

THE DEFENSE SCIENCE BOARD  
1999 SUMMER STUDY TASK FORCE

on

---

21<sup>ST</sup> CENTURY DEFENSE  
TECHNOLOGY STRATEGIES

---

Volume I





OFFICE OF THE SECRETARY OF DEFENSE  
3140 DEFENSE PENTAGON  
WASHINGTON, DC 20301-3140

DEFENSE SCIENCE  
BOARD

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE (ACQUISITION, TECHNOLOGY  
& LOGISTICS)

CHAIRMAN, JOINT CHIEFS OF STAFF, Summer Study Task Force  
on 21<sup>st</sup> Century Defense Technology Strategies

SUBJECT: Report of the 1999 Defense Science Board (DSB) Summer Study Task Force on 21<sup>st</sup>  
Century Defense Technology Strategies

I am pleased to forward the final report of the 1999 DSB Summer Study Task Force on 21<sup>st</sup> Century Defense Technology Strategies, Volume I. This effort, co-chaired by Mr. Donald Latham and Mr. Larry Lynn, was tasked to examine the national security challenges of the next two decades and to provide technology strategy recommendations for meeting these challenges.

This Task Force believes that the DoD needs to develop a joint and combined rapid response capabilities that can support a wide range of contingency operations and that there are three enablers for developing this capability: strategic agility, information for decision superiority, and force protection. To that end, achieving a joint-rapid response operations capability should become a major organizing construct for the Department's pursuit of *Joint Vision 2010* and beyond. In addition, the Task Force concluded that true transformation requires major changes in the following: joint responsibility and accountability, intelligence, technology and development approaches, and acquisition processes and resource balance.

I endorse all of the Task Force's recommendations and encourage you and your staff to review the Task Force Chairman's letter and report.

A handwritten signature in black ink, appearing to read "Craig I. Fields".

Craig I. Fields  
Chairman



DEFENSE SCIENCE  
BOARD

November 1, 1999

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Final Report of the 1999 Defense Science Board Summer Study Task Force on 21<sup>st</sup> Century Defense Technology Strategies

The final report of the 1999 Defense Science Board Summer Study Task Force on 21<sup>st</sup> Century Defense Technology Strategies, Volume I, is attached. This report consists of two volumes. Volume I presents the major findings and recommendations and Volume II, which is planned to be finalized in December, provides the supporting materials.

As the nation moves toward the 21<sup>st</sup> century, the United States faces a dynamic international environment that will impose new complexities in military operations. The Department of Defense is embarking on a process of transforming the military to stay ahead of future security challenges. Although the United States currently enjoys military superiority, retaining this advantage will require a balance between maintaining relevant legacy forces, facilities, and systems and developing new and different capabilities. This transformation must be accomplished while today's high operational tempo continues.

The Department of Defense needs a way to focus the transformation process. Our task force found that developing a full spectrum – air, land, space and sea – joint-rapid response operations capability can be an effective way to focus the activities of the Department. Thus, our task force focused on capabilities, technologies, and organizational changes associated with developing joint and combined rapid response capabilities that can support a range of contingency operations – a major priority for the Department today.

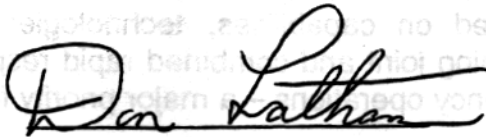
In this study, we address three enablers essential for developing this capability: strategic agility, information for decision superiority, and force protection. We also conclude that effective transformation will require major changes in joint responsibility and accountability, intelligence, technology and development approaches, and acquisition processes and resource balance.

The task force came to several overarching conclusions in its investigation of defense technology strategies for the 21<sup>st</sup> century:

- The CINCs need clearer responsibility and authority for identifying and prioritizing the needed capabilities to bring Service-provided forces together into an effective joint and/or coalition force. Some of these capabilities need to be "born joint", particularly in the C3 area.
- An Integrated Information Infrastructure (III) is required as the joint, interoperable means to meet DoD 21<sup>st</sup> century network needs.
- The Chairman, Joint Chiefs of Staff (CJCS) and the CINCs need increased engineering and integration support focused on joint C<sup>4</sup> systems and integrating intelligence, surveillance, and reconnaissance systems in support of joint operations.
- The CINCs' need for superior intelligence requires a transformation by the intelligence community to a mission focus in support of the warfighter.
- "Grand challenges" can focus technology on seeking order-of-magnitude improvements in operational capabilities.

In summary, achieving a joint-rapid response operations capability should become a major organizing construct for the Department's pursuit of *Joint Vision 2010* and beyond. It addresses a central and critical challenge facing the U.S. military and will provide needed focus for transformation to a 21st century force.

We thank the Task Force members and the talented group of government advisors for their hard work and valuable insights. Their dedication reflects their belief in the importance of this challenge to the Department.



Donald Latham, Co-Chair



Larry Lynn, Co-Chair

---

# TABLE OF CONTENTS

## VOLUME I – FINAL REPORT

PREFACE .....	iii
EXECUTIVE SUMMARY .....	v
CHAPTER 1. INTRODUCTION .....	1
Background .....	1
The 1990 DSB Summer Study.....	2
CHAPTER 2. JOINT RAPID RESPONSE OPERATIONS.....	7
Operational and Threat Environment.....	7
Transforming <i>Joint Vision 2010</i> and Beyond .....	9
Joint Rapid Response Operations Capability.....	10
CHAPTER 3. ESSENTIAL ENABLERS.....	21
Strategic Agility.....	21
Information for Decision Superiority.....	25
Force Protection.....	32
Synergy and the Need for Experimentation.....	35
CHAPTER 4. MAKING IT HAPPEN .....	39
Joint Responsibility.....	39
Transforming Intelligence.....	45
Technologies and Development.....	50
Acquisition and Resources.....	56
CHAPTER 5. SUMMARY AND RECOMMENDATIONS.....	63
ANNEX A. TERMS OF REFERENCE .....	A-1
ANNEX B. STUDY ORGANIZATION AND MEMBERSHIP .....	B-1
ANNEX C. INTEGRATED INFORMATION INFRASTRUCTURE .....	C-1
ANNEX D. TECHNOLOGY GRAND CHALLENGES .....	D-1
ANNEX E. LOGISTICS INFORMATION SUPERIORITY CONSIDERATIONS.....	E-1
ANNEX F. GLOSSARY .....	F-1

## **VOLUME II – SUPPORTING REPORTS**

PART 1. Intelligence Needs and Adversaries

PART 2. Information Superiority

PART 3. Defense Technology Strategy and Management

PART 4. Strategic Agility

PART 5. Analysis and Quantitative Results

---

# PREFACE

The Defense Science Board (DSB) 1999 Summer Study Task Force on *21<sup>st</sup> Century Defense Technology Strategies* continues a series of studies that have examined key challenges facing America's military in the post Cold War era. Through a decade of study, the DSB has undertaken a "Transformation Campaign," providing vision to guide the evolution of America's armed forces into the 21<sup>st</sup> century. The foundation of this campaign was a 1990 study that set forth a research and development strategy for the Department of Defense for the 1990s. In 1995, the DSB began to address the challenges of a new kind of adversary: an asymmetrical and adaptive adversary posing a threat to U.S. forces that differs from the "traditional" threat addressed over the last fifty years. In 1995, the Board also identified the possibility of a "Revolution in Business Affairs," pointing out the opportunity to achieve better resource allocation by addressing inefficiencies in support and infrastructure functions.

In 1996, the DSB described the concept of a distributed joint expeditionary force as a key military capability for the future. At the same time, the Board began to examine, in more detail, how savings in infrastructure costs could free up resources for investments in force modernization and research and development. The groundbreaking 1997 summer study addressed transnational threats, force protection, and the ability to cope with weapons of mass destruction. Last year, the Board examined force projection and how to create a joint, light – but potent – early entry force as a centerpiece for underwriting *Joint Vision 2010* and beyond. Also, for the first time, the Board focused its attention on the integration of logistics and operations – a theme carried forward in this year's study.

In the past decade, the Defense Science Board has also examined many other topics related to this transformation campaign, including Coalition Warfare, Globalization and Security, Nuclear Deterrence, Underground Facilities, Information Warfare Defense, Ballistic and Cruise Missile Defense, and Urban Warfare.

These studies have all addressed the wide range of threats facing the United States. The potential adversaries range from re-emergent peer competitor to rogue nation to the criminal and transnational threat. The weapons range from familiar, conventional threats – high performance platforms, centralized command and control, precision weapons, and even nuclear weapons – to asymmetric, unconventional threats that include biological, chemical, and information warfare. The command and control systems utilized by potential adversaries may include the Internet and other commercial communication networks. And their means of force projection may include the use of commercial carriers, common throughout the business community.

This spectrum of threats is individually and collectively difficult and challenging. There is special concern about an adaptive enemy that is clever, takes risks, and is ruthless. It is possible for even an adversary with a relatively small budget to become a significant regional threat. Large quantities of inexpensive missiles, even last-generation weapons, require thoughtful counters. Underground facilities, land and sea mines, and unconventional threats such as information warfare are in the hands of many potential adversaries today and are likely to be available to even more in the future. Particularly given America's high concern for human life



and the lack of such concern in many adversaries, the 21<sup>st</sup> century threat is diverse and formidable.

This year's summer study continues the transformation campaign by building on key recommendations made by the Board during the 1990s. The task force has identified some important underlying themes:

- ***Strategic Agility.*** The nation needs, but does not now have, sufficient capability for rapid response, rapid presence, and firepower in the first days of a contingency. The 1998 summer study described the Department's need to globally attack targets in the first hours and first days of combat. To achieve this kind of rapid response, the Department must design agility into its systems and capabilities from the outset beginning with the requirements process.
- ***Information for Decision Superiority.*** Much has been said and written about information superiority. The task force believes that achieving and sustaining information superiority, narrowly defined, will be difficult. However, understanding how to provide the information and information tools required for smarter and faster decisions can have a more lasting impact. The path toward decision superiority begins with data collection from a wide variety of sources and involves transforming that data first into information, then knowledge, and finally the understanding that enables better combat decisions. Faster and better decisions enabling faster and better execution is the metric by which to measure information superiority.
- ***Force Protection.*** The ability to deter adversary actions against U.S. national interests is strongly tied to the ability to protect forces both in the continental United States and once deployed. U.S. forces must be capable of dealing with the full range of possible weapon effects, including those inflicted by chemical and biological weapons. The Department needs to develop effective means to counter the threat of biological weapon use against U.S. forces.

Taken together, these enablers are essential to the Department's ability to transform its forces to meet the demands of the future security environment. They are also the foundation for defense technology strategies for the 21<sup>st</sup> century – the subject of this report.

---

# EXECUTIVE SUMMARY

As the nation moves toward the 21<sup>st</sup> century, the United States faces a dynamic international environment that will impose new complexities in military operations. Today's potential adversaries are more adaptive and have increasing access to asymmetric capabilities to offset U.S. military capabilities. The Department of Defense is embarking on a process of transforming the military to stay ahead of future security challenges. Although the United States currently enjoys military superiority, retaining this advantage will require a balance between maintaining relevant legacy forces, facilities, and systems and developing new and different capabilities.

The 1999 Summer Study Task Force was asked to examine 21<sup>st</sup> century defense technology strategies to meet the national security challenges of the next two decades. Specifically, the Terms of Reference asked the task force to

- Review and consider the broad spectrum of topics addressed in the 1990 DSB summer study
- Address 21<sup>st</sup> century intelligence needs and adversaries
- Expand and build on the recommendations for technologies, operational capabilities, and force characteristics developed in the 1998 DSB summer study
- Examine the need for and use of all forms of information to achieve full spectrum battlespace dominance
- Examine defense technology strategy, management, and acquisition

In addressing these issues, the task force paid special attention to several areas: assuring jointness, accelerating DoD's transformation to a 21<sup>st</sup> century force, organizing to transform the intelligence community to support changing requirements, and focusing science and technology research and development. The central focus of the task force was on the capabilities, technology, and organization associated with developing joint and combined rapid response capabilities that can support a range of contingency operations – a major priority for the Department today.

## *Transforming Joint Vision 2010 and Beyond*

The U.S. military faces a complex set of contingencies. Future adversaries are expected to be less predictable and thus more challenging, exploiting asymmetric approaches to oppose America's conventional strength. Particularly worrisome are countries and hostile groups that have seen the successes of Desert Storm and more recent U.S. military operations and are adapting their strategies in an attempt to offset some U.S. advantages.

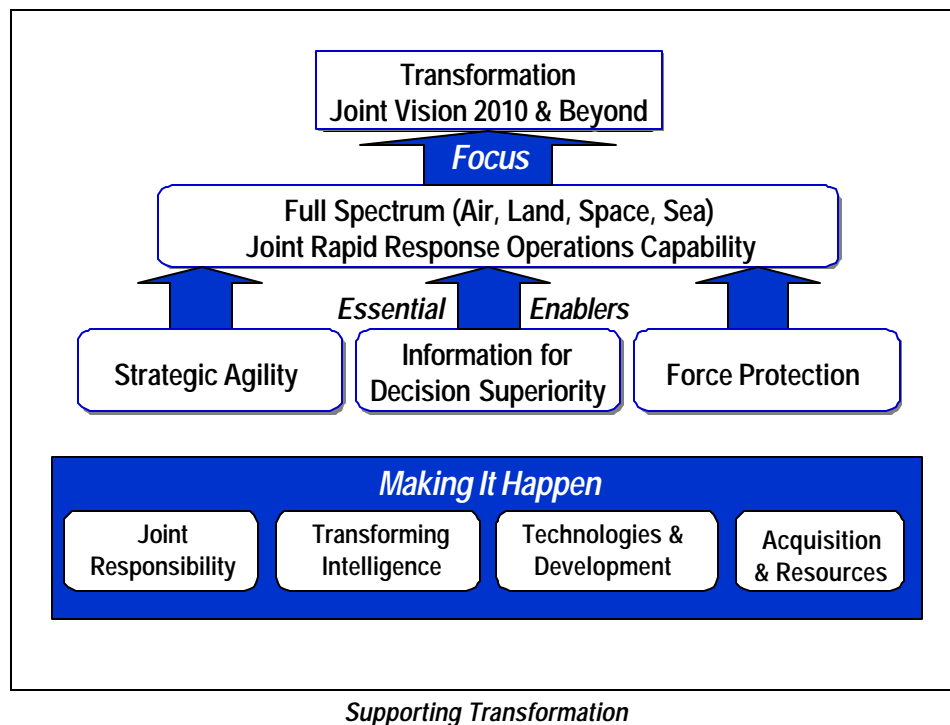
Biological and information warfare, in particular, pose direct threats to both America's deployed forces and to the homeland, as adversary nations, radical movements, and criminal groups become more ambitious in their aims and more aggressive in their pursuits. Against that backdrop, decision times will necessarily be short and there will be a premium on terminating conflicts – both large and small – quickly and decisively to minimize their consequences, potential to spread, and chances of recurrence.

Transforming the capabilities of U.S. forces will be challenging, particularly with today's high operational tempo, which is expected to continue. Thus, a central challenge for the Department becomes to

*Transition to military capabilities that underwrite the future vision with no breathing space in the demand for use of current capabilities.*

The Joint Chiefs of Staff have provided a vision for this transformation in *Joint Vision 2010*, which provides a conceptual template for the attributes of America's future armed forces and for new levels of joint warfighting effectiveness. The individual Services are currently developing a rich array of operational concepts and capabilities to enhance the combat and quick-reaction ability of the military forces. The effectiveness of these enhancements, however, will depend heavily on integration in joint operations.

***The Department of Defense needs a way to focus its transformation to a 21<sup>st</sup> century joint force. Developing a full spectrum – air, land, space and sea – joint rapid response operations capability is an effective way to focus the activities of the Department and the transformation to Joint Vision 2010 and beyond.*** This study addresses three enablers essential for developing a rapid response capability: strategic agility, information for decision superiority, and force protection. It also concludes that effective transformation will require major changes in joint responsibility, intelligence, technology and development approaches, and acquisition processes and resource balance.



## JOINT-RAPID RESPONSE OPERATIONS CAPABILITY

A joint rapid response operations capability, as both a warfighting capability and a strategic deterrent, is a critical need for the Department of Defense. Today, with enough time and warning, the United States is able to build up a joint force that can respond to almost any operational contingency. Also, the United States has a rapid response capability in some of its forces that can respond effectively to certain requirements, especially in support of smaller contingency operations. But the nation lacks an effective response when the contingency requirement calls for a more capable and potent force that is needed fast – that is, within 24 to 96 hours. A joint rapid response operations capability is essential to fill the gap in U.S. warfighting response options, enabling the United States to set the conditions of an operation from the outset rather than responding to conditions already set in place by an adversary.

Furthermore, a demonstrated rapid response capability and credible will to use it has strategic value as a deterrent against potential aggressors. Such a capability could provide a stabilizing influence prior to conflict and could help to shape the strategic environment. A rapid response capability could deter and dissuade adversaries from commencing operations and could also add a great deal of power to other crisis resolution tools, including diplomatic, economic and political responses.

Developing a joint rapid response operations capability could lead to the creation, in several years, of Joint Rapid Response Operations Forces (J-ROFs). These forces would provide rapid response with substantial offensive combat power but minimum footprint in-theater. They would be designed for efficient logistics support, and could be used in conjunction with forward-deployed, coalition, and follow-on forces – all of which can be moved into the theater of operations rapidly.

An early capability that can defend and take the offense is important in securing early conflict resolution and termination. The modular, building-block type capability of the J-ROFs, as envisioned, will provide DoD with a flexible set of force concepts and capabilities that can be reconfigured as required to meet the changing demands of the future strategic environment.

Implementing the J-ROF will be a multi-faceted, multi-year effort combining development and operational experimentation. As a focal point for implementation, the task force recommends that the Department establish a permanent, experimental joint rapid response operations headquarters under United States Joint Forces Command (USJFCOM). A critical element in implementation is integrating coalition partners prior to a contingency, with continuous experimentation, training, and planning. Communication practices, frequencies, and control; information system protocols and access security; and logistics roles, modes, and packaging all need to be planned and exercised if the joint and combined force is to become a capable military entity.

## ESSENTIAL ENABLERS

To implement a joint rapid response capability in the next five years, the Department needs a number of key operational enablers. As already noted, the task force focused its efforts on three – strategic agility, information for decision superiority, and force protection – essential to creating joint rapid response operations capabilities.

## Strategic Agility

“Strategic agility” is the ability to rapidly move personnel, materiel, and weapons when and to where they are needed and to maneuver them in the battlespace as required. The objective is to move forces into the battlespace before the enemy sets the conditions and before these conditions are too hard to change. The need is to have sufficient military power arriving fast enough to be both a credible conventional deterrent and a potent combat force. To make such a capability credible, the United States must focus on the force capabilities needed and on the more vulnerable elements of strategic agility – the ports, the airfields, and the infrastructure on which the military currently depends – as well as on a robust, ready-to-use joint command, control, communications, computers and intelligence, surveillance, and reconnaissance (C<sup>4</sup>ISR) system.

Achieving strategic agility involves changing major event time-lines as well as resolving a myriad of movement and support issues. But most importantly, it requires a change in the characteristics of U.S. forces. ***DoD must design strategic agility into its systems and capabilities from the beginning – from concept definition to fielding capabilities.*** Operations and logistics should be treated as an integrated whole in requirements, design, operational planning, and execution – including planning and exercising coalition capabilities and support agreements.

Strategic agility is enabled by a variety of capabilities including advanced logistics planning tools, advanced munitions that lighten the force while increasing its potency, commercial air and sea lift assets, intermediate staging bases, access to austere ports and airfields, and nodeless, distributed logistics systems.

## Information for Decision Superiority

“Decision superiority” is the ability to use information and experience to make battlespace decisions faster and better than any adversary to ensure a continuing and overwhelming pace and effectiveness of operations. If adversaries and potential adversaries believe the U.S. military is consistently able to use decision superiority to achieve execution superiority, the nation will have created a useful strategic deterrent in addition to a superior capability in conflict and other operations.

Decision superiority plays a key role in the efficient and rapid execution of military missions. The objective is to provide information to commanders in such a way that they can absorb it, understand it, and use it quickly and effectively to shape battlespace decisions. At the core of decision superiority is a high-level operational architecture. ***The centerpiece of the architecture is the premise that the warfighter must be responsible for defining and assembling his or her own information ensemble using information made available through systems provided by the information community.*** Each warfighter – whether Commander-in-Chief (CINC) or platoon leader – has the responsibility to assemble needed information into a tailored ensemble to support battlespace requirements.

The infrastructure of the operational architecture is the Integrated Information Infrastructure. This level has a suite of tools developed by the technology community to enable the warfighter to receive and assess information. The concept is based on a “pull” system, where the warfighter pulls information from the infrastructure, using automation to sort, arrange, filter, and find items of interest – much like the commercial Internet. At the input level of the operational architecture is data and information gathering. Here, data and information contributors “push” information

into the information infrastructure where it is indexed, categorized, and assessed. This architecture for supporting decision superiority also enables the need for greater mission focus for the intelligence community. Responding to the warfighter's needs, both proactively and reactively, the intelligence community can provide relevant information to the integrated information system.

### *Force Protection*

Protecting forces, infrastructure, and lines of communication has long been part of any military mission – whether it be active combat in the Gulf or a peacekeeping mission in Bosnia. The 1996 bombing of Khobar Towers, like Beirut more than a decade before, highlighted the difficulty of protecting forces and the potentially devastating consequences of an attack.

The findings of the 1997 DSB summer study, *DoD Responses to Transnational Threats*, emphasized a three-tiered response to the transnational threat challenge: a global response, a regional response, and *a force level response, which focuses on force protection as a fundamental readiness mission requirement across the spectrum of threats*. A robust force protection capability is critical to meeting U.S. security needs and maintaining the nation's ability to project its forces abroad, as the force protection challenge continues to evolve. Threats to the U.S. homeland and defense against these threats are a growing concern, particularly as the United States becomes more effective at joint rapid response operations capabilities. Many new operational concepts, such as split-basing and long-range strike, involve reachback to or staging from installations in the continental United States. Another area of increasing concern is protection against and counters to biological warfare attack.

The 1997 DSB task force identified the need for an enhanced force protection program with the following emphasis: an end-to-end mission orientation, expanded vulnerability assessments, patching the “seams” created by diverse responsibilities, focusing intelligence programs and capabilities, and exploiting promising technologies, including the creation of a test bed focused on force protection. These recommendations remain applicable today.

## MAKING IT HAPPEN

The task force also identified key transformation needs: the responsibility of the joint and coalition force commanders; changes in the nation's intelligence, both the community at large and those elements more directly in support of rapid, potent force elements; new technological capabilities, both in the near term using today's technology, and in the longer term requiring new inventions and innovations; and changes in acquisition processes and a resource balance between modernization, infrastructure, and support functions.

### *Joint Responsibility*

Goldwater-Nichols laid the groundwork for involving the warfighting customer in the process of matching available force capabilities to tasks and identifying gaps in capabilities for the joint operational commands. Today, the CINCs and joint forces have greater authority and responsibility for current operations and are being consulted and informed to an unprecedented

extent. Nonetheless, giving the ultimate customer greater influence in establishing *future capability priorities* remains ad hoc in nature.

***The DSB Task Force suggests that more attention by the warfighting CINCs is needed in addressing future capabilities, with special emphasis on those capabilities that are inherently “joint” such as C<sup>4</sup>ISR.*** There is clear responsibility, in the military Services and Defense Agencies, for providing forces to the CINCs. However, the authority and responsibility is not nearly as clear for providing the capabilities needed to employ those forces in an effective “joint force.”

To enhance “joint” involvement in establishing future capabilities, a field representative for the CINCs is needed. While the Chairman of the Joint Chiefs could, himself, assume this responsibility, he already has a complex set of responsibilities, and this effort needs more attention than he is likely to be able to give it. *Thus the Task Force believes that the United States Joint Forces Command is the logical organization to perform the role of “futures” CINC,* given that USJFCOM has already been assigned responsibilities in related functional roles. USJFCOM would continue to be the “force provider,” responsible for joint training, and would become the representative for “future joint capabilities,” to include responsibility for joint experimentation. Other USJFCOM responsibilities not directly related to these roles should be reassigned.

***C<sup>4</sup>ISR.*** C<sup>4</sup>ISR systems are an example of capabilities that should be “born joint” – that is, C<sup>4</sup>ISR assets should be treated as a joint system from the start rather than “kluged together” at the time of a crisis. Joint C<sup>4</sup>ISR systems must be standing capabilities – proven, exercised, interoperable with joint and coalition forces, and continuously evolving – if they are to match the response time expected from Joint Rapid Response Operations Forces.

Creating a joint C<sup>4</sup>ISR system requires a joint and combined focus and therefore someone responsible for designing, testing, operating, and continuously upgrading the system. Currently, C<sup>4</sup>ISR components are developed independently by each Service. There is no single focal point for designing and managing a joint system. The task force recommends assigning such responsibilities to the CINCs – the responsible warfighters. Responsibility for overall system development and for the deployable system would be given to USJFCOM. Such systems must be exercised by the CINCs in the manner appropriate for their area of responsibility. The CINCs also need to test and continuously operate their C<sup>4</sup>ISR system with coalition forces – and must be funded to do so.

The CINCs will need technical assistance to perform such functions and to oversee the evolution to interoperable and fully capable joint and combined C<sup>4</sup>ISR systems. They will also need technical assistance in upgrading these systems on a continual basis to maintain capabilities in the face of very rapid evolution of communications and computer systems. ***The task force recommends forming a Joint Systems Engineering Organization (JSEO), reporting to USJFCOM.*** Such an organization would provide technical support to USJFCOM and the other regional CINCs for joint and combined C<sup>4</sup>ISR systems. The Services and Agencies would continue to provide the component systems.

## *Transforming Intelligence*

The United States holds a position of incontestable dominance in intelligence based on technical means. This situation is likely to continue as no other nation is likely to be both able and willing to make the investment required to overcome this superiority anytime soon. However, adversaries have begun to adapt to the well-publicized success of U.S. intelligence methods.

Customer needs for intelligence are being driven by the changing character of adversaries and their abilities to threaten U.S. interests. Customer priorities are increasingly dynamic, and the issues of concern are expanding in diversity. Rather than focusing on a few major threats, the intelligence community must continually analyze a wider range of potential adversaries and base judgements and estimates more on motivation, capability, and access rather than observation of hard evidence. This represents a major cultural change for the intelligence community. Timelines within which the intelligence community must respond are shrinking, and while the need to protect sensitive sources and methods is unchanged, virtually every action taken by U.S. warfighters and policymakers is executed in a combined environment – driving the demand to share intelligence products with coalition partners.

At the same time, the technology-enabled, information-rich global environment is shaping customer expectations. DoD customers are increasingly reliant on information networks and databases to enable their operations. Thus, information provided by the intelligence community is of limited value unless it is readily accessible within this electronic operating environment.

The task force grappled with the question of how to transform the nation's intelligence apparatus to support the Department of Defense, and specifically the warfighters, in a way that allows for more inputs and better capabilities across the spectrum of applications. The intelligence community is collector-centric with “stovepipe” collection systems. ***To support greater customer demand, the intelligence community needs to become more mission-centric, focused on the specific missions of the CINCs as well as that of other customers.*** In turn, DoD needs to take action to motivate a stronger intelligence pull by the CINCs. Persistent, dedicated, involved customers can help change the supplier culture. To create a more mission-centric approach, the intelligence community needs mission managers that deliver focused intelligence to the warfighters as well as other customers.

## *Technologies and Development*

DoD's science and technology base is, to a great extent, unfocused and fragmented. This study assessed important technology areas and concluded that four were changing rapidly and in ways that will have an impact on future military capabilities. The four areas are biotechnology, information technology, microsystems, and energy and materials. While the commercial sector investments in most areas of these technologies substantially exceed DoD's, most of the civilian investments have a time horizon of only a few years. As a result, DoD needs to focus on the long term, more speculative aspects of these technology areas. But more importantly, DoD needs to focus on the *interfaces* between these technologies because it is from these intersections that the truly revolutionary advances in military capability will come.

The study concluded that “grand challenges” should be created as the focusing mechanism for a significant fraction of DoD science and technology investment. The task force identified



four examples of grand challenges, each with the potential for order-of-magnitude improvements in military capabilities. The four are

- **Bioshield:** real-time detection, characterization, response, and attribution of conventional and unconventional biological threats
- **No Place to Hide:** ubiquitous, intrusive, and inescapable target sensing
- **Fast Forward:** rapid, decisive force application from the continental United States
- **Cognitive C<sup>4</sup>:** warfighter-matched, agile, secure, and available C<sup>4</sup> systems

Grand challenge military capabilities are not the only science and technology investment areas that DoD should pursue. But, in the judgement of the task force, they are a good basis for providing badly needed focus for science and technology.

### *Acquisition and Resources*

An acquisition approach that recognizes changing system requirements during the development and production life cycle provides a process to field useful military capabilities early while continually upgrading them to attain desired “ultimate” capabilities in the longer run. Three inter-related elements can accomplish this goal: an iterative requirements process, an evolutionary acquisition process, and a modular open system approach to overall program execution. Because the key recommendations of this study revolve around the concepts of frequent joint field exercises, rapid fielding of prototype hardware and software, and continuous upgrading of concepts of operations, tactics and equipment, these evolutionary procurements approaches are a key enabler to successful implementation.

In 1996, the Defense Science Board Summer Study, *Achieving an Innovative Support Structure for 21<sup>st</sup> Century Military Superiority*, examined DoD infrastructure costs and concluded that the Department could realize \$30 billion in annual potential savings by improving efficiencies in the business side of its operations. This would allow DoD to shift these resources into operational accounts for readiness and modernization initiatives. The Department has made significant progress in reducing support costs through outsourcing, logistics transformation, and reducing personnel. The Office of the Secretary of Defense for Program Analysis and Evaluation (OSD PA&E) currently estimates that there are \$8-9 billion in savings currently programmed in the Future Years Defense Program. However, the task force feels that there are still many opportunities to realize further savings and recommends that the Department continue to aggressively seek savings in infrastructure and support.

## SUMMARY AND KEY RECOMMENDATIONS

The task force came to several overarching conclusions in its investigation of defense technology strategies for the 21<sup>st</sup> century:

- Filling the challenging need for joint rapid response operations capabilities can be a powerful vehicle to focus transformation to *Joint Vision 2010* and beyond
- This capability, leading in several years to Joint Rapid Response Operations Forces, must include coalition partners capabilities and needs up front

- Two of several key enablers of this capability are strategic agility and information for decision superiority
- The CINCs need clearer responsibility for identifying and prioritizing the needed capabilities to bring Service-provided forces together into an effective joint and/or coalition force – some of these capabilities need to be “born joint”
- An Integrated Information Infrastructure is the joint, interoperable means to meet DoD 21<sup>st</sup> century network needs
- The Chairman, Joint Chiefs of Staff (CJCS) and CINCs need increased engineering and integration support focused on joint C<sup>4</sup> systems and integrating ISR systems in support of joint operations
- The CINCs’ need for superior intelligence requires a transformation to a mission focus by the intelligence community in support of the warfighter
- “Grand challenges” can focus technology on order-of-magnitude improvements in operational capabilities

The task force makes the following set of recommendations for transforming the Department’s current capabilities to those needed for effective joint rapid response operations capabilities.

## **RECOMMENDATIONS**

### **Transformation to Underwrite *Joint Vision 2010*:**

- The Secretary of Defense should assign USJFCOM responsibility for establishing a core, joint rapid response operations force headquarters
  - For joint experimentation now
  - Evolving to initial deployable joint capabilities in the future
  - Bringing coalition partners into Limited Operational Experiments

### **Integrated Information Infrastructure:**

- Implement the Integrated Information Infrastructure by 2005
- Fix responsibility and authority for implementation
  - Overall responsibility: Deputy Secretary of Defense and Vice Chairman, Joint Chiefs of Staff (VCJCS), assisted by an Executive Office reporting to the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) (ASD(C<sup>3</sup>I))
  - Operational architecture: VCJCS with CINC and Military Services participation
  - Technical architecture: Under Secretary of Defense for Acquisition and Technology (USD(A&T)) assisted by ASD(C<sup>3</sup>I), Joint Staff, Military Services, and Information Technology Advisory Board
  - System architecture: ASD (C<sup>3</sup>I) assisted by Joint Staff and Military Services

**Joint Responsibility:**

- The Secretary of Defense should assign USJFCOM responsibility as the joint institution that provides field representation on joint system needs and priorities

**Joint C<sup>4</sup> and ISR:**

- The Deputy Secretary of Defense should direct strong technical support and funding to USJFCOM consistent with responsibility for
  - Future joint C<sup>4</sup> and ISR systems architectures and technical capabilities
  - Support of warfighting CINC's with current C<sup>4</sup> and ISR systems
  - Creating the Joint Systems Engineering Organization reporting to USJFCOM with responsibilities for supporting CJCS and other CINC's
- Fund the CINC's to operate standing C<sup>4</sup> systems to assure their readiness for any contingency to include exercising customer pull for intelligence support
  - Use the same types of metrics as for combat and combat support force elements: capability, response requirement, readiness standards

**Research and Development:**

USD(A&T) and Director, Defense Research and Engineering (DDR&E) should

- Commit a major fraction of the science and technology budget to providing complete technology solutions to the warfighters for a few urgent grand military challenges
- Start with two of the most critical grand challenges:
  - “No Place to Hide” – deny enemy hiding
  - “Bioshield” – protect the force against biological threats
- Make the science and technology leadership accountable for delivering against these grand challenges as a fundamental change in their role
  - Measure progress frequently in cooperation with the user through experimentation, against quantifiable parameters
  - Empower to make changes
- Gain support from the Secretary of Defense for strong control of research and development funding by USD(A&T) and delegate control of science and technology to DDR&E

*Achieving a joint-rapid response operations capability should become a major organizing construct for the Department's pursuit of Joint Vision 2010 and beyond. It addresses a central and critical challenge facing the U.S. military and will provide needed focus for transformation to a 21<sup>st</sup> century force.*

---

# CHAPTER 1. INTRODUCTION

## BACKGROUND

The Defense Science Board has been exploring the “Revolution in Military Affairs” and the “Revolution in Business Affairs” since the 1990 Defense Science Board summer study on *Research and Development Strategy for the 1990s*. During the past decade, the United States has experienced huge shifts in global relationships, power structures, economics, technology development, and the rise of new adversaries that have access to the latest technologies and are able and willing to employ new forms of warfare. Of particular concern is the proliferation of nuclear, chemical, and biological weapons technology and the many means by which such weapons can be delivered. In addition, a dramatic revolution in the access, sharing and utility of global information has occurred. Information is now a critical and powerful enabler of economic, political, and military power and its significance will continue to increase. At the same time, access to much of this information is becoming available to potential enemies.

The 1999 Summer Study Task Force was asked to examine these dramatic changes and their impact on the Department over the next two decades. Specifically, the task force was asked to<sup>1</sup>

- Review and consider the broad spectrum of topics which were addressed in the 1990 DSB summer study
- Address 21<sup>st</sup> century intelligence needs and adversaries
- Expand and build on the recommendations for technologies, operational capabilities, and force characteristics developed in the 1998 DSB summer study
- Examine the need for and use of all forms of information to achieve full spectrum dominance
- Examine defense technology strategy, management, and acquisition

Over the past several years the DSB has been asked to pay special attention to resources, particularly the resource trade-off necessary to pursue its recommendations. To address this question, the task force reviewed the Department’s implementation of recommendations from the 1996 DSB summer study, *Achieving an Innovative Support Structure to Enhance Early 21<sup>st</sup> Century Military Operations*. In this review, the task force focused on identifying recommendations that have not been aggressively pursued by the Department but which could result in substantial savings in the business side of DoD operations.

Two other aspects of this study are worthy of special note. The task force spent a considerable amount of time analyzing incentives, particularly incentives that would allow the Department to accelerate the transformation to meet the new challenges of the 21<sup>st</sup> century. The task force also evaluated the disincentives that would prevent more rapid implementation. This report contains recommendations derived from these evaluations and which the task force believes are important to motivate change.

---

<sup>1</sup> The complete Terms of Reference for the Defense Science Board 1999 Summer Study Task Force on *21<sup>st</sup> Century Defense Technology Strategies* is in Annex A.

In addition, the task force paid special attention to the transformation required of the intelligence community in order to accomplish joint-rapid response operations. Although this community includes elements outside the jurisdiction of the Department of Defense, the task force concluded that, *unless transformation of the intelligence community takes place along with transformation of DoD*, it will be difficult to achieve the desired National Security outcomes of the 21<sup>st</sup> century.

The 1999 summer study was organized around four task forces that addressed the facets of defense technology strategy shown in Figure 1.<sup>2</sup> This volume presents an overview of the findings of the summer study, integrating the work of the four task forces. Volume II of this report contains more detailed information on individual task force results, findings, and conclusions.

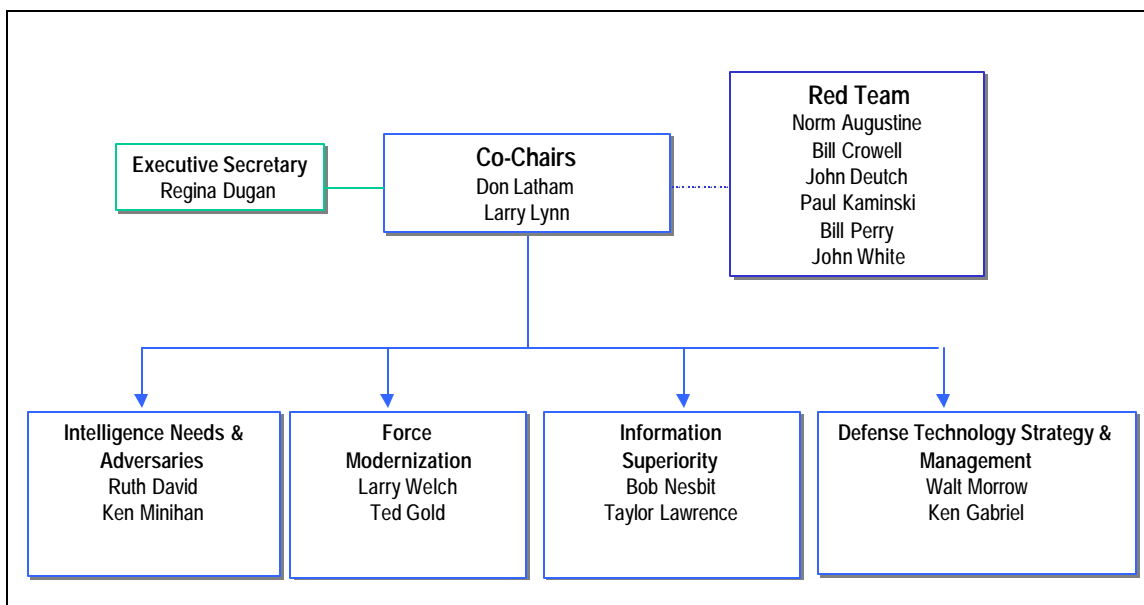


Figure 1. Task Force Organization

## THE 1990 DSB SUMMER STUDY

The 1990 DSB summer study had a broad Terms of Reference, specifically:

*“What should be the DoD’s technology strategy and thrust in the 1990s to meet the challenge of the next two decades?”*

In 1990, the Department of Defense faced a significantly different national security environment than it had during the Cold War. A new world was beginning to emerge after the collapse of communism. Also emerging was an increasingly multi-polar security environment with shifting allegiances as well as a reordering of economic and industrial relationships. The

<sup>2</sup> Annex B contains a complete list of the members of the 1999 Summer Study Task Force.

collapse of the Soviet Union led to a perception by some that the United States did not need as large a defense budget as it enjoyed during the Cold War. While the central Soviet Union and Warsaw Pact threat seemed to dissipate, many persisting regional threats were growing and the United States was taking on a more active role.

For many decades, the Department of Defense had planned its budget around a set of cold war scenarios, with the most demanding being a high intensity war with the Soviet Union and its surrogates. The 1990 study found that DoD needed to look at alternative futures to drive its planning. The Department was urged to take this historic opportunity to shape U.S. capabilities to deal with the most likely future. In addition, the task force recommended efforts to establish the groundwork for responding to the potential for a “peer” threat to emerge in the future. In order to accomplish these objectives, the Department needed to look at changing the intelligence community, refocusing the nation’s nuclear modernization programs, and developing defense concepts around a light and more flexible strategic force.

