commitment of Air Force leadership to field particular types of capabilities (see Table 1)

Commercial needs will dominate the evolution of many technologies important to the Air Force. For example, commercial mobile bandwidth is becoming ever cheaper for business users, but remains expensive when bought as military airborne systems. An adoption path for use of emerging commercial technologies on military aircraft could be built around programs underway both inside and outside the military laboratory system. Phased array antennas, software radios, and satellite broadcast television are examples of such technologies.

The Air Force should make a strong effort to match research programs to the serious long term intent of Air Force leaders. Extending the period covered by mission area plans would permit research goals to be meaningfully related to the needs of the Air Force. We have offered several long term research goals above. Funding limitations imply that laying a stronger emphasis on the items listed above will lead to program reductions in other areas. The Air Force should give much thought to its long term objectives, however they may be selected, and focus its research groups on these key goals in a very clear way.

## **Can Radical Changes Help in the Information Sciences?**

Most of the research goals listed above will take years to achieve. Patient, stable research programs matched to clearly enunciated long term goals will allow the Air Force to dominate the information sphere throughout the 21st century.

With a long term view in mind, how can the Air Force attract high quality officers and civilians with an information sciences background? If information is the key to the future, qualified professionals will be required. Thought should be given to attracting graduates of major universities with strong information science programs. This could be done through an Air Force ROTC program established at a university recognized for its leadership in information sciences. In return for service in the Air Force, undergraduate scholarships could be granted. In this manner, it would be possible to attract young motivated individuals into service. These individuals would not be oriented toward flying airplanes, but would be slotted from the start for active leadership roles in key laboratories and command and control facilities.

Would it be appropriate to consider alternative business models for a portion of the Air Force laboratory work in information science? One model for doing so is the Advanced Research Projects Agency, which operates in part with a management that is drawn for a limited period from industry and the universities. Focused on vanguard technologies, such a program management staff could initiate and maintain a momentum for the Air Force in these areas. The Air Force might locate such a program management staff near a major university strong in

information science, with a view toward pursuing focused programs of long term interest to the Air Force.

## Key Recommendations of the Information Applications Panel

Our primary recommendation is the following:

*It should be the goal of the Air Force to achieve information dominance to enable the execution of its missions through the unconstrained but protected use of the infosphere, including segments that the Air Force does not control.*

This goal has several elements, outlined in Table 1. Each entry of Table 1 corresponds to monographs written by panel members.

*Table 1. Recommendations of the Information Applications Panel.*

- **Get the right knowledge, to the right place, at the right time for all aerospace missions--** “Situation Awareness in the 21st century” (research directed toward automating the tasks of data fusion)
- **Protect all Air Force computers, software, and data regardless of platform or location, particularly those involved in warfighting--** “Defensive Information Warfare in the 21st century” (research into the issues of computer security)
- **Achieve global communication between the air, ground, and space assets of the Air Force, as well as those with whom we operate--** “Communications and Networking” (research associated with the evolution of the Air Force toward a densely internetworked environment)
- **Maximize the speed and quality of Air Force coordination, planning, and execution--** “Coordination, Planning, and Execution in an Information Rich World” (research supporting new capabilities for command and control)
- **Dominate the information battlespace--** “Information Warfare in the 21st century” (steps toward an Air Force view of information warfare)
- **Develop doctrine needed for the use of information in dynamic command and control of joint forces--** “Information in Warfare: Toward Dynamic Command and Control” (thoughts on the participation of the Air Force in future Joint operations)

What should be done in the near term? What are the longer term research goals? The individual monographs record our detailed ideas. Some critical extracts are listed below:

- Fusion short term: increased speed in key fusion applications through operator cueing
- Fusion research goals: automated fusion
- Protection short term: protect all Air Force computers, software, and data following best commercial practice and military security policy
- Protection research goals: strong security for networked computer systems
- Communication short term: increased number of airborne platforms with data communication links, better interoperability, global dissemination broadcasts
- Communication research goals: cheap two-way global communication between all Air Force platforms