The 1990 task force identified a need for DoD to focus its tactical force development on then-apparent trends in developing nations, particularly the increasing proliferation of high technology capabilities around the world. Because such proliferation was, and still is, occurring widely, U.S. forces faced an uncertain future environment. Among the most important U.S. force enhancements recommended were

- Continuous, real time surveillance for regional to local commanders
- Capabilities to conduct precision strikes at long range with no collateral damage and no losses
- Greatly improved force defenses, especially defenses for ships against infrared guided missile threats
- Rapidly deployable forces that are also highly capable on arrival against sophisticated threats
- Anti-submarine warfare to deal with third world submarines
- Less manpower-intensive, more reliable and less logistically demanding systems
- Anti-tactical ballistic missile capability

Other findings of the 1990 summer study include:

- Stealth and counter-stealth were major developments over the previous two decades and would be an urgent continuing requirement for a variety of applications in the coming decade
- DoD needs a different technology investment strategy, one that systematically ties military needs to capabilities and capability priorities to resource priorities
- Major changes are needed in technology transfer policies and management, with the objective of providing stronger controls over fewer technologies and incorporating third world proliferation concerns
- DoD needs to protect science and technology base funding even if defense budgets decline

In this report, the 1990 task force also outlined many challenges for DoD including:

- A smaller budget, which dictates discipline in the Department's attempt to identify where budget increases could be offset by reductions
- A defense industrial base that will become smaller than it is in 1990
- Smaller procurement quantities and fewer new program starts
- A force inventory that is growing older and needs to be selectively upgraded
- Technology that is advancing at a rapidly growing pace and will continue to do so on a global basis, with both friends and adversaries having greater access to advanced technology

The 1999 Summer Study Task Force believes many of the principal findings of the 1990 summer study remain relevant today. Further, many of the concerns raised about the 21<sup>st</sup> century environment from the 1990 study have not yet been fully addressed by DoD. The following table provides a list of the specific recommendations made in 1990 along with a qualitative assessment of the status of implementation and impact, if any, on the Department.

As shown in this table, the Department has made considerable progress in implementing many of the 1990 recommendations. Compared to a decade ago, there is more emphasis on transforming the Department and its varied activities to meet the demands of an evolving security environment. DoD is more focused on responding to national security situations across the globe that range from peacekeeping to contingency operations while, at the same time, preparing for the potential of a major theater war.<sup>3</sup> Today, the Department's priorities include:

- Joint, rapid, and potent response capabilities supporting the range of contingency operations
- Preparing responses to threats, both to the homeland as well as deployed forces, from the use of weapons of mass destruction and information warfare
- Detering and preparing for the re-emergence of a peer competitor

The 1999 task force placed its emphasis on the capabilities, technology, and funding associated with the first of these three priorities – developing joint rapid response capabilities. The following chapters discuss the findings and recommendations of this study.

---

<sup>3</sup> It is interesting to note that approximately one week after the 1990 summer study concluded, Iraq invaded Kuwait, and Desert Storm followed months later.

Recommendation	Action	Impact
1. Establish a “CEO” for technology, with responsibility to develop and implement a research and development (R&D) strategy that responds to a future characterized by lower budgets, fewer opportunities for new program starts, and more uncertainty about future adversaries.	Re-established DDR&E	Uncertain
<ul style="list-style-type: none"> <li>a. Establish a fast-track initiative with the intent of: 1) fielding many more components and systems quickly to stimulate real world use and feedback, and 2) retaining critical design teams that would otherwise be lost with fewer new program starts: <ul style="list-style-type: none"> <li>▪ Identify a few candidate systems and assign a single individual to establish the fast-track process.</li> </ul> </li> </ul>	Initiated Advanced Concept Technology Demonstration (ACTDs)	Many Successes such as Global Hawk and Predator Unmanned Aerial Vehicles (UAVs)
<ul style="list-style-type: none"> <li>b. Place special emphasis on technology insertion to upgrade performance and keep old platforms current: <ul style="list-style-type: none"> <li>▪ Ensure that acquisition regulations give preference to upgrading existing platforms/major systems.</li> <li>▪ Require that breakthrough/leap-frog capability be demonstrated (primarily from prior fieldable prototypes) before approving major system new starts.</li> </ul> </li> </ul>	Initiated Preplanned Product Improvements	Many Successes Such as M1 to M1A2
<ul style="list-style-type: none"> <li>c. Maintain ability to generate new technology: <ul style="list-style-type: none"> <li>▪ Implement a scenario-based methodology to objectively allocate funds to core and critical technologies.</li> <li>▪ Assure needed science and technology funding, including independent research and development (IR&amp;D).</li> </ul> </li> </ul>	Established Elaborate Science and Technology Planning Process	Too Much Paper Planning
<ul style="list-style-type: none"> <li>d. Exploit civil technology for defense purposes: <ul style="list-style-type: none"> <li>▪ Remove barriers to the DoD use of off-the-shelf civilian technology and advocate its use;</li> <li>▪ Establish criteria for identifying critical defense industry technologies and advocate its use;</li> </ul> </li> </ul>	Aggressive Technology Reinvestment Program & Dual-Use Program	Many Successes such as the new attack submarine fire control system
<ul style="list-style-type: none"> <li>e. Develop the means to produce small quantities of hardware efficiently, while preserving surge potential: <ul style="list-style-type: none"> <li>▪ Identify several prototype initiatives and assign responsibility;</li> <li>▪ Increase resources and management attention devoted to manufacturing technology, and encourage the use of IR&amp;D resources in this area.</li> </ul> </li> </ul>	No Specific Action	None
2. Recognize the significance of stealth/counterstealth technology as one of the major breakthroughs of this quarter century: <ul style="list-style-type: none"> <li>▪ Take full advantage of low observable technology and make modifications where possible to give U.S. forces both offensive and defensive edges;</li> <li>▪ Give high priority to counterstealth in view of the proliferation of low observable technology.</li> </ul>	Continued Emphasis	Operational Successes such as F-117 and B-2
3. Ease of deployability should be a major criterion for all tactical systems: <ul style="list-style-type: none"> <li>▪ Demonstrating system/lift compatibility should be mandatory, and highly capable light forces should be deployed to complement heavy forces.</li> </ul>	Some Change in Emphasis – C-17 Fielded	Little Impact So Far
4. Re-orient strategic programs and continue force modernization to meet the challenge of the restructured world – numerically reduced U.S./Soviet forces, increasing Third World nuclear threat: <ul style="list-style-type: none"> <li>▪ Create more flexibility in planning the use of strategic forces;</li> <li>▪ Maintain the triad for the foreseeable future but with single reentry vehicle silo-based replacement for Minutemen II (preserve R&amp;D options for a mobile intelligence community ballistic missile);</li> <li>▪ Develop a strategic defense option effective against small attacks (tens of warheads),and seek allied participation;</li> <li>▪ Develop new nuclear weapons that are safe and reliable in a low or no-test environment.</li> </ul>	Area of Major Emphasis	National Missile Defense Program  START II  No new nuclear weapons development
5. Reprioritize intelligence needs and resources guided by the following principles: strengthening the ability to provide worldwide intelligence; and, seeking more efficiency and productivity in the worldwide intelligence workforce. <ul style="list-style-type: none"> <li>• Use an integrated military-civilian intelligence “reserve force.”</li> </ul>	Continuous Re-Thinking in the ‘90s Toward This End	Significant Issues Remain
6. The Department of Defense should initiate policies to attract and retain the most capable people available to provide the underpinnings for the above recommendations.	No Significant Progress	Area of Even Greater Concern Today





---

# CHAPTER 2. JOINT RAPID RESPONSE OPERATIONS

## OPERATIONAL AND THREAT ENVIRONMENT

Coping with challenges of the 21<sup>st</sup> century security environment requires unprecedented change in the Department of Defense. U.S. military forces will likely face increasingly complex contingency operations. Future adversaries are expected to be less predictable and thus more challenging through their use of asymmetric approaches to combat, more urban and civilian intermixing, uncertain warning, preparation and conflict termination time of their choosing, and different and challenging geographies. Most contingencies will occur at great distance from U.S. shores, but there will be fewer permanent bases of operations in overseas areas for U. S. forces. The deterrent impact of nuclear weapons will be less certain against many of the nation states that might be adversaries in future contingencies and is likely to be ineffective against non-state actors.

The situation on the international scene is further complicated by U.S. domestic attitudes. Combat is shrouded by an aversion to casualties – military and civilian, friendly and adversary – an aversion to collateral damages, a sensitivity to world opinion, and an aversion to prolonged conflict.

During the past decade, U.S. forces have participated in a host of regional operations, most often in conjunction with coalition forces. These operations have required a variety of responses, including combat, peacekeeping, and humanitarian. Deployments have become typical and currently include the following:

- ~7,000 Americans patrol sector of Kosovo as part of NATO-led multinational force
- 7,700 manage relief for refugees in Albania and Macedonia
- 5,916 participate in a NATO-led multinational force separating factions from Bosnia's civil war, which ended in 1995
- 5,760 provide relief following Hurricane Mitch and work to stop drug trafficking
- 270 help a multinational force keep peace in Haiti
- 21,000 patrol southern "no flight" zones; 1,200 patrol northern "no flight" zone over Iraq
- 870 serve in a multinational observer force monitoring peace between Egypt and Israel
- Many special forces personnel deploy globally every day

These examples illustrate the variety and frequency of operations in which the United States is involved and which are expected to continue into the next century. Thus the central challenge for DoD becomes to

*Transition to military capabilities that underwrite the future vision with no breathing space in the demand for use of current capabilities.*

In response to the changing security environment, the Department of Defense must and is moving beyond the simpler, scenario- and threat-based force of the Cold War era, where containment was the concern and contingencies were handled as included demands. Today, DoD's forces are in a period of transition, as Figure 2 illustrates. The force guidance evolved from the Base Force that was intended to bridge the gap from the Cold War to the emerging world to a force guidance for two major regional conflicts (MRCs). But as the Department anticipates fewer wars, yet more conflict confronting adaptive enemies, there is a need for a capabilities-based approach that provides a high probability of success across a very broad spectrum of contingencies.

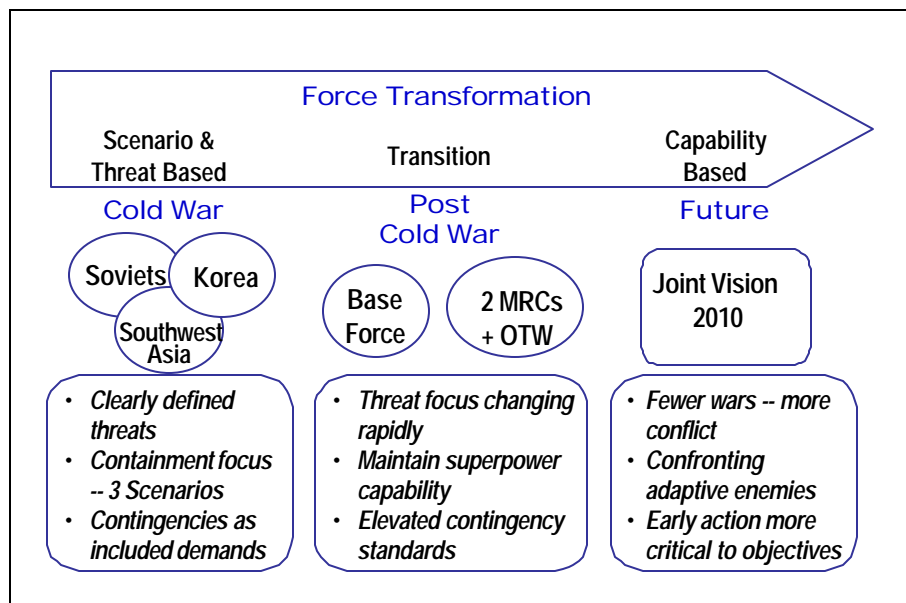


Figure 2. Force Transformation

Still, the Department moves toward the future carrying with it the "burden" of success from Desert Storm. Figure 3 illustrates some of the features of the coalition force engagement in Operation Desert Storm and the context for achieving success against the forces of Saddam Hussein. The success of Desert Storm has set a level of expectation that "adaptive enemies" can, do, and will continue to exploit.

Such an enemy goes beyond the asymmetric adversary; the challenge will come from responsive, smart and adaptive adversaries. The adaptive enemy has, in military history, exhibited all of the traits noted below – with the sole exception (so far) of using chemical and biological weapons to deny operations of key facilities such as ports, airfields, and staging bases. However, it was over a decade ago that Iraq used chemical and biological weapons on defenseless civilians. Some salient features and culture of an "adaptive enemy" are

- Time, will, and the power of the defensive
- Patience: swift success is not essential to ultimate victory – a prolonged stalemate equals victory
- Willingness to maintain or sacrifice an army in the field at all costs, even in the face of the most damaging punishment

- Ability to interfere with an intruding power’s intention to end the conflict quickly and at minimum “cost”
- Willingness to use chemical and biological weapons to degrade and deny operations of key facilities such as ports, airfields, and staging bases or against civilian targets such as Iraq did against the Kurds
- Seeks local successes by taking apart a “string of pearls,” one “pearl” at a time
- Initiative to strike at the time and place of its choosing and to effectively use concealment, decoys, and deception
- No longer geographically anchored

<u>Features</u>	<u>Context</u>
Air supremacy	... <i>over an inept adversary</i>
Clear view of the battlespace	... <i>in unimpaired desert terrain</i>
Lethal precision weapons	... <i>enough for critical target set</i>
Unchallenged C <sup>3</sup>	... <i>no adversary capability</i>
An enemy without ISR	... <i>could not maneuver to see</i>
Non-adaptive enemy	... <i>did not anticipate US response</i>

**These features have set levels of expectations that adaptive enemies can, do, and will exploit**

*Figure 3. Desert Storm: The Burden of Success*

This is the operational environment that DoD faces. It is an environment that is rapidly changing and that will require varied and flexible response from U.S. forces. Transforming the force to one with the envisioned future capabilities in a period of high operational tempo will be challenging. But the Department can meet this challenge by focusing its transformation on critical capability requirements and starting now to transform the force in increments.

## TRANSFORMING *JOINT VISION 2010* AND BEYOND

*Joint Vision 2010* provides a guiding vision for modernizing America’s armed forces as the United States enters the 21<sup>st</sup> century. It sets a high standard for the four military Services – to be persuasive in peace, decisive in war, and preeminent in any form of operation across the full spectrum of conflict. To achieve the vision of a “preeminent joint force” as embodied in *Joint Vision 2010*, the Department must have the capability to deploy rapidly with high lethality, achieve decision superiority, and support deployed forces with efficient logistics. This force must be able to operate in a fully integrated, joint, or combined manner and ensure full spectrum dominance.

Despite the dedicated efforts of the individual Services to enhance the combat and quick-reaction capabilities of the military forces, there are still gaps in the effectiveness of these efforts, particularly in joint operations. The Department of Defense needs a way to focus its transformation to a 21<sup>st</sup> century force amid the high operational tempo that is likely to continue in the future.

*A useful framework to focus and transform Joint Vision 2010 and beyond is a full-spectrum joint rapid response operations capability.* As shown in Figure 4, such a capability draws on many important enablers that are embodied in the pillars of *Joint Vision 2010*. This study examines three in particular – strategic agility, information for decision superiority, and force protection – and also identifies key initiatives necessary to “make it happen.” A new and enhanced rapid response operations capability will provide a focal point for both new and ongoing efforts that will lead to a force able to meet the full spectrum of future contingencies.

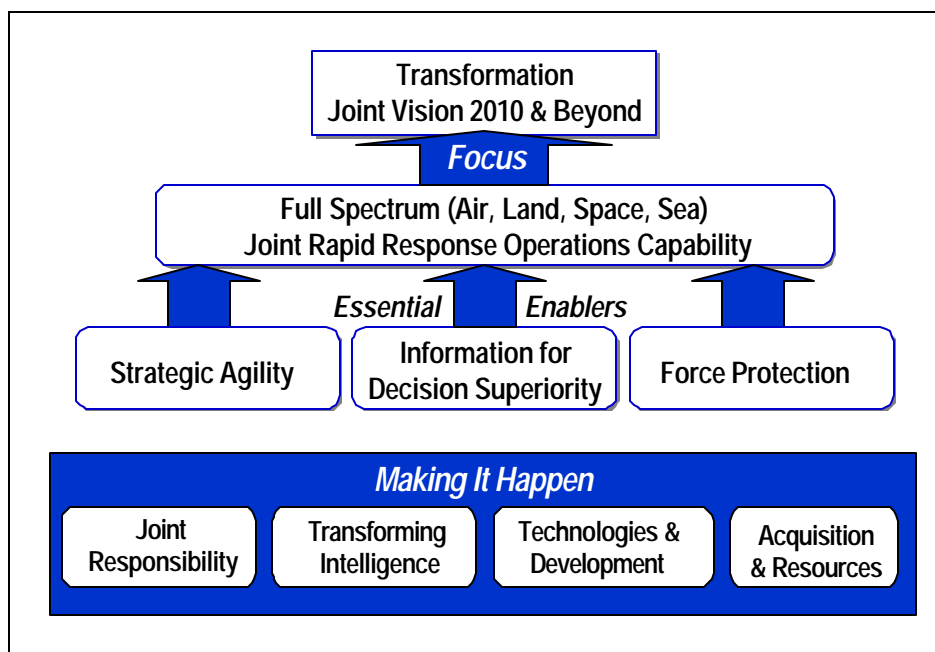


Figure 4. Supporting Transformation

## JOINT RAPID RESPONSE OPERATIONS CAPABILITY

A joint rapid response operations capability, as both a warfighting capability and a strategic deterrent, is a critical need for the Department of Defense. With enough time and warning, the United States can build a joint force that can do almost anything required, as shown on the right side of Figure 5. In addition, the United States already has a rapid response capability in some of its forces that can respond effectively to certain requirements, especially in support of smaller contingency operations, as demonstrated in Panama, Haiti, and Grenada operations. But when the combat requirement calls for a more capable and potent force that is needed fast – that is within 24 to 96 hours – there is a gap in existing military force capabilities, as shown in Figure 5.

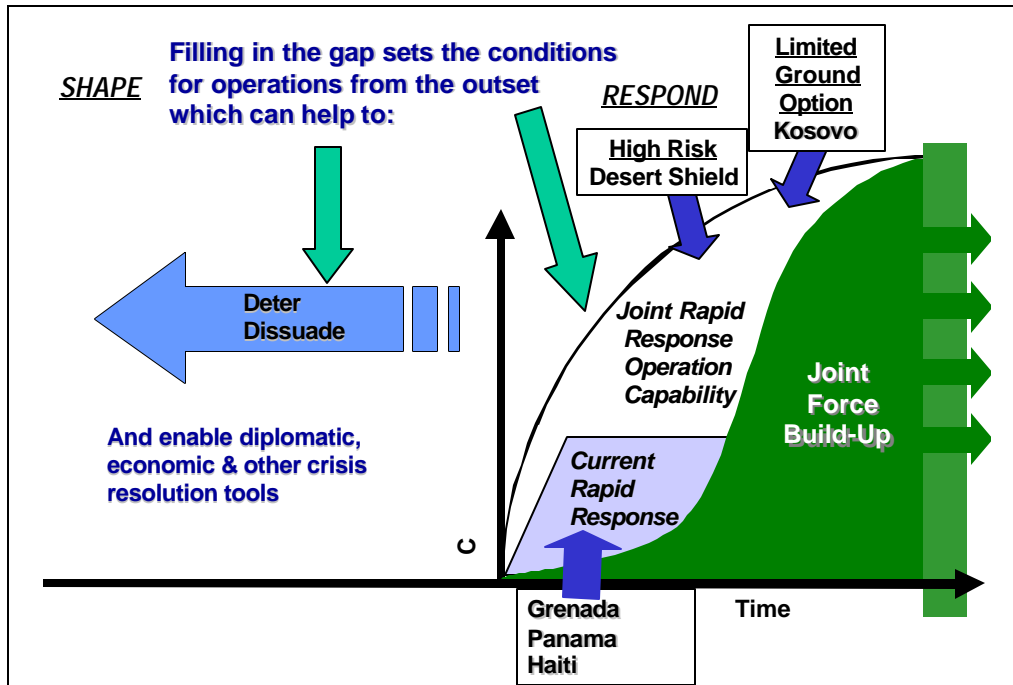


Figure 5. Joint Rapid Response Operations Capability – The Strategic View

Several examples illustrate the point. During Operation Desert Shield, the United States had to respond quickly even without the needed potent, joint rapid response forces. To manage this scenario, the United States took a high-risk approach by sending in light forces that were perceived to be inadequate to meet the adversary's ground forces challenge. This approach was then referred to as a "speed bump" for Iraqi armor, in the event that Iraqi forces had advanced into Saudi Arabia. In the case of the Kosovo operation – setting aside the political issues of whether or not to use ground forces – the United States did not have an adequate rapid response ground capability able to set the conditions of ground operations before Milosevic's forces were able to do so. In this case, the National Command Authority was without a viable, sufficiently rapid response and potent ground force option. A joint rapid response operations capability is intended to fill the gap in U.S. response options, enabling the United States to set the conditions of operations from the outset, rather than responding to conditions already set in place by an adversary.

Furthermore, possessing such a capability, and a demonstrated will to use it, has strategic value as a deterrent against potential aggressors. A rapid response capability can provide a stabilizing influence prior to conflict and help to shape the strategic environment. During the pre-conflict phase of an operation, the existence of the force can buy the U.S. command authorities critical time for negotiations, analysis, and assessments. Such a force could deter and dissuade adversaries from commencing operations and could also add power to other crisis resolution tools, including diplomatic, economic and political responses.

Providing time for the National Command Authority to use appropriate non-military measures to influence a crisis environment is important and, in some cases, could reduce or eliminate the need for committing military forces.

Moreover, having time to prepare for coalition involvement in contingency operations – particularly achieving intra- and inter-nation consensus – without being forced into a premature commitment of forces can be beneficial and stabilizing.

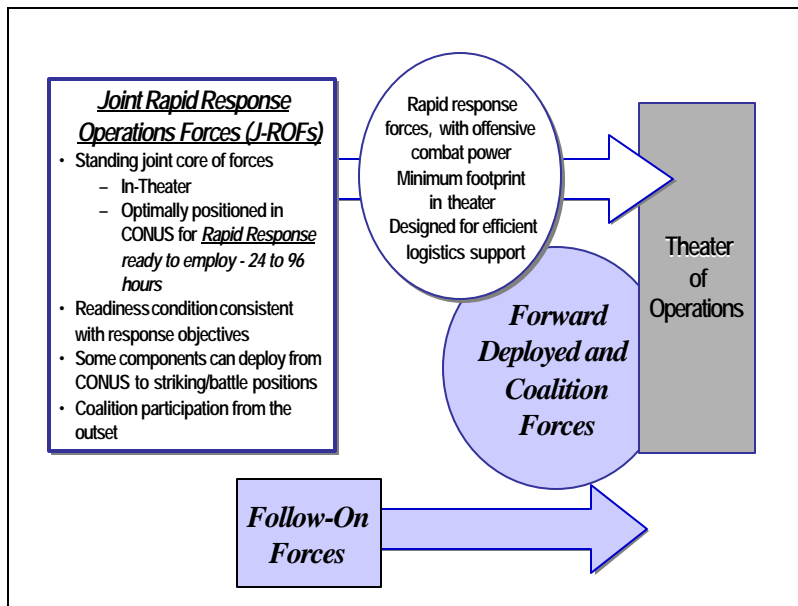


Figure 6. J-ROF Concept of Operations

The concept of operations for employing joint rapid response operations capabilities is illustrated in Figure 6. These forces are to provide rapid response with offensive combat power but

minimum footprint in-theater, and they will be designed for efficient logistics support. But they will also be used in conjunction with forward deployed and coalition forces. Follow-on forces are likely to be heavier for some time to come but will also be more lethal and robust. Over time, as transformation continues and expands, more lethal and robust follow-on forces will exhibit much the same responsiveness as the initial rapid response force. The objective is an early capability to both defend and take the offense, both of which are important in securing early conflict resolution and termination.

Several parameters are essential to support this concept of operations. These parameters are also key to achieving the desired goals of deterrence, stability in the pre-conflict environment, and a rapid and decisive win if conflict occurs. The rapid response capability requires forces that are able to

- Effectively move into the theater of operations utilizing both **military and commercial strategic lift** assets in 24 to 96 hours
- **Enter immediately into combat operations** once deployed in theater
- Operate independently of large vulnerable overseas bases and ports by achieving **assured access** to the theater through austere ports and airfields
- Move rapidly throughout the theater of operations by air and land to ensure a high degree of **battlespace mobility**
- Provide **increased lethality for early deployment elements** of the force, employing combined arms capability
- Operate in a manner which achieves full **coalition integration** in all phases of the operation

- Access improved intelligence and joint inter-operable command and control using the **Integrated Information Infrastructure**
- Deploy both **overt and covert sensors systems**, some of which are deployed before forces are committed
- **Use tailored logistics** support to ensure that operations and logistics function as fully integrated elements in force execution
- **Maximize survivability** of all forces throughout all phases of operations

It is necessary to enhance current force capabilities in these areas to achieve a joint rapid response operations capability.

While the military need for a joint rapid response capability is the subject of this discussion, it is important to note that this capability builds on existing Service concepts. The Army Strike Force, Army After Next, the Navy's *Forward from the Sea*, the Air Expeditionary Force, and the U.S. Marine Corps' *Operational Maneuver From the Sea* are examples of Service concepts that reflect evolution to a capability-based force with more joint consideration. All of these concepts share common themes that include the following: battlespace awareness, distributed operations, split basing and reach back to the continental United States to reduce presence ashore, use of remote fires, precision engagement, lean logistics, and agile forces that can rapidly reach the theater and rapidly move around the battlespace. Further, these concepts rely on survival through knowledge and agility, not on an ability to absorb hits.

Developing the joint rapid response operations capability would lead to the creation, in several years, of Joint Rapid Response Operations Forces with characteristics that are different from today's light or heavy forces. The J-ROF will be a modular, building-block-type capability that will provide DoD with a flexible set of force concepts and capabilities that can be reconfigured as required. *Flexibility is essential since force requirements demanded by the future strategic environment cannot be met by a one-size-fits-all force.* As DoD experiments with, trains, and builds J-ROFs to deal with various types of contingencies, new force concepts and capabilities will evolve.

Figure 7 illustrates conceptually how the DoD might build such a capability, beginning with an experimental joint rapid response operations headquarters in the near term which conducts a series of limited operational experiments to evolve force concepts and characteristics for the J-ROFs. In the mid-term an experimental set of forces would evolve into deployable forces, which, over the longer-term, would be propagated throughout U.S. and coalition forces. Throughout this evolution, experimentation will continue to mature operational concepts and force characteristics of the J-ROF. Thus, the J-ROF will serve as a focus for bringing emerging Service concepts into a joint, interdependent force with interfaces built in for operation with coalition forces.



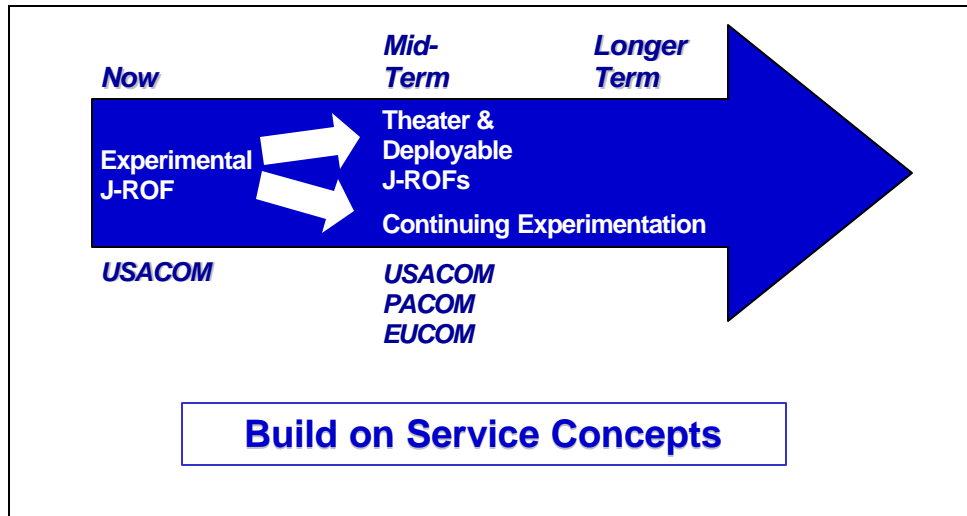


Figure 7. Transforming Capabilities

### Force Characteristics

Some capabilities and characteristics of the J-ROF are shown in Figure 8. The force, as envisioned, will be rapidly deployable and able to arrive in a battlespace, anywhere in the world,

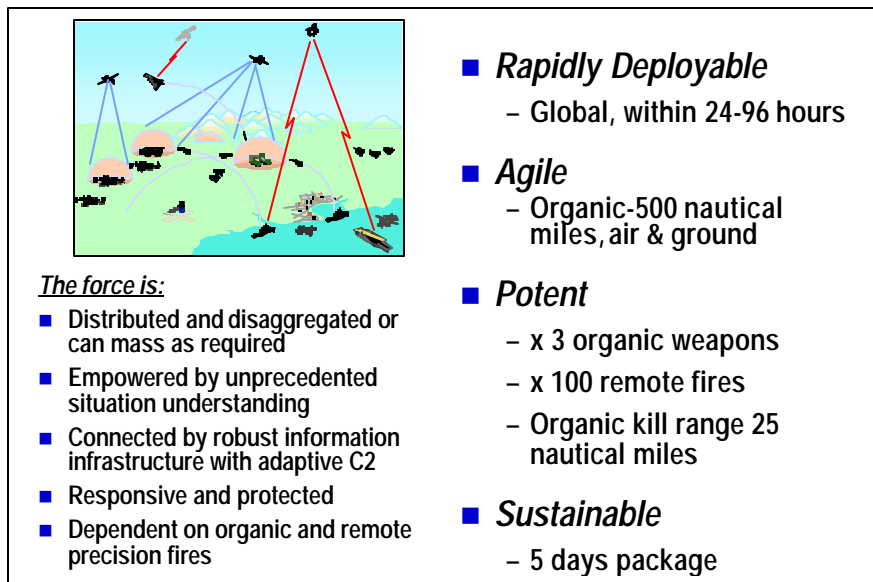


Figure 8. J-ROF Characteristics

within 24 to 96 hours of receiving notice. The J-ROF will be task-organized and have a self-deployable aviation element. These air, ground, sea and space combined arms forces will not depend on major ports and airfields for theater entry. This force will have organic tactical mobility with both air and ground force mobility at ranges up to 500 nautical miles. The force will be self-sustaining for five days in theater with its own sustainment package, which

can be augmented with air-delivered package resupply for additional days if required. Of great importance will be the combat-to-tail ratio of the force – the ratio of combat warriors to support personnel. Today, light forces have a ratio of 4 to 6 and heavy forces a ratio of about 1 to 14. The goal for the J-ROF is 8 to 2. This force will be able to fight in a distributed and desegregated mode, but will be able to re-mass if necessary. The Joint Rapid Response Operations Forces will be responsive and protected and depend on both organic and remote precision fires. These forces, with proper training, will be able to fight in any terrain – open or closed, forest or urban. Finally,

this diverse mix of capabilities will be affordable – its cost should not exceed that of comparably sized forces today.

The J-ROF will have dramatically enhanced weapons lethality. It will be a potent force that will offer significant capability improvement over current U.S. forces in organic weapons, effectiveness of remote fires, and organic kill range.<sup>4</sup> The J-ROF will have a very low profile, with a goal of 10 times improvement in signature – stealth and emissions – by the 2010 to 2015 timeframe.

Systems to support organic mobility will include self-deploying vertical/short takeoff and landing aircraft with ranges of 500 nautical miles and advanced ground mobility vehicles that weigh less than 5000 pounds. These systems will be able to be transported internally in intra-theater aircraft or sling-lifted by helicopter. A J-ROF may have to fight in urban terrain, so attention must be paid to how this force is equipped and trained to fight in such a setting. For example, in urban warfare, a J-ROF might carry a family of assets to provide individual mobility, such as horizontal, vertical, or individual lift up to 40 stories and out to ranges of a half nautical mile.

For tactical mobility and intra-theater lift, the J-ROF will draw on capabilities recommended in the 1998 Defense Science Board summer study, *Joint Operations Superiority in the 21<sup>st</sup> Century*, as illustrated in Figure 9. These include new Maritime Prepositioned Force ships, which should replace current ones by 2010; Super Short Take-Off and Landing (SSTOL) aircraft; very high-speed Fast Shuttle Sealift; and hybrid electric vehicles for ground transport. These capabilities will enable the force to maneuver in more demanding terrain, in areas without access to major ports, and in areas with only short runway space, which will allow a very different way of inserting and sustaining the force. Many of these initiatives are well underway today and are important to the J-ROF concept.

To enable unprecedented situational understanding, any deployed force must have access to a rich menu of sensor systems and sophisticated processing. A J-ROF will be equipped with a distributed network of airborne and ground sensor systems that, in combination with access to all-source information systems, will provide enhanced situational awareness and enable the lethality of the force. Sensor management and handling of the array of sensor information will be supported by the Integrated Information Infrastructure, described in the next chapter. Urban sensor systems will be used to detect and locate people in buildings, halls, stairs and sewers. The sensors may number in the hundreds or the thousands for a single operation and will be delivered by several means. On some missions, for example, a Tactical Tomahawk could be loaded with sensors that are very accurately dispersed throughout the battlespace.

---

<sup>4</sup> Volume II includes a chapter describing analytic work and simulation analysis on the operational impact of organic and remote fires.

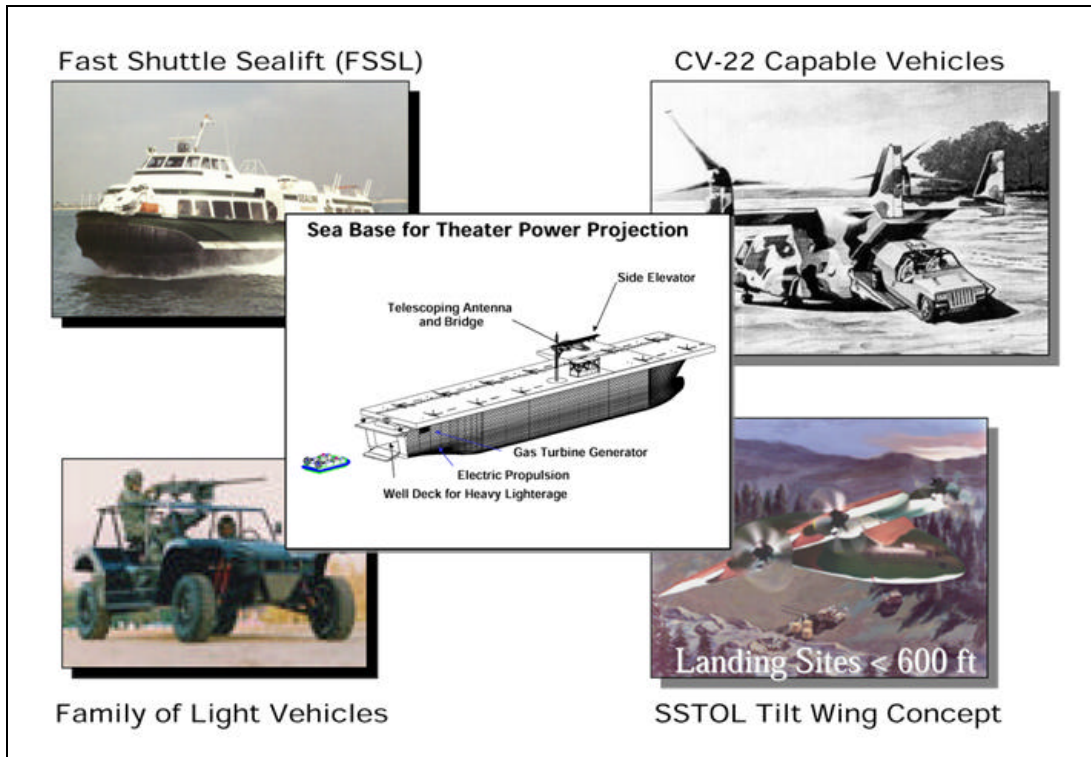


Figure 9. Tactical Mobility and Intra-Theater Lift

The ability to “see” and kill anything within a 250 nautical mile “tactical bubble” is an operational goal, which can be supported by tactical unmanned aerial vehicles under the control of each J-ROF commander. Thus, multi-sensor-equipped UAV systems will be needed in a variety of environments to perform a range of surveillance and targeting missions as well as enable new capabilities including precision strike and communications relay. Eventually, UAVs will serve as a weapon carrier. Systems like Global Hawk, with a ground moving target indication radar capability, and the joint, interoperable Tactical Control System, which is a common control system for all UAVs, will contribute to realizing extended UAV capabilities that are supported by this study. In addition, the Department needs to support initiatives in the Army, Navy, and Marine Corps to acquire tactical UAVs. The development work on micro-UAV technology should also be continued. And, finally, an assessment needs to be performed to determine whether additional assets are required, such as a stealthy, high-altitude, long-range system; a low-cost, high-speed, under-the-clouds penetrator; a long-range vertical take-off and landing (VTOL) system for combat search and rescue and dispersed unit support; and a heavy-lift sustainment VTOL system such as the Defense Advanced Research Projects Agency (DARPA) Hummingbird concept. Integrating more UAVs into the force will strengthen J-ROF capabilities and is a concept recently advocated by the Secretary of Defense.

## Implementation

To implement the Joint Rapid Response Operations Force concept, the Department needs to embrace this approach in policy and commit sufficient resources for the long-term, including well-trained people. Figure 10 indicates at least six steps or actions necessary to implement this capability, some of which transcend the Department of Defense. Overall, implementing the J-ROF concept will be a complicated, multi-year effort.

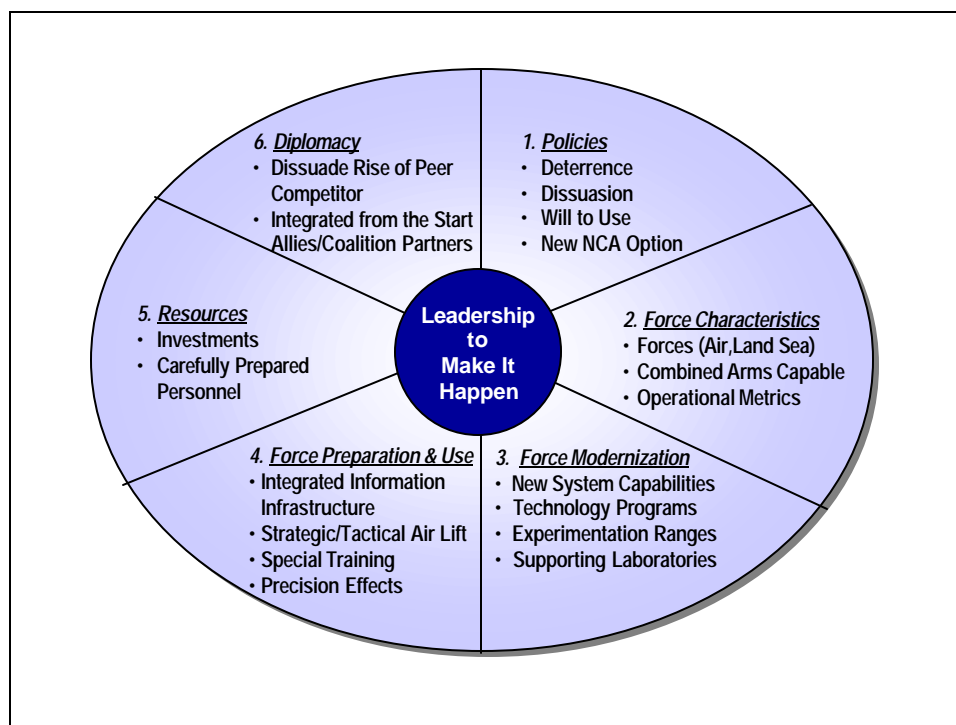


Figure 10. Implementing the J-ROF Concept

**Coalition Partners.** A critical element in implementing a truly effective rapid response operations capability is integrating coalition partners. Today, the expectation for coalition operations is high. Yet, militarily a rapid response operations capability could reduce coalition participation without a more aggressive approach to integrating coalition partners early. To avoid this dichotomy, the United States must begin to work more closely and on a regular basis with potential coalition partners, prior to decisions to deploy.

Coalition partners need to be engaged in many areas, and in some cases with direct assistance in affordably modernizing their force capabilities, particularly C<sup>4</sup>ISR systems. New roles and responsibilities need to be defined. These might include shared air and missile defense; dealing with the realities of weapons of mass destruction; interoperability of systems, especially command, control, and communications; sharing technology, systems, and military capabilities such as C<sup>4</sup>ISR; and shared intelligence, surveillance, and reconnaissance.

The rapid response environment means that today's ad hoc approach to integrating coalition forces and systems will no longer be sufficient. Instead, serious and continuous experimentation by military and non-military units in pre-contingency training teams with coalition partners is

needed. Communication practices, frequencies, and control; information system protocols and access security; and logistics roles, modes, and packaging all need to be planned and exercised. Otherwise, the U.S. rapid response force could have to operate alone, at least initially – a situation that would require clear policy guidance should it arise. United States Joint Forces Command faces a considerable challenge in involving coalition partners, as appropriate, and in integrating the joint, combined force into a capable military entity.<sup>5</sup>

***Experimentation.*** In addition to being a vehicle to integrate coalition partners into the J-ROF implementation process, experimentation will be important for testing and developing force concepts and capabilities. ***After concept development and planning are mature, the Department should establish a permanent, experimental joint rapid response operations headquarters under USJFCOM.*** This is a natural role for the Joint Forces Commander, who also has responsibility as force provider and for joint experimentation. The JFC Service components would provide the operational forces for each experiment, with the force structure being tailored to the design of the experiment.

The experimentation process should include developing and executing a series of short-duration, discrete, limited-objective experiments as well as an annual large-scale culmination experiment. A spectrum of limited-objective experiments could include operations such as standing-up a command element in less than 6 hours; standing-up the C<sup>4</sup>ISR system and linking it with all force elements within one hour; a ground and air operational maneuver experiment in which a force (1000 personnel and equipment) would be transported 1000 miles in less than 24 hours; a strategic maneuver experiment that entails moving 8000 miles in less than 24 hours; and an other-than-war response experiment, in which the force deploys, feeds and evacuates 1000 people in 24 hours. A notional annual experiment might combine some of these limited experiments and include deploying and seizing an urban center 5000 miles distant in less than 48 hours.

A set of notional implementation milestones is shown in Figure 11. Within the next year, USJFCOM, directed by the CJCS, could begin to develop concepts for these experiments, including participation from NATO and other coalition partners as appropriate. This planning phase would be completed in 9 to 12 months. In the 2000-2001 timeframe, the experimental headquarters for the J-ROF would be established at USJFCOM. In subsequent years, limited objective experiments would be conducted so that, by 2004, USJFCOM could conduct a major combined/joint integrating experiment. By the end of 2004, the Department would be able to determine how the J-ROF concept would work under certain circumstances, leading to an initial capability available for operational deployment in 2005.

---

<sup>5</sup> As of October 1, 1999, United States Atlantic Command (USACOM) was re-designated as the United States Joint Forces Command.

When	What	Who
1999-2000	Concept development and experimentation plan and design – solicit NATO and other coalition partner inputs	USJFCOM
2000-2001	Stand-up J-ROF (command element experimental)	USJFCOM
2001-2003	Conduct limited objective experiments	USJFCOM
2004	Conduct major combined/joint integrating experiment with the following elements: <ul style="list-style-type: none"> <li>• Deploy overseas</li> <li>• Employ force</li> <li>• Seize objectives</li> <li>• With coalition</li> <li>• Full range of coalition/joint capabilities</li> </ul>	USJFCOM
2005	Initial Operational Capability: J-ROF multiple capabilities	USJFCOM

Figure 11. Notional J-ROF Implementation Milestones

### Thinking Strategically

The full benefit of the joint rapid response operations capability will best be achieved if DoD adopts a basic principle. *Increased joint operations, with increased coalition participation, and employing new and enhanced early entry and sustained combat capabilities, are a warfighting necessity for the 21<sup>st</sup> century.*

Without this capability, the United States and its coalition partners face greater risk of being challenged by potential aggressors on a more frequent basis. The power to deter or reduce such challenges is a key element of the *strategic value* of a rapid response operations capability. A fully integrated, joint and coalition force will have great deterrent power. A key to its deterrence is that the capability be real and that potential adversaries perceive that the United States is willing to use it. Visible exercises employing joint and coalition forces will demonstrate to potential adversaries that the capability is part of the U.S. arsenal – much like the nuclear deterrence capability developed during the Cold War, which remains viable today. Thus, the need for a strategic rapid response capability should be reflected in the Defense Guidance and in the Department’s budget priorities.

This chapter has described the military need and force characteristics for the J-ROF and established an implementation path for reaching an initial capability in the next five years. In order to reach this goal, however, the Department must ensure that the essential enablers are in place.



## CHAPTER 3. ESSENTIAL ENABLERS

The previous chapter described a full spectrum – air, land, space and sea – joint rapid response capability as a focus for transforming *Joint Vision 2010* and beyond. While there are many enablers that contribute to developing such a capability, the task force has chosen to focus on three that are, in its view, the most essential: strategic agility, information for decision superiority, and force protection. They are described in this chapter, with particular emphasis on the first two. The DSB conducted a significant study of force protection in the 1997 summer study.<sup>6</sup> The task force draws from that effort, focusing especially on force protection as it relates to biological warfare issues.

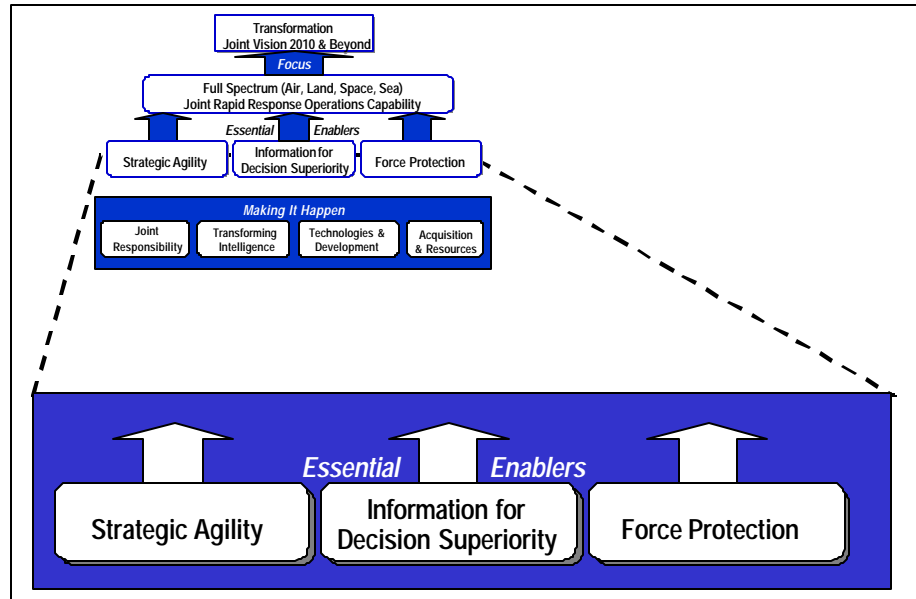


Figure 12: Essential Enablers for Transforming Joint Vision 2010

### STRATEGIC AGILITY

“Strategic agility” is the ability to rapidly move personnel, materiel, and weapons when and to where they are needed and to maneuver them within the battlespace as required.<sup>7</sup> The United States needs a demonstrable capability to insert enough military power fast enough into any region of the world to be a credible conventional deterrent. If deterrence is not successful, U.S. forces need to be able to move into the battlespace before the enemy sets the conditions and those conditions become hard to change. The United States must deal with the more vulnerable aspects of strategic agility – the ports, the airfields, and the infrastructure on which the military currently depends. And the joint and combined forces need a functioning and exercised C<sup>4</sup>ISR capability when a contingency begins.

Achieving strategic agility involves changing major event timelines. Also, there are myriad movement and support issues that are important and need to be resolved. However, solving those

<sup>6</sup> The Defense Science Board 1997 Summer Study Task Force on *DoD Responses to Transnational Threats*, Volume II, Force Protection, October 1997.

<sup>7</sup> Volume II contains an expanded discussion of strategic agility.



concerns alone will not address strategic agility challenges unless the *characteristics* of U.S. forces are also changed.

**The task force concluded that DoD must design strategic agility into future forces from the outset.** In many systems fielded today, the primary focus in development has been on the “performance parameters” of most concern to operations, such as those listed in Figure 13. This is not meant to imply that DoD has not paid attention to logistic issues. However, in many cases, logistics and support concerns have been the purview of a different community – the logistics community – and considered in a separate category from performance parameters and often after the fact. The result of this legacy approach has been to appliqué the “ilities” – moving the system, maintaining it, and supporting it with less materiel – onto already established strategies. Further, considerations of interoperability and interface with the command and control system are often after-the-fact issues. In future systems, the features listed on the right hand side of the figure *all* become performance parameters. **DoD should no longer treat operations as something supported by logistics – rather, operations and logistics must operate as a single entity in the battlespace and in providing capabilities for use in the battlespace. They are inseparable elements.** The term “opergistics” was coined to convey the concept of totally integrated operations and logistics.<sup>8</sup>

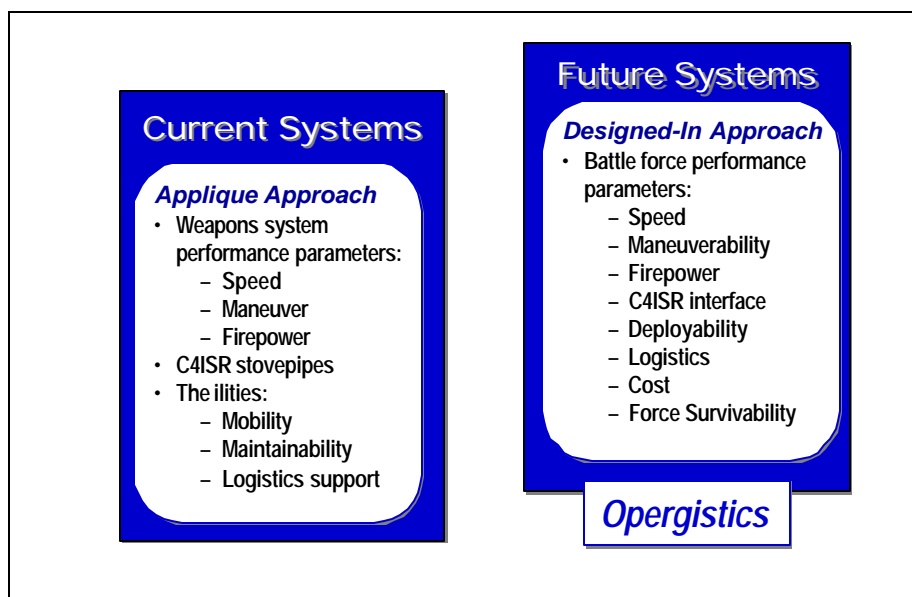


Figure 13. Designing In Strategic Agility

### Enabling Strategic Agility

Enabling strategic agility requires making preparations and arrangements with coalition partners. Effective rapid response operations, in collaboration with coalition partners, require that host nation support agreements be in place in advance of contingency operations. Coalition partners need to be brought into discussions of how to counter weapons of mass destruction, including both intelligence and response issues. The United States should also share theater air

<sup>8</sup> Annex E describes the current logistics system and steps toward achieving more seamless operations and logistics functions.

and missile defense objectives, doctrines, and capabilities with coalition partners in order to develop a joint understanding of each other's capabilities. Other areas that need to be developed with coalition partners include C<sup>4</sup>ISR interoperability, security release procedures for ISR products, and a Civil Reserve Air Fleet (CRAF) concept – especially with the NATO nations, given their extensive commercial airlift capability.<sup>9, 10</sup>

To meet the need for shorter strategic maneuver timelines, significant improvements in integrating operational and logistics plans are necessary. Tools are being developed that can facilitate combined logistics and operational planning, such as the DARPA Advanced Logistics Program (ALP) architecture. This program allows the Department to move from today's planning approach to an environment where execution, monitoring, and planning can occur in real time based on real information – a fundamental change in logistics planning. ALP is now maturing to the point where a tailored logistics plan can be developed in one to two hours based on a detailed operations and deployment plan. The Army Science Board has investigated ALP and endorses this planning tool for use by the Army. The Army might also become the Executive Agent to assist DARPA in transitioning ALP into a Joint Planning Tool.

The development of advanced munitions is another strategic agility enabler. Some of the advanced munitions initiatives now underway will lighten the force while increasing its potency, thereby significantly reducing a major logistics challenge. Small precision bombs, such as a 250- and 500-pound Joint Direct Attack Munition (JDAM), are examples of low cost-per-kill, all-weather, precision weapons. Loiter and in-flight update weapons, such as the Tactical Tomahawk and the Low Cost Autonomous Attack System (LOCAAS), are currently under development as well. Additionally there is a family of anti-armor weapons under development, an example of which is the U.S. Marine Corps' 20 pound shoulder-fired, anti-tank Predator launch-and-leave weapon. Refitting the Predator warhead enables a man-portable wall-breach and bunker-defeat mission capability that can be fired from inside a building.

To help assure safe force insertion without access to large ports and airfields the United States and coalition partners need to be prepared, at least initially, to use austere ports and airfields. This applies to benign environments and to the disrupted- and opposed-entry cases, since the latter two are increasingly likely in the coming years. Two mechanisms are key in operating in such environments. First, the Department needs austere and unpredictable air- and sea-force insertion points, as contrasted with known ports-of-entry and airfields. Secondly, DoD will need to move from the fixed reception, staging, onward movement, and integration (RSOI) process for forces and supplies at large airfields and ports, to an insertion strategy using points that are transient and dispersed.

Forces should be ready to fight upon insertion and to be employed in distributed formations composed of network-centric teams. These smaller teams should be endowed with great lethality, mobility, and multi-faceted survivability and configured to mass fire-effects. The forces should be self-sustaining for a period of time with both organic resources and non-nodal joint logistics capabilities that do not require interior protected logistics lines.

---

<sup>9</sup> In the recent Kosovo Coalition Air Operation, six different security systems were used. These conditions are highly detrimental to effective coalition integration and operations.

<sup>10</sup> An analysis of the airlift challenge is contained in the Army Science Board 1999 Summer Study Report on *Strategic Maneuver*, July 1999, unclassified.

By employing these concepts, DoD builds a system that is much more agile, with supply points much more difficult to locate and target. Materiel could be delivered to unprepared landing areas by a SSTOL or to an unprepared beach using fast-shuttle sealift craft. A key challenge is how to enter through unprepared locations and sustain the force. Sustainment should be viewed as a distributed, “pipeline” function, not one that is based on specific nodes – a concept referred to as “node-less logistics.”

Protecting the movement of systems from the continental United States to entry points abroad is a significant challenge. Some goals for future force movement and sustainment are shown below in Figure 14. To achieve these objectives, the Department needs to take advantage of commercial shipping technology and standards. The task force recommends that DoD adopt containers that conform to commercial and FedEx guidelines. The requirements for rapid strategic entry and operational/tactical mobility suggests that loads with 10-ton and 8 × 8 × 20 foot limitations could maximize use of commercial and military airlift and high-throughput handling.

<b>Air- and Sea-Delivery Objectives</b>	
Benign case (2005)	35 kilometers per day to theater for 10 days starting at C+2
Disrupted/opposed case (2005)	Air deliveries at C+6 of 20 kilometers per day into theater for 10 days through distributed intermediate staging basis to many uncertain entry points at C+3
Benign case (2015-2020)	70 kilometers per day for 10 days starting at C+3
Disrupted/opposed case	40 kilometers per day through intermediate staging basis starting at C+3
High speed surface ship deliveries	10 kilotons per ship start at C+12 (10 kilometers per day for 4 days). DoD and Voluntary Intermodel Service Agreements (VISA) shipping deliveries of 50 kilometers per day at C+20

*Figure 14. Goals for Future Force Movement and Sustainment*

If DoD moves beyond 20-ton loads, use of *the entire* commercial airlift fleet (including 747s) would be lost. Figure 15 quantifies this reality. The right-hand side of the chart shows the status of today’s airlift capability of all types, including commercial aircraft, C-5s, C-130s, C-17s, and the VTOL. A large procurement of commercial airlift is predicted out to the 2015 timeframe to accommodate the rapidly expanding commercial air market. If this expansion occurs, there will be a substantial increase in the availability of commercial air in the 21<sup>st</sup> century. If loads are constrained to approximately 10 tons (top “bar” in the chart), airlift can transport up to 150 kilotons per day. If loads are increased to near 20 tons (second “bar” in the chart), the heavy-lift VTOL can no longer be used in-theater. An advanced, heavy-lift VTOL could be developed. For loads greater than 20-tons, the Department will encounter serious airlift shortfalls unless an unexpected decision is made for a large procurement of C-17s.

DoD should maximize its planned use of commercial air- and sealift assets and prepare to use intermediate staging bases.<sup>11</sup> This approach will help to counter a smart, adaptive adversary who will try to disrupt, delay, and degrade any rapid response efforts. It will also help to provide force protection across all zones of responsibility and to assure access to areas in which the location and time of enemy access are highly uncertain. This approach will transform logistics into a nodeless, distributed system that will help enable rapid and secure global deployments.

The Chairman of the Joint Chiefs recently directed USJFCOM and United States Transportation Command

(TRANSCOM) to become involved in the global deployability problem. The task force recommends a joint USJFCOM/ TRANSCOM effort to lead a design consortium – with participation from the commercial and aerospace industries – to develop a plan and implementation path. The lift and deployment concepts should be evaluated using red teams, experimentation, and exercises.

DoD can achieve strategic agility by making improvements in each of the areas addressed above. Decreasing the timelines for deployment planning, developing a robust deployment and employment process, establishing commercial partnerships to leverage commercial strengths, modifying existing platforms and systems, and developing future platforms for early entry missions will improve the Department’s ability to rapidly move assets to and within a theater of operations.

## INFORMATION FOR DECISION SUPERIORITY

“Decision superiority” is the ability to use information and experience to make battlespace decisions faster and better than any adversary, ensuring a continuing and overwhelming pace and effectiveness of operations, as illustrated in Figure 16. If adversaries and potential adversaries believe the U.S. military is consistently able to use decision superiority to achieve execution superiority, the nation will have created a useful strategic deterrent in addition to a superior capability in conflict and other operations. Decision superiority is a central enabler for achieving

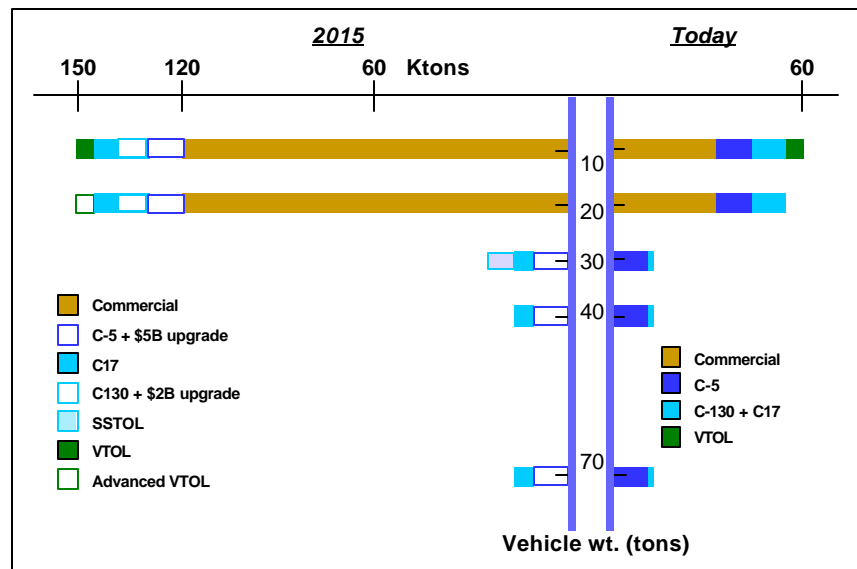


Figure 15. 20-Ton Loads: Upper Limit for 21<sup>st</sup> Century Warfare

<sup>11</sup> The Army has entered into some interesting agreements and discussions on sealift and airlift with the U.S. Navy and commercial vendors, which are discussed in The Army Science Board 1999 Summer Study Report on *Strategic Maneuver*, July 1999, unclassified. The Army has also had in-depth discussions with companies, such as Boeing, about the airlift issue and what loads can be handled.

U.S. military dominance in future crises. It is also a potential vulnerability, since it depends on C<sup>4</sup>ISR resources that an adversary might disrupt in a variety of ways.

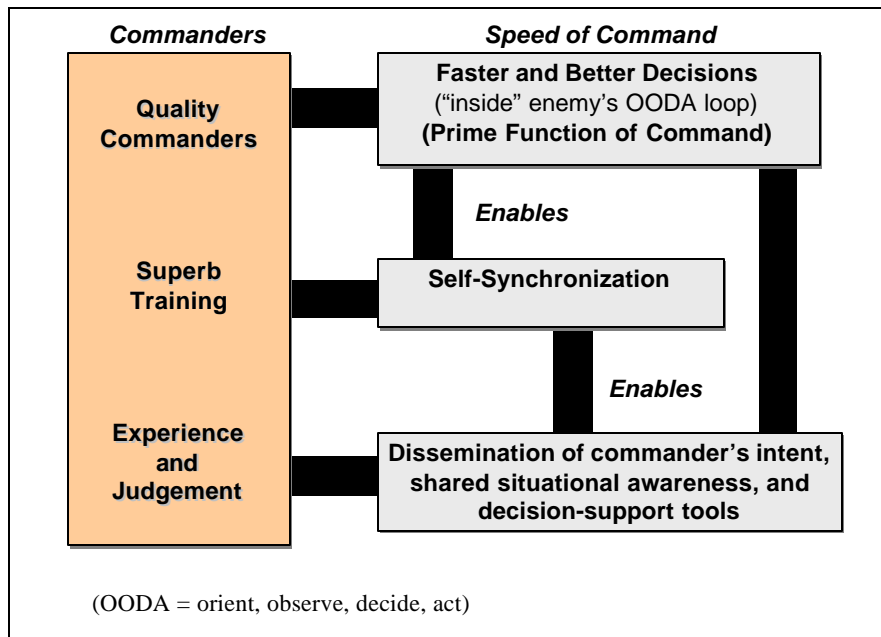


Figure 16. Decision Superiority

The task force focused on decision superiority because of its key role in efficient and rapid execution of military missions. It is a central and difficult challenge for the Department. Effective decision superiority requires that every commander at every level know what the next higher commander wants him to accomplish – the purpose, the commander’s intent, and what is going on in and around an individual unit, regardless of unit size. While there are technical aspects to this objective, the challenges in providing operational decision superiority have more to do with human capability and human understanding. The task is to provide information in such a way that commanders can absorb it, understand it, and use it quickly and effectively to shape their battlespace decisions.

“Information superiority,” as it has generally been understood, is essential to achieving decision superiority, but not sufficient. Given the rapid growth of wide-band commercial communications and high-resolution commercial imagery, many adversaries will have access to information similar to that available to U.S. forces. The ability to gain decision superiority will be based on two general areas: the cognitive capability and preparedness of the decision-maker and the available technical tools. The cognitive issue revolves around quality people and quality training.

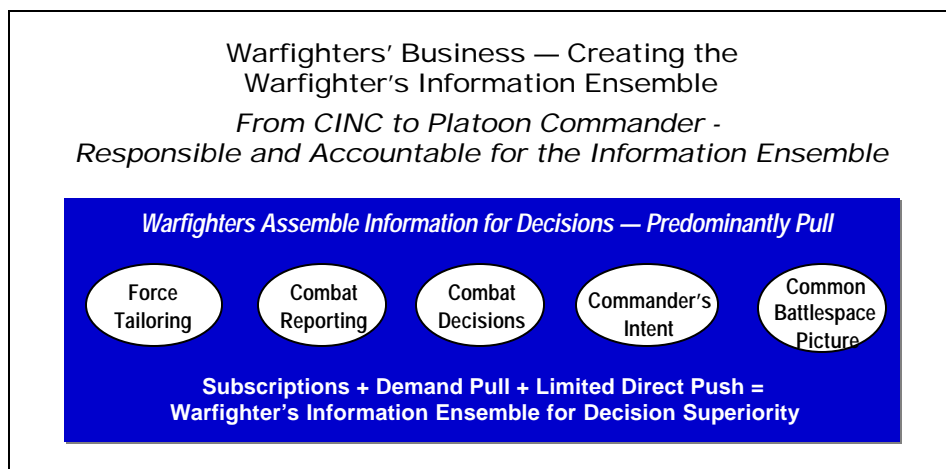
Quality personnel – with training and experience – are an essential basis for decision superiority and the goal is to provide technical tools to enhance the commander ability to make decisions. Enhanced communications, better information presentation, expanded bandwidth, decision support agents, and intelligent agents are all keys to enhancing the commander’s ability to gather, assess, analyze, and act on data. These tools also enhance the commander’s ability to

transform decisions to actions, assess the response of the actions, and iterate through the decision loop. These requirements frame the “grand challenge” for the decision system: to create data and translate it into information at a rate adequate for a commander to access the information and convert it into decisions.

The goal is to ensure a speed of command, pace of operations, and level of operational efficiency and effectiveness that no adversary can manage, regardless of available information resources. Decision superiority comes from the ability to leverage the quantity and type of information available about the battlespace and the forces within it – both friendly and adversary. More timely and better-informed decisions will allow decision-makers to operate “inside” the enemy’s orient-observe-decide-act (OODA) loop, generating an operational tempo with which the enemy is unable to cope. Thus, information superiority will lead to decision superiority, and ultimately, to execution superiority.

### *Operational Architecture*

At the core of decision superiority is a high-level operational architecture. The centerpiece of the architecture, as illustrated in Figure 17, is the premise that ***the warfighter must define and assemble his or her own information ensemble using information sources made available and accessible by the information community***. No single individual or group of people can decide, in advance, what kind of information needs to be assembled and pushed to commanders under constantly changing operational conditions, at multiple-command levels, and in multiple complex situations. Thus, the task of assembling needed information must be left to the individual – from CINC to platoon leader.



*Figure 17. Warfighter's Information Ensemble*

The rest of the operational architecture needs to enable the warfighter in creating a tailored information ensemble. Thus, the warfighter must be responsible and accountable for assembling an information ensemble *and* for ensuring that information needs are known. Commanders must be aggressive in making certain that the right information is made available when and where it is needed.

The infrastructure level of the operational architecture is the *Integrated Information Infrastructure*, as shown in Figure 18.<sup>12</sup> This level requires a set of enablers to help the warfighter access, absorb, and assess information. The infrastructure is composed of a warfighter-tailored battlespace information display, distributed information collection and storage repositories, and automated aids for reliable transmission, storage, retrieval, and management of large amounts of information. It will provide a common operating picture for all users. In effect, the Integrated Information Infrastructure contains a “super database” of everything relevant to the battlespace.

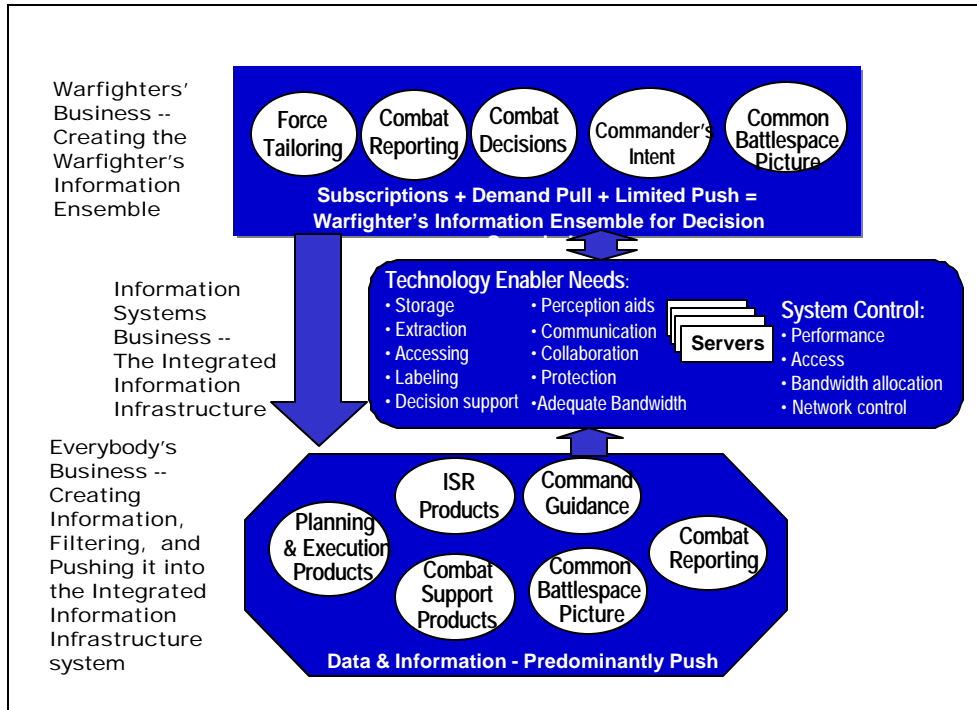


Figure 18. Operational Architecture for Decision Superiority

The warfighter will be able to create a personalized information ensemble using a suite of tools developed by the technology community and embedded as services in the Integrated Information Infrastructure. These will include software tools such as browsers and search engines in the near term and intelligent software agents in the future to both manage the infrastructure and the information residing therein. The guiding principal is that the decision-maker be able to “pull” information from the architecture, using automation to sort, arrange, filter, and find items of interest. A “pull” system works in a variety of ways. The user may subscribe to information known to be available. The system must also allow for “demand” pull for specific information that the commander needs but to which he did not subscribe at the outset. And, at times, the system will need to accommodate a limited amount of information “push” – such as the Commander’s intent or warnings. The Internet has validated that the “pull” system works. The user needs information that is presented and tailored to his needs and the

<sup>12</sup> Annex C describes both a conceptual and systems view of the Integrated Information Infrastructure, as well as a series of recommendations for its implementation.

system provides automation to help the user find information quickly and without error. “Information overload” should not be a problem in a pull-dominated system, unless commanders intentionally choose to overload themselves.

To enable the warfighter to receive and assess information, the Integrated Information Infrastructure provides housekeeping and information management services that ensure accurate, timely, synchronized, and consistent information. For example, if new intelligence is gathered that raises inconsistencies between various pieces of information, the infrastructure must ensure that the information is re-analyzed to sort out and resolve the inconsistency. When the issue is resolved, the infrastructure must make sure that related databases are updated and relevant information is brought into synchronization. Methods for accomplishing this task include circulating dynamic smart agents, constant error checking software, and effective and robust synchronization capabilities. Other functions include managing information and data flow, modifying network architectures, and presenting information to network managers so that it can be adapted in response to changing mission needs.

The input level of the operational architecture is the *data and information gathering* layer. At this level, data and information contributors “push” information into the information infrastructure level where it is indexed, categorized, and assessed. Analysts and automated processes work with the data to create information, which is then “pulled” from the system by the warfighter, as described above. It is important to note, as shown by the feedback arrow in Figure 18, that warfighters at all levels are responsible for ensuring that deficiencies in data and information are well understood and transmitted to those pushing information into the system. This will be effective only if the information system is in continual use. It cannot work if it is assembled and exercised only periodically and sporadically in response to contingencies and exercises.

The concept of the decision superiority operational architecture is included in some Service experiments. Figure 19 illustrates the example of the Army Force XXI Army Warfighting Experiment. In this case, the Army established six functions: planning and replanning, graphical commander’s intent, monitoring the battles, situational awareness, logistics issues, and force tailoring. Data was made available to users in each of these functions through a common repository. Each member of the combat team could pull information as needed and tailor the information display to serve individual requirements. While the Army experiment did not work perfectly, it was successful enough to create confidence that the concept can work.



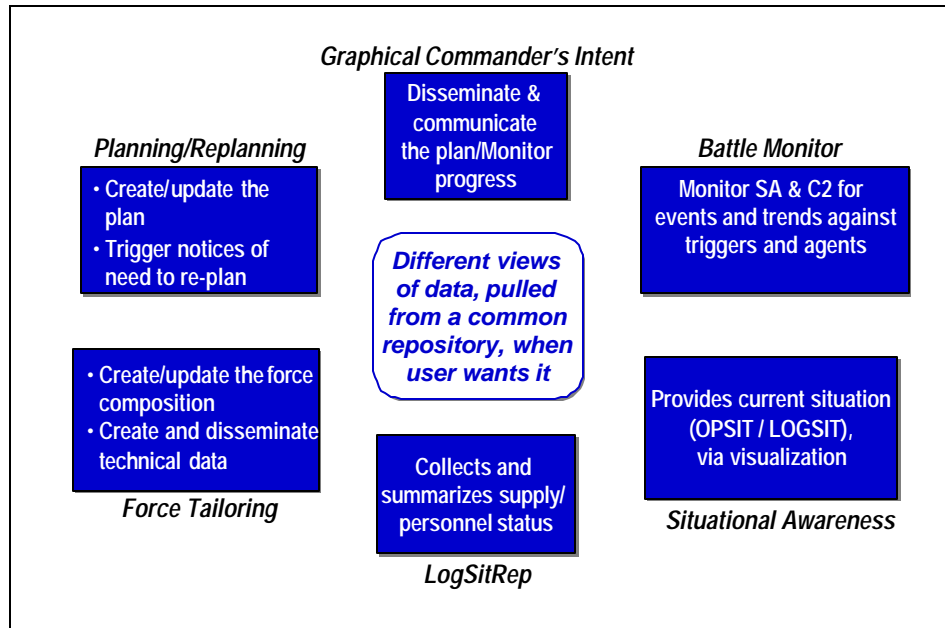


Figure 19. Army Force XXI Army Warfighting Experiment

*Intelligence, Surveillance, and Reconnaissance Systems*

Decision superiority also requires exceptional intelligence as described in the table below:

Prepare/Shape	Respond	Offense/Defense
Understanding the adversary as a system <ul style="list-style-type: none"> <li>• Leadership, political, and cultural</li> <li>• Geographic</li> <li>• Offensive and defensive capabilities</li> </ul>	“Precision Intelligence” for Precision Weapons <ul style="list-style-type: none"> <li>• Assured GPS geolocations and precision time</li> <li>• Situational understanding</li> <li>• Mission results</li> </ul>	Analyze adversary options and intentions <ul style="list-style-type: none"> <li>• Adaptive adversaries</li> <li>• Emphasis on gaming and alternative scenarios</li> <li>• High fidelity simulations</li> </ul>

There is a need for greater mission focus for the intelligence community to support warfighter requirements, which is discussed in more detail in the next chapter. Figure 20 depicts how mission-focused intelligence would respond both proactively and reactively to the warfighter’s intelligence and information needs. Tasking, collection, and analysis that is focused on missions ensures that the intelligence community provides relevant information to the integrated information system.

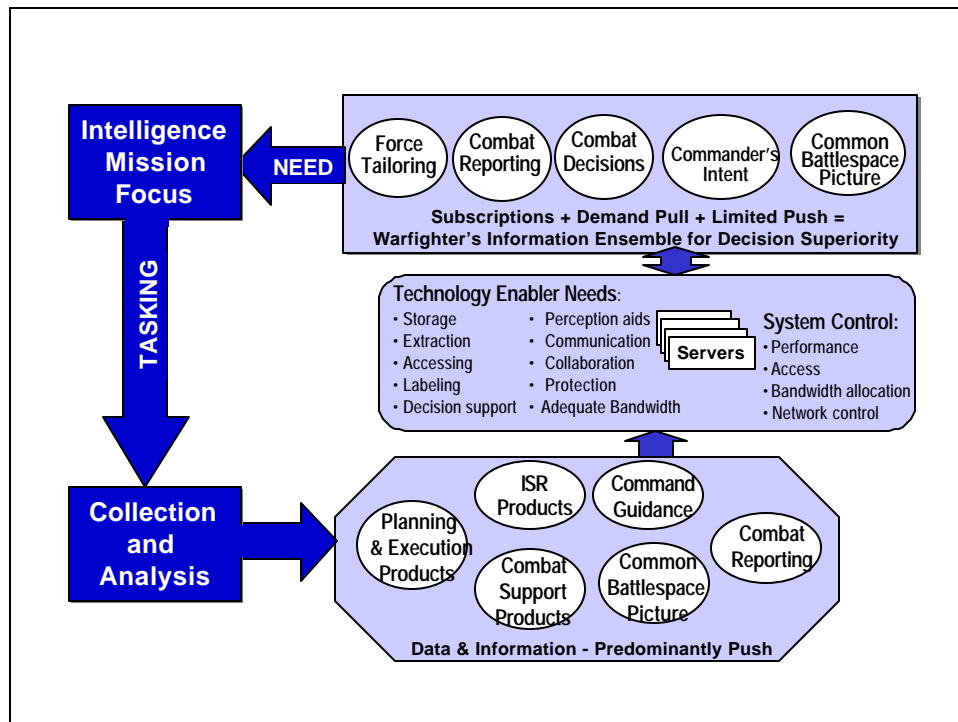


Figure 20. Intelligence Mission Focus

To support decision superiority, the Department must also build an affordable capability for near-continuous, on-demand global surveillance.<sup>13</sup> This system will need to provide day/night, any-weather operation, an ability to image and track tactical mobile entities on land and on the ocean surface, and the capability to penetrate foliage and wooden structures to identify, locate, and track moving targets. The capability to provide fire-control-quality geolocation for targeting is also needed. The Department needs a more aggressive program to build a radar system that can meet these needs.<sup>14</sup>

The task force encourages the continued development of the Discoverer II space-based radar system. This initiative could, and should, be an affordable, initial step to near-continuous global surveillance. The task force also recommends developing a family of new, highly-mobile, close-in sensor systems that can function in all terrain with many different sensor modalities. DoD needs a sensor tasking, processing, exploitation and management capability to accompany these sensor systems. Finally, a family of counter-ISR systems needs to be developed to deny, disable, and deceive enemy sensing systems.

UAVs offer extraordinary potential as the Department moves toward a goal of continuous surveillance and should be more aggressively exploited. Despite success with reconnaissance drones during the Vietnam War and more recently with DARPA UAV technology demonstrations, the military has made only modest investment in developing and incorporating these unmanned systems into the regular force structure.<sup>15</sup> However, this situation is expected to

<sup>13</sup> Volume II contains additional details on intelligence, surveillance and reconnaissance systems.

<sup>14</sup> The task force is aware of one small program at DARPA, being executed by the U.S. Army Communications Electronics Command, to put a foliage penetration radar on an aircraft, but without moving target indication. There is also a slow-paced effort to put such a system in space.

<sup>15</sup> Three successful DARPA UAV technology demonstrations are the 1980s Amber endurance advanced technology demonstration, the Predator ACTD, and the successful-to-date Global Hawk ACTD flight test program.

change in response to recent guidance issued by the Secretary of Defense stating that “the opportunity is here to develop, acquire, and integrate unmanned airborne reconnaissance vehicles into the force structure.”

A number of initiatives currently funded and under way should, if carried to fruition, result in the fielding of significant unmanned ISR capabilities within a few years. These capabilities will include a new tactical UAV replacement for the Army’s Hunter, a vertical take-off and landing tactical UAV to replace Pioneer in the Navy and Marine Corps, and the joint Tactical Control System. The Tactical Control System facilitates cross-utilization of UAV sensor information, and in some cases flight and sensor control, between the military Services. Further, there are proposals to provide both Global Hawk and Predator with additional or improved sensors. The task force supports these initiatives.

Two needs in the field of unmanned airborne reconnaissance and surveillance vehicles have not yet been addressed. The first is a stealthy, high-altitude, long-range system that would replace the DarkStar program that was cancelled in early 1999. The second is a low-cost, high-speed, under-the-clouds penetrator that would fulfill the need for damage assessment imagery and pre-strike target intelligence under environmental and terrain conditions which limit or preclude employment of more conventional UAVs, satellite systems, and high-risk manned airborne reconnaissance assets. Candidate vehicles include modified cruise missiles or aerial targets, the former mid-range UAV, a new design, or a derivative of the Bombardier CL-289, used by the Germans and French in Serbia.

The Department needs to identify criteria and measure of effectiveness that value ISR and other information-related resources as a prelude to determining the right mix of space-based, manned aircraft, and UAV platforms. Today’s solution to the demand placed on the existing low-density, high-demand set of ISR systems needs a comprehensive review to highlight the most cost-effective options. Before determining a solution, DoD needs to understand what can be done, for example, with Global Hawks (current generation and evolving) and from space with Discoverer II and beyond. This issue needs to be carefully analyzed.

Effective ISR systems that can withstand attempts at enemy disruption are critical to achieving decision superiority. The Department needs to increase efforts to meet these challenging demands.

## FORCE PROTECTION

The 1996 bombing of Khobar Towers in Saudi Arabia refocused the Department’s attention on a problem that is not new to the military: force protection. Protecting forces, infrastructure, and lines of communication has long been part of any military mission – whether it be active combat or peacekeeping. Khobar Towers, like Beirut more than a decade before, highlighted the difficulty of protecting forces and the potentially devastating consequences of successful attacks. To reduce risks, force protection must become a way of life for every member of the U.S. armed forces, whether stationed in the United States or abroad. It must become part of the culture or state of mind in everyday operations and a central component of mission planning and execution.