- Coordination short term: construct a system prototype that includes automated planning and scheduling tools, and hierarchical modeling and simulation
- Coordination research goals: a distributed collaboration system that marries real-time automated planning with globally connected human interfaces
- Information Warfare short term: develop an Air Force view of information warfare, and develop the software tools needed to monitor military infosphere
- Information Warfare research goal: a rigorous fundamental understanding of the possible futures for software munitions
- Dynamic command and control: near-term investments are needed to integrate doctrine with technology for joint warfighting

## Speculating About the Future

This summary introduces the Information Applications Panel's monographs. Our emphasis throughout is on the long view. Our ideas and system concepts, if adopted by the Air Force, will require years to accomplish. To Air Force leaders who may look through these monographs: before you read our thoughts, read a good science fiction novel (Neal Stephenson, Bruce Stirling, or William Gibson come to mind). In doing so, you will see how very conservative our thoughts about the future have been.

Throughout the history of the Air Force, the discipline of physics has greatly influenced the thinking of its leaders. Today, many of us accept the idea that we live in the age of information. We have built the thoughts of our panel around this idea, as have other panels in the New World Vistas effort. However, think about this: most of the papers in the periodicals *Science* and *Nature* are not devoted to information science. They are devoted to biology.<sup>5</sup> The intersections of these three worlds (physics, information, and biology) are many. For example, we see a potentially important thread in Len Adleman's recent use of deoxyribonucleic acid (DNA) to carry out computations analogous to those needed for automatic information fusion and planning.<sup>6</sup>

We are passing from a world dominated by physics, through one dominated by information, toward one dominated by biology. Biology will likely change our future more profoundly than physics or information science. The paradigms that inform our thoughts on military matters will shift, and (perhaps) shift again over the professional lifetimes of those entering the service today. The Air Force is a young military service, and information science is only the first of the paradigm shifts that it will experience in the 21st century.

Many thanks to the Information Applications Panel membership for their hard work and dedication to our joint task. The leading edge of the millennium is a great time to be thinking about the future. We have all tried to write documents that reflect our honest assessment of the future.

*Chuck Morefield, Beckman Center, 1995*

---

5. See the monographs by the Human Systems/Biotechnology Panel.

6. See the accompanying monograph "Situation Awareness in the 21st Century" for a discussion of DNA-based computation.



# Contents

Executive Summary Air Force Information Applications in the 21st Century .....	iii
1.0 Situation Awareness in the 21st Century .....	1
2.0 Defensive Information Warfare in the 21st Century .....	17
3.0 Communications and Networking .....	32
4.0 Coordination, Planning, and Execution in an Information-Rich World .....	47
5.0 Offensive Information Warfare in the 21st Century .....	66
6.0 Information in Warfare: Toward Dynamic Command and Control .....	72
Appendix A Panel Charter .....	A -1
Appendix B Panel Members and Affiliations .....	B -1
Appendix C Panel Meeting Locations and Topics .....	C -1
Appendix D List of Acronyms .....	D -1

# Illustrations

Figure 1 Telecommunications and computer technology will transform the Air Force .....	iv
Figure 2 Future data links between aerospace platforms .....	x
Figure 3 Distributed data fusion .....	xi
Figure 4 Current fusion architecture .....	3
Figure 5 An example of a coherent future architecture .....	3
Figure 6 Fusion and sensor systems will monitor the military infosphere .....	4
Figure 7 Multisensor fusion .....	7
Figure 8 Core technologies for the fusion (more important denoted in bold) .....	8
Figure 9 Fusion systems constructed to a common reference model, operating in concert across a computer communications network. ....	11
Figure 10 An unbounded domain viewed as a collection of bounded systems .....	21
Figure 11 Relationships among threats. ....	28
Figure 12 .....	33
Figure 13 Global Networks for Tactical Theater Operations .....	33
Figure 14 Connectivity Requirements for Future Air Force Communications Network .....	35
Figure 15 SATCOM Systems .....	38
Figure 16 The C4I System of the Future .....	48
Figure 17 C4I Security Is Critical to Operations .....	50
Figure 18 The Many Faces of Architectures .....	55
Figure 19 The Geospatial Reference Grid .....	57
Figure 20 Intelligent, Distributed, Collaborative Planning .....	58
Figure 21 Intelligence flow .....	76
Figure 22 Requirements and response flows .....	77

# Tables

Table 1 Recommendations of the Information Applications Panel .....	xiv
Table 2 Threats and Countermeasures .....	22