The findings of the 1997 DSB summer study, *DoD Responses to Transnational Threats*, emphasized that the transnational threat challenge requires a three-tiered response: a global

response, a regional response, and a *force level response, which focuses on force protection as a fundamental readiness mission requirement across the spectrum of threats.*<sup>16</sup>

The force protection challenge continues to evolve. Threats to the U.S. homeland and defense against these threats are a growing concern, particularly as the United States becomes more effective at the joint rapid response operations capabilities discussed within this report. Many new operational concepts, such as split-basing and long-range strike, involve reach back to or staging from installations in the continental United States. A robust force protection capability both inside and outside the continental United States is critical to meet U.S. security needs and maintain the nation's ability to project its forces. Full-dimensional protection for U.S. forces extends to family members, civilian employees, and facilities as well as installations, ports, and airfields in both the United States and overseas.

There is a strong synergy between the demands of force projection, force protection, and civil protection. The requirements for protecting military facilities against attacks by transnational adversaries have much in common with protecting civilian facilities and people in metropolitan areas. This commonality allows the United States to leverage DoD capabilities and expertise both for force protection and to assist in civil protection. There is a vast experience base in the civilian community among first responders – the firefighters, emergency medical personnel, and law enforcement officers who are first on the scene in the event of a crisis. And the existing resources and experience in DoD for coping with the battlefield use of weapons of mass destruction provide another experience base from which to draw.

Of special note in 1997 was the DSB's observation that both the Department and civilian communities can benefit from improving the integration and interoperability between local, state, and federal agencies. Improvements in communication, training, information sharing, operations, and resource transfers would help to streamline emergency response operations and interfaces across all levels of responders. In particular, more effective use of state-level assets, such as the National Guard, could strengthen the linkages between civil protection and force protection, with benefit to all participants. In 1998, the Secretary of Defense initiated a pilot program whereby the Guard began to establish a national consequence management capability to support state and local agency responses to domestic incidents, particularly those involving chemical or biological agents, and to support sustainment training and exercises with first responders.

Responsibility for force protection rests on the shoulders of each regional and local commander. However, despite efforts to elevate the importance of force protection, some apathy remains, as the 1997 DSB task force pointed out. Risk mitigation measures sometimes come at the expense of mission requirements and/or quality of life and as a result are not always adequately implemented. Deficiencies exist in training and equipping security personnel, and in some situations, in physical security and protection against non-nuclear weapons effects. Notable shortfalls also exist in capabilities for chemical and biological attack detection, characterization, warning, and mitigation. Personnel are particularly vulnerable in transit from one installation or post to another. In addition, in many posts overseas, U.S. personnel are heavily reliant on host nation, third country, and contract labor that can raise unique security concerns. Moreover, overseas rules of engagement can be restrictive, thus limiting the influence of U.S. forces outside the base perimeter. There is a need for local, organic, tactical intelligence collection and fusion

---

<sup>16</sup> Volume II of the 1997 DSB summer study on Transnational Threats contains a detailed discussion of Force Protection.

capabilities that bring together information specifically relevant to addressing unique force protection challenges in specific locations.

A long-term, sustained campaign plan must be developed and executed to achieve full-dimensional protection for U.S. forces – in or out of combat. Force protection should become an integral part of the design and creation of joint and combined rapid response operations capabilities. The 1997 panel’s recommendations for this plan are summarized below, and they are still largely current today. This task force endorses these recommendations with the added emphasis on the need for a strong science and technology program aimed at countering the threat of biological warfare attack.

- ***Reemphasize force protection as a mission responsibility.*** Force protection must be part of day-to-day operational missions worldwide, not just a contingency issue. An end-to-end focus should expand force protection to include capabilities for deterrence, detection, and prevention in addition to mitigation and response. The Secretary of Defense should reemphasize force protection as a mission responsibility by elevating its priority in departmental strategy, guidance, and investment and by making force protection a readiness issue. Improving force protection capabilities should also capitalize on the synergy between this DoD mission and civil protection, to the benefit of both.
- ***Expand scope and breadth of vulnerability assessments.*** Vulnerability assessments should be continued, but should be expanded to address a full range of threats. Thus far, the vulnerability assessments have focused primarily on protecting people, but should be expanded to include mission-related targets, essential infrastructure, and lines of communication. The assessments have emphasized ways to mitigate the effects of high explosives, but should be expanded to provide more attention to addressing the chemical, biological, radiological, and even nuclear transnational threats.
- ***Patch the “seams” created by diverse responsibilities.*** Force protection responsibilities span many organizations and offices in the Office of the Secretary of Defense, the Joint Staff, and the Services. Many organizational and functional gaps and overlaps exist as a result of these diverse responsibilities and impact the crucial areas of budget, policy, plans, and programs. The Secretary of Defense needs to clarify force protection responsibilities within the Office of the Secretary of Defense, the Chairman needs to do likewise within the Joint Staff, and the Services need to review existing assignments of responsibilities.
- ***Exploit promising technologies.*** The Department should better exploit current and emerging technologies to reduce force protection vulnerabilities. There are a substantial number of technologies that can be employed to enhance force protection capabilities both in the near term using commercial, off-the-shelf products, and in the long term as various new technologies mature. To ensure that the Department exploits these technologies where they add the most value for the dollars invested, DoD should create an enduring test bed capability (at the Defense Special Weapons Agency) to help facilitate the transition of technology in support of force protection requirements. In addition to the test bed, the Department should establish a five-year technology investment plan for rapid technology insertion.

- ***Enhance intelligence operations for force protection.*** DoD needs to sharply increase its focus on force protection intelligence needs, particularly at the tactical level. Intelligence collection and analysis remain focused on supporting major theater warfare, but the organization, methodology, and practices that support operational plans do not fully support force protection requirements. There is a need to reorient, improve, and accelerate tactical collection, analysis, and all-source information fusion programs to include coalition partner national assets. Additional human intelligence assets are needed – which are crucial elements in understanding the transnational threat. Intelligence analysts need access to a broader set of national and international data bases. Finally, the task force urges the deployment of tactical intelligence capabilities organic to local units overseas.

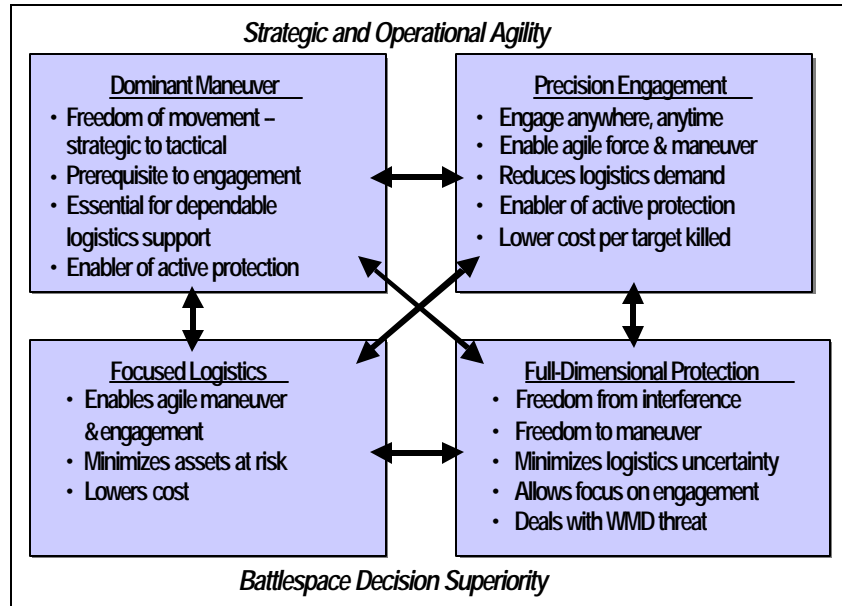
The task force believes that many of the thrusts of *Joint Vision 2010* will mitigate future threats, but DoD still needs to place more emphasis on force protection – especially against weapons of mass destruction. Intelligence and open source information will help, by enhancing U.S. capabilities to find and deal with enemy stocks and production facilities. DoD needs to continue to pursue development of affordable nuclear, biological, and chemical sensors and warning systems. The task force is aware of a biological weapon sensor and identification system that the Canadian government has funded, developed, and tested – and it works.

To improve response options, the United States should develop non-nuclear strike capabilities with effects comparable to nuclear weapons, both physical and psychological; consider an improved U.S. capability for special responses tailored for particular attack modes or targets; and create counter-force capabilities for nuclear, biological and chemical weapons. In this way, the would-be users of weapons of mass destruction would understand that the United States has developed offensive response options to force protection.

## SYNERGY AND THE NEED FOR EXPERIMENTATION

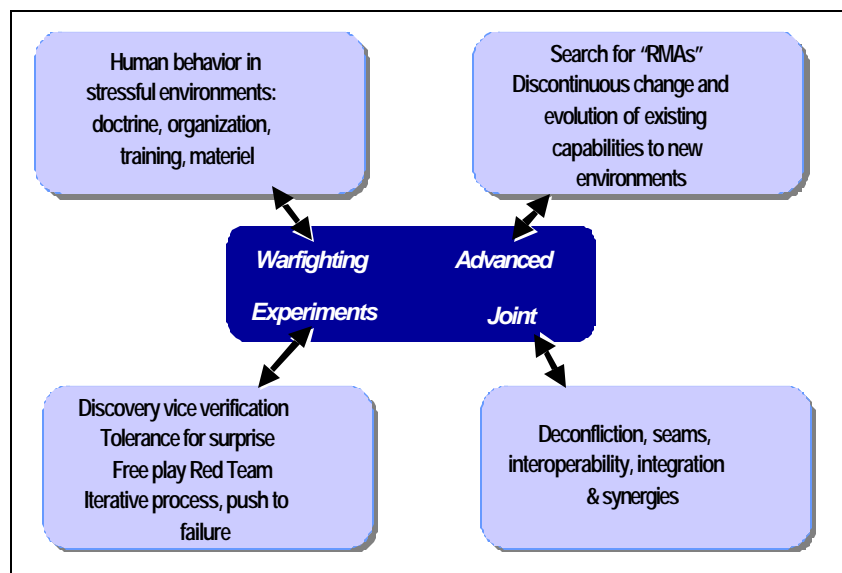
There are significant operational interactions and dependencies between the four pillars of *Joint Vision 2010* – dominant maneuver, precision engagement, focused logistics, and full-dimensional protection – with potential for great payoff, as Figure 21 illustrates. The task force believes that the Department should more explicitly seek to explore these benefits by emphasizing the interplay and dependencies between the pillars. Specifically, the Joint Staff needs to assign responsibility to a staff element for organizing *Joint Vision 2010* activities around the synergies as well as around the pillars themselves.

Human performance is an integral part of all aspects of these synergistic interactions. While technology plays an important role in achieving *Joint Vision 2010*, human performance drives the outcome of battles. Complex technologies, the expected speed of events in combat, the need for rapid decision-making, and other similar factors increase the demand for superb human training and performance. While models and simulation tools are useful in assessing combat situations, they are not particularly effective in measuring human performance. Joint warfighting experiments, which enable people to experience the stress of combat situations and the operations of rapid response forces, are a more effective mechanism for evaluating the human dimension of doctrine, organization, training, and equipment.



*Figure 21. Synergy Among the Pillars of Joint Vision 2010*

Figure 22 illustrates the interaction of human behavior with other elements addressed in joint warfighting experiments. These experiments should emphasize the “joint glue” that enables individual capabilities to operate effectively as an integrated force, including command and control, seams, interoperability, integration and synergies. The experiments seek to identify true revolutions in military affairs and discover what is needed to make revolutionary capabilities realities. Unlike test or training activities, experimenters expect the unexpected, expect discovery, and tolerate surprise. Through an iterative process that pushes the system to failure and allows extensive free play by red teams, it is possible to better understand how forces can effectively operate to achieve battlefield superiority.



*Figure 22. Advanced Joint Warfighting Experiments – A Different Perspective Required*

It is through the process of experimentation that the enablers for joint rapid response capabilities can be brought together and tested – ultimately leading to the formation of Joint Rapid Response Operation Forces. The next chapter describes a set of key implementation initiatives that will further this process.





## CHAPTER 4. MAKING IT HAPPEN

Creating a joint rapid response capability will require the Department to undertake a wide range of new initiatives, as highlighted in Figure 23, and to work with the larger national security

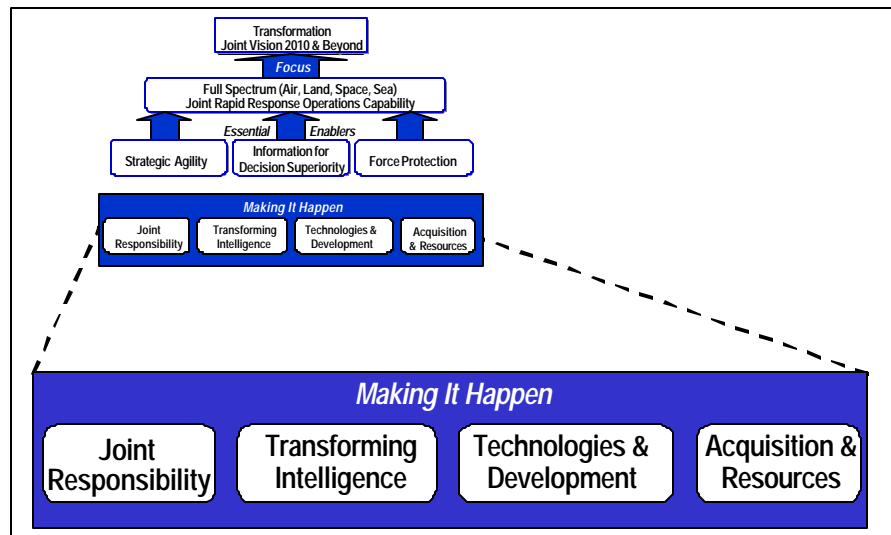


Figure 23. Making It Happen

community in a number of areas as well. This chapter identifies and discusses four areas that will be key to long-run implementation of a rapid response capability. They are: the roles of the joint and coalition force commanders, particularly for joint C<sup>4</sup>ISR systems; the need for changes in intelligence support, both from the community-at-large and those elements more directly in support of a rapid response capability; new technical capabilities that need to be developed, both in the near term using current technology and in the longer term requiring new inventions and innovations; a new acquisition process and a resource balance between force modernization and infrastructure and support functions.

### JOINT RESPONSIBILITY

Goldwater-Nichols laid the groundwork for involving the warfighting customer in the process of matching available force capabilities to tasks and identifying gaps in capabilities for the joint operational commands. Today, the CINCs and joint forces have greater authority and responsibility for current operations and are being consulted and informed to an unprecedented extent. Nonetheless, ensuring that the ultimate customer, the CINC, exercises greater responsibility for establishing *future capability priorities* remains ad hoc.

*The Task Force suggests that more attention by the warfighting CINCs is needed in addressing future capabilities, with special emphasis on those capabilities that are inherently “joint” such as C<sup>4</sup>ISR.* There is clear responsibility, in the military Services and Defense Agencies, for providing forces to the CINCs. However, the authority and responsibility is not nearly as clear for key capabilities needed to employ those forces in an effective “joint force.” For example, the start of real-world joint operations is often characterized by shortfalls in joint command and control capabilities.

Thus, the “joint world” needs to become more involved in the process of identifying the capability priorities that must ultimately be met by the force providers. In addition, there needs to be a mechanism for the CINCs to be involved in experimentation as part of the concept development process in areas of particular interest. There also needs to be more attention paid to involving the CINCs in developing joint operational doctrine, joint operational architectures, and joint technical architectures.

To undertake these roles, the CINCs would need to:

- Maintain cognizance of near- and far-term technologies and programs that drive mission capabilities
- Provide mission capability assessments to identify key theater or functional area gaps in capabilities
- Provide priority lists of mission capability needs
- Play a role in establishing operational architectures focused on interoperable systems with coalition partner forces in mind
- Track, test, and exercise solutions to joint needs and identify what is still missing

To enhance “joint” involvement in establishing future capabilities, a field representative for the CINCs is needed. While the Chairman of the Joint Chiefs could, himself, assume this responsibility, he already has a complex set of responsibilities, and it needs more constant attention than he is likely to be able to give it. Moreover, it is the CINC who must be responsible for ensuring that the theater is ready to accept and utilize forces in effective joint and command operations. ***Thus the Task Force believes that the United States Joint Forces Command is the logical organization to perform the role of “futures” CINC,*** given that USJFCOM has already been assigned responsibilities in related functional roles. USJFCOM would continue to be the “force provider,” to include joint training, and would become the representative for “future joint capabilities,” to include joint experimentation. Other USJFCOM responsibilities not directly related to these roles should be reassigned.

### *C<sup>4</sup>ISR Systems*

C<sup>4</sup>ISR systems are an example of a capability that should be “born joint” – that is, C<sup>4</sup>ISR assets should be treated as a joint system from the start rather than “kluged together” at the time of a crisis. Joint C<sup>4</sup>ISR systems must be *standing capabilities* – proven, exercised, interoperable with joint and coalition forces, and continuously evolving – if they are to match the response time expected from Joint Rapid Response Operations Forces.

Currently, C<sup>4</sup>ISR components are developed independently by each Service and frequently do not work well as a system when brought together in warfighting situations. Often, the ability for joint and combined C<sup>4</sup> to exploit intelligence, surveillance, and reconnaissance is a limiting factor in operational efficiency, as was the case during the Gulf War, Bosnia, and Kosovo operations.<sup>17</sup> C<sup>4</sup>ISR systems are typically assembled when a crisis arises, and dedicated people make the components function as a system through hard work and ingenuity. Many of the

---

<sup>17</sup> An analysis of the C<sup>4</sup>ISR aspects of the Kosovo operation is described in Task Force on Kosovo Operations Report, *Noble Anvil After Action Review*, GEN James P. McCarthy, USAF (Ret), July 30, 1999, SECRET.

resulting solutions, although quite effective, are transitory as there are few, if any, feedback processes in existence today that can lead to permanent improvement between crises.

A “pick-up” approach to C<sup>4</sup>ISR systems is not effective for today’s complex contingencies, yet it has become the norm. Instead the Department needs to build, operate, and exercise joint C<sup>4</sup>ISR as a system. This requires a joint and combined focus, including joint responsibility to design, test, and continuously operate the system.

This conclusion is supported by the analysis of Kosovo operations which report that:

*“C<sup>2</sup>ISR assets are assigned to different organizations and carry out different peacetime missions. They attempt to operate in an integrated way only in crisis or conflict except for a few major exercises. Consequently, operational integration and multi-mode collection is difficult to achieve.”*

*“... most of our joint operations are an ad hoc group of available and ready land, naval, and air units, what they need in the world of C<sup>2</sup>ISR is the ability to assemble and integrate the right communications, sensors, databases, command and control, and information systems to support each different [joint task force] JTF – and to have well established processes and procedures that make the use of this “ad hoc” array of C<sup>2</sup>ISR capability compatible with doctrine and workable within flexible [tactics, techniques and procedures] TTPs.”<sup>18</sup>*

**System Management.** There is no mechanism today for designing and managing a joint C<sup>4</sup>ISR system. Progress is made primarily by *ad hoc* arrangements, committees, integrated product teams, designated groups, and oversight organizations – each with some responsibilities. A single focal point is needed with responsibility and authority for designing, testing, continuously operating, and upgrading C<sup>4</sup>ISR as an integrated system. ***The Task Force recommends that the Secretary of Defense and the Chairman, Joint Chiefs of Staff assign this responsibility to the warfighting CINCs for their areas of responsibility and to United States Joint Forces Command for the deployable C<sup>4</sup>ISR system.***

This recommendation involves a new responsibility for USJFCOM and an expanded role for the CINCs. Today, USJFCOM has overall responsibility for training all CONUS-based forces and deploying these forces to the warfighting CINCs as required. Thus it is logical for USJFCOM to have responsibility for ensuring that the command and control system that would be deployed along with these forces is defined, tested, ready to deploy and operate, and capable of exploiting available ISR systems. The individual CINCs would focus on special problems and requirements in their geographic areas and have responsibility for solving these problems within the common core command and control system architectures and interfaces.

**System Architecture.** Creating a system design for a large, diverse C<sup>4</sup>ISR system is a difficult task, from both a technical and management standpoint. As a result, many large systems of this complexity evolve gradually from the bottom up, under pressure from their users. Communication and transportation infrastructures, even cities themselves, are created in this way. While a bottom-up approach has some attractive attributes, large systems need standards, building codes, and system planning in order to evolve efficiently. The Internet, for example – perhaps the archetype of a bottoms-up system – has the Internet Engineering Task Force to perform these system-engineering functions.

---

<sup>18</sup> Ibid, p. 12 and 18.

The same concept applies to a joint C<sup>4</sup>ISR system. A systems engineering organization, with an individual appointed as an overall systems architect, is needed to lay out an architecture or overall systems design. The systems architect is responsible for defining an open-system architecture with standard interfaces, rather than a detailed design. This will allow the system to evolve easily as new components or subsystems are built to those standards. The architect should report to USJFCOM and play a major role in exercises and short-term system development.

The CINCs play a role in this process by developing operational architectures for the C<sup>4</sup>ISR systems that support their areas of responsibility. In performing this role, the CINCs need to:

- Maintain an up-to-date description of the joint operational architecture including descriptions of the components, how they are used, and how they are supposed to work together, including new component systems under development.
- Run extensive joint exercises, demonstrations, and tests in as realistic and stressful a manner as possible. These exercises should use real forces and equipment and be suitably instrumented to find out how well the system works, particularly the large number of interfaces required. Immediate feedback should be provided for short-term improvements in equipment and software. Exercises are the foundation on which system improvements are based, and can provide reasonable assurance that the existing joint system will work effectively when needed.
- Back up the exercises with simulations. Simulations provide the opportunity for exercising the system more extensively because they are less expensive and more flexible than real exercises. Simulations must be consistent with exercises, however, if their results are to be trusted and useful. Simulation results also feed into the system improvement process.
- Work with the Services and OSD acquisition agents to design major improvements and new component systems based on the results of exercises and simulation. This involves participating throughout the program acquisition process.
- Participate in mission planning at the highest level of DoD. CINC participation will help ensure that joint C<sup>4</sup>ISR system needs are understood and taken into account in the planning process.

**System Testing.** A joint C<sup>4</sup>ISR system will not work unless it is tested under a variety of conditions and used on a regular basis. Unlike civilian communication systems, DoD cannot regularly operate its systems in the operational environment for which they are designed – that is in contingency situations. Thus, testing and training is often focused on subsets of the system, with only occasional large exercises or small-scale operations. However, to ensure information superiority in contingency operations, warfighters need to exercise both their *forces and information systems* in as realistic an environment as possible – the most likely being joint test and evaluation (JT&E) exercises. Currently, USJFCOM plans to test the joint C<sup>4</sup>ISR system in 2004. Instead, the exercises involving C<sup>4</sup>ISR should be frequent, with the time between tests measured in weeks or months rather than in years. JT&E must contribute early and often in the development process.

Designing exercises should be a critical element of C<sup>4</sup>ISR system development. Exercises need to be explicitly designed to stress the C<sup>4</sup>ISR as a system. Appropriate performance metrics

need to be developed for the system and incorporated into the exercises, which should include requirements for appropriate instrumentation to measure results. Because the CINC's have the joint forces and are responsible for being ready to fight when needed, these exercises should be planned and carried out by the joint commands, with support from the Services and agencies. The Chairman and the CINC's need adequate funding for these exercises. They should be able to "buy services" from the Service component suppliers to encourage and fund their participation.

**System Transition.** Given focused responsibility, adequate funding, and an overall C<sup>4</sup>ISR system design end-goal, the next step is to create a transition plan for moving from the existing myriad information systems into an integrated, overarching systems design. Transition is a difficult challenge using current processes, as there will be a strong tendency to add new components one-by-one to the wide world of legacy components.

The C<sup>4</sup>ISR system will change by evolution, not by replacement. Driven by continuous, realistic JT&E exercises and guided by an overall architecture and standards, the C<sup>4</sup>ISR system should evolve into a more flexible, interoperable system, able to support joint and combined operations on very short notice. There are two distinct needs: fix the existing system and enable long-term improvements.

*Fix the existing system.* The warfighters need to make what they have now work better, rather than starting over. In this context, DoD must improve the mechanism for rapidly fixing the deficiencies identified in exercises. The joint users are probably best performing this role. Hence, they should be responsible for deciding how to fix problems they identify in joint tests and experiments. To meet this responsibility, they will need resources (money and people) to apply to short-term (days or weeks) fixes. This does not mean that the Services give up responsibility for their system components. The Services will continue to manage resources as before, but will need to "sell" their developments to the users. Still the Services need to be more aggressive and responsive to joint command and control system needs.

*Longer-term improvements.* Proposals for longer-term improvements will come from multiple sources including the Services, development organizations, and private sector contractors. An ACTD process test-bed could be an effective vehicle for managing a long-term, continuous improvement process. ACTDs are designed to allow the warfighting community to sponsor and then evaluate the utility and operational impact of novel, relatively mature technologies before committing to a formal acquisition program. ACTDs typically take 2-4 years to complete and need to be fully-funded in the five-year budget. After the demonstration, operational units can continue using the hardware if appropriate, given the necessary support. To expand on the ACTD approach, the task force envisions a joint test-bed, owned and operated by the USJFCOM, that is designed to focus on ideas for both the mid-term (the first few years past the Future Years Defense Plan) and the long term (beyond 10 years).

By the long term, most existing legacy systems will be obsolete. Legacy systems should evolve to fit new systems rather than forcing new components to fit the legacy systems. Major improvements should be designed to fit the new open system design. As at the present time, the Services and Agencies will continue to provide new information system components crafted to joint standards. But the CINC users must have influence in determining the characteristics of these systems and in choosing which systems are actually acquired. The CINC's should have the final authority on changes to their command and control system.

## *The Joint Systems Engineering Organization*

A Joint Systems Engineering Organization should be established at USJFCOM to support the CINCs in their new role in developing a joint C<sup>4</sup>ISR system. The CINCs will need technical support in two areas: system architecture and system integration and testing. Technical support for the system architecture will involve analyzing options to ensure that new components are “born joint” rather than “appliquéd” onto the current system. In addition, technical knowledge can be incorporated into clear capability requirements for the C<sup>4</sup>ISR system for use in the Department’s planning and resource processes. The second level of support – systems engineering – will involve expert integration advice. As the joint C<sup>4</sup>ISR system evolves, there will continue to be legacy systems to integrate. The systems engineering organization will be involved in helping to ensure that sub-components work together, in testing sub-components, and in capturing lessons learned for use in future solutions – in exercises, operations, and experiments. As such, the JSEO would become the corporate memory and focus for the technical architecture.

The JSEO should:

- Maintain a current C<sup>4</sup>ISR system technical and operational description
- Ensure that there is a current system architecture
- Establish and maintain interface standards which should be largely based on commercial standards
- Maintain system simulations, provided by component suppliers, as needed
- Provide planning, instrumentation, and analytical support for JT&E exercises, and define problems made apparent by the exercises
- Work with all DoD elements that have intersecting responsibilities

To ensure that the JSEO has sufficient influence in the joint system, it should be led by a flag officer reporting directly to the Joint Forces Command. The staff should include about 300 professionals, mostly contract personnel.<sup>19</sup> The staff should also include top young military officers to help solve joint operational problems and to build technical capability in the military forces in support of the joint C<sup>4</sup>ISR approach. The estimated cost of the organization is about \$50 million per year, but this is a modest amount compared to the cost of “fixing” C<sup>4</sup>ISR systems after operations such as Desert Storm, Bosnia, and Kosovo. Each of the other warfighting CINCs would need five to ten individuals, linked to the JSEO, to provide technical support in meeting geographic or mission-unique C<sup>4</sup>ISR needs.

There are initiatives already underway to help address the challenges and opportunities of joint C<sup>4</sup>ISR. DoD has an Interoperability joint warfighting capability assessment underway and USD(A&T) has a new director for interoperability. There are many allied and coalition centers that address C<sup>4</sup>ISR issues as well. Still, the proposed system engineering organization fills a unique need to provide technical focus for the provider of joint C<sup>4</sup>ISR systems. USJFCOM needs

---

<sup>19</sup> The Report of the Defense Science Board 1996 Task Force on *Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C<sup>4</sup>ISR) Integration*, February 1997, discusses staffing for a JSEO-type organization. The study recommended a staff of about 300 technical experts. Ten to twenty professionals would provide technical support to each CINC; thus, approximately 100 people would support the various regional CINCs. In addition, a staff of about 200 would be resident at USJFCOM, half focusing on the system architecture and half focusing on systems integration to include test and technical support.

the JSEO capability to fulfill its responsibilities as Joint Force Provider, Joint Forces Trainer, Joint Forces Integrator and for C<sup>4</sup>ISR in support of joint operations. This is a coherent and essential set of joint forces command responsibilities – many of which are already assigned to USJFCOM. This is a challenging set of responsibilities and it will take time and support to grow the capability to meet them. USJFCOM will need to build acceptance of this role by the other CINCs and the Services.

## TRANSFORMING THE INTELLIGENCE COMMUNITY<sup>20</sup>

The United States holds a position of dominance in intelligence. This situation is likely to continue as no other nation is likely to be both able and willing to make the investment required to overcome this superiority anytime soon. However, adversaries have begun to adapt to the well-publicized success of U.S. intelligence methods.

For example:

- Aware of satellite intelligence, national and transnational actors adjust movements to deny and deceive U.S. overhead systems while simultaneously seeking information from these same satellite sources.
- Aware of the effectiveness of U.S. signals intelligence (SIGINT), adversaries are employing potent encryption and other sophisticated means to ensure the privacy of their communications; they are also increasingly aware of the power that SIGINT means could confer upon them.
- Aware of the U.S. intolerance for collateral damage, adversaries are mixing civilian and military populations and installations.
- Aware of poverty and instability in the former Soviet Union, adversaries – both national and transnational – may have opportunities to obtain both weapons of mass destruction *and* the skills to deploy them. This has the potential to enable even transnational adversaries to threaten consequences heretofore reserved to advanced nations.
- Aware of the U.S. legal system, which seeks to preserve the freedoms that have created America's unique society, terrorists know they can operate within the U.S. homeland with an astonishing degree of discretion.

These developments represent a new challenge to the U.S. national security apparatus. Existing U.S. capabilities, developed for the Cold War, may not be as effective in this new security environment. U.S. technical intelligence assets were designed to ferret out the intentions and capabilities of a nation state using remote, sophisticated, technical means. Like the military forces they support, these means may not be well matched to a world where enemies move like shadows to target embassies, computer networks, vital commercial supplies, and perhaps, even the general population with biological or chemical weapons. Accustomed to a qualitative as well as quantitative edge in all encounters, the United States must be increasingly cautious, given adversary access to advanced technologies through commercial and criminal networks. Moreover, the nation will have to deal with adversaries that have far greater knowledge of the

---

<sup>20</sup> Volume II contains the complete report of the Intelligence Needs and Adversaries task force.



United States, and have developed the sophistication to blunt, if not outright defeat, some of its most effective technical means.

The objective of the intelligence apparatus is to enhance U.S. national security by informing policymakers and supporting warfighters in military operations – the primary customers for intelligence. Customer needs for intelligence are being driven – in a variety of dimensions – by the changing character of adversaries and their abilities to threaten U.S. interests. Customer priorities are increasingly dynamic and expanding in diversity. Rather than focusing on a few major threats, the intelligence community must continually analyze a wider range of potential adversaries. While timelines within which the intelligence community must respond are shrinking, the need for greater precision and detail is growing. And while the need to protect sensitive sources and methods is unchanged, virtually every action taken by U.S. warfighters and policymakers is executed in a combined environment – driving the demand to share intelligence products with coalition partners – or with state and local officials in the case of homeland defense.

At the same time, the technology-enabled, information-rich global environment is shaping customer expectations. DoD customers are increasingly reliant on information networks and databases to enable their operations. Information provided by the intelligence community is of limited value unless it is readily accessible within this electronic operating environment. All customers have a wealth of relevant information at their fingertips and the ability to apply sophisticated commercially available tools to help them mine that information space. There is a growing desire by key customers to have the option to customize their information ensemble to meet individual needs rather than receive standard reports and serialized products. Customer opinions are generally shaped by what they learn from an information-rich open source environment – driving the need for the intelligence community to put its unique information and analytic judgments into this broader context.

Intelligence has been described as *knowledge that reduces risk or uncertainty for decision-makers*. Whether for a warfighter or a policymaker, effective intelligence is critically important throughout the full spectrum of peace, crisis, and war. And at any given time, different customers will be dealing with different issues and objectives – but all are important. To more fully characterize the customer needs for intelligence, the task force developed a model based on the key themes of the National Military Strategy, as shown in Figure 24.

<b>Prepare for the Future</b> <i>Understand the Threat as a System</i>	<b>Shape the Environment</b> <i>Provide the National Command Authority (NCA) with Options</i>	<b>Respond to Contingencies</b> <i>Support Strategy Execution Support Force Protection</i>
<b>Dissuade</b>	<b>Deter</b>	<b>Dominate</b>
<b>Protect the Homeland</b> <i>Provide Warning Enable Prevention or Disruption Enable Attribution Support Consequence Management</i>		

Figure 24. Key Themes of the National Military Strategy

The task force grappled with the question of how to transform the nation's intelligence apparatus to support the Department of Defense, and specifically the warfighters, in a way that allows more inputs and provides better capabilities across the spectrum of applications.<sup>21</sup>

In recent years, a number of reports, studies and assessments have expressed significant concerns regarding both current performance of the intelligence community and its ability to adapt to the emerging needs of our national security apparatus.<sup>22</sup> Concerns with the performance of the U.S. intelligence community are unlikely to diminish as the United States enters the 21<sup>st</sup> century. Instead there will be increasing pressure on the intelligence community to take aggressive steps to redress the conditions that limit its current performance. The task force realizes that the intelligence community components are aware of shortcomings and that there has been extensive external and internal examination. However,

- Personnel reductions, coupled with technical advances in collection systems, have resulted in fewer analysts being tasked to produce more intelligence about an increasing array of topics.
- The collapse of the Soviet Union and the fall of the Berlin Wall fueled the national desire for a “peace dividend.” This desire led to a decade of budgetary decline and constrained hiring across the national security community. Almost simultaneously, the World Wide Web became prominent and the information technology environment exploded. In an attempt to cope with the realities of the changing global environment, the intelligence community accommodated budget cuts by trading away investment – in people as well as in technology – to sustain operational capacity.
- There is a growing tension between readiness and modernization. In the absence of stable foreign policy and clear national priorities, the intelligence community is driven to attempt to be *all things to all people*. Successful performance given today's suite of issues is due to motivated and committed personnel.
- The intelligence community is, and has been since the end of World War II, purposefully oriented toward detecting and counting traditional military threats such as weapons, weapon platforms, and forces. Thus, the dominant share of intelligence resources has been focused on remote technical collection. These legacy collection assets cannot by themselves meet the demands of today's increasingly diverse and dynamic national security environment, and their utility is limited in detecting emerging strategic threats such as biological warfare developments.
- The voice of the intelligence customer is inadequate in today's intelligence resource allocation process. Although consumers have a role in establishing intelligence requirements, the path between their input and delivered intelligence is arduous and unclear.

Since the intelligence community crosses agency and department boundaries across the government, very diverse customer demands are placed on the Director, Central Intelligence

---

<sup>21</sup> The task force focused on the larger intelligence community, not the Joint Intelligence Centers that are within the direct organizations of the CINCs.

<sup>22</sup> The following studies, in particular, have addressed these concerns: “Preparing for the 21<sup>st</sup> Century: An Appraisal of U.S. Intelligence,” “IC21: The Intelligence Community in the 21<sup>st</sup> Century,” “The Rumsfeld Commission,” “Combating Proliferation of Weapons of Mass Destruction.”

(DCI) and his agencies. Figure 25 summarizes the current intelligence situation as well the needed outcome. The intelligence community has become too collector-centric with its “stovepipe” collection systems. To support greater DoD customer demands, the intelligence community needs to become more mission-centric, focused on the specific missions of the CINCs. In turn, DoD needs to take action to motivate a stronger customer pull from the CINCs. Persistent, dedicated, involved customers can change the supplier culture. The DCI needs to participate in addressing this challenge and adopt the view that suppliers need to be part of transformation – because eventually they will *have* to be.

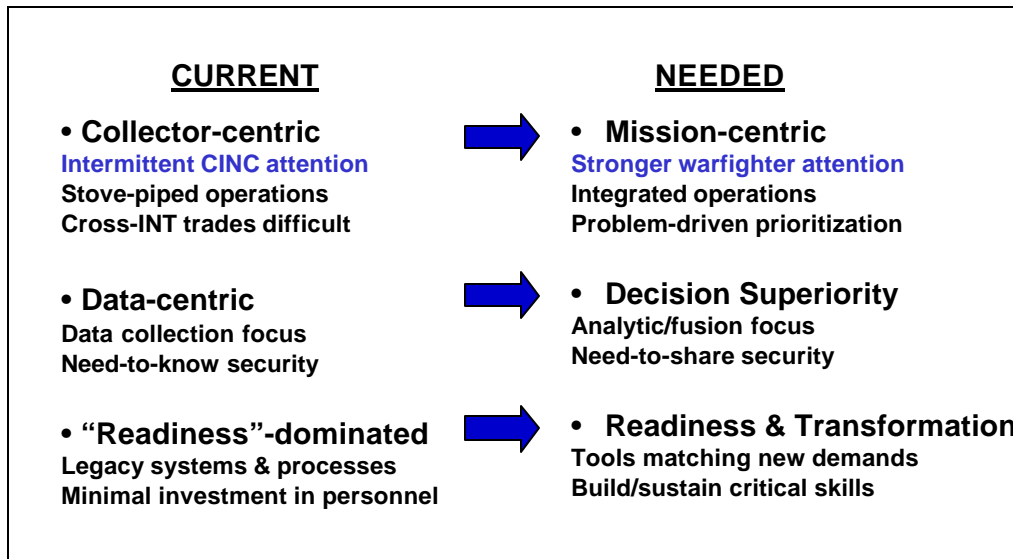


Figure 25. Superior Intelligence will Require Transformation for Mission Focus

To create a more mission-centric approach, the intelligence community needs mission managers who deliver focused intelligence to the warfighters as well as other customers. Mission managers would be required to understand the regional adversaries for a particular CINC. They would drive priorities in order to generate critical battlespace information that would, eventually, drive investments in collection, processing, analysis, and people.

Mission managers should be accountable for delivering intelligence to primary customers on issues involving their area of responsibility. The task force recommends assigning the following suite of responsibilities to mission managers, together with the authority needed to enable success:

- Deliver requisite intelligence to support customer mission objectives
- Establish priorities – derived from CINC inputs and the national security strategy – to support resource allocation decisions
- Develop and maintain system-level strategic understanding of adversaries
- Drive collection and exploitation via prioritized tasking
- Develop *measures of effectiveness* against which collection assets are evaluated

- Prioritize investment across the full spectrum of the needed personnel and technology-based capabilities

Under this construct, the intelligence disciplines – the “INTs” – retain the responsibility for developing and deploying required new capabilities, just as the Services are responsible for equipping future warfighters. Their challenge is to optimize in a different dimension – across the priorities established by the various mission managers – knowing that their ability to respond to the unique needs of each area of responsibility will be measured by that mission manager.

To be effective, the incentives of the entire intelligence community must be realigned to promote successful mission execution. Requiring joint service by community personnel, that is, service in a mission-focused component before progression to the ranks of Senior Intelligence Service (or Senior Executive Service) among intelligence professionals could contribute to this goal.

### *Underlying Enablers*

Virtually every previous assessment of the intelligence community has noted the need for better collaboration among the individual components, more routine engagement of the expertise that exists outside the community, and robust integration and sharing of information between the community and the customers it serves. Four parameters enable such behaviors: security policy, information infrastructure, operational processes, and experimentation.

**Security Policy.** Primary customers in every segment have expressed the need for more intelligence that is designed with customer objectives in mind. A frequent issue that arises is the inability to share intelligence with coalition partners, or to use it for diplomatic purposes, for fear of exposing sensitive sources and methods. Today’s security policy tilts the scales toward the protection of sources and methods and inhibits sharing intelligence information.

The intelligence community needs to take a fresh look at its security policy across the board. In place of today’s collector-centric *need-to-know* security framework, the community should establish a mission-centric *need-to-share* construct.<sup>23</sup> Although there have been some attempts to establish communities of interest around specific missions, the success has been constrained by the collector-dominated security model in place today. Maturing technologies, such as public-key-infrastructures, offer an opportunity to support effective collaboration and sharing while still protecting sensitive data. Further, emerging tools will enable more robust real-time auditing and adaptive security management, providing even stronger protection for sensitive sources and methods. Personnel incentives must be realigned to motivate collectors and analysts alike to identify the means to appropriately share intelligence while still maintaining vigilance over sensitive sources and methods.

**Information Infrastructure.** The challenge for the intelligence community is twofold: it must create an integrated information infrastructure to enable its own operations and it must act as a “feeder” to the warfighter information domain to support warfighter operations.<sup>24</sup> Both demand a robust global information infrastructure built using commercial standards and

---

<sup>23</sup> The C<sup>4</sup>ISR Kosovo Task Force found six different security systems in use by the United States and coalition/NATO partners.

<sup>24</sup> Annex C contains a detailed description of the proposed Integrated Information Infrastructure.

protocols and both demand that intelligence data, tagged with precise temporal and spatial attributes, be accessible – to customers and intelligence community components alike – via this infrastructure.

**Operational Processes.** Collaboration, enabled by effective decision support tools, and tasking, processing, exploitation and dissemination are critical enablers. Both require a foundation of enabling security policy and a robust integrated information infrastructure. Collaboration – especially distributed collaborative planning – is a powerful performance enabler. Ingenious decision support systems have been created to solve complex problems by exploiting distributed collaborative computing and using artificial intelligence methodologies and rule-based systems. These decision support systems define, with great precision, the relationships between all known and related variables of a manageable and bounded problem set, and then integrate the solutions to these problems with other related sub-problems through software services, communications, and human agents. Such sophisticated decision support systems will have a positive effect on the current hierarchical command and control structures and will be key enablers to the collaborative process in the 21<sup>st</sup> century intelligence enterprise.

**Experimentation.** With fairly predictable adversaries in a slowly changing environment, the conventional approach to creating and introducing new intelligence capabilities was adequate. However, with the present high operational tempo and an environment of chaos, where adversaries are continually using new methods to deny and defeat previously successful capabilities, the United States must embark on a different strategy to deal with these challenges. One effective method for introducing new technologies and capabilities into proven applications is “field” experimentation. The basic concept is to “try a lot of stuff and keep what works.” The barrier to this approach in a highly regulated bureaucratic environment is the tyranny of requirements, namely that “if it is not prescribed, then it is not permitted.” This demand for requirements discourages experiments and taking chances with new ideas that might fail.

The task force recommends that the CINCs operate standing C<sup>4</sup>ISR systems *to include intelligence capabilities*. Thus, intelligence systems should be subject to the same kind of metrics as other force components – metrics to define the capability, define the response requirement, and define the readiness standards. The CINC should be responsible for meeting requirements for intelligence capabilities within their joint C<sup>4</sup>ISR architecture.

## TECHNOLOGIES AND DEVELOPMENT

Technology advances have continually enabled dramatic and new warfighting capabilities for the military forces of the United States. During the Cold War, these advances typically had DoD-unique objectives and interests and were usually developed by defense-sector industries. Areas of particular emphasis in the past included aerospace, nuclear, electronics, missile and marine/undersea technologies. Characteristically, technology evolution cycles and transition times were measured in years to decades, and the technologies were difficult and costly for adversaries to develop or acquire. Many important capabilities derived from these past technology investments and advances.

Since the late 1980s, however, the technology landscape has changed in fundamental ways:

- Advances in some of the most important technology disciplines are now – and will increasingly be – driven primarily by commercial interests
- The pace of advance in those technology areas that have military relevance is increasing
- The commercial technologies that have military relevance are changing and increasing in number
- New capabilities and improvements in old capabilities are occurring more and more often at the intersections between different technologies

With commercial interests driving advances in many technologies, the resulting capabilities are increasingly within the reach of all. The pace of technology advance now means that the slow cycle time of systems development in the DoD is almost guaranteed to produce military systems with embedded technology that is *three to four generations behind* the commercial state-of-the-art at the time of their introduction unless more innovative acquisition processes are routinely employed by DoD.

Moreover, the rate and range of technology dissemination makes it harder today for the United States to maintain a “technology edge” for as long as it could in the past. Technology areas and capabilities previously at the periphery of DoD’s focus, most notably biotechnology and information technology, are increasingly critical to future military operational capabilities. Most of the significant advances in biotechnology in the past five years have happened outside the traditional DoD-sector industries, outside the DoD laboratories, and with little-to-no DoD science and technology funding or involvement. Of late, there is a similar trend in information technology. Moreover, the DoD’s R&D management process – technology program area selection, initiation, review, reporting, and transition – is, for the most part, structured along individual technology areas. Finally, useful technology is slow to transition to the military as the focus on military capability continues to drift to technology advance alone.

The task force has identified four overarching technology areas that are likely to dominate as the basis for new military capabilities in the coming decades: biotechnology; information technology; microsystems (electronics, photonics, micro electro-mechanical systems) and energy and materials. Figure 26 illustrates the explosive growth occurring in each of these four areas.

Importantly, advances at the *interfaces* between these technology areas will likely be as significant as advances in any one area by itself. DoD is currently ill-prepared to either exploit or catalyze this revolution. In two of the technology areas – microsystems technologies and energy and materials – DoD today provides a major, if decreasingly important, influence on the direction and pace of technology advancement. In information technology, DoD was the leader 15-20 years ago and provided the foundation for today’s revolution but is now increasingly dependent on the information infrastructure, services, and applications of the commercial computer and telecommunications industry.

Biotechnology is a subject that deserves special attention. The Department has neither resident expertise in this area nor established relationships with the biotechnology industry. Establishing these relationships should be a higher priority for DoD in order to attain and

maintain a robust defense against biological threats and to capitalize on broader biotechnologies to provide new capabilities.

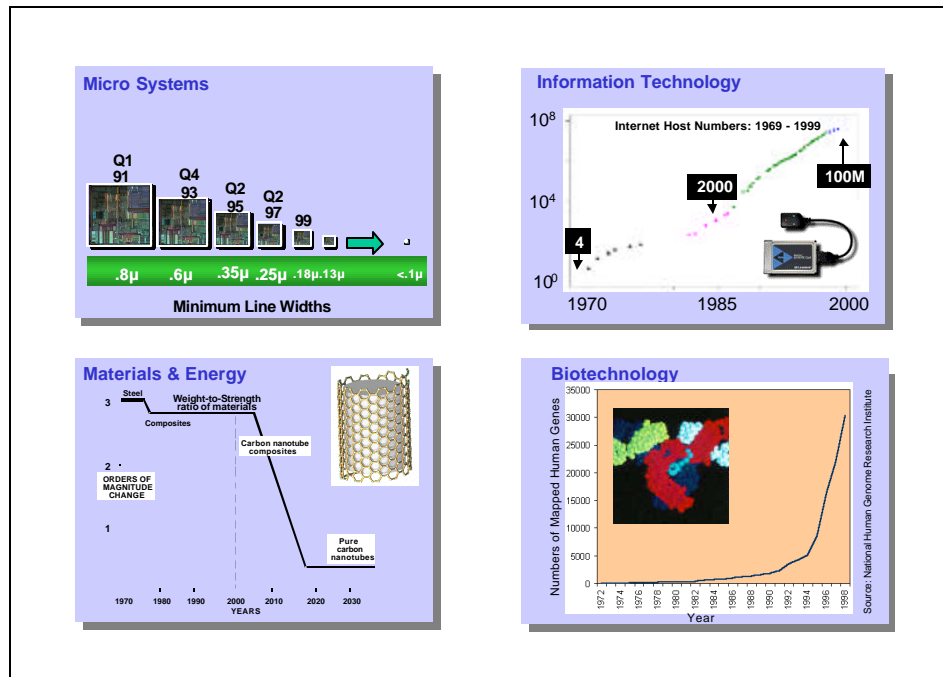


Figure 26. Nurturing the Technology Base: Four Areas of Explosive Growth

DoD has an opportunity to harness and accelerate advances in commercial technologies to ensure that continued unique and overwhelming offensive and defensive capabilities are placed in the hands of the military forces of the United States. With its mission orientation, the Department is unique in its role and ability to focus on capabilities, influence the course of technology advancement, and drive the integration of technology areas. However, in order to take advantage of opportunities in the commercial sector in a timely way, the Department will need to develop a more strategic approach to research and development investments. In addition, changes are needed in the science and technology management process and in the balance and role of DoD and commercial industry interactions.

### Grand Challenges

*The interdisciplinary development of critical technologies will be central to obtaining new military capabilities that support joint rapid response operations.* The task force recommends adopting “grand challenge” military capabilities as a means of focusing cross-disciplinary technology development. While a “grand challenge” is aimed at solving specific military needs or achieving new capabilities, it is also an appropriate mechanism to drive and focus the science and technology base.

As a focus for technology development, grand challenges need to be far-reaching, but should not “set the bar too high” and thus be seen as unattainable. Grand challenges should

- Represent militarily significant goals that provide the basis for enhancing or fundamentally changing military operations
- Achieve a quantum jump in performance (at least 10x increase in performance and/or major cost reduction)
- Drive technology development, integration, and experimentation which is challenging but feasible
- Be managed with defined objectives with measurable, intermediate stages of progress

The task force identified a set of grand challenges that incorporate the four technology areas identified above and that support improvements in broad military capabilities, particularly for joint rapid response operations. These challenges are expected to yield at least an order-of-magnitude increase in the warfighting capability of future U.S. military forces.<sup>25</sup>

- **“Bioshield” – Response to a Major Threat to the United States.** In the 1990 Gulf War, serious concerns were raised about the potential impact of a biological warfare attack on U.S. forces in the field or civilians in the homeland. In the intervening years, further study has indicated that this threat is far more serious than originally imagined. Some progress has been made in developing technology to detect biological attacks, to protect troops, and to treat exposed individuals. However, U.S. citizens and troops still remain vulnerable.
- **“No Place To Hide” – Ubiquitous Micro-Sensors.** Recent experience in Kosovo and Iraq has indicated the extreme difficulty of remotely targeting military vehicles and forces hidden under foliage, in buildings, and in underground facilities. Such targets, in the past, have traditionally been handled by ground troops who often suffer losses in the process. As adversaries react to known U.S. surveillance capabilities, observations from close-in sensors will be increasingly important.
- **“Fast Forward” – Rapid Global Power Protection.** Technologies are needed in direct support of rapid deployment capabilities for forces and their logistics.
- **“Cognitive C<sup>4</sup>” – Information and Command Systems with Near-Human Capabilities.** Even if the combination of distributed surface sensors with satellite and UAV-based sensors can find hidden and moving targets, there remains the problem of understanding and acting on the flow of data coming from such sensors. This grand challenge focuses on developing information and command systems that can manage this kind of data flow and turn it into useful information rapidly.

### *Managing Science and Technology Investments*

The DoD system of technology development and system acquisition is a relic of the past and is not well suited to cope with the critical national defense problems of the future. For example,

- The current DoD and Service science and technology laboratory system tends to concentrate on technology related to military systems that are already developed.

---

<sup>25</sup> Annex D of this volume and Part 3 of Volume II provide additional information on each of these grand challenges.



- Civilian technology in key areas that are relevant to military capabilities has outstripped DoD technology development. DoD technology is not well coupled to commercial technology advances in many areas.
- Globalization of industry and technology permits all nations to have access to leading defense technology and equipment, provided they have the resources to procure them and the integration capabilities to effectively absorb them.
- The competition with the private sector for technical staff has left the Defense Department and Service laboratories unable to attract sufficient qualified staff because of the severe constraints imposed by the Civil Service Personnel System.
- Acquiring technology advances – from either the private sector or the Department’s science and technology programs – is difficult and slow because acquisition processes retain much of the character and approaches of the Cold War and because so few new systems are being developed.

The Department has a fairly ad hoc approach to science and technology investments as Figure 27 depicts. While there is considerable planning, it tends to be a rationalization of existing programs rather than a fresh formulation of how to achieve objectives. Current science and technology programs are reviewed relatively infrequently and with very limited success in changing the course or direction of those programs. On the transition end, there has been some success, particularly where the ‘warfighter pull’ was involved. ‘Warfighter pull’ should have a stronger role in formulating science and technology strategy, plans, and program execution. The grand challenge initiatives recommended herein must be strongly influenced by warfighter inputs.

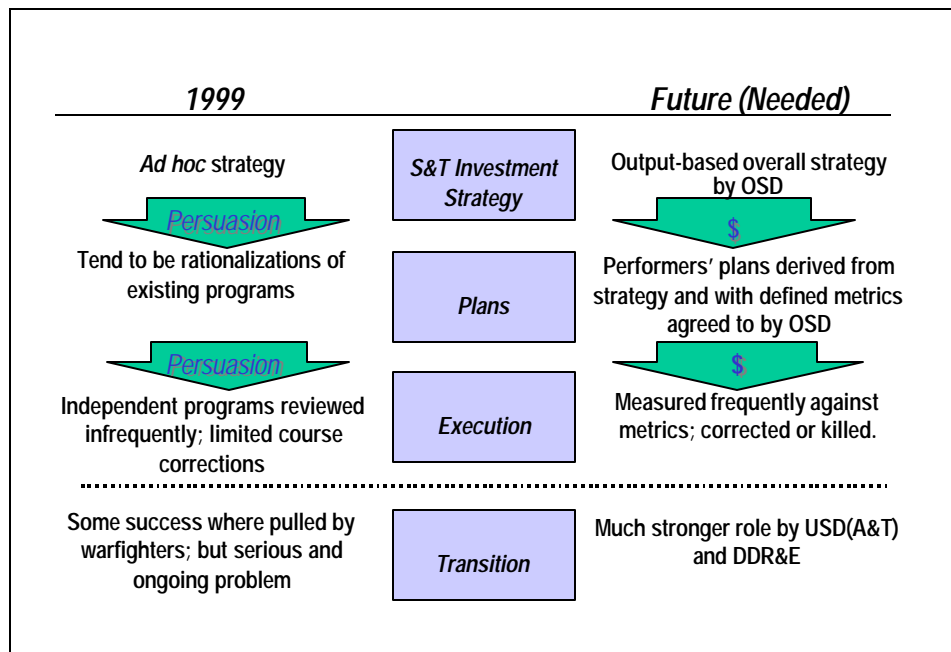


Figure 27. Science and Technology Investment Strategy

The task force recommends a more deliberate investment approach, as shown in Figure 28, with investments consciously concentrated and managed in three areas: grand challenges, technologies likely to make a big difference, and evolutionary technologies. Specifically, a set of five to ten grand challenges would drive a major portion of the science and technology budget. This approach would not result in military demonstrations but would emphasize resolving the deep technological problems underlying military needs for the future.

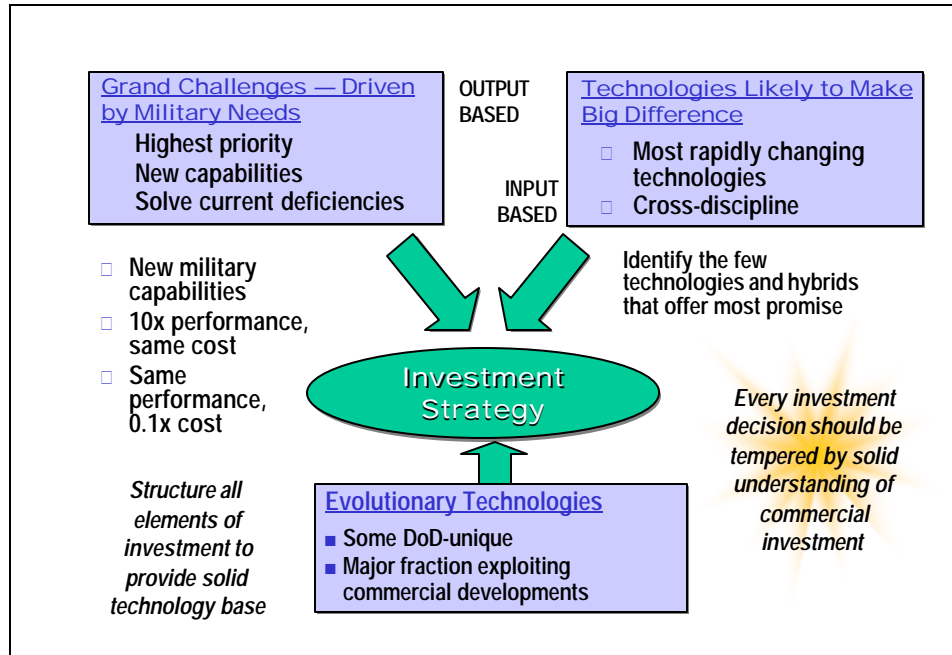


Figure 28. Science and Technology Management

The Department needs to continue to invest significant resources in the area of “technology push” – technologies that are likely to make a big difference. The four technology areas described earlier – biotechnology, information technology, microsystems, and energy and materials – are certainly areas where resources need to be concentrated, with emphasis on the intersections between these and other technologies. The Department will also need to continue investing in evolutionary technologies to support legacy systems and routine operations; however, the task force suggests reducing the investment in this area. Within this overall strategy, each investment decision must be made with a clear understanding of the state-of-the-art in commercial technology and the ways in which DoD could capitalize on commercially available technology to meet its needs.

In the view of many, the Office of the DDR&E was a more powerful institution in the past. When that was the case, science and technology investment and technology transition were managed more effectively, and an overall science and technology strategy tied to direct control of resources was the norm. An ideal approach to science and technology investment would be to measure performance against a strategy. Metrics should be developed to measure progress and determine whether it is consistent with the overall investment plan. The task force believes that

discipline has eroded in the current system and recommends stronger involvement from the Office of the Secretary of Defense in providing direction for long-term science and technology initiatives. Such involvement should result in greater management discipline and more careful and focused resource allocation.

***The task force recommends the following steps be taken to improve the management of science and technology investments. Specifically, the USD(A&T) and DDR&E should***

- Commit a major fraction of the science and technology budget to providing technology solutions to the warfighters for a few urgent grand military challenges
- Start with the four grand challenges outlined in this report
  - “Bioshield”
  - “No Place to Hide”
  - Fast Forward
  - Cognitive C<sup>4</sup>
- Hold the science and technology leadership accountable for delivering against these grand challenges – a fundamental change in their roles
- Measure progress periodically in cooperation with the user through experimentation against quantifiable parameters
- Be empowered to make changes
- Obtain support from the Secretary of Defense for enhanced control of R&D funding by USD(A&T) and the DDR&E

## ACQUISITION AND RESOURCES

Changes in the acquisition process and in the allocation of resources for modernization and support requirements can have a significant impact on the Department’s ability to develop joint rapid response operations capabilities. Initiatives in these areas can help accelerate transition to *Joint Vision 2010*.

### *A New DoD Acquisition Process*

In July 1999, the Vice Chairman, Joint Chiefs of Staff and the USD(A&T) signed a new policy mandating transition to a revised requirements and acquisition process for both new programs as well as upgrades and retrofits to existing DoD systems. These new initiatives represent a watershed change in the way DoD specifies and acquires systems and capabilities. Fundamentally, this approach recognizes for the first time that, with very rare exception, it is not feasible to understand in advance all of the changes and variables that affect how a military system can and will be used some years in the future, how technological advances will impact its design and producibility, and how the world geo-political situation will alter demands placed upon operators. There are three inter-related ingredients which bear on this new approach:

- An Iterative Requirements process

- An Evolutionary Acquisition process which stresses early user hands-on involvement, early fielding of a useful baseline capability, and a continuing block upgrade approach to attain desired “ultimate” capabilities
- A Modular Open System Approach to overall program execution

Because the key recommendations of this study revolve around the concept of frequent joint field exercises, rapid fielding of prototype hardware and software, and continuous upgrading of concepts of operations, tactics, and equipment, these evolutionary procurement approaches constitute a key enabler toward successful implementation of the study recommendations.

***Iterative Requirements.*** An initial set of “requirements” is necessary to initiate a DoD acquisition program. Evolutionary requirements are generally driven by military need and/or new technology. A cursory review of current acquisition programs indicates that a substantial number of these programs were generated by technology push rather than military need pull. In either case, the classic approach is to proceed through a lengthy process resulting in a validated set of requirements that form the basis for a procurement action. Much has been done in recent years to simplify and reduce formal requirements to a more basic set of operational needs as opposed to voluminous sets of design details. However, the classic approach still views requirements primarily as a one-time action.

An Iterative Requirements process takes a fundamentally different tack. It recognizes, in advance, the potential for a large number of unknowns and accommodates them by formally planning on future iterations when more is known about true capabilities and needs. Along with stating a future vision, the key factor in this approach is to initially define a baseline capability that, if successfully fielded, will provide an affordable improvement in military capability.

This approach has a number of fundamental advantages that could yield shorter cycle time to first fielding, reduced program cost, and better products for the warfighter. As more is learned during the execution phase of a program, the baseline requirements can be modified to adapt to changing needs and take advantage of a better understanding of true capabilities. The evolving requirements that arise through the Joint Forces Command experiments as well as those associated with configuring J-ROFs to CINC-specific theatre needs can also be accommodated.

***Evolutionary Acquisition Process.*** Evolutionary Acquisition makes use of a spiral development approach – a flexible process designed from the outset to accommodate change during program execution. During program execution, at least three primary factors drive change:

- Better understanding of technological limitations and capabilities
- Producibility considerations and continuous cost as an independent variable trades
- Better user understanding of system capabilities and new concepts of operation

An important enabler, in many cases, is rapid fielding of prototype hardware and/or software for early user evaluation. This allows early feedback relative to baseline capabilities and deficiencies, pointing the way for both quick fix modifications and needed future changes. This iterative or spiral process of feedback to the initial baseline capability continues through development, low-rate initial production, full-rate production, and initial operational capability.

When closely coupled with the Iterative Requirements process, where a prudent set of baseline requirements has been selected, it should be possible to complete this initial phase of the Evolutionary Acquisition process in much shorter time relative to the classic acquisition approach – a reduction in time by a factor of two or three based on comparable commercial examples.

Although the baseline capability in general will not include every feature desired of an “ultimate” system, getting it entirely through every step of the process on a much shorter time scale greatly accelerates learning at every step. Most importantly, it also accelerates getting new capabilities into the hands of the warfighter. This early deployment further permits the users to train and develop new concept of operations, accelerating useful exploitation of the new capabilities.

After initial operational capability of the baseline system, a block change preplanned product improvement approach is used to formally introduce further improvements. This overall approach is essential to implementing the recommendations of this study, as it allows needed changes that evolve from the lessons learned through continuous experimentation and field exercises to be expeditiously incorporated into equipment in a formal, disciplined manner.

***Modular Open Systems Approach.*** Key to making the Iterative Requirements and Evolutionary Acquisition processes affordable is application of a Modular Open Systems Approach in all phases of program execution. This not only accommodates the need for future change but also addresses the growing problem of diminishing manufacturing sources and technological obsolescence plaguing both new development programs and legacy systems. It can further reduce acquisition cost and cycle time by drawing on specifically tailored variants of modular families of like hardware and software while minimizing development risks through use of more proven items. In most cases, interoperability is also a beneficial fallout.

The “modular” aspect is the more important tenet, as it can be applied widely and to great advantage. Conversely, there are various degrees of “openness” which are applicable – often involving legitimate business issues – making a case-by-case approach more appropriate when applying the “open system” tenet.

The modular concept involves a detailed attention to interfaces – be they hardware or software – with the goal of isolating internal implementation characteristics from the external inputs and resulting outputs. The familiar “plug and play” feature of modern digital hardware and software is a subset of this. However in the modular open systems context, modularity applies to all aspects of a system – both digital and analog electronics, electrical subsystems, mechanical systems, and all types of software. It can also be applied to infrastructure as well, including computer-aided design and manufacturing tools, manufacturing systems, and even business and financial processes.

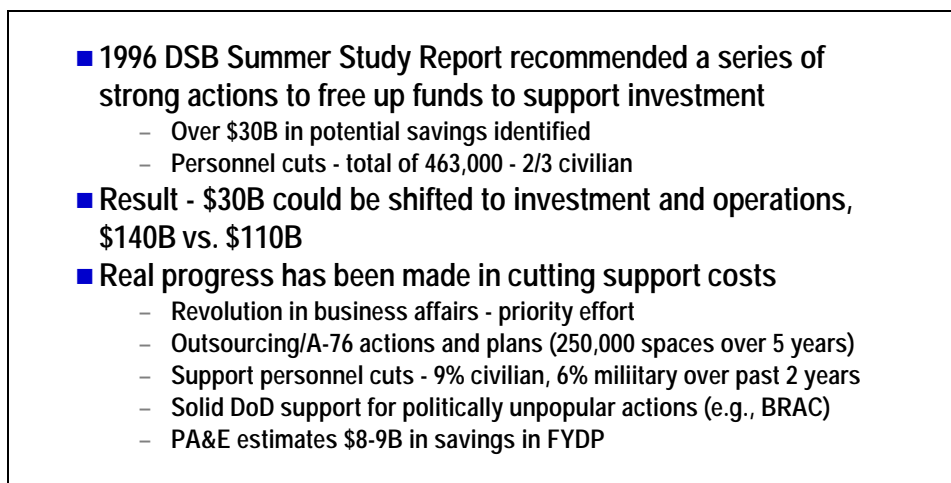
In the extreme case, universal open system standards would be applied to all interfaces, greatly simplifying system integration and permitting competition devoid of proprietary considerations. In most DoD applications that extreme is neither achievable nor necessarily desirable. Establishing open system standards is generally a time consuming, sometimes contentious process that has payback only in a subset of areas of high usage and wide applicability such as communications protocols, electrical connectors, printed wiring assembly sizes, screw sizes, and electrical power system characteristics.

However, most of the desired benefits can be realized if defacto standards are established that apply only within a given platform or for common equipment that is used on a number of different platforms. The degree of "openness" may be quite limited in these cases, but when coupled with a modular design approach, can still provide technology transparency, reduced risk and cycle times, and facilitate subsystem competition. The result is reduced total ownership costs and greatly reduced time to initial operational capability for providing new capabilities to the warfighter.

***Application of modular open system principles is an important requisite for affordably implementing other recommendations of this study. The Task Force therefore recommends that the Modular Open Systems Approach be mandated for acquisition programs involving both new or legacy systems.***

### *Resource Balance*

In 1996, the Defense Science Board summer study, *Achieving an Innovative Support Structure for 21<sup>st</sup> Century Military Superiority*, examined DoD infrastructure costs and concluded that the Department could realize \$30 billion in annual potential savings by improving efficiencies in the business side of its operations. This would allow DoD to shift these resources into operational accounts for readiness and modernization initiatives. The Department has made significant progress in reducing support costs through outsourcing, logistics transformation, and reducing personnel as shown in Figure 29. OSD PA&E currently estimates that there are \$8-9 billion in savings currently programmed in the Future Years Defense Plan. However, the task force feels that there are still many opportunities to realize further savings.



*Figure 29. Reform of the Defense Support Infrastructure*

The task force reviewed the actions taken to date and others underway in response to the 1996 report. Compared to the allocation of funds between support and operations in 1996, progress was evident in several instances.

- Procurement funds increased from \$42 to \$50 billion (from 16 to 19 percent of DoD total obligation authority) by FY 2000.

- Spending for research, development, test and evaluation increased from \$20 billion to nearly \$24 billion. However, spending on science and technology programs was down to \$7.5 billion from \$9 billion.
- Funding for some central support functions (such as C<sup>3</sup> infrastructure) had been reduced modestly.

On the other hand, little or no progress appears to have been made in other areas including installation support (level at 8 percent and \$21 billion). Several areas actually increased.

- Funds for force management appear to have increased from \$12 billion to over \$16 billion (from 5 to 6 percent).
- Spending for central medical also increased from \$14 to \$16 billion, probably reflecting increased numbers of retirees and medical cost inflation.
- Personnel related costs also were higher, including both central personnel support (from \$8 to \$11 billion) and central training (from \$16 to \$20 billion).

The impact of some planned actions may not be reflected until later in the planning cycle. In addition, changes in reporting categories could be distorting the results and the flow of dollars through the working capitol funds complicates any analysis.

A different set of PA&E reports also shows progress in shifting funds from support to operational forces and modernization. These reports treat logistics differently than the 1996 DSB study so the percentages differ, but they show a steady increase in funds for the forces growing from 55 percent of DoD total obligation authority to 57 percent in 2000 and 60 percent in 2005.

Despite these encouraging trends, the task force believes the Department must continue to be aggressive in this area: build on the progress of the past two years and plan for an aggressive push in 2001 when a new administration is in place. DoD should also keep up the pressure to reduce support personnel, cut the size of the civilian work force, and free up military personnel who can be shifted from support tasks to operations.

The task force recommends that DoD:

1. Continue to aggressively pursue reduction of the support infrastructure
  - Maintain focus and priority for the Revolution in Business Affairs
  - Execute current outsourcing and reengineering programs
  - Build on progress of the past two years to expand efforts in these areas
2. Keep up pressure to reduce support personnel
  - Planned civilian manpower strength appears to be leveling out (less than 1 percent reduction over next 2 years)
  - Funding wedges for outsourcing, A-76, and reengineering, however, will result in further reductions
  - Military manpower strength is flat, but people still need to be shifted from support to operations

- Clarify and strengthen competitive sourcing and A-76 policies and procedures
3. Focus senior level support from OSD, the Services, and the joint world on key targets for further cuts
- An additional BRAC round is needed; 2 rounds would be ideal
  - Significantly downsize the depot complex (the Services are moving some non-depot work into underutilized depots)
  - Increase investments in existing systems to reduce and maintain life cycle costs
  - Plan for an aggressive push in 2001 focused on “political” impediments





---

## CHAPTER 5. SUMMARY AND RECOMMENDATIONS

This report has described a transformation process for *Joint Vision 2010* – ***one that focuses on creating a needed joint rapid response operations capability***. While achieving this goal will be challenging for DoD, many elements of the transformation are already evolving in the military Services and Defense Agencies. By focusing these efforts on a single, overarching capability, the transformation process will lead to more effective military forces sooner.

A joint rapid response operations capability is a *warfighting necessity* for the 21<sup>st</sup> century. It fills a gap in U.S. military force capabilities, allowing the United States to respond *rapidly* with *potent and sustained* combat capabilities. Without this capability, the United States and its coalition partners face greater risk of being challenged by potential aggressors on a more frequent basis. Equally important, however, is the *strategic value* of a rapid response operations capability – providing a stabilizing influence prior to conflict and helping to shape the strategic environment.

Creating such a capability requires many enablers. Three of the most essential are:

- ***Strategic Agility***. Strategic agility involves changing major event timelines in order to rapidly move people, materiel, and weapons into and within the battlefield. Operations and logistics should be treated as an integrated whole – in requirements design, operational planning, and execution.
- ***Information for Decision Superiority***. The warfighter needs the means and responsibility for building tailored information ensembles for decision-making. The Integrated Information Infrastructure provides the operational architecture.
- ***Force Protection***. The force protection challenge continues to evolve. Today there is growing concern about threats to the U.S. homeland and defense against these threats. Protection against and counters to biological warfare attacks is an issue of increasing priority. Effective full dimensional force protection remains critical and will be an integral part of the design and creation of joint rapid response operations capabilities.

In addition, the task force has identified a number of key transformation needs that will be required in order to implement this capability. Four of the most important are:

- ***Joint Responsibility***. More attention by the warfighting CINC's is needed in addressing *future* capabilities, with special emphasis on those capabilities that are inherently "joint" such as C<sup>4</sup>ISR. United States Joint Forces Command is the logical organization to perform the role of "futures" CINC. USJFCOM should also have responsibility for a deployable, joint command and control system that includes the ability to exploit the range of ISR systems, with the other geographic CINC's responsible for unique system requirements in their individual areas of responsibility.
- ***Transforming Intelligence***. The intelligence community needs to become more mission-centric, focusing on the specific missions of the CINC's. In turn, DoD needs to take action to motivate a stronger customer pull from the CINC's.

- **Technologies and Development.** Technology “grand challenges” can focus technology on order-of-magnitude improvements in operational capabilities. Four that deserve priority attention by the Department are “No Place to Hide” from U.S. surveillance, “Bioshield” to protect from biological attack, “Fast Forward” global power projection, and “Cognitive C<sup>4</sup>” with near-human capabilities. In addition, the management of science and technology needs to be strengthened.
- **Acquisition and Resources.** An acquisition approach that recognizes changing system requirements during the development and production life-cycle provides a process to field useful capabilities early while continually upgrading them to attain desired “ultimate” capabilities in the longer run. In balancing resource requirements, the Department has made significant progress in reducing support costs through outsourcing, logistics transformation, and reducing personnel. But there are still many opportunities to realize further savings for infrastructure and support, which should be aggressively pursued.

The task force believes that the Department of Defense is capable, both technologically and financially, of building a joint rapid response operations capability. Implementing the needed mix of initiatives will be a complex undertaking, exacerbated by the many competing demands for resources. The task force recommends the following overarching tasks to the Department’s leadership:

**Secretary of Defense lead implementation by:**

- Issuing defense guidance with emphasis on building the joint rapid response operations capability as a strategic capability of the nation
- Assigning USJFCOM responsibility for standing up a core, joint rapid response operations force headquarters
- Assigning USJFCOM responsibility as the “Futures CINC” and make a full partner in resource forums and processes

**Deputy Secretary of Defense should:**

- Direct strong technical support and funding to USJFCOM for joint C<sup>4</sup>ISR systems architectures and technical capabilities, support of warfighting CINCs with current C<sup>4</sup>ISR, and creation of the Joint Systems Engineering Organization
- Fund CINCs to operate and test standing C<sup>4</sup>ISR systems to assure their readiness and interoperability

**Chairman, Joint Chiefs of Staff:**

- Provide a vehicle for assigning the CINCs clear responsibility for joint capability priorities and for ensuring the availability and readiness of the joint systems needed to effectively employ Service-provided forces in joint and coalition operations.
- Validate with Joint Rapid Response Operations Forces established for experimentation across the spectrum of potential contingencies

**Under Secretary of Defense for Acquisition and Technology:**

- Work with the Vice Chairman, Joint Chiefs of Staff to implement the Integrated Information Infrastructure by 2005
- Make plans to shift the focus of a major portion of the science and technology program toward technology solutions to a selected set of “Grand Challenges”

*Achieving a joint rapid response operations capability should become a major organizing construct for the Department's pursuit of Joint Vision 2010 and beyond. It addresses a central and critical challenge facing the U.S. military and will provide needed focus for the transformation to a 21<sup>st</sup> century force – one with full-spectrum dominance, the central theme of Joint Vision 2010.*



---

## ANNEX A. TERMS OF REFERENCE



---

# ANNEX A. TERMS OF REFERENCE



ACQUISITION AND  
TECHNOLOGY

THE UNDER SECRETARY OF DEFENSE  
3010 DEFENSE PENTAGON  
WASHINGTON, D.C. 20301-3010



FEB 22 1999

## MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

**SUBJECT:** Terms of Reference -- Defense Science Board 1999 Summer Study Task Force on 21<sup>st</sup> Century Defense Technology Strategies

You are requested to form a Defense Science Board (DSB) Summer Study to examine 21<sup>st</sup> Century Defense Technology Strategies to meet the national security challenges of the next two decades.

This study should review and consider the broad spectrum of topics, which were addressed in the 1990 DSB Summer Study entitled "Research and Development Strategy for the 1990s". Since that earlier study, we have experienced huge shifts in global relationships, power structures, economics, technology development, and the rise of new adversaries who have access to the latest technologies and are able and willing to employ new forms of warfare. Of particular concern is the proliferation of nuclear, chemical, and biological weapons technology and the many means to deliver such weapons. In addition, we have experienced a dramatic revolution in global information access, sharing, and utility. Information is now a critical and powerful enabler of economic, political, and military power and this importance of information will almost certainly continue to increase; much of this information access is available to potential enemies as well.

To address these dramatic changes, the 1999 Summer Study will organize into *four interdependent, topic-specific Task Forces*. An overarching fifth Task Force will integrate the overall study into a cohesive set of findings and recommendations. The Task Forces will undertake the following initiatives:

- Task Force One: 21<sup>st</sup> Century Intelligence Needs and Adversaries

This Task Force will focus on the global national intelligence system needed to provide the U.S. and its allies adequate warning, with specifics, of developing military and technology capabilities which could threaten national security. The focus should include improved intelligence on development of nuclear, chemical and biological weapons, their means of delivery, and associated adversary intelligence, command, control and communication systems. Of particular concern is the potential rapid evolution of a major regional power and our intelligence capability to early and accurately detect evolving adversary capabilities and intent. The Task Force will take a "Red Team" view and consider how various potential adversaries might choose to invest in asymmetric capabilities which could threaten U.S. full spectrum conflict dominance over the next two decades. Detection of adversary developments which could threaten U.S. asymmetrical strengths (such as stealth, GPS, ISR, ASW, etc.) or take advantage of asymmetric weaknesses (such as information system vulnerability, casualty aversion,





etc) is of high importance. Recommendations will be made for improving current systems and approaches.

- **Task Force Two: Force Modernization Underwriting Joint Vision 2010 and Beyond**

This Task Force will review the 1990 study and expand and build upon the technologies, operational capabilities, operational concepts, and force characteristics developed in the 1998 DSB Summer Study "Joint Operations Superiority in the 21<sup>st</sup> Century." The expansion might address improved concepts for integration of operations and logistics, how to deal with the land attack cruise missile and long-range (2,000km) ballistic missiles with MIRVed payloads of all types, U.S. homeland defense options, and other operational challenges. This Task Force should also develop an implementation roadmap for the development and acquisition of the force capabilities needed to conduct 21<sup>st</sup> Century warfare in 2010 and beyond. A major output of the Task Force will be recommendations on modification of current and planned DoD RDT&E programs to enable the development of the desired new capabilities for 21<sup>st</sup> Century forces.

- **Task Force Three: Information Superiority**

This Task Force will focus on the need for and use of all forms of information for the U.S. and coalition partners to achieve full spectrum dominance. As a starting point, this Task Force will review, expand, and further develop the Integrated Information Infrastructure (III) initially described in the 1998 DSB Summer Study and the surveillance recommendations of the 1993 DSB Summer Study on Global Surveillance. Superior battlespace Intelligence, Surveillance and Reconnaissance (ISR) and counters to it are almost certainly the technologies that will make the difference in any future conflict. This Task Force will examine the current ISR programs, countermeasures to U.S. ISR systems, defensive information warfare operations, and command and control of 21<sup>st</sup> Century forces. In particular, this Task Force will reexamine the approaches being taken to deal with the ever growing volume of information and how that can be best presented to provide information that can be assimilated by the commanders. The review of ISR systems must also address other important topics such as the detection, combat identification, tracking and targeting of tactical targets obscured by foliage. The Task Force will recommend modifications to existing or planned R&D programs, technical approaches, and management of this area to maximize U.S. force superiority.

- **Task Force Four: Defense Technology Strategy, Management and Acquisition**

This Task Force will interact with the other three Task Forces to identify and examine a wide range of technologies. The goal is to identify those technologies with high potential to enable the development of unique and superior operational capabilities in 2010 and beyond. This Task Force will also develop a roadmap and investment recommendations to ensure that the DoD is able to always retain an affordable force capability in the 21<sup>st</sup> Century that is well matched to the foreseeable needs and that DoD retains the ability to surge with the greatest capability if and when necessary. Recommendations on technology policy, management, acquisition and use of commercial technologies will also be developed.

- **Task Force Five: Strategy Integration**

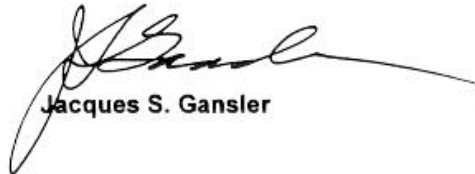
This Task Force will be composed of the overall study co-chairmen and the co-chairmen of the four other Task Forces. The aim is to integrate the outputs of the four Task Forces and arrive at a set of recommendations and conclusions that are seamless across all Task Forces.

This study will be co-sponsored by the Under Secretary of Defense for Acquisition and Technology, and the Chairman of the Joint Chiefs of Staff. Mr. Donald Latham and Mr. Larry Lynn will serve as co-chairmen of the overall study and the Strategy Integration Task Force.

Intelligence Needs TF: Dr. Ruth David, LTG Ken Minihan (USAF Ret)  
Force Modernization TF: Gen Larry Welch (USAF Ret), Dr. Ted Gold  
Information Superiority TF: Mr. Bob Nesbit, Dr. Taylor Lawrence  
Technology Strategy TF: Mr. Walter Morrow, Dr. Ken Gabriel

Dr. Regina Dugan will serve as Executive Secretary of the overall study. Major Tony Yang, USAF will be the DSB Secretariat representative. Executive Secretaries will also be appointed to support the other four Task Forces as determined by the respective Task Force co-chairmen.

The Task Forces will operate in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act," and DoD Directive 5105.4, the "DoD Federal Advisory Committee Management Program." It is not anticipated that this Summer Study will need to go into any "particular matters" within the meaning of Section 208 of Title 18, U.S. Code, nor will it cause any member to be placed in the position of acting as a procurement official.



Jacques S. Gansler



---

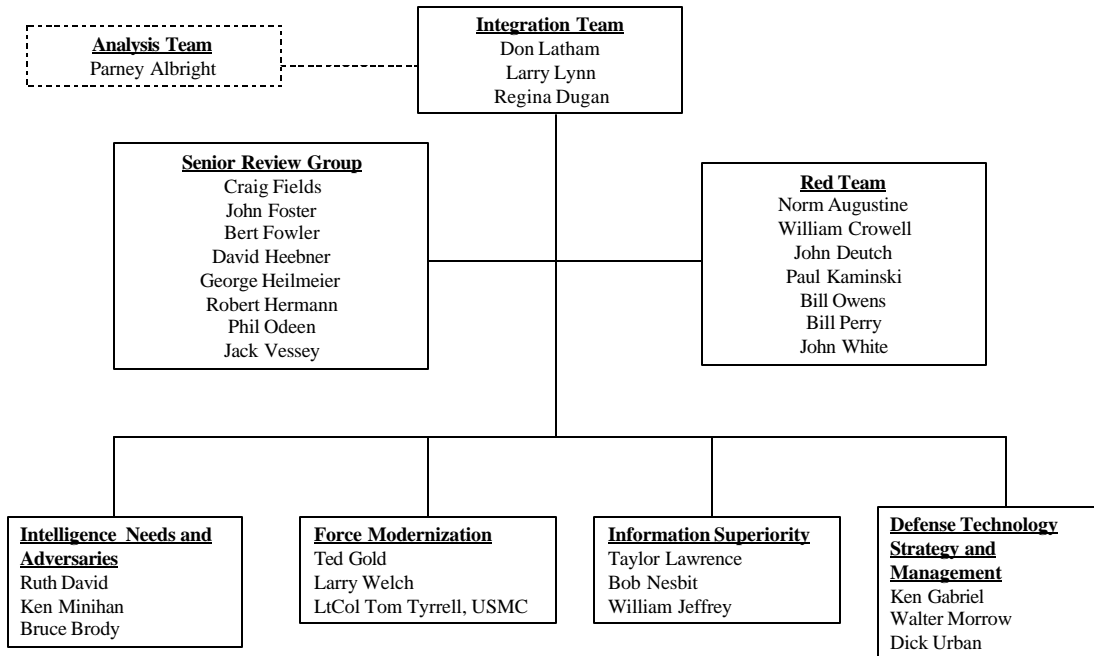
## ANNEX B. STUDY ORGANIZATION AND MEMBERSHIP



---

# ANNEX B. STUDY ORGANIZATION AND MEMBERSHIP

## *1999 DSB Summer Study Organization*



---

# 1999 DSB SUMMER STUDY MEMBERSHIP

## **Integration**

Don Latham  
Larry Lynn  
Regina Dugan  
Maj Eugene Bose, USMC  
Col John Clauer, USMC  
MG George Close, USA  
Col Mike Fallon, USMC (Ret)  
MG Emmitt Gibson, USA  
Jim Miller  
Maj Tony Yang, USAF

## **Red Team**

Norm Augustine  
William Crowell  
John Deutch  
Paul Kaminski  
Bill Owens  
Bill Perry  
John White

## **Senior Review Group**

Craig Fields  
John Foster  
Bert Fowler  
David Heebner  
George Heilmeyer  
Robert Hermann  
Phil Odeen  
Jack Vessey

## **Analysis Team**

Parney Albright  
Michael Bailey  
Mike Bauman  
Regina Dugan  
John Dyer  
George Koleszar  
Lisa Porter  
LTC Gary Sauer, USA  
Arnie Warshawsky

## **Staff**

Marya Bavis Bergloff  
Barbara Bicksler  
Christopher Bolkom  
Julie Evans  
Garnette Fauntleroy  
Stephanie Freer  
David Greinke  
Diane O'Neill  
Bradford Smith, Jr.  
Chip Smith  
Leslie Sowers  
Christopher Szara

## **Intelligence Needs & Adversaries**

Ruth David  
Ken Minihan  
Bruce Brody  
Brian Cullen  
Charlie Hawkins  
Ed McMahon  
Frank Marchilena  
Peter Marino  
Rich O'Lear  
Jerry Tuttle  
Paul Weiss  
George Whitesides  
James Williams  
Gerry Yonas  
*MAJ Jerry Blixt, USA*  
*Robert Boyd*  
*CAPT J. Katharine Burton, USN*  
*Charles Cunningham*  
*John Gannon*  
*Regina Genton*  
*Col Tom Hardwick, USMC*  
*COL Hal Johnson, USA*  
*Maj Ed Loxterkamp, USAF*  
*MajGen Frank Moore, USAF*  
*Patrick Neary*  
*David Osias*  
*Maj Michael Parkyn, USMC*  
CDR Brian Hughes, USN – DSB Rep.

## **Force Modernization**

Ted Gold  
Larry Welch  
LtCol Tom Tyrrell, USMC  
Joseph Braddock  
Mike Carns  
John Cashen  
James Evatt  
Alec Gallimore  
Matt Ganz  
Michael Hopmeier  
Bill Howard  
Dave Maddox  
Glen Otis  
Bill Owens  
Neil Siegel  
John Stewart  
Frank Sullivan  
Paul Van Riper  
Michael Vickers  
Rich Wagner  
*MG George Close, USA*  
*Col Leonard Finley*  
*MG Emmitt Gibson, USA*  
*Col Tom Hardwick, USMC*  
*Maj Ed Loxterkamp, USAF*  
*Lou Kratz*  
*Jim Miller*  
*Melinda Montgomery*  
*Earl Rubright*  
*Maj William Schultz, USMC*  
*MGen Norton Schwartz, USAF*  
*Don Woolever*  
*Michael Zoltoski*  
Maj Tony Yang, USAF – DSB Rep.

---

Note: Names in italics indicate government advisors.



## **Information Superiority**

Taylor Lawrence  
Bob Nesbit  
William Jeffrey  
Stan Alterman  
Theodore Bially  
Werner Dahm  
Nicholas Donofrio  
Bob Everett  
Bran Ferren  
Michael Frankel  
Charlie Gandy  
Bob Gormley  
Ken Israel  
Anita Jones  
Noel Longuemare  
Greg Poe  
Jeffrey Sands  
Howard Schue  
George Spix  
Vince Vitto  
Dick Wishner  
Owen Wormser  
Lawrence Wright  
*Luis Acosta*  
*LTC(P) Stephen Broughall*  
*Michael Fleming*  
*MG Emmitt Gibson, USA*  
*Col Tom Hardwick, USMC*  
*BrigGen Paul Lebras, USAF*  
*Maj Ed Loxterkamp, USAF*  
*Michael Powell*  
*CDR James Steele, USN*  
Maj Clinton Wadsworth, USMC  
Maj Tony Yang, USAF – DSB Rep.

## **Defense Technology Strategy and Management**

Ken Gabriel  
Walter Morrow  
Dick Urban  
Ivan Bekey  
Denis Bovin  
Curt Carlson  
Bob Colwell  
Darryl Greenwood  
Bill Howard  
Ira Kuhn  
Reuven Leopold  
Edward Marram  
George Poste  
David Shaver  
Vic Weedn  
*William Berry*  
*Don Daniel\**  
*Maj Stephen Kirkpatrick, USMC*  
*Robert Kolesar*  
*LtCol Earnest Liberatore, USAF*  
*Maj Ed Loxterkamp, USAF* \Ed Mazzanti  
*Walter Morrison*  
*LtCol Richard Moore, USAF*  
*RADM Charlie Young, USN*  
*CDR Randolph Young, USN*  
LTC Scott McPheeters, USA – DSB Rep.

---

Note: Names in italics indicate government advisors.

---

## ANNEX C. INTEGRATED INFORMATION INFRASTRUCTURE



# ANNEX C. INTEGRATED INFORMATION INFRASTRUCTURE

## INTRODUCTION

There is no question that information is critical to modern warfare. Information, information processing, and communication networks—collectively, an integrated information infrastructure—are the core of virtually every aspect of military activity, including combat operations, navigation and geo-positioning, surveillance, weapons support, force enhancement, information control, and logistics support. Improvements in the integrated information infrastructure (III) enhance each of these military activities and improve our ability to conduct them in a coherent, synergistic fashion to enhance lethality, precision, and force effectiveness. Figure C-1 depicts the relationship between the III and several primary areas of military activity. The III is shown in the center of the figure because, as indicated in *Joint Vision 2010*, information superiority is necessary for achieving dominant maneuver, precision engagement, focused logistics, and full-dimensional protection. The III is necessary for achieving information and decision superiority.

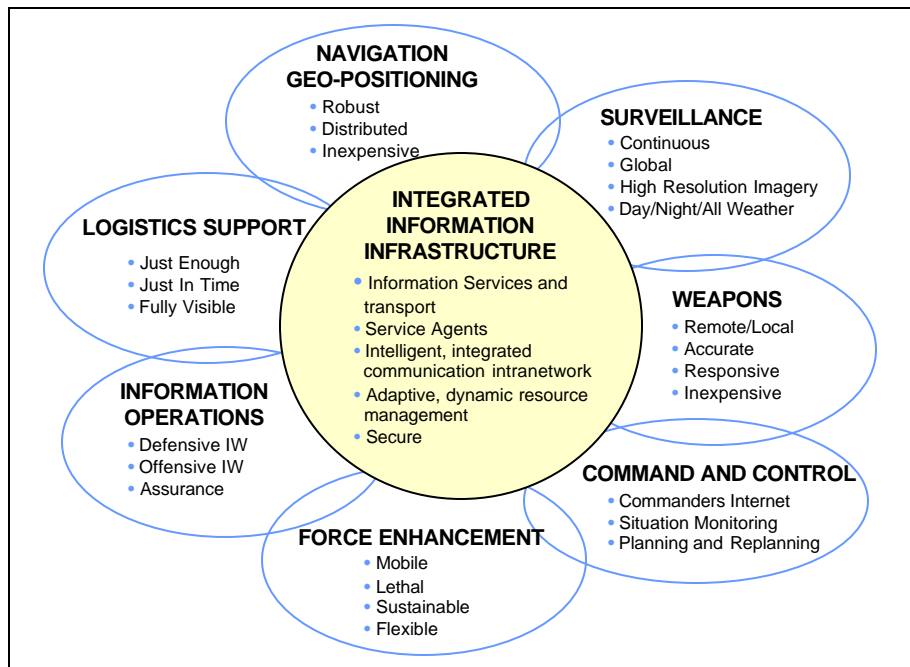


Figure C-1. Information: The Key to Successful Military Operations

The ability to achieve information superiority is the pacing item in realizing the goals of *Joint Vision 2010*. The inadequacies of current service information infrastructures prevent commanders from realizing the full benefit from the current family of intelligence, surveillance, and reconnaissance (ISR) systems—space-based, airborne, or surface—much less profiting from advances in sensors and weapons. Because of uncertainties about whether crucial information will be available when needed, the Services are driven to develop unique, local-only

reconnaissance, surveillance, and target acquisition (RSTA) and command and control systems. Overall, this tendency has resulted in redundant investment in, and proliferation of, “stovepipe” communication, sensor-data processing systems, and command and control information systems.

Increasingly, the armed forces are shifting to an operational concept wherein surveillance and targeting sensors are separated physically from the command node location, which in turn may be remote from the weapons launch platform. In the case of air platforms, for example, no longer will the sensors, commander (pilot), and weapons necessarily be colocated in a single aircraft. Further, third-party targeting data sources and weapons magazines are proliferating. Examples of this evolving trend appear in such concepts as forward pass, cooperative engagement capabilities, the arsenal ship, and the transfer of tactical situation information derived from a variety of off-board sources directly into cockpits.

This evolution promises major improvements in the tactical flexibility and combat effectiveness of forces. The realization of this promise is not without challenges, however, because the operational concepts are inhibited by the inadequacy of the traditional military communication and information-services infrastructure as well as continuing interoperability problems between the C<sup>4</sup>ISR systems of each military Service and between such systems within a given Service.

To realize the potential benefit of these new concepts, a future integrated information infrastructure must be capable of reliable transmission, storage, retrieval, and management of large amounts of information. Today all systems are segmented into communications links, computers, and sensors that in turn are stovepiped to support specific functions such as intelligence, logistics, and fire control. Furthermore, these component entities are now constrained by a lack of (1) the bandwidth necessary for high-resolution imagery transfer; (2) the processor capacity needed for target recognition and interpretation; (3) memory sufficient to handle massive amounts of archival data; and (4) software to search the many data repositories quickly in order to provide commanders with critical command and control information in a timely manner. These constraints are magnified by difficulties in integrating a myriad of legacy information systems with newly developed, service-unique stovepipe and joint systems. These limitations can be overcome and the full capability of joint forces realized, if we set as our goal to integrate all military C<sup>4</sup>ISR systems into a ubiquitous, flexible, interoperable C<sup>4</sup>ISR system of systems—the Integrated Information Infrastructure.

A summary description of the III is provided in Figure C-2 along with a brief description of its operational implications.

- Description
  - An integrated, scaleable, fully distributed processing and transport environment, that is based on commercial technology, and that:
    - Moves information from any source to any destination
    - Provides tailored information through intelligent software agents
    - Is dynamic, adaptive, self reconfiguring, robust and secure
    - Integrates legacy C4ISR systems
    - Permits full exploitation of sensor, weapon & platform capabilities
      - Joint cooperative component
      - Sensor to sensor for cueing
- Implications
  - Permits geographic separation and functional integration of command, targeting, weapons delivery, and support functions
  - Provides single, integrated infrastructure for all military information needs: C4ISR, fire control, logistics
  - Supports: split base, force projection, information reachback
  - Joint forces with common situational understanding, common operating picture, and informed/rapid decision making

*Figure C-2. Description and Operational Implications*

## REQUIREMENTS AND VISION

### *Requirements*

The Integrated Information Infrastructure must meet several key requirements if it is to realize its potential to enable future combat operations to support a wide spectrum of missions, threats, and environments.

As stated in *Joint Vision 2010*, and refined in the 1999 DSB Summer Study, a military force must be able to receive or transmit all of the information it needs for the successful and efficient prosecution of its mission, from any point on the globe, in a flexible, adaptive, reconfigurable structure capable of rapidly adapting to changing operational and tactical environments. The information infrastructure must support these needs, while allowing force structures of arbitrary composition to be rapidly formed and fielded—ranging from Joint Rapid Response Operations Forces (J-ROF) to full-up joint forces for a major regional conflict. Furthermore, the infrastructure must adapt to unanticipated demands during crises and to stress imposed on the system by adversaries.

The infrastructure must allow information to be distributed to and from any source or user at any time: its architecture must not be constrained to support a force-structure (enterprise) hierarchy conceived *a priori*. Most importantly, the information and services provided to an end user through the *infrastructure must be tailored to the user's needs, and be relevant to the user's mission, without requiring the user to sort through volumes of data or images*. A summary of these and related warfighter needs is provided in Figure C-3.

- Provides facilities to move information from any source to any destination
  - Sources = sensors => eyes and ears of teams
  - Users = warfighters and weapons => muscle
  - Information infrastructure = processors and communications = neural system
- Provides tailored information when and where required
  - Automatic data storage, retrieval, and management
  - Automatic data fusion
  - Intelligent information dissemination
  - Supports multimodal information
- Facilitates force-structure tailoring
  - Assure interoperability of all Service C4ISR systems
  - Close existing seams between military communication systems
  - Close existing seams between C4ISR systems intra/inter Service
- Provides robust, reliable information services
  - Survivability through replication and self adaptation
  - Quality of service to meet dynamic requirements
- Exploits commercial information technologies
  - Adopts open-system standards and protocols
  - Minimize use of service/system unique C4ISR hardware and software
- Does not place warfighters at risk of being detected and targeted

*Figure C-3. Warfighter Needs*

Another way of representing the functions supported by the III is provided in Figure C-4. This figure shows that information must be pulled and pushed by all warfighters from a common information infrastructure. Any (all) warfighters select (pull) information to meet their needs to effectively conduct their mission. This information pull is supported by a set of services provided within the infrastructure; services such as information caching, retrieval, posting, fusion, and the other "technology enablers" noted in the figure.

In order to provide information services that support "Operational Decision Superiority," the infrastructure must also allow each warfighter to tailor, through selective pull, the information he/she receives. These tailoring services are supported by software tools that permit the warfighter to adaptively profile their needs in such a manner that the infrastructure understands what information is required and when.

In addition to information pull, there will be circumstances where information will be resident in the infrastructure that is critical to warfighters given unplanned/unpredicted circumstances the individuals find themselves in. Under such conditions, the infrastructure must take the initiative to intelligently "push" this information to the warfighter.

In Figure C-4 the III is framed in the context of supporting "Operational Decision Superiority." However, the infrastructure must also support dynamic processes such as requesting and receiving ISR products as shown in Figure C-5. Although this intelligence mission example is shown outside of the III for clarity, it must be emphasized that this function is supported within the III – the need and subsequent posting of ISR products are information services provided within the III framework.

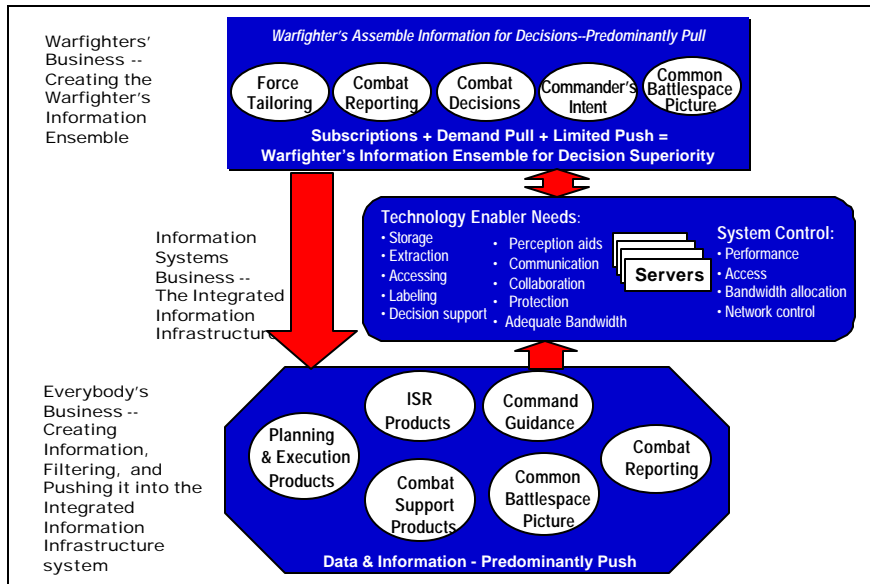


Figure C-4. High-Level Operational Architecture: The Information Input Segment

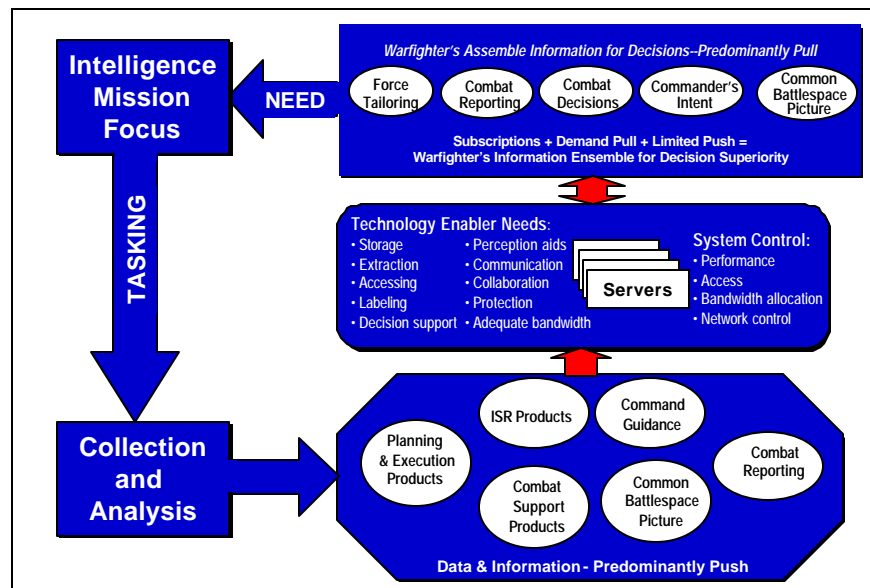


Figure C-5. High-Level Operational Architecture: Intelligence Mission Focus

The intelligence mission is one example we have chosen for illustrative purposes. Other “mission areas” or military capabilities that would be supported by the III include: request and delivery of indirect, remote precision fires; sensor-to-commander-to-shooter integration; sensor-to-sensor cueing and cross cueing; cooperative engagement, and many other such mission or functions.



## Long-Term Vision

The information infrastructure must include multimode data transport media including land-line, radio, and space-based elements. All of these media must be integrated into a ubiquitous, store-and-forward data internetwork that dynamically routes information from source(s) to destination(s), transparently to the user. This data transport segment of the infrastructure must be self-managed, be adaptive to node or link failure, and provide services to its users based on quality-of-service requests. These services include bandwidth, latency, reliability, precedence, distribution mechanisms (point to point, point to multipoint), and the like.

The infrastructure will link the user to a distributed processing environment that includes all types of computers situated at locations appropriate with their needs for power, environment, and space. This distributed computing environment will be integrated via the transport component of the infrastructure, thus enabling these processors to exchange information dynamically, share computation loads, and cooperatively process information on behalf of and transparent to the user. These attributes are summarized in Figure C-6.

- “An integrated, scaleable, fully distributed processing and transport environment” that
  - As dynamic, adaptive, self reconfiguring, robust, and secure
  - Provides tailored information automatically as required when required
- The information services
  - Are hosted on distributed computers, of many types, fully interconnected via the transport segment
  - Are provided via intelligent software agents
- The transport services
  - Are based on a network of networks (i.e., an internetwork)
  - Provides intelligent, adaptive routing of information at network/internetwork levels
  - Are self-managed, self-healing, and scalable

*Figure C-6. Integrated Information Infrastructure Attributes*

The infrastructure is an adaptive entity that integrates communication systems, computers, and information management resources into an intelligent system of systems. Each component of the III exchanges state information with each other, in order to enable the entire infrastructure to adapt to user requirements and any stresses imposed on the network by an adversary. This adaptability also enables the infrastructure to change its scale as necessary to support force structure(s) of arbitrary size, or to incorporate new processing, network, and communication technologies as they are developed. Thus, this infrastructure is a scaleable computing environment.

The information infrastructure must provide tailored information services to diverse users ranging from a single person to a collection of people, sensors, and/or weapons by means of intelligent agents – software entities, under the general control of the user, that are goal directed,

migratory, and able to create other software entities, and provide services or functions on behalf of the user.

Each user is served by one or more intelligent software agents that *proactively* push and pull appropriately packaged information. These agents perform such functions as fusing and filtering of information, and delivering *the right information to the right user at the right time*. They are proactive in the sense that they are aware of the user's situation and needs, and can provide information relevant to those needs without a specific user request. Figure C-7 provides a conceptual rendering of these agents.

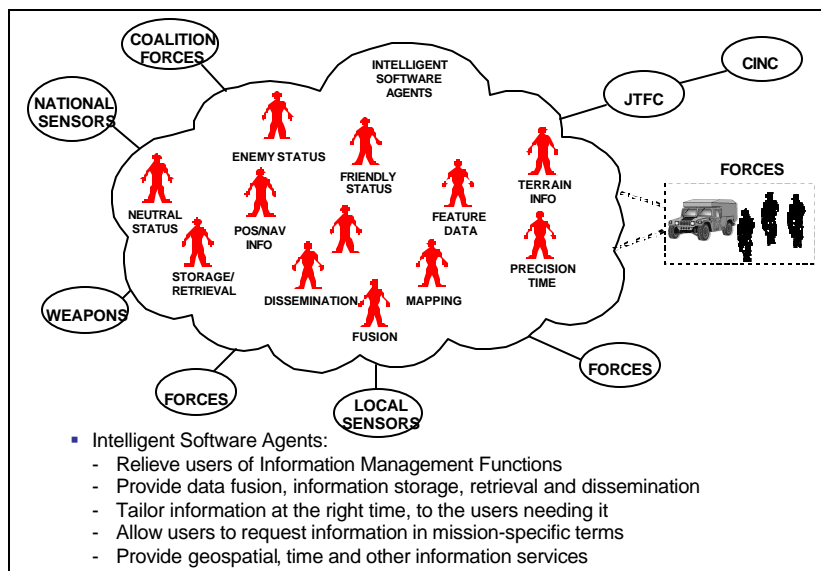


Figure C-7. Intelligent Software Agents

These agents multiply the personnel resources available to combat units by gathering and transforming data into actionable information to support unit operations, just as unit members would have to do were the software agents not provided. Warfighters are therefore freed of routine chores in favor of actual operations.

Because computing resources are distributed throughout the infrastructure, the infrastructure can adjust the amount of processing resources given to a force entity. The entities' processor need only provide access to the infrastructure, provide an adequate interface to the user entity, and enable the acquisition and presentation of information to the user. Thus, for example, a dismounted infantry person's information resources would be dedicated to supporting a rich human-computer interface (with voice recognition, heads-up display, speech synthesis, and communications). General computing resources to support this person(s) would reside within the infrastructure itself.

To the maximum extent feasible, the infrastructure's transport layer takes advantage of commercial technology and networks, by utilizing open-systems standards and protocols, and minimizes the use of service or function-unique hardware and software. For applications where military-unique capabilities (such as antijam, low probability of intercept, spread-spectrum waveforms and the like are required), military products will be developed or adapted to interface

with the overall architecture. Figure C-8 provides a conceptual summary of the entire Integrated Information Infrastructure.

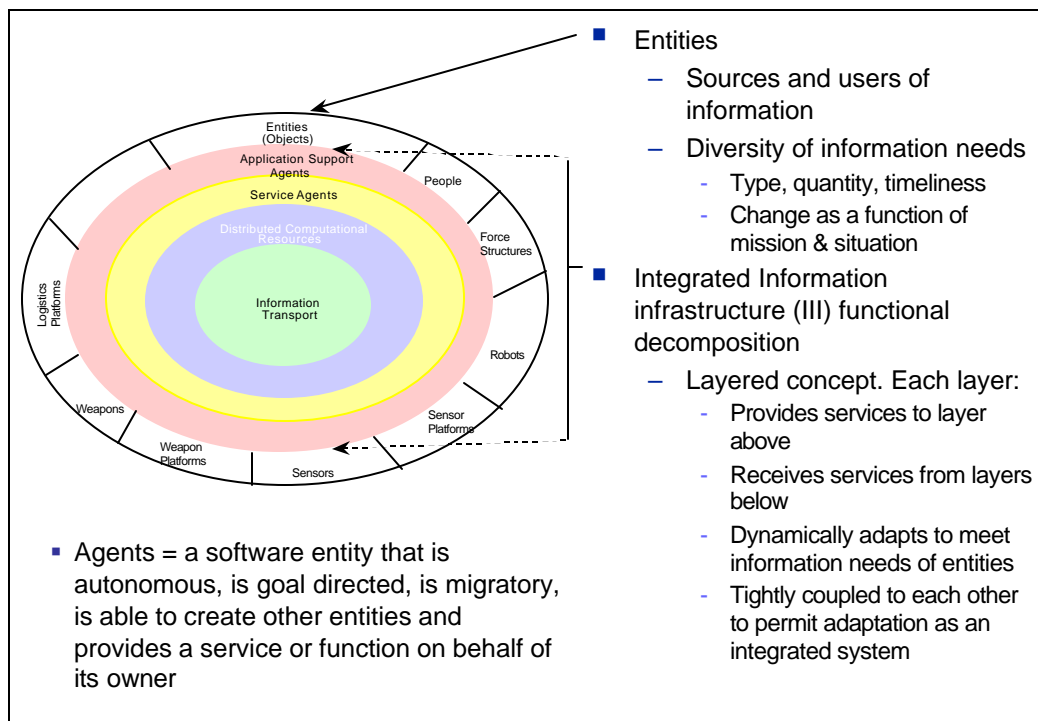


Figure C-8. Integrated Information Infrastructure: A Conceptual View

### Near-Term Vision

The value of the SIPRNET and NIPRNET have proven themselves in several recent real-world contingencies. Both of these systems of systems are integrated information infrastructure (albeit functionally focused) and are modest versions of the commercial World-Wide Internetwork (the “Web”) that is also an III on a grand scale.

The Web today integrates many diverse information sources and systems, many types of computers, people, sensors, many diverse types of devices, and supports many diverse information-based functions (financial services, logistics, video distribution, imagery distribution and so on). The Web also supports push, pull and subscription-based information services. Information is posted on Web pages by content providers and is utilized by consumers to conduct mission-essential decision making.

Using the Web, SIPRNET and NIPRNET as examples, let us assume that the near-term version of the III is an internetwork that integrates all C<sup>4</sup>ISR military systems into a single internetwork. For argument’s sake, let us assume that we start with the SIPRNET, extend/augment its transport (communication) component such that it integrates all (most) military communication systems into a common-user, digital data transport internetwork and that all Service C<sup>4</sup>ISR systems [TBMS, ATCCS (all BOSS’s), FBCB2, IT-21, and the like] are made

Web compatible and part of the near-term III. We now have the beginning of an integrated C<sup>4</sup>ISR infrastructure as envisioned in Figure C-8.

However, let us not stop here. Assume also that we integrate our weapon systems and sensors into this near-term vision — sensors, people, weapons, C<sup>4</sup>ISR computers are now entities that can generate, request or exchange information in much the same way that we do today on the commercial Web. Then, using Web type search engines, browsers and the like, we would have a reasonable ability to provide information push, pull and subscription services that would begin to meet the needs identified previously. The Services are, of course, experimenting with this vision from their own perspectives. Examples include the Army Tactical Internet, Navy and Marine Corps-wide Intranet, and the Air Force Theater Deployable Communications. We need to take advantage of these initiatives, broaden their vision and scope and move forward with a joint III objective that has both a near-term and longer-term set of milestones.

### *Summary*

We must set a goal the realization of the III vision in an evolutionary manner. As we succeed, we will enable, over time, the following military capabilities:

- Geographic separation and functional integration of command, targeting, weapons delivery, and support functions
- Support for split-base operations, force projection, information reachback, combat, and force protection for units large and small
- Common situational understanding, common operating picture, and informed and rapid decision making for joint forces
- Enhanced operational flexibility for commanders at all levels
- Reduce the logistics footprint in immediate combat area
- Full exploitation of sensor, weapon, platform, and processing capabilities
- Real-time or near real-time responsiveness to commanders' requests for information, fire support, and urgent logistics support

The sections that follow provide a high-level perspective of several of the four layers comprised by the III as shown in Figure C-8, beginning with the innermost layer and working toward the uppermost service layers.

## THE TRANSPORT LAYER

### *Global Connectivity*

The transport layer of the infrastructure consists of four tiers. These tiers are conceptual, because the interfaces between them are seamless and transparent to the user—tiering serves only to relate the information infrastructure to organizational and doctrinal concepts (see Figure

C-9). In fact, any entity in the information infrastructure can virtually and automatically be connected to and interact with any other entity directly. While such ubiquitous connectivity is expected to be a very powerful force multiplier, traditional organizational and doctrinal constructs are expected to change more slowly than the technology that makes such connectivity possible.

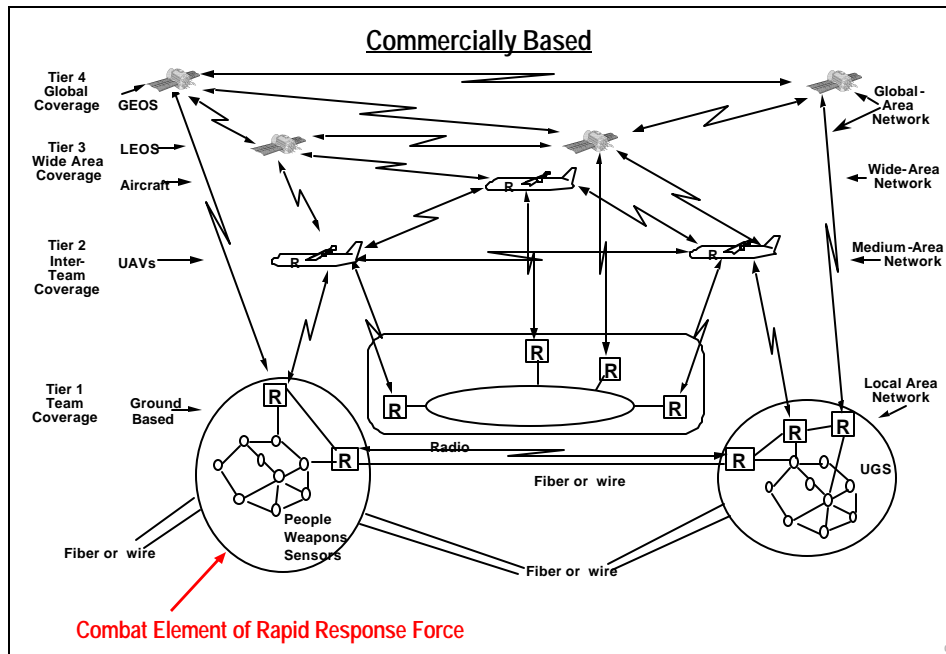


Figure C-9. Integrated Information Infrastructure: The Tiered-Transport Layer

### Tier 1

The first tier of the transport layer is the ground-based component. This infrastructure component comprises local-area networks that provide voice and information services to entities operating together in integrated or support missions. These transport networks are store-and-forward, packet-switched systems that are self-managed and adaptive, and provide peer-to-peer data relay and processing. The networks adapt to changes in the locations (i.e., the mobility) of its users; they have no centralized nodes or base stations that would enforce the use of a vulnerable star topology; and they automatically route information among participating nodes, based on real-time assessments of the network connectivity. These local-area transport networks can support a single person or a force structure of any size through appropriate subnetting.

Although there are a few modest examples of peer-to-peer, wireless, packet-data communication systems deployed in the private sector, the fundamental work in this type of technology has been and continues to be funded by DoD. This trend will likely continue, given that the private sector's present view of ground-based wireless data communications is predicated on the notion of deployed fixed infrastructure (base stations connected to the wireplant) to which, and through which, each mobile subscriber establishes a communication circuit. This commercial wireless system architecture is based on many years of legacy, point-to-point, voice-based telephony systems. This system architecture also facilitates billing and related revenue generating processes for mobile subscribers.

In contrast, the military has relied primarily on push-to-talk, broadcast, wireless communication systems for its mobile users. This system architecture, however, proves to be severely limited in supporting highly mobile users; dynamic, flexible force structures; and mission/time varying information transport requirements. These systems are also wasteful of spectrum and bandwidth.

For these reasons, the Defense Advanced Research Projects Agency initiated a Packet Radio program in the 1970s. This technology-based program was intended to explore the notion of building intelligent radios that would be networked to provide the highly mobile warfighter with data services while on the move. These radios would self-organize into networks, automatically route (relay) information from any source to any destination within the radio network (or across the internetwork to other users), automatically adapt to failed nodes or stress exposed on the network by an adversary, and perform other similar network services. This technology has resulted in systems such as the Army's Surrogate Data Radio developed by Hazeltine Corporation, and the Near-Term Data Radio developed by ITT.<sup>26</sup>

However, these systems only partially fulfill the vision for Tier 1 of the III. It is the research and development being pursued in the DARPA Small Unit Operations and Global Mobile projects, if appropriately focused and guided, that will lead toward technology that will meet the joint, mobile, warfighter needs. These programs will provide the fundamental knowledge and technology that will meet the network requirements set forth in the Joint Tactical Radio System (JTRS) Operational Requirements Document. The JTRS, with appropriate attention paid to providing network-level services as envisioned for the III, is a key program for realizing our vision.

It is anticipated that as these DoD-supported, technology-based programs generate stable technology (specifically, network algorithms and software), those technologies will ultimately be embraced in the private sector, as the need for supporting data and voice services to mobile commercial subscribers manifests itself. This technology transfer to the private sector is occurring today as evidenced by the acquisition of a start-up communication company by a large, traditional, personal-communication phone manufacturer. The startup was focused on using DoD packet radio technology for commercial applications. Development of wireless packet-switched data communications will continue to be driven by consumer demand for flexible, reliable, mobile information services and by the ascendancy to leadership positions in the telecommunications industry of individuals who relate to internetwork-based mobile data services.

## Tier 2

At the second tier, the transport layer incorporates airborne networks and processors for data transport and information services among force entities that require connectivity beyond that supported by their local area network. To support this broader area coverage, we envision autonomous air vehicles and manned/mission aircraft that support medium-area networking services. These platforms are cross-linked between themselves and other airborne and spaceborne networks, as required, and are linked to the local-area networks (LANs).

---

<sup>26</sup> All product or company names mentioned in this document are the trademarks of their respective holders.

The private sector is pursuing similar concepts of airborne-relay telecommunication platforms. Two such activities, which are currently raising capital, are the Skystation and Air Relay. The Skystation is conceived to be a station-keeping, lighter-than-air platform located 22 kilometers above the earth. This proposed activity would provide data services at 10 megabits per second to every home within the service area covered by each platform. The air relay, in turn, is intended to be an aircraft-based telecommunication relay that provides data services to ground-based users.

In both of these and similar commercial concepts, however, the system architecture (the location of platforms, relaying and switching, and bandwidth allocation) consists of parameters that are predefined and managed through centralized facilities. The military, however, needs much greater flexibility, adaptability, and autonomy for Tier 2 if the warfighting requirements noted above are to be met. Thus, in our vision of the III, the airborne platforms carry intelligent network-based radio nodes (JTRS) that perform all of the functions and services noted for the Tier 1 LAN. Consequently, the airborne nodes provide automatic, adaptive, packet-data routing and switching. All airborne nodes automatically integrate themselves into an airborne network, and the unmanned aerial vehicle platforms automatically position themselves to provide survivable, fail-safe coverage of the ground-based units. Other airborne elements, such as mission aircraft, automatically provide relays of opportunity within the Tier 2 segment. A DoD program that is beginning to address this extended set of network services for Tier 2 is the DARPA Airborne Communication Node program.

As noted in Figure C-9, the airborne nodes are cross-linked not only to themselves and the ground LANs but also to the space segment of the transport element. The notion here is that the airborne nodes act as pseudolites, and carry payloads that are integrated into the various commercial satellite telecommunication systems that have been and will be deployed in the next 10 years. As an example, preliminary analysis indicates that a Teledesic satellite package (700 kg) could be accommodated on a DoD high-altitude, long-enduring platform. With an appropriate antenna, an active phased array, on the UAV, the resulting pseudolite could provide high-bandwidth communication services to and between ground elements and could route traffic automatically to the commercial space segment for long-haul services. Other approaches can also be envisioned: for example, the pseudolite could use commercial satellites as trunk facilities between the airborne relays. The critical technical issues in realizing this richly interconnected, survivable airborne transport segment of the III are associated with the development of protocols and algorithms to provide the adaptive network services we have discussed.

### Tiers 3 and 4

At the third tier, the information transport infrastructure provides connectivity over widely dispersed areas through the incorporation of low earth orbiting (LEO) satellites. The fourth tier includes medium earth orbiting (MEO) and geostationary earth orbiting (GEO) satellites for global coverage. The space-based transport segment of the III should be based primarily on emerging commercial technologies. At the present time, many such systems of widely varying characteristics are expected to be available by 2005. Figures C-10 and C-11 summarize the systems that are currently being discussed. Table C-1 gives the maximum altitudes of LEO, MEO, and GEO satellites.

System	IRIDIUM	GLOBALSTAR	ICO	ELLIPSO	ECCO
<b>Company</b>	Motorola	Loral Space and Communications/ QUALCOMM	ICO Global Communications	Mobile Communications Holdings	Constellation Communications
<b>Number of Active Satellites</b>	66	48	10	14	46
<b>Orbit Planes</b>	6 circular polar (86.5°)	8 circular inclined (52°)	2 circular inclined (45°)	2 elliptical inclined (116.6°); 1 elliptical equatorial (0°)	7 circular inclined (62°); 1 circular equatorial (0°)
<b>Orbit Altitude (Km)</b>	780 (LEO)	1,414 (LEO)	10,355 (MEO)	527-7,846 (MEO) 4,223-7,846 (MEO)	2,000 (LEO)
<b>Satellites per Orbit Plane</b>	11	6	5	4 per elliptical; 6 per equatorial	5 per inclined; 11 per equatorial
<b>Beams per Satellite</b>	48	16	164\3	61	32 per inclined; 24 per equatorial
<b>Reported cost (\$B)</b>	3.4	2.6	4.6	0.91	2.8

Source: Evans, J.V. 1998. "New Satellites for Personal Communications," *Scientific American*, Vol. 278, No. 4, pp. 70-77 (April).

Figure C-10. Voice-Oriented Personal Communications Satellite Systems

System	ASTROLINK	CELESTRI	CYBERSTAR	SPACEWAY	GE*STAR	MORNING-STAR	TELEDESIC
<b>Company</b>	Lockheed Martin	Motorola	Loral Space and Communications	Hughes	GE Americom	Morninostar	Teledesic
<b>Number of Active Satellites</b>	9	63 LEO 9 GEO	3	20 MEO 16 GEO	9	4	288
<b>Orbit Planes</b>	Equatorial (0°)	7 inclined (48°); 1 equatorial (0°)	Equatorial (0°)	4 inclined (55°); 1 equatorial (0°)	Equatorial (0°)	Equatorial (0°)	12 inclined (98°)
<b>Orbit Altitude (Km)</b>	GEO	1,400 (LEO) and GEO	GEO	10,352 (MEO) and GEO	GEO	GEO	1,375 (LEO)
<b>Estimated Satellite Capacity (gigabits/s)</b>	6.0	1.5	9.0	4.4	4.7	0.5	10.0
<b>Estimated Capital Investment (\$B)</b>	4.0	12.9	1.6	6.4	4.0	0.82	9.0

Source: Evans, J.V. 1998. "New Satellites for Personal Communications," *Scientific American*, Vol. 278, No. 4, pp. 70-77 (April).

Figure C-11. Data-Oriented Personal Communications Satellite Systems

Table C-1. Maximum Satellite Altitudes

<b>LEO</b>	Low earth orbit below 2,000 km
<b>MEO</b>	Medium earth orbit approximately 10,000 km
<b>GEO</b>	Geosynchronous earth orbit, 36,000 km

\*Source: Evans, J.V. 1998. "New Satellites for Personal Communications," *Scientific American*, Vol. 278, No. 4, pp. 70-77 (April)



The challenge for DoD is to determine how best to leverage these emerging capabilities: more specifically, how to integrate these various systems with the other segments of the transport layer so that a ubiquitous, survivable, flexible, self-managed infrastructure results. A need exists for network- and internetwork-level algorithms that will enable integration of these disparate systems. These algorithms must be compatible with and exploit commercial internetwork standards and protocols. Specifically, the algorithms must be Internet Protocol aware and the entire transport layer of the III must adhere to evolving Internet standards, such as Internet Protocol V6 and Mobile Internet Protocol, and must adhere to the well-established Internet naming and addressing conventions.

The routers, labeled “R” in Figure C-9 are commercial Internet devices that maintain, in real time, knowledge about the entire transport layer’s topology and connectivity.<sup>27</sup> In conjunction with the intelligent software agents, the routers make dynamic decisions, based on this understanding, to ensure that information is transported from all sources to all destinations, as required. The dynamic routing is accomplished through protocols and distributed algorithms that are used in the commercial sector today.

## THE INFORMATION SERVICES LAYERS

The Integrated Information Infrastructure will provide tailored information to all users when and where needed. These services, provided in the future by the intelligent software agents, include (among many):

- Information fusion
- Terrain information (topographical and feature) dissemination
- Situational awareness (friendly and enemy) distribution
- A common grid reference to permit joint, distributed targeting and geolocation
- Precision time
- Information storage, retrieval, and tailoring

These agents – software entities that are autonomous, goal directed, migratory, and able to create other agents – will act on behalf of their owner. Achieving this level of intelligent behavior will be a technological challenge, but will be realized to a great extent by the year 2010.

The private sector is developing information-service technology for the World-Wide Web (Internet). Such services include Web browsers, search engines, information-push systems and the like. In each of these instances the conceptual framework of the service is modest: static profiling and filtering based on a-priori preferences established by the user. The software supporting these services does not (yet) learn users preferences, does not fuse data into information, does not adaptively manage information on behalf of a user, and is not adaptive to changes in transport services induced by failures, fluctuating user traffic, or intentionally induced performance degradation by a malicious adversary. These software tools do, however, provide access to storage, retrieval, and dissemination of large volumes of information to millions of users every day.

---

<sup>27</sup> Routers are currently used in the Internet.

In the near term, the III would exploit these limited private sector information management and dissemination technologies. In a manner similar to DoD's implementation of the SIPRNET, NIPRNET and the Joint Worldwide Information Communications System, information services will be provided through the use of commercial browsers, standardized Web pages, standardized relational databases, standardized user interfaces, and a standardized geospatial coordinate system to which information would be registered. In addition, a common messaging system and defined data-elements and associated dictionary must be established for DoD.

Using commercial standards such as hypertext transport protocol (HTTP), hypertext markup language (HTML), virtual reality markup language (VRML) and other commercial internet network standards called out in the Joint Technical Architecture (JTA), critical legacy and future DoD C<sup>4</sup>ISR systems would be integrated onto and post information to the III. The warfighter would then pull information from the III to support their operational needs. Furthermore, because information on the III would be geospatially registered, critical information can be selectively pushed to forces who are in or transiting to a threatened geographic location.

Using emerging Web-based technology, our warfighters would have access to unprecedented amounts of information through the near-term III. Using Web search-engine technology, the warfighter could extract from the III intelligence, maneuver control, fire control, logistics, and other such information from C<sup>4</sup>ISR systems generating and posting this information.

From a system-to-system perspective, a DoD common message set and data elements would permit real-time updates from applications/databases to applications/databases of the C<sup>4</sup>ISR systems integrated into the III. Systems such as Maneuver Control System (MCS-Army), Theater Battle Management Command Systems (TBMCS-AF), Joint Maritime Information System (JMISIS, Navy), and Global Command and Control System (GCCS, Joint) would then be able to update each other's information bases, thus providing a common, integrated picture of the joint battlespace to the warfighter.

In the long-term, information needed by the warfighter would be managed through the intelligent software agents. These agents would, as noted earlier, reduce the effort imposed on the warfighter to collect his or her information ensemble. Research and development on intelligent software agents is presently being pursued both in the private and public sectors. Within DoD, DARPA has several programs that are investigating software agents. One program has defined these agents as:

- An agent is a software component or system that is:
  - Embedded in, and “aware” of, an environment (communicative)
  - Dynamic in its behaviors (not single I/O mapping) (autonomous)
  - User enabled and steered, but “empowered” to act for user (capable)
  - Able to improve its behavior over time (adaptive)

Because of this broad definition, the term “software agent” is used to describe many different implementations depending on the capabilities of the software that is being described. Examples of these descriptions include:

- Mobile code
- “Disembodied” code with temporal duration or persistent state
- Web search tools
- Semantic broker and name space services
- Electronic commerce with message-passing entities
- Interface animation
- Dynamic services

These definitions are diverse and not necessarily synonymous. However, they encompass what will eventually be the types of services provided by intelligent software agents in the future.

A key program at DARPA in this technology area is called Cooperative, Agent-Based System (CoABS). The goal of this program is to design, implement and test a prototype “agent grid” – a collection of intelligent software agents that collaborated to provide a service to users. The focus of the prototype will be to address issues related to diverse agent types cooperating through an agent broker to do collective problem solving.

The output of this science and technology program will be an experiment wherein the intelligent agent grid will be used to support a Network Centric Warfare experiment. This experiment is structured as indicated in Figure C-12.

- Warfighter Hypothesis
    - Warfighting processes supported by new concepts and technology allow the Navy to enter and remain in the littorals indefinitely with the ability to provide protection, fires and C4I support to forces ashore
  - Program Hypothesis
    - Cooperating agents, by correlating reach-back and on-ship data, can exploit currently unused data to focus surveillance assets for more effective TBMD
  - Potential Impact
    - Enabled region-specific tasking of Fleet Surveillance Assets
    - Enabled Preemptive Strike

*Figure C-12. Testing Use of Intelligent Agents in Network Centric Warfare*

In summary, DoD should exploit the information-management standards and technologies being developed by the private sector, and must also continue to fund the science and technology initiatives that will lead to the intelligent agents envisioned herein. DARPA and the Service laboratories have focused their resources on developing intelligent agent technology that

leverages and supplements private-sector technologies and concepts in order to meet warfighter needs.

## INFORMATION INFRASTRUCTURE: CURRENT DEVELOPMENTS

The vision and requirements for the III have evolved during a period of remarkable rate of change in information technology. Within the past six years, commercial investment has propagated a Web of information services. Commercial activity is moving aggressively to set standards fostering open, interoperable systems. The commercial information technology industry investment in research and development is very substantial and growing, as companies compete to rapidly transition information technology to the market place.

Within DoD, numerous studies on C<sup>4</sup>ISR have been completed or are in progress. These studies recommend various strategies, visions, interoperability approaches, requirements, and architectures, but there is no overall, organizing principle against which these competing ideas may be measured. Further, DoD is sponsoring numerous and diverse technology development efforts, including multiple radio programs, C<sup>4</sup>ISR platform and product initiatives, and programs to explore new technology in the areas of information collection, fusion, and management. These, too, are poorly coordinated, duplicative, and not organized along a central set of protocols and standards. To its credit, DoD is reorganizing to focus on C<sup>4</sup>ISR, by appointing a Corporate Information Officer, among other steps. The success of this effort remains to be seen, since it resembles many such efforts in the past that had little real effect on the way DoD C<sup>4</sup>ISR -related systems are planned and procured.

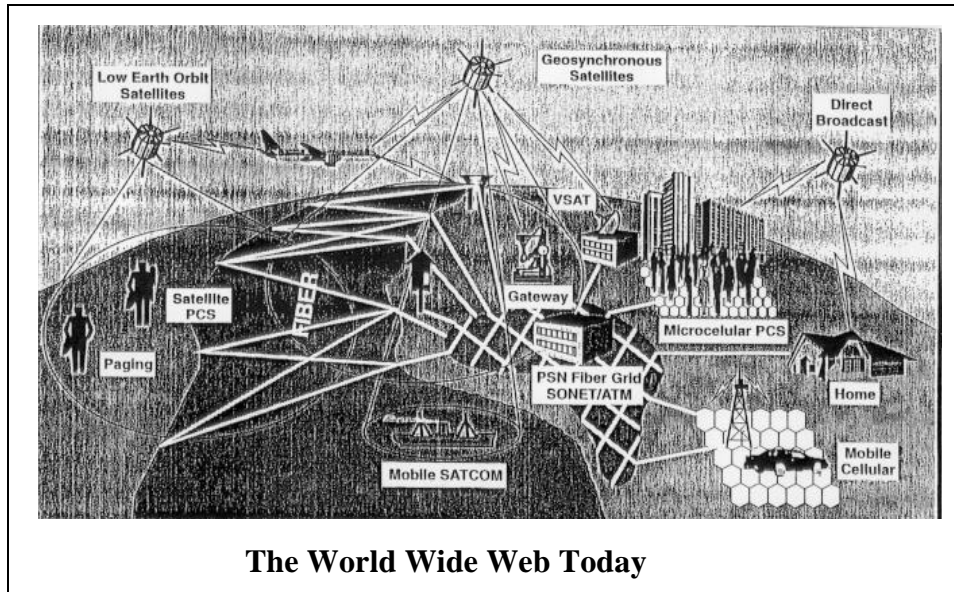
Similarly, DARPA and the Service laboratories are developing elements of the III. Examples include, as described above, the Global Mobile program (investigating technologies to support mobile computing); the AICE (investigating broadband, broadcast information distribution); Intelligent Information Integration (investigating accessing and aggregating information for many heterogeneous databases); Cooperative, Agent Based System and network management technology development.

However, in all of these initiatives, the program goals have been pursued nearly independent of each other. Furthermore, the envisioned environment in which the various technologies are to be applied is modest compared to that envisioned for the III. In the latter case, we foresee many hundreds of thousands of communication and processing nodes distributed globally, all cooperating to provide robust, reliable information transport and intelligent information services to the combat units and other users.

The Global Information Infrastructure, also known as the "Web", serves as an example of the ubiquitous connectivity that the distributed information infrastructure will require. The limitations of today's Web, especially at a "point of conflict" under stressed conditions, highlights the need for technology development to put an Integrated Information Infrastructure in place.

Figure C-13, which shows the transport infrastructure that exists as part of the Web, provides an example of what is envisioned for the III. Similarly, the information services (data storage and retrieval software) emerging on the Web are very early examples of what is envisioned for the intelligent software agents. This is not meant to suggest that the Web become the III, but that Internet technologies (protocols, standards, algorithms, and information

application concepts) provide a starting point for establishing a baseline III in support of military operations. This baseline III, owned by DoD, would then be augmented through a DoD science and technology program to realize the vision presented herein. Similarly, as commercial information technologies mature, they would also be integrated into the III.



*Figure C-13. The World Wide Web-Transport Infrastructure: An Existence Proof*

## SECURING THE INFORMATION INFRASTRUCTURE

Security for the integrated information infrastructure merits special discussion. The exploitation of commercial protocols and standards provides the technology base necessary for the 21st century integrated information infrastructure. Because portions of the infrastructure will incorporate commercial network technology, and much of the infrastructure will be based on commercial technology, security must be an integral design consideration throughout the infrastructure's development. Further, because the infrastructure will also necessarily incorporate commercial telecommunication systems, these systems must be carefully evaluated to balance the benefit versus the risk each such incorporation presents to the III user community.

There are market forces that will continue to aggressively motivate the private sector to provide security for the Web. Specifically, the growth of electronic commerce has already motivated the development of standards and technology for conducting secure information transactions. Examples of these standards and technologies are Internet Protocol Security; Secure Socket Layer; X.509; public key infrastructure, and key distribution mechanisms; strong encryption algorithms; intrusion detection systems and inexpensive biometric systems (fingerprint readers and retinal scanners). These standards provide for information authentication, nonrepudiation, and secure transport.

Furthermore, the private sector is starting to address the issues of security for mobile code and for countering denial-of-service attacks and the insider threat. As noted earlier, examples of mobile code are Java applets that are downloaded onto a user's machine and executed locally, or

migratory intelligent software agents as described previously. Several approaches have been identified for securing such code – such as sandboxing, code signing, firewalling, and proof-carrying code – however, these approaches have yet to be implemented, tested, and standardized.

For the transport layer of the III, careful attention to information operations is mandatory. DoD must work with industry to ensure that the space-based segment of the III is made robust against information operations performed by an adversary. For example, protection of the control and signaling channels for the space nodes is critical.

Similarly, the DoD will continue to be the focal point for developing low probability of intercept (LPI) and low probability detection (LPD) waveforms for the networked, primarily ground-based communication networks described previously. Software-programmable radios, such as JTRS radios, provide the flexibility needed to implement an adaptable, self-managed system. This same flexibility provides an opportunity to enhance information assurance services. For example, the network-level protocols for these radios could make every node look the same (in a traffic analysis) as any other node, thereby limiting an adversary's ability to identify and target high-value, force-structure entities such as command and control centers. Similarly, the network-level protocols could, if the system detects it is being attacked, change its waveforms in such a manner that the radio emissions appear to be those of an adversary's unit, or change it to cause a radio node to appear to be a radar site. Network protocols and algorithms could achieve radio-network-based cover, concealment, and deception in ways never thought of in the past.

Appropriate security for the distributed information infrastructure must be realized through the development of a comprehensive security architecture, policy, training, and testing. Leveraging the security technology and techniques developed in the private sector, the architecture must provide flexible, dynamic, adaptive, and rapidly reconfigurable security in support of the software agents at work in the infrastructure.

Security technology is available today from the private sector which, when combined with DoD developed network encryption systems, now also available commercially, can provide good security for the III. Employing a defense-in-depth architecture, leveraging network encryption systems, firewalls, application gateways, and certificate-based selective access to information bases should provide protection for the III if appropriate security policies, system configuration and management processes, and security accountability are enforced.

## IMPLEMENTING THE III

The Integrated Information Infrastructure must be implemented in an evolutionary manner. A plan must be established that sets specific functional objectives, technical milestones, and system architecture objectives that are to be achieved over reasonable periods of time. The plan will evolve as a result of lessons learned in the joint warfighter experiments, but nonetheless goals must be set.

Figures C-14 and C-15 provide a conceptual description of the III in about 2005. The cost of implementing this mid-term, baseline realization of the III would be in the range of several billion dollars over five years. These costs include funds already being expended or earmarked for C<sup>4</sup>ISR system acquisitions and upgrades, and the average yearly DoD science and technology investment for information technology. These existing expenditures must be used in part to

support the transition of the legacy C<sup>4</sup>ISR systems to comply with the JTA, and their integration into the III.

- Users and sources know location of repositories and store/retrieve information using commercial push/pull technologies and services, such as
  - Browsers (Pull)
  - Channels (Push)
  - Multicast, broadcast and unicast
- Military resources are augmented by commercial transport technologies, such as
  - Commercial satellite telecommunications
  - Commercial satellite direct broadcast
  - Fiber (as available)
  - Secure end-to-end encryption of voice and data using public key encryption systems, technologies, and standards
- Tiers 1, 2 and parts of Tier 3 deployed:
  - Tier 1: JTRS, PCS, and NTDR-like components
  - Tier 2: NTDR-like and JTRS components
  - Tier 3: PCS and Tier 2 trunking components

*Figure C-14. Mid-Term III Vision*

- Fully integrated legacy C4ISR systems augmented with JTRS and some commercial information management and transport technologies:
  - C4ISR information elements and types defined and implemented (messages, images, video)
  - C4ISR information types implemented via open standards (e.g., MPEG2/4, WGS-84, object-based)
  - C4ISR legacy transport systems seamlessly integrated via Internet standards and protocols (IPVG, Mobile Internet Protocol, RSVP, Quality of Service)
  - Messaging protocols and standards implemented to allow C4ISR applications to interoperate (such as JVMS augmented for multimedia)
  - Service transport systems integrated within and across service boundaries [e.g., living Internet (Army) integrated with AF and Navy Internets]
  - Integrated information repositories defined and accessible to all sources and users (e.g., relational databases, image and video databases, Web pages)

*Figure C-15. Mid-Term III Vision*

Of necessity, the mid-term III will include a significant amount of DoD C<sup>4</sup>ISR systems augmented with commercial information technology and services. The end game for the III, however, is that it be based primarily on commercial information technology augmented by

military-unique information technology, if and when absolutely necessary and justified by cost/benefit/risk analysis. The evolution from the mid-term to the long-term III would occur over an additional five years. A high-level definition of the long-term III is given below in Figure C-16.

- Fully integrated infrastructure using primarily commercial information management technologies
  - Object-based representation of C4ISR entities
  - Intelligent software agent supporting information push/pull
- Transport infrastructure includes commercial LEO/MEO/GEO satellite communications systems:
  - Area, theater and global coverage
  - Cross-linked to each other
  - Cross-linked to airborne communications platforms
- Ground units supported by:
  - JTRS for mobile, adaptable, flexible, networked and internetwork
  - Commercial PCS for complementary services
- DoD ISR resources augmented with commercial and allied/coalition sensor satellites
  - SPOT
  - QUICKBIRDS
  - WIS
  - Many others

Figure C-16. Long-Term III Vision

The recommendations suggest using the DoD Architecture Coordination Council (ACC) to implement the III. The ACC will have to harmonize the near-term, mid-term, and long-term operational, system, and technical architectures; develop the plan and road maps for evolutionary deployment; and ensure that DoD and Service funds committed to or planned for C<sup>4</sup>ISR infrastructure acquisitions are focused on and supportive of achieving the III vision – a large but critically important task, if information and decision superiority are to be achieved.

## INSTITUTIONALIZING THE III

Realizing the III vision, and thereby achieving information superiority as proposed in *Joint Vision 2010*, and consequently, decision superiority as proposed by the DSB will not be a simple undertaking. Broad issues will have to be addressed, such as the use and integration of existing military C<sup>4</sup>ISR infrastructures (both technical and capitalization issues); the definition of Service Title 10 responsibilities; the development of a C<sup>4</sup>ISR acquisition policy; the definition of a single, unified DoD III vision and champion; and the development of a single, integrated Joint Technical Architecture supporting the III. However, all such issues can be successfully addressed if a unified commitment by the Office of the Secretary of Defense, Joint Chiefs of Staff, and Service Chiefs is forged.



Assuming that such a commitment is achieved, the III could be implemented in an evolutionary manner over the next 10 years. In 5 years, a significant system could be in place which will be an integrated, flexible, efficient, joint C<sup>4</sup>ISR infrastructure to support joint-force operations from strategic through tactical force levels. However, to achieve the near- and longer-term goals for the III, several critical DoD activities need to be started or reinforced immediately.

First, a **single, unified OSD/Service vision** for the III should be established. Over the past years, several visions for an integrated, joint C<sup>4</sup>ISR infrastructure have been proposed by JCS, the Services, and the Service Science Boards. These visions include the Network Centric Warfare (JCS); InfoSphere (Air Force Scientific Advisory Board); Living Internet (Army); Integrated Information Infrastructure (Defense Science Board); IT-21 (Navy); and Advanced Battlespace Information System (JCS and DDR&E). Now is the time to develop a single DoD vision for an III leveraged by bringing together the best ideas from each of these various visions. The integrated vision should to be achieved by 2020.

Second, to achieve Service C<sup>4</sup>ISR interoperability and leverage the III with private-sector information technology, DoD and the Services must embrace a **primarily commercial, standards-based joint technical architecture**. Very significant work within the Army and in OSD has resulted in the establishment of the JTA-Army and a JTA. However, it is imperative that the JTA be a *minimum set of essential commercial information processing and transport standards and protocols*, augmented by DoD-unique standards only when absolutely necessary. A *minimum set* is critical to interoperability between Service and DoD C<sup>4</sup>ISR infrastructures.

Third, **the JTA should be used as a basis for setting acquisition policy for all C<sup>4</sup>ISR systems**. For example,

- All new solicitations for C<sup>4</sup>ISR systems should include compliance with the JTA as a technical evaluation criterion
- All C<sup>4</sup>ISR systems under procurement must include implemented transition plans for achieving compliance with the JTA when the systems are delivered
- All legacy C<sup>4</sup>ISR systems that are critical to the Services and that will remain in the inventory should also develop transition plans to be implemented through preplanned product improvement processes.

Although not all transition plans would be put into effect, (possibly due to cost or other factors), at least DoD can make an enterprise-level decision as to why the plans should not be implemented and what impact these decisions will have on joint C<sup>4</sup>ISR interoperability. However, OSD, JCS and Service goals should be to aggressively limit the number of non-JTA-compliant systems that remain in the DoD inventory after the transition period (about 5–8 years). The Army has implemented such policies, although waiver policies have become less stringent over time, and their experience might serve as a basis for defining and establishing DoD-wide policies.

Fourth, although commercial information technology will provide a wealth of systems, concepts, and resources necessary for implementing the III, it will be necessary to develop **DoD-unique capabilities that must augment the technology exploited from commercial sources**. Intelligent agent technology; adaptive, peer-to-peer, ground-based mobile communication networks; and LPD/LPI wireless waveforms are examples of a few areas that will require

continued DoD science and technology funding. Similarly, experimentation with commercial information technology will be mandatory, in a military context and integrated with legacy and military-unique C<sup>4</sup>ISR technology in order to evaluate the commercial technology, and to understand its potential impact on military operations. Thus, a complementary DoD science and technology program should be established that is consistent with a “revised” JTA (revised to constitute a minimum set of standards) and the associated new DoD acquisition policies. Specifically, the C<sup>4</sup>ISR technology development supported through science and technology funding (as well as advanced technology demonstrations and advanced concept technology demonstrations) should be compliant with the JTA to the maximum extent possible, or at a minimum must be compatible with the JTA, so that these technologies can be integrated into the III when completed. These new technologies will also provide input to periodic JTA updates when they result in commercial or DoD open standards that augment the JTA set.

Fifth, **a set of operational architectures** must be established that provides a framework for the type of joint forces that will be deployed for the spectrum of operations envisioned in this study. Although it is clear that the United States has “never fought the war we planned for,” having an exemplar set of joint-force operational architectures that specifies which force elements must exchange information with which, as well as what they have to exchange, over what time frames, and how often will help set the requirements for the system architectures that realize the III. The III will allow DoD to mix and match force elements; however, the set of operational architectures will help set boundary conditions for the III. The operational architectures should be developed with this objective in mind.

Sixth, **mid-term and a long-term system architectures** should be established for the III. The mid-term architecture should identify all DoD C<sup>4</sup>ISR systems that the mid-term III will comprise, as well as the commercial protocols and standards used to integrate these systems and the commercial technologies used to augment them. Examples of DoD systems and technology that the mid-term architecture might include are CTAPS, JMSIS, ATCCS, GCCS, GCSS, WIN-T, SINCGARS, JTRS, and commercial LEO satellites.<sup>28</sup> The architecture should, for each layer of the III, define the JTA-based protocols and standards used by each system, the interface specifications between the systems, a common application-level message system (e.g., the Joint Variable Message Format), standards for image and video representations that flow between the systems, and the like.

Similarly, for the 2010 time frame a conceptual system architecture that supports the ultimate III vision should be developed. This system architecture will set the direction for the evolution of the III system of systems.

Finally, a **series of joint warfighter experiments** should be planned that allows for the evolutionary deployment of the III. These time-phased experiments will serve to provide concept/technology/architecture course corrections as the III vision is realized. At the same time, these experiments will permit warfighters to adapt tactics, techniques, and procedures based on their having an integrated C<sup>4</sup>ISR infrastructure that will provide joint information superiority.

---

<sup>28</sup> CTAPS: Contingency Theater Automated Planning System; ATCCS: Army Tactical Command and Control System; GCCS: Global Command and Control System; WIN-T: Warfighter Information Network–Terrestrial; SINCGARS: Singles Channel Ground and Airborne Radio System.

Figures C-17 to C-20 summarize the above recommendations. These figures also assign responsibilities for these (and other related) recommendations and indicate an anticipated level of funding to achieve each.

To the above recommendation list one overarching recommendation should be added: Implement the III. Developing the architectures is essential to realizing the III, but an entity must be assigned the responsibility for ensuring that it is implemented. Thus, the charter of the Architecture Coordination Council should be broadened from its present role of coordination to one of proactive management and oversight for the implementation of the III. Its mission will be to facilitate, motivate, and guide the realization of the III.

## I. Implement the III

### I.I Architecture Coordination Council (ACC) Play Lead Role For Implementation

- ACC Must:
  - Accelerate the development of the three joint architectures
  - Ensure compatibility of Joint and Service architectures
  - Ensure JTA is promulgated within services
  - Develop III time-phased implementation plan
  - Oversee Implementation of Baseline III (2005) and full III (2010)

**Who: USD A&T, ASD/C3I, J6**

**When: Immediately**

*Figure C-17. ACC Implementation Responsibility*

II. Establish Acquisition and Technical Architecture Framework

II.I. Designate USD A&T (DAE) as the DoD Technical Architect with supporting Executive Director and Staff

- Make Executive Director Executive Secretary of ACC

<b>Who:</b>	<b>Sec Def Direction</b>
<b>When:</b>	<b>Immediately</b>
<b>Cost:</b>	<b>\$10M/Year</b>

II.II Technical Architect Will:

- Publish a unified technical vision for the Integrated Information Infrastructure that incorporates the concepts from:
  - Network Centric Warfare (J6)
  - IT - 21 (Navy)
  - Infosphere (AF SAB)
  - "Living" Internet (Army)
  - Information Infrastructure (DSB)
- Revise the Joint Technical Architecture (JTA) as a *minimal essential* set of commercial information technology Standards and Protocols to:
  - Become the building code for the III and all C4ISR systems
  - Limit military-unique standards
  - Establish policies for acquisition of all new C4ISR systems to ensure compliance with JTA
  - Require JTA compliance transition plans for legacy C4ISR systems
  - Make tradeoff decisions, as appropriate, for transition-plan implementation
  - Establish annual JTA update process:

<b>Participants:</b>	<b>ASD (C3I), Joint Staff and Military Service Chiefs</b>
<b>When:</b>	<b>First delivery December 1998</b>
<b>Cost:</b>	<b>\$15M/Year</b>

II.III Establish an information technology advisory board to the executive director

- Composition: The best minds from the Service laboratories and academia
- Mission: Facilitate the realization of the III by:
  - Monitoring and understanding commercial technology and military needs
  - Conducting risk/benefits analyses
  - Recommending DoD III technical investment to leverage commercial information technology
  - Striving to minimize DoD-unique infrastructure
  - Provide Inputs to DoD System Architect

<b>Implementation Responsibility:</b>	<b>Executive Director with assistance from Service Laboratories</b>
<b>When:</b>	<b>Now</b>
<b>Cost:</b>	<b>\$10M/Year</b>

II.IV Develop a science and technology investment strategy that allocates resources to meet military-unique aspects of the III

- Require technology to be compliant with JTA
- Require ATDs, and other initiatives to integrate, develop and demonstrate technologies compliant with JTA

<b>Who:</b>	<b>DDR&amp;D with Service Participation</b>
<b>When:</b>	<b>September 1999</b>
<b>Cost:</b>	<b>Within Present Funding Resources</b>

Figure C-18. Acquisition Policy, Vision, and Technical Framework

- III. Establish System Architecture and Development Strategy
- III.I ASD/C3I, as DoD system architect, is responsible for:
- Developing and publishing joint system architecture
  - Provide technical input to achieve III security and information assurance
  - Assessing C4ISR transition plans and providing inputs to DoD investment strategies
  - Track and provide technical guidance for all C4ISR and weapons platform acquisition, ACTDs and ATDs to ensure compliance with JTA and fit into III System Architecture
  - Provide technical inputs to JTA updates and configuration management

**Who: Joint Staff and Service Participation**  
**When: Now**  
**Cost: \$30M/Year**

*Figure C-19. System Architecture*

- IV. Establish Operational Architecture and Deployment Strategy
- IV.I JCS develop and publish Warfighter Joint Operational Architecture that captures
- Operational concepts
  - Processes and procedures for information generation, conditioning, fusing and use
  - Weapons, sensor and platform functional characteristics
  - Force structures
- IV.II ACOM conduct a continuing series of experiments, with joint forces, to incrementally realize the III
- Exploit already scheduled Joint and Service exercises
  - Design and plan experiments
  - Address and evaluate results
  - Provide recommendations to joint operational architecture and joint system architecture
  - Establish III Battle Laboratory as executive agent for experiment program

**Who: With Service Participation**  
**When: June 1999**  
**Cost: \$25M**

**Who: JCS Direction, ACOM Execution**  
**When: Start Now**  
**Cost: \$40M/Year**

2

*Figure C-20. Operational Architecture and Experimentation*

## SUMMARY

Figures C-21 and C-22 summarize the ideas and recommendations presented in this section of the 1998 DSB study on *Joint Operations Superiority in the 21st Century – Integrating Capabilities Underwriting Joint Vision 2010 and Beyond*. The focus of this section has been on an III; however, the III must be implemented with reference to the ideas and recommendations

presented in the other sections. For example, Information Operations will play a critical role in development of the III: they must be secure, provide information assurance, and be resistant to enemy attacks. Furthermore, weapons and sensors (as well as people) will use the III for information dissemination, exchange, cueing, fusion, and enemy engagement. As noted in Figures C-1 and C-5, the III will be common to and support all military platforms and their many diverse military functions. Thus, elements of the III will be embedded in all sensors, weapon platforms, and command and control systems. Consequently, the JTA will apply to these entities as well. It is this view, *that all military entities and functions are part of and serviced by a common integrated information infrastructure that will permit DoD to exert, to the maximum extent possible, the power of its military forces in future contingency operations.*

- To realize the promise of Joint Vision 2010, information superiority is a must
- To achieve information superiority, an integrated information infrastructure is a must
- An Integrated Information Infrastructure must
  - Be based on a unified DoD-wide III vision
  - Provide joint forces with common situational understanding and common operating picture and support informed, rapid decision making
  - Integrate legacy C4ISR systems and fully exploits commercial information technology such as the Internet, PCS and satellite sensors
  - Be secure and provide information assurance by:
    - Setting responsibilities and policies for developing and publishing joint operational, technical and system architectures
    - Establishing policy and procedures to exploit commercial information technology
    - Setting milestone targets for III deployment
    - Conducting evolutionary warfighter experiments leading to milestones/deployment/goals set for 2010 and 2020

*Figure C-21. Integrated Information Infrastructure: Summary*

# Integrated Information Infrastructure

<p><b>Description and Rationale of the III</b></p> <ul style="list-style-type: none"> <li>• An integrated, scalable, fully distributed processing and transport environment that             <ul style="list-style-type: none"> <li>– Moves information and command orders from any source to any destination</li> <li>– Provides tailored information automatically as required, through intelligent software agents</li> <li>– Is dynamic, adaptive, self reconfiguring, robust, and secure</li> <li>– Combines appropriate legacy C<sup>4</sup>ISR systems and modern information technology</li> </ul> </li> <li>• Permits full exploitation of sensor, weapon, platform, and processing capabilities             <ul style="list-style-type: none"> <li>– Sensor-to-shooter/commander, cooperative engagements</li> <li>– Sensor-to-sensor for self tasking and cueing</li> </ul> </li> </ul>	<p><b>Implications of Force Characteristics</b></p> <ul style="list-style-type: none"> <li>• Permits geographic separation and functional integration of command, targeting, weapons delivery, and support functions</li> <li>• Provides single, integrated infrastructure for all military information needs: C2, ISR, fire control, logistics, etc.</li> <li>• Supports split base, force projection, information reachback, small-unit combat, force protection, etc.</li> <li>• Supports joint forces with common situational understanding, common operating picture, and informed and rapid decision-making</li> <li>• Provides enhanced operational flexibility for commanders at all levels</li> <li>• Permits logistics footprint in immediate combat area</li> </ul>
<p><b>Enablers</b></p> <ul style="list-style-type: none"> <li>• Explosive growth of commercial information technology             <ul style="list-style-type: none"> <li>– Wideband satellite and fiber networks</li> <li>– High-capacity terminals, switches, intelligent software</li> <li>– Commercial security architectures and technology</li> </ul> </li> <li>• Commercial internetwork technology             <ul style="list-style-type: none"> <li>– Open protocols and standards</li> <li>– Automatic information push and pull</li> </ul> </li> <li>• Joint Technical Architecture</li> <li>• Investments by DoD to keep abreast of commercial technologies, to subsidize adoption of commercial systems to meet military needs, and to develop military-unique capabilities</li> </ul>	<p><b>Major Uncertainties</b></p> <ul style="list-style-type: none"> <li>• Degree of OSD/JCS/Service commitment to             <ul style="list-style-type: none"> <li>– Overcoming stovepipes and information technology legacy burden</li> <li>– Developing and implementing policy to exploit COTS information technology</li> <li>– Understanding, evaluating, and employing commercial information technology</li> <li>– Developing and gaining acceptance of DoD and Service Technical Architecture to achieve information technology interoperability</li> </ul> </li> <li>• Sustained DoD R&amp;D investments that address military-unique information technology requirements, including             <ul style="list-style-type: none"> <li>– Automated, adaptive, internetworks; intelligent software agents</li> <li>– Continuing DARPA involvement in data and communication networking technologies</li> </ul> </li> <li>• Technology to provide security for nomadic agent-based software</li> </ul>

Figure 22. Critical Operational Capabilities: Enabled by the III

---

## ANNEX D. TECHNOLOGY GRAND CHALLENGES





---

## ANNEX D. TECHNOLOGY GRAND CHALLENGES

The task force recommends adopting “grand challenge” military capabilities as a means of focusing cross-disciplinary technology development. Grand challenges are aimed at solving specific military needs or achieving new capability, but can also serve as a mechanism for driving and focusing science and technology investments. The task force identified a set of four grand challenges particularly related to developing joint rapid response capabilities. These grand challenges are expected to yield at least an order-of-magnitude increase in warfighting capability of future U.S. military forces. Each is discussed below.

### BIOSHIELD

In the 1990 Gulf War, concerns arose about the potential impact of a biological warfare attack on U.S. forces in the field or on civilians in the U.S. homeland. In the intervening years, further study has indicated that this threat is more serious than originally imagined. In the eight years since the Gulf War, some progress has been made on developing technology to better detect biological attacks as well as to protect U.S. troops and treat exposed individuals. However, today U.S. citizens and troops remain vulnerable.

Figure D-1 lists some of the challenges posed by the threat of biological warfare. Potential threats range from natural pathogens that have evolved or been mutated to carefully designed pathogens. There are a variety of ways by which these agents can be directed. Potential targets include not only humans, but also animals, plants, and materials. Of particular concern, are mechanisms by which specific groups of people can be targeted. Today we do not have to go very far down the threat spectrum to find threats to which the United States is vulnerable – so developing more exotic biological threat agents is, from the attacker’s point of view, largely unnecessary.

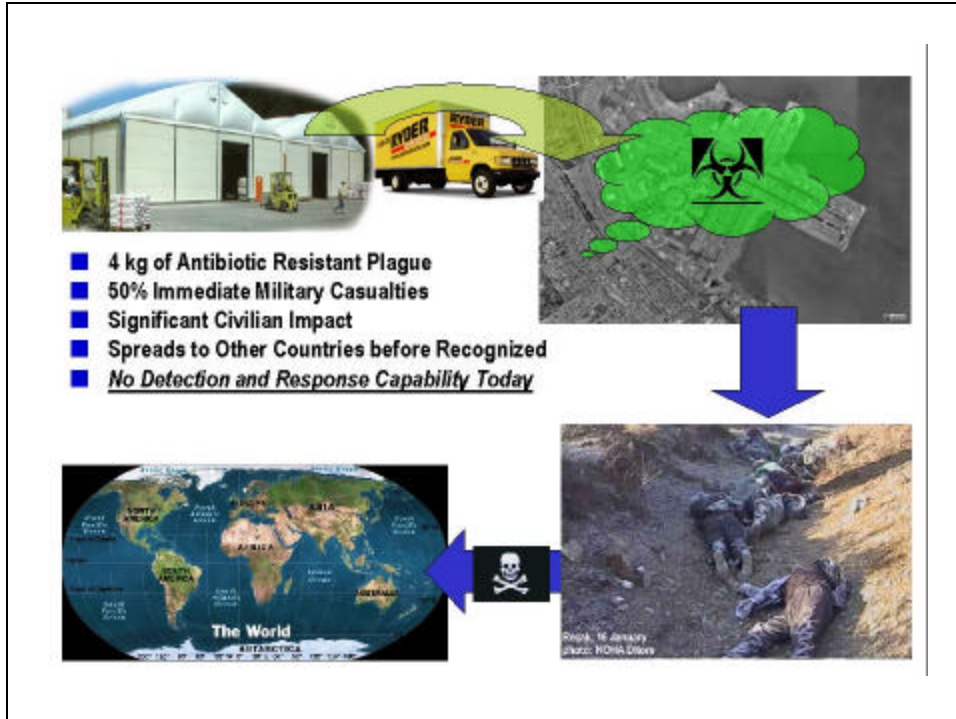
A biological attack on a major population center could mean that 10s or 100s of thousands of people would suffer from casualties or be affected by contaminated or sick people. That creates an enormous logistics problem, for which neither the United States nor any other nation is prepared. The difficulty of understanding and characterizing the threat compounds this problem.

Facilities that produce pathogenic agents can be quite small and unobtrusive, and thus present little or no signature or footprint. Figure D-2 depicts a hypothetical scenario. Pathogenic agents are fabricated in a warehouse or house, they are distributed by a fogger in the back of a rental truck and are distributed over a wide area. In ~72 hours, (“immediate”) casualties begin to appear. A seventy-two hour onset period has several implications. Probably the most important is that what is happening will not be recognized immediately, and, during the interim until it is recognized, the agent could be spread widely over very large areas by contaminated people.

- Diversification of threat spectrum
  - Pathogens resistant to drugs and vaccines
  - Latent agents, trigger at will
  - Never-existed-before pathogens (synthetic)
  - Pathogen-induced disregulation of body control circuits
- Diversification of targets
  - Ethnic populations
  - Animals and plants
  - Degradation of materiel (fuel, materials decay)
- Escalating logistical problem for drug/vaccine supply
  - On-demand, surge production (<7 days)
- Increased complexity of surveillance and inspection

- Deliver means to:*
- Detect and characterize conventional and unconventional bioattacks
  - Contain and neutralize environmental contamination threat
  - Effectively treat casualties and protect exposed
  - Provide accurate attribution

*Figure D-1. Genetic Engineering and Escalating Risk to Military Forces and the Homeland*



*Figure D-2. A Hypothetical Biological Threat Scenario*

A biological attack timeline is shown in Figure D-3. The center vertical line represents the time of attack. To the left of this is the realm of intelligence warning. Relying on intelligence to predict what is going to happen may be misplaced, since intelligence is not particularly well matched to this problem. In the post-attack, to the right of T=0, the United States is in a reactive, consequence-management mode. A reactive mode takes time, and time equates very much to life-and-death in the case of a biological attack. The United States must develop the tools to become more proactive, able to deter and/or treat as the need arises.

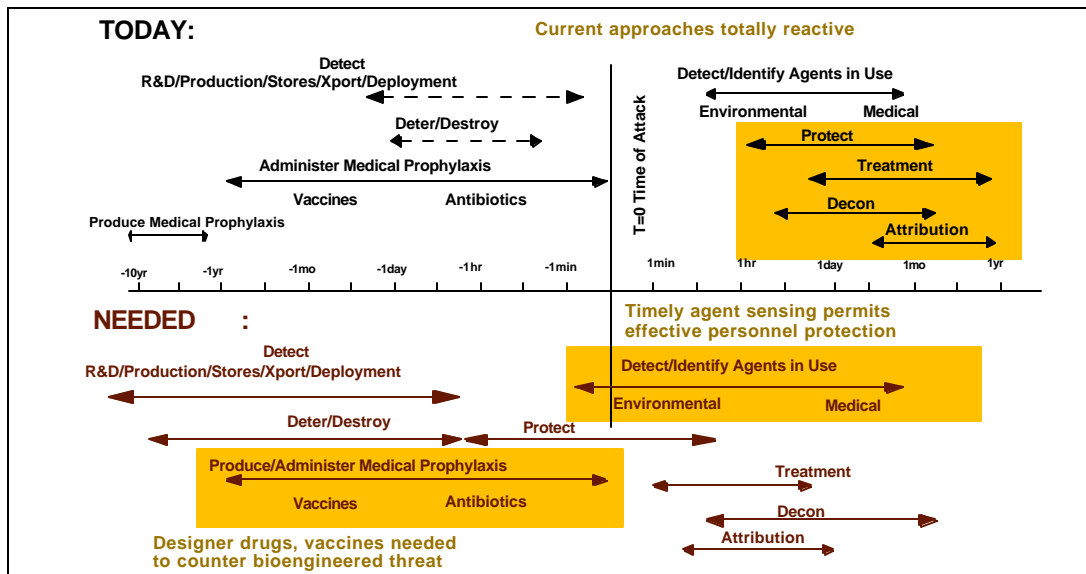


Figure D-3. Biological Attack & Response Timeline Challenges

“Bioshield” is the concept for developing the technologies which could enable a comprehensive defense of U.S. military forces and the homeland against conventional and unconventional bio-weapons. The almost total vulnerability of U.S. forces and homeland to biological warfare (BW) attack constitutes a strategic challenge equal to that created by nuclear weapons and ballistic missiles. The prospect of continued escalation in the potency, sophistication, and diversity of BW agents, and the unthinkable consequences of a massive attack, constitute an overwhelming case for elevating BW to a strategic threat that demands radical changes in national defense policy.

Major deficiencies currently exist in bioterror surveillance, detection, and protection capabilities, including gaps in current information and intelligence capabilities and knowledge — spanning the spectrum from weapons production to deployment. Moreover, there has been an erosion of international cooperation on export controls for dual-use technologies with BW relevance and a continuing lack of methods and sensors to support interdiction and retribution on grounds credible to the international community. In addition, considerable bureaucratic barriers stand in the way of effective planning, organization, and technology acquisition. Despite improved governmental coordination, the large number of agencies and organizations involved in biological defense makes achieving substantial progress difficult, and private industry is poorly engaged. Lastly, DoD lacks a comprehensive and integrated national

biological defense science and technology strategy and transition plan, and it is clear that biological warfare defense does not enjoy adequate priority in the budget allocation process.

The BW problem poses a multidimensional strategic challenge as a consequence of diverse threat scenarios that require very different responses, for example, bioweapons production, battlefield attack, ground zero, collateral in-theater forces, homeland defense, homeland attack, and credible attribution. The U.S. government must develop a proactive strategy for BW defense, moving from ‘detect to protect’ to ‘detect to preempt,’ from voice alerts to automated neutralization responses, from immobilizing protective gear to maintenance of effective fighting forces, from vulnerable buildings to protected facilities, from post-symptomatic diagnosis to presymptomatic diagnosis, from limited treatment options to multiple broad spectrum agents, and from limited drug/vaccine stockpiles to on-demand surge supply chain.

Sorely lacking is a strategic vision to grapple with the larger picture posed by the biothreat. DoD has classical expertise in identifying known conventional pathogens and toxins and in vaccine development, but has yet to provide the commanders with a comprehensive solution. Commanders need the capability to detect threats in real-time, to neutralize or impede the environmental contamination threat, to prophylax and treat casualties, and to attribute the source of traditional and genetically-engineered conventional and unconventional biological threats. This challenge is so daunting that the problem transcends DoD and must be viewed as a national survival challenge as is the case of nuclear weapons.

What has changed within the last few years, and what makes a Bioshield Project urgent and technologically feasible, is the revolutionary knowledge gained from the human genome project and biotechnology. The ability to understand diverse biologic systems at the molecular level is now in sight. The United States is simultaneously presented with a greater threat challenge and the opportunity to comprehensively address the spectrum of biothreats.

Specific elements of a Bioshield project include developing technologies to enable a national bioshield with the following capabilities:

- Wide coverage by affordable networks of detectors and sensors
- Biosignature recognition of engineered BW agents
- Automatic triggering of neutralization, protection, and containment responses
- Pre-positioned infrastructure protective systems
- Presymptomatic detection of infected individuals for infection control and early therapy
- Novel non-agent-specific immune enhancement pharmaceuticals, available to protect against novel agents and agents engineered for resistance
- Revolutionary production capability for rapid supply (less than 7 days) of synthetic designer vaccines and therapeutics
- Source attribution credible to the international community through pathogen biosignature, intelligence, and forensics

In the Bioshield grand challenge, DoD should establish a set of intermediate goals to go along with the longer-term goals described. As shown in Figure D-4, the task force identified a set of reasonable technological goals for a period of four or five years – typically the life of any

specific project. A grand challenge may have 20-100 projects ongoing at varying levels of maturity. But each project, or group of projects, needs to have quantitative metrics against which to judge progress.

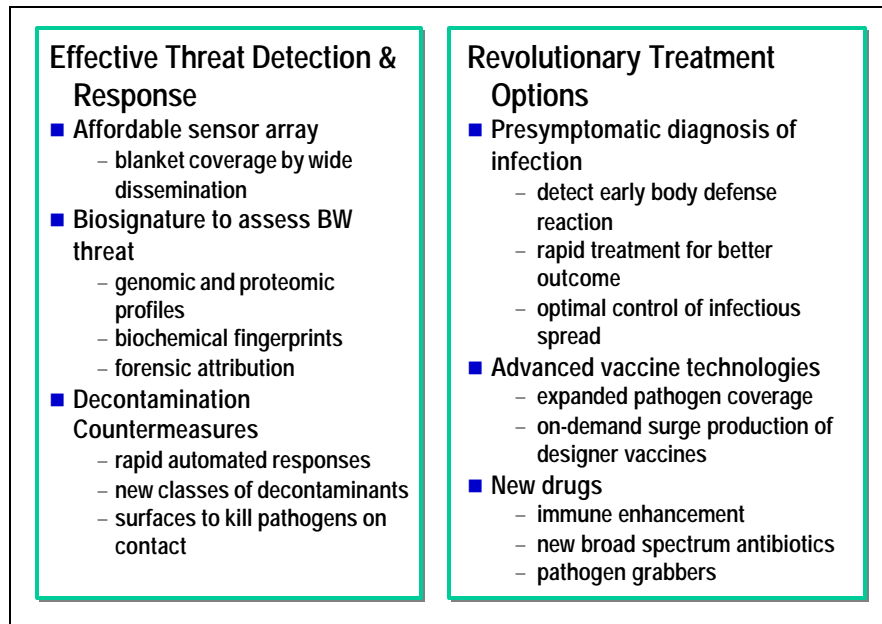


Figure D-4. Possible Intermediate Output Examples – “Bioshield”

The escalating risk and serious vulnerability of the U.S. military and the homeland to BW attack demand radical action. The U.S. Government must mobilize the financial and technical resources to create a strategic defense system against both conventional and unconventional bioweapons and to deter the proliferation and use of such agents. A detailed discussion of the specific and detailed measures that must be taken in support of Bioshield are described in Volume II.

### “NO PLACE TO HIDE”

Desert Storm served to advertise U.S. surveillance capabilities to all potential adversaries, and recent experience in Kosovo and Iraq indicates that they have learned well. Current U.S. systems have extreme difficulty remotely targeting military vehicles and forces hidden under foliage, in buildings, and in underground facilities. Such targets, in the past, have traditionally been located by proximate ground troops, which often suffer losses in the process.

Today, the United States has superb surveillance capability, but this capability has many critical limitations, which are being exploited by adversaries and which need to be addressed with great urgency. Adversaries will find ways to hide and to keep their forces useful while hidden. There are a variety of things DoD needs to do to cope with adaptive enemies. Today’s situation can be characterized by the following:

- Cannot efficiently find, identify, track, and strike tactical targets that move
- Great difficulty finding fixed targets protected by camouflage, concealment, and deception
- Sensor revisit times are unacceptable
- Adaptive enemies are hiding and reacting within U.S. targeting cycle times
- No foliage penetration radar capability

To achieve more robust and persuasive sensor networks, DoD needs to develop harder-to-avoid sensors and sensing strategies with orchestrated combination of:

- Close-in, covert, and unwarned collection
- Continuous, on-demand, surveillance (wide area coverage)
- Dynamic information exploitation and cross-sensor data integration

*Close-in, covert, and unwarned collection*

Present and planned surveillance and reconnaissance systems are predominately based on active or passive electromagnetic remote sensing from airborne or spaceborne platforms. These systems have some significant limitations in providing critical information and targeting data, especially in real-time. First, remote sensors perform inadequately in certain environments such as urban canyons or under foliage. Second, enemies can engage in camouflage, concealment, and deception by timing activities to coincide with gaps in coverage or by masking or duplicating the remotely sensed signatures. Third, many types of information can not be satisfactorily or cost-effectively obtained by remote sensing. One solution is to complement stand-off sensing by placing sensors in the area under surveillance and reading the data from those sensors remotely, permitting continuous sensing of a wide range of signatures.<sup>29</sup> Many interesting observables are present at close ranges that are difficult or impossible to sense remotely. These include:

- DC to mm-wave electromagnetic emissions
- Magnetic fields and magnetic anomaly detection
- Acoustic signatures, including Doppler shifts
- Chemical emissions: single substance detection to full chemical analysis
- Biological agents: detection, comprehensive agent identification
- Nuclear radiation
- Pressure and vibration sensing
- Air flow sensing
- Short-wave ultraviolet emission
- Infrared emissions
- Imaging, object recognition, or image change detection

---

<sup>29</sup> Other technological solutions are discussed in the Information Superiority section of Volume II.

Though close-in point sensors exist today, their utility has been severely limited for several reasons. First, the power consumption requirements of the sensors, combined with limitations in battery technology, has resulted either in large, battery-dominated sensors (such as those used in Vietnam), or in smaller sensors with very limited functionality, transmission range, and mission lifetime. Limited range, “dumb” sensors are inconsistent with providing wide area coverage. The size, cost, and performance of current sensors, combined with the difficulties in emplacing them, have limited their use to small numbers against high value targets. In addition, the technology has not existed to create small, lightweight, low-cost sensors for several desired observables, such as chemical and biological agents; emerging technologies promise to dramatically alter that situation. Finally, point sensors have been viewed as either stand-alone devices or for use in locally controlled clusters. An architecture to integrate these into a wide-area, information-on-demand surveillance system has not yet been developed.

Advances in energy sources, microsystems technology, and biotechnology promise low-cost, miniaturized sensors, which could be cost-effectively distributed (for example, by air or missile delivery systems) over a theater of interest, providing real-time, continuous, all-weather, day-night surveillance, which an enemy could not practically evade. Key attributes of the proposed capability are

- Ability to measure such a wide range of signatures that concealment and deception becomes a very difficult problem for an enemy and greatly reduces his mobility and agility.
- Continuous real-time monitoring, with information provided on demand through a wide-area network controlled from overhead or terrestrially. Utilizing an aircraft or a space-based system employing a large aperture sparse antenna array, the sensors could be geolocated and “polled” to deliver their unique identification and stored data. Alternatively, ground-based networking options would allow a robust-connectivity, low probability of detection, secure, low-power communications network which could be used by forces operating in the area. Because data delivery would typically be in short bursts, and timing of transmissions would be remotely controlled by the user, major power reductions and improvements in covertness could be expected compared to present systems. Sensors could be kept dormant until needed, or commanded to report back only if high value events were detected. For example, using an airborne synthetic aperture radar one could command and access sensors to be “read-out” very covertly. There is even potential for reflective rather than reactive communications using active standoff “interrogation.”
- Small size and low-cost sensors (on the order of one cubic inch and costing less than \$10 each) that can be dispensed in overwhelmingly large numbers (e.g. 100,000 sensors over the area of interest.) This system would not only enable wide-area coverage from what would be essentially a point sensor, but would also make location and neutralization very difficult for the enemy. Even less expensive decoys could further complicate detection and cleanup by an enemy.
- Covertness. This would be achieved through small size, camouflage, mobility, and low probability of detection communication enabled by on-board intelligence. However, depending on the application, the very large numbers envisaged, coupled with extensive intermixing of “penny” decoys, might obviate the need for covertness by simply overwhelming the enemy with too many sensors to pick up or destroy. A



sensor survival rate of as little as 20-30 percent could still provide the required functionality.

- Survivable sensors capable of long duration operations. Depending on the sensor type and intended application, and particularly on advances made in power supply technology, operational periods of the network (not necessarily of an individual sensor) of from months to years is conceivable.
- Innovative deployment and emplacement. Non-traditional deployment means, such as “crop dusting” or “air burst,” inadvertent transport into inaccessible areas by the enemy (sensors clinging to vehicles or clothing), or the sensor’s own robotic or biologically-aided mobility could be used, along with other means such as missile or UAV delivery and hand emplacement (sowing), either overtly by troop units or covertly by operatives behind the lines.

Such a system could have covered Kosovo with sensors spaced approximately every 30 meters, with the cost for the sensors totalling only several tens of millions of dollars. The data from these sensors, integrated into a C<sup>4</sup>ISR system with other data acquired from more traditional stand-off sensors, would have provided a comprehensive view of the battlefield, of enemy capabilities, and of enemy movements. Of particular interest is that such a sensor system would have the capability of gathering information on weapons of mass destruction, of perhaps characterizing concealed and hardened facilities, and of providing information on targets obscured by foliage.

## FAST FORWARD

The body of this report deals with the need to assure rapid deployment of U.S. forces. The proposed “Fast Forward” grand challenge encompasses the development of technologies which could make a big difference in the military capability per unit of strategic or tactical lift and thus contribute to the development of rapid-response capabilities. Some of the desired attributes for effective regional operations are outlined in Figure D-6.

<p><b><u>Fast</u></b></p> <ul style="list-style-type: none"><li>- Rapid planning</li><li>- Rapid arrival and assured entry</li><li>- Intra-theater agility</li><li>- Small footprint forward</li></ul> <p><b><u>Effective</u></b></p> <ul style="list-style-type: none"><li>- Pervasive, intrusive surveillance and intelligence</li><li>- Adequately sized, tailored, and trained force</li><li>- Appropriate presence and force application</li><li>- Timely, efficient sustainment</li></ul> <p><b><u>Humane</u></b></p> <ul style="list-style-type: none"><li>- Minimal casualties for coalition, neutral, and sometimes, enemy personnel</li><li>- Low collateral damage</li></ul>
---

*Figure D-6. Desired Characteristics of Regional Operations*

Major advances in materials, energy systems, and robotics will be central to enabling substantial improvements in deployment and sustainment of U.S. forces by air. Specifically, increases in the strength-to-weight ratio of materials and in the energy density of fuels, propellants, and explosives, along with miniaturization of power sources, will drastically lighten the entire deployment package. This will extend the range of U.S. ground and air vehicles and weapons, make space weapons practical, extend the operating life of equipment, and increase potency of warheads. While advances in each of these technologies have been very modest for decades, new materials design approaches and fuel formulations hold promise for order-of-magnitude improvements over the next two decades, as shown in Figure D-7.

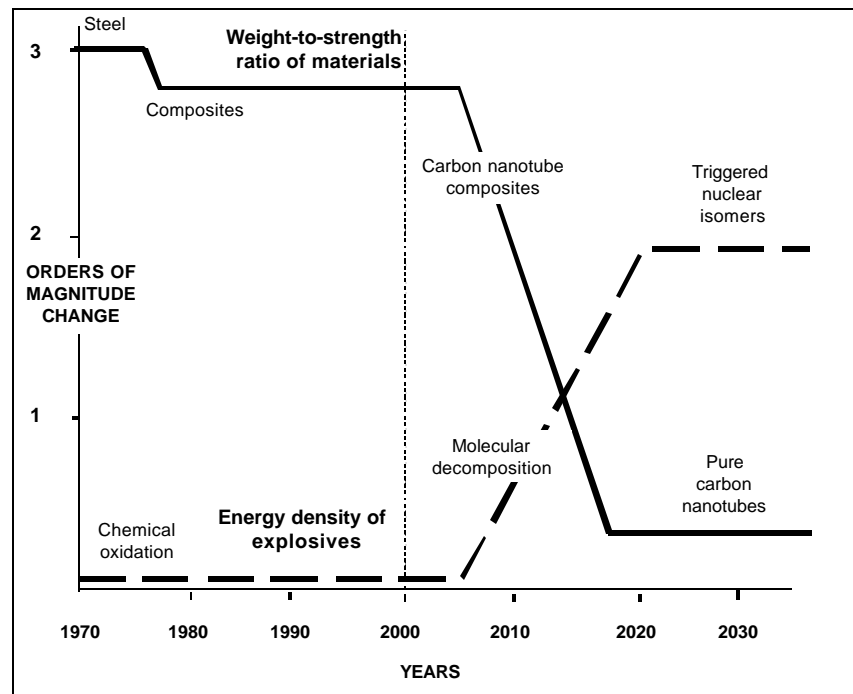


Figure D-7. Potential Gains in Performance of Structure and Energetic Materials

While many technologies will contribute to enabling future capabilities, the task force has identified three that have the greatest leverage and can provide revolutionary capabilities for the military. These technology areas are structural materials, energy, and robotics. They promise to reduce the weight and cost, and increase the effectiveness of essentially all military vehicles and craft by an order-of-magnitude when applied together. Even greater gains are possible in selected applications. These technologies are discussed below.

### Structural materials

Carbon nanotubes, also known as Buckytubes, alone hold promise for weight reduction. Their existence was discovered only nine years ago, and their properties are already proving phenomenal. They have 100 times the strength-to-weight ratio of steel, and about 25 times that of graphite-epoxy carbon composites. In addition, they stretch up to 30 percent before breaking,

and buckle without permanent deformation. The characteristics of nanotube structures are noted in Figure D-8.

Technology	Today	Promise	When	Funds	%DOD
<b>Strength of structural materials*</b>					
Steel	0.15-0.3 M psi	--	Now	--	--
Graphite composite fibers	0.5-1.0 M psi	--	Now	--	--
Carbon nanotube composite fibers	--	2-10 M psi	5 years	\$20-50 M/yr	90
Pure carbon nanotubes	--	25 M psi	10 years	\$20-50 M/yr	90

\* Working tensile strength

*Figure D-8. Technology Development Overview*

Carbon nanotubes are in their early research phases, and the programs to support related research have little if any DoD funding. Although some \$10 million per year is being spent for nanotube research in the United States, most of it is applied to electronic and other non-structural characteristics and uses of nanotubes, with only about \$500,000 being applied for structural research. A focused, U.S. national research initiative, led by DoD, is warranted to ensure that the United States reaps the benefits of these super-strong materials.

Carbon nanotubes will be able to make trucks, cars, aircraft, spacecraft, launch vehicles, rifles, artillery, missiles, antennas, wheels, engines, suspension parts, electronics, pressure vehicles and indeed most articles now made from metal. As a result, their weight would be reduced to as little as one-tenth of today's embodiments. This change would indeed be revolutionary. For example, a spacecraft weighing 10,000 pounds today would weigh 100 pounds. Launch vehicles could be easily built that would cost less than \$100-per-pound-of-payload to orbit.

Such structures alone, without any other advances in energy, have the potential to cut the weight of the logistics tail of engagements by at least by a factor of two.

### *Energy*

A number of possibilities exist for increasing the energy density of fuels, propellants, explosives, and micro-sized energy sources for miniaturized remote sensors, as shown in Figure D-9.

Technology	Today	Promise	When	Funds	%DOD
<b>Energy density of materials</b>					
Fuels	43.3 kJ/g (JP-8/air)	120 kJ/g (H <sub>2</sub> /air)	5 years	\$3-10 M/yr	20
Propellants	290-460 sec (Solids-H <sub>2</sub> /O <sub>2</sub> )	500-1,000 sec (meta N <sub>2</sub> -H <sub>2</sub> )	5 years	\$2-4 M/yr	100
Explosives	5-6 kJ/g (TNT-HMX)	20-94 kJ/g (Meta N <sub>2</sub> -H <sub>2</sub> )	5 years	\$2-4 M/yr	100
		500 kJ/g (Triggered Isomer)	10 years	\$2-10 M/yr	100
Micropower sources	660 Wh/kg (Lithium Primary)	3,300 Wh/kg (H <sub>2</sub> /air)	5 years	\$5-10 M/yr	50

*Figure D-9: Potential Advances in High Energy Density Fuels*

Molecular decomposition techniques have been recognized for years as the first step in attaining a greater energy density than traditional high energy explosives. Metastable solid states of nitrogen are known to liberate 4-fold greater energy upon reversion to the gaseous state than combustion. A step up is the exploitation of metastable solid hydrogen, which would offer more energy upon decomposition to the rest state than high energy sources by a factor of ten.

The ultimate in intermediate-scale energy sources are the so-called triggered nuclear isomers, in which large quantities of low energy gammas are released upon a triggered relaxation of the spin or shape of the nucleus. These nuclear isomer techniques liberate more than one hundred times the energy per weight than chemical combustion, yet stop short of the nuclear radiation residuals and other major consequences of nuclear explosives.

Another important area of high energy-density materials is in micro-power sources for long-life remote miniature sensors and other demanding small-scale applications. These power sources include miniaturized fuel cells, nanomachined turboalternators, and other technologies. Though there is some university activity in this area, a focused, better-funded activity is needed. The activity should be aimed at micro-power sources the size of a watch battery but with at least a three-fold greater energy storage capacity.

### *Robotics*

Rapid deployment of overwhelming combat forces can also be greatly enhanced through the use of robotic vehicles for three purposes.

- Carrying both broad-area and local-area sensor systems into combat areas before enemy air defenses have been defeated

- Flying low-cost precision weapons into position over enemy formations also before enemy air defenses are defeated
- Logistical supply of ground forces after their injection into combat areas

In all these applications, potential losses of manned air vehicles during initial combat can be avoided. Such robot vehicles can be made smaller and lighter by eliminating human pilots.

## COGNITIVE C<sup>4</sup>

Developing decision dominance requires the integration of a family of complimentary capabilities. These include situational awareness, augmented human capability, and mobility. In order to provide these capabilities it is also necessary to satisfy two requirements:

- **Assurance:** the ability to protect the availability of core capabilities, such as GPS, from both accidental and overt interruption. Information warfare will become an increasingly serious concern.
- **Cost Performance:** DoD C<sup>4</sup> systems must leverage commercial and consumer capabilities and those that are interoperable with them to provide the performance and low cost required.

Because of the speed, information flow, and processing power that will be available over the next 20 years, the task force refers to the capabilities that need to be developed as “Cognitive C<sup>4</sup>.” By 2020, computer and other interaction technologies will surpass today’s capabilities by orders of magnitude. Some functions that are wholly inadequate today, such as automated target recognition from imagery sources, will be performed at near-image-analyst levels by 2020. Other complex human functions will be supported by course-of-action contingency analysis to augment human decision-making processes.

The need for situational awareness from the commander down to the individual soldier, the need for force mobility, and the need to augment human capabilities to provide near real-time decision-making capabilities all have analogues in the evolving commercial and consumer worlds. In Volume II, Part 3, the task force describes some of the general technological trends that will evolve over the next twenty years that can have a profound effect on military operations. They include:

- **Very fast computers:** personal computers that provide ten thousand times the performance, using less than 50 watts of power
- **Mobile, high-rate communications:** megabit per second, universal availability
- **Assured navigation capability:** robust GPS and inertial systems
- **Augmenting human capabilities:** near-image-analyst capable automated target recognition, information search, and decision support systems
- **Universal connectivity:** complete interoperability in military information systems with commercial and consumer information systems

- **Human-matched interfaces:** ubiquitous computer environments with presentation technologies matched to human capabilities
- **Trusted environments:** multi-level security systems that employ biometric and user identification systems, water-marked documents, and embedded computers and network security tags

The desired capabilities listed above outline the need for a cognitive C<sup>4</sup> system that collects and distributes the appropriate information to users in near-real-time. The system will also need to intelligently adapt that information so it extends and augments the human capability to use it. The following describes basic concepts and capabilities under development, along with the task force vision of C<sup>4</sup> system development.

One of the most significant developments in information technology is the World Wide Web. Although the web concept is effectively less than five years old, it has already begun a complete transformation of the way humans work and live. Today consumers are effectively limited to Internet speeds of 10-100 kilobits per second. By 2010 the average consumer will have access to many megabits per second, and by 2020 every personal computer will be able to receive multiple channels of streaming high definition video at tens of megabits per second. There will be a continuous transformation of society over this period as interactions move from email and images to movie-quality video and realistic “you are there” 3D teleconferencing. At the same time, displays will evolve from small 1k x 1k pixel systems to wall size displays with 10k x 10k pixel resolution.

In addition to these capabilities, the consumer and commercial world have an insatiable appetite for developing portable, high-speed information systems. These include direct broadcast satellite, video distribution networks, space-based cellular phones and data systems, and new high-speed local-area networks such as LMDS. At the same time, high-speed LANs within homes and offices are under development. Clearly this *zeitgeist* represents the basis for future military communications systems. But it is more.

The web-centric infrastructure described will create the basic infrastructure for wide-band person-to-person communications and the environment for “each individual as their own broadcast network.” Advances in computing are going to allow these advances to have even greater impact. They will open up unprecedented means of interacting with humans, not at the data level, but increasingly at the information and knowledge level, hence the term “Cognitive C<sup>4</sup>.”

The combination of wideband web-centric communications, wall-sized immersive displays and other sensory interface technologies, plus new computer power will allow applications to be developed that will profoundly affect how people work and how DoD conducts warfare. For example, it will be possible to practice worldwide collaborative planning with the ability to simultaneously involve hundreds of sites and interact with those people as if they were across the table. In addition, fast-forward mission planning and contingency analysis will be routinely used to explore options and novel concepts. Another example is automated target recognition. Image-based target analysis is an extraordinarily difficult task, even for highly trained image analysts. It is not surprising that current automatic target recognition systems are woefully inadequate. It is not possible to merge or integrate the necessary data in real time, nor is it possible to apply the levels of computer power required to replicate the skills of a trained image

analyst. By the year 2015-2020 it will be possible to perform many human image analyst tasks with computer-based automated techniques.

The technological capabilities described are necessary to make the progress required but are not sufficient. One other element needs to be added to facilitate the transformation of data to information and information to knowledge: an active program that incorporates the user in those systems. In the future, these tools must be designed to augment human capabilities. Humans must be an integral ingredient in the design of these systems if meaningful contributions are to be made.

Today, the nation is developing the basic infrastructure to be able to communicate information rapidly to users. Yet the ability to process that data and turn it into useful information is still very limited. Search engines and simple artificial intelligence agents provide the most rudimentary support. But by the year 2010, these tools will be advanced enough to begin to convert considerable amounts of data into a form that is easily understood and accessible to a user. Information will be customized to user needs. By the 21<sup>st</sup> century, the availability of high-speed networking and computers that perform at human-equivalent rates will make it possible to convert information into knowledge. At this point, the computer tools will be powerful enough to provide insights and expertise that is beyond ordinary human capacity. These capabilities will extend to provide in-depth understanding of novel new environments. The challenge over the next 10 to 20 years is to create information systems that fully exploit the inherent capability of human users.

Thus, the task force believes that the next 20 years should be devoted to developing C<sup>4</sup> systems that not only allow secure, robust, wide band communications and computing, but also are increasingly designed to extend and augment human warfighting capabilities. Technologically, this requires that systems be designed to present information to people in a compelling and intuitive way, by developing advances that are as significant as the transition from punch cards to the modern mouse-driven personal computer interface. This transformation will require extremely high resolution, immersive displays and other sensor modalities that fully engage and augment users. The benefits will be an unprecedented ability to visualize the battlespace and the enemies' capabilities, plan contingencies, employ ordinance, and control the tempo of operations. In addition, it will allow U.S. forces to anticipate the actions of its adversaries and to conduct appropriate psychological operations and influence public opinion.

---

ANNEX E. LOGISTICS INFORMATION SUPERIORITY  
CONSIDERATIONS





---

# ANNEX E. LOGISTICS INFORMATION SUPERIORITY CONSIDERATIONS

## INTRODUCTION

Information is the backbone of modern logistics. In its most basic form, the logistics support challenge is primarily one of rapidly coupling “providers” to “users with needs” as directly as possible such that user downtime and total inventory are either minimized or eliminated entirely. The scope of the DoD logistics operations is enormous and incredibly complex, having evolved to its present state over many decades from the bottom up, with little if any overall system engineering. Consequently, there are over 1000 different aging “logistics systems” in use, contributing to long cycle times and large inventories. Although the Department has made real progress in achieving interoperability between these systems at a technical level, most of the necessary business process changes to take advantage of this interoperability have not been made, resulting in continuing inefficiencies and higher than necessary costs.

The demands of *Joint Vision 2010* and advanced concepts such as Joint Rapid Response Operations Forces will require a massive overhaul of the logistics information technology systems. Because the requirements for logistics information directly parallel those associated with warfighting operations, the new concept of “*Opergistics*” has been adopted from the Marine Corps and developed as part of this study. Opergistics refers to a unified, seamless approach to operations and logistics functions. The following sections provide a more detailed description of the current situation, a view of the desired future, and some recommendations on how to get there. By the nature of this study, these tend to remain at a relatively high level, but nevertheless represent steps that, if taken, can make dramatic improvements for the future.

## CURRENT STATUS AND EMERGING THRUSTS: 1999 TO 2002

Over the years the Logistics Information Systems have been developed in a largely independent manner by the Services and Agencies, Major Commands, repair depots, and supporting defense contractors. Many thousands of different data bases exist and are in use, and largely independent communications resources are used to transmit and distribute logistics information between the more than 1 million personnel who are actively engaged in this process. Over 1,000 aging (some over 30 years old) legacy systems of the Military Departments, U.S. Transportation Command and the Defense Logistics Agency (DLA) support logistics operations. While these systems provide adequate support to current military operations, they are costly and time consuming to improve.

As an example, 10 years ago DoD’s component organizations agreed to rules that would allow the automatic redistribution of assets among field organizations. However, because of the technical difficulty of making the needed software changes and weak management processes to ensure that changes are made, only now is that important process being implemented.

Improvements such as fewer transactions to get materiel to the warfighter, more accurate forecasting of requirements, and more secure information are needed to enable logistics to respond to the dynamic environment of future military engagements. Concepts such as “near just-in-time spares” plus better use of the commercial/industrial infrastructure are required to reduce inventories and cut cycle time. Clearly, implementing these changes will require significant changes to business operations as well as the introduction of improved information technology systems.

Fortunately, significant efforts are underway within all the Services, DLA, TRANSCOM, and OSD to address many of these issues, although they remain relatively stovepiped. The need for improvement is now widely recognized, and many individual thrusts are being initiated independently to improve various segments in the process. Some of the more significant initiatives include:

- Army: Global Combat Support System (GCSS)-Army, Army Wholesale Logistics Modernization
- Navy: Navy ERP, MRP2, Shipyard Depot Modernization
- USMC: Integrated Logistics Capability, ATLASS II
- Air Force: GCSS-Air Force
- DLA: Business System Modernization, Fuel Automated System
- TRANSCOM: GTN, TC AIMS II (Army is EA), GATES II, WPS

The aim of these initiatives is to improve the ability of the components to provide logistics support to combat operations. However, not all of the components have linked their programs to enterprise-wide plans for process improvement, and the Department lacks an operational architecture linking the component efforts with community services or objectives. An example of this is the implementation of GCSS. As originally envisioned the GCSS was to be the support analog of the Global Command and Control System, and was to provide a single interoperable system for all users. However, it has now evolved into individual approaches by each Service – GCSS-Army, GCSS-Air Force – in recognition of the substantial differences in legacy systems and fundamental support approaches that exist between the Services. Hopefully the goal remains to make these tailored systems interoperable. However, these component efforts and the need for joint GCSS capabilities are not yet synchronized.

Furthermore, not all component efforts are taking advantage of commercial software to rapidly adopt best commercial practices. Some efforts that are trying to adopt COTS applications are encountering hostile management processes and organizations unwilling to change their ways to adopt the practices embedded in software.

#### *Demonstrations and Pilot Programs*

There are also a large number of individual demonstration and pilot program initiatives within each Service, DARPA, and DLA. Although each taken by itself represents a worthwhile initiative, there is little cross-coupling between them. Moreover, there are often no concrete plans

to migrate these demonstrations into main stream capabilities within a specific time scale and budget allocation. This can be illustrated by the following three key programs:

### Advanced Logistics Program

One of the more far reaching information technology initiatives is DARPA's Advanced Logistics Program, an R&D effort that promises advanced planning and execution capabilities in support of joint logistics operations. ALP is a five-year initiative aimed at gaining unprecedented control over the logistics pipeline. Its goal is to develop and demonstrate enabling technologies that will allow logistics and transportation assets to be deployed, tracked, refurbished, and re-deployed more efficiently. The Joint Staff/J4, DLA, and TRANSCOM are supporting the project. Briefly, its goals are:

- Automated Logistics Plan Generation: produce executable, level-5, time-phased force deployment database within 1 hour
- Real-Time Logistics Situation Assessment: identify plan deviations and re-plan within 30 minutes
- End-To-End Movement Control: minimize staging while globally optimizing lift resource usage across the spectrum of movement activities
- End-To-End Rapid Supply: continuously assess the demand and sourcing of materiel and supplies from DoD and commercial inventories

### Log ACTD

The Logistics ACTD promises tools for displaying and manipulating logistics data from the component supply chains. It initially developed and demonstrated the innovative Log Anchor Desk which was deployed to Bosnia in 1996 but is no longer operational there. (Like many new ideas, there were some flaws in the concept, but rather than institute corrective measures and build on the good aspects of what was initiated, the entire concept was abandoned. Thus, little of lasting benefit remains from the effort and resources expended.)

A second capability – Joint Decision Support Tools, which provides web-based decision support for the logistician and warfighter – was demonstrated by the U.S. Atlantic and European Commands (ACOM/EUCOM) in April 1999, and is to undergo further assessment on GCSS. For the future, LogACTD Phase III is to demonstrate real-time focused logistics by FY 2001.

### Joint Total Asset Visibility (JTAV)

JTAV is another capability that proved its usefulness in Bosnia in 1996, providing for the first time an ability for viewers to track the location and status of specific joint component assets by use of tag, data base, and related information technology. It represents a key tool in addressing both the in-transit and in-theater rapid materiel distribution and retrograde problems by fusing component asset data for use by joint commanders.

Although each of these three capabilities is an important improvement, they are being developed independent of one another. For example, no plan connects these key capabilities so that the data provided by JTAV is focused on the requirements of ALP and the Log ACTD.

Equally troubling, there is no plan or budget line to ensure that the capabilities promised by ALP and Log ACTD will be mainstreamed as operational systems.

### *Additional Pilot Programs*

Reducing the logistics footprint is an important aspect of focused logistics. Currently there are several ongoing simulation-based acquisition demonstrations of the ability to use advanced simulation techniques with intelligent models of a weapon system to improve system performance. However, these demonstrations have no requirement that these weapon systems, in addition to being modernized, also be more agile, be designed to comply with modular open system concepts, and fail less – all of which would contribute significantly to strategic agility and lower total ownership cost.

### *Security Issues and Related Items*

The defense information infrastructure/common operating environment, while achieving interoperability among command and control applications, is oriented more toward developed software and less to the integration of commercial off-the-shelf (COTS) applications. The current direction of emerging security policy is to apply public key encryption techniques to build a public key infrastructure (PKI). However, the current PKI emphasis is oriented more toward human access and less toward the computer-to-computer communications that comprise the vast majority of logistics transactions – over 2.5 billion per year.

To ensure that logistics does not become the area of vulnerability exploited by our information warfare adversaries, DoD needs to protect computer-to-computer communications as well. We also need logistics-specific security policies to control aggregated logistics information and logistics information that is used in planning and conducting military operations.

DoD's approach to PKI implementation is focused on building the capability internally, rather than looking to existing commercial PKI service providers. Although COTS may be used in this effort, scalability of selected COTS has been raised as a challenge by Defense officials. Scalability diminishes as an issue if the alternative of combining DoD's non-classified PKI workload with the requirements of sensitive commercial traffic is considered.

### *Computing and Communications Infrastructure*

Logistics computing infrastructure is acquired inefficiently, as part of the acquisition of individual applications. Communications access is inadequate during operations, as has been shown in all of our most recent engagements. Even though logistics traffic may be crucial to force projection progress, it receives low priority for bandwidth access. (Instead, logistics systems and information should be viewed as part of the Integrated Information Infrastructure, with logistics information flowing across the transport component of the Infrastructure within the continental United States.)

### *Government – Industry Interface*

Until recently, the primary thrust for information transfer between industry and the government had been DoD unique standards for electronic data interchange and non-standard formats for exchanging product or weapon system structural data. In a step forward, the Department now has emerging policy to require commercial transactions standards be used for electronic data interchange and the establishment of central services for standards adoption and a reinvigorated data exchange rule adoption process. Still remaining, the Department has not yet determined the relationship between central data translation services and the JTAV program.

Programs such as Joint Computer-Aided Acquisition and Logistics Support (JCALS) and Joint Engineering Data Management Information and Control System (JEDMIC), among others, are used as internal stovepipes to access product data. It has now become apparent that it is essential to transform access to weapon system drawings and data away from this stovepiped legacy systems and instead to Web-based access using standard generalized markup language technology and central services for product data translation. This transformation is not yet part of a managed program which will ensure that quality product data is provided to the simulation-based acquisition (SBA) function and used for daily configuration management.

## FUTURE VISION: 2006 TO 2010

Although much good work is being done in many areas, it is clear that some radical top-level changes in approach are needed if the capabilities of *Joint Vision 2010* are to be accomplished, and if the critically important reductions in cycle time and cost of support are to be realized.

Table E-1 illustrates the transition states for the key logistics modernization factors. Transforming the “emerging” picture into this vision of the future requires recognition that “the probability of success is not independent of the speed of implementation.” Only by focusing resources and putting agile management processes in place can the Department assure attainment of this vision. All of the recommendations that follow have this effect.

## RECOMMENDATIONS

The logistics modernization challenge facing DoD is to achieve focused and timely execution. There are few if any technical barriers and no inventions are required – virtually all the needed techniques have already been proven in today’s fast advancing commercial world.

Because of the enormity of the task and the large number of players involved, it is essential that OSD, the CJCS, the Service Chiefs, and CINCs jointly embrace, support, and provide sustained reinforcement to a common vision for this important area. The following recommended actions are offered as positive steps to facilitate this:

Table E-1. Logistics Information Architecture

<i><b>KEY AREA</b></i>	<i><b>CURRENT STATUS 1999</b></i>	<i><b>EMERGING STATUS 2002</b></i>	<i><b>FUTURE VIEW 2006-2010</b></i>
<i><b>Decision Support</b></i>	Stovepiped Decision Support	Reporting Using New Metrics	Unified “Opergistics”  Focus – Management Data an Automatic Product of Operations
<i><b>Acquisition Focus</b></i>	Initial Operational Capability Focused Acquisition	Total Ownership Cost  Simulation Based Acquisition  SBA Pilots	Reduced Logistics Demand & Simulation-Based Lifecycle Management
<i><b>Logistics Planning and Execution</b></i>	Minimal Automated Support Static-Rigid	Advanced Logistics Program  Log ACTD/JTAV	“Opergistics” & Simulation Based Lifecycle Management
<i><b>Metrics</b></i>	Functional and Sub-Optimal	Mission Oriented	Outcome Oriented
<i><b>Component Supply Chain Systems</b></i>	Numerous, Expensive and Time-consuming to Improve	Modernized but Costly and Change Still Difficult	Network-centric, Secure, COTS-based, Adaptable
<i><b>Government Industry Interface</b></i>	Military Standard Logistics Systems & Limited Commercial Electronic Data Interchange  Non-Standard Product Data Interchange	ANSI/EDFACT Commercial Electronics Data Interchange  Web-based, Industry Standards for Product Data Exchange	Standard Interface to Industry Enables Efficient Partnering
<i><b>User Interface</b></i>	Legacy System Unique	Modernized but Highly Vendor Unique Multiple Interactive Electronic Technical Manual	Common User Interface
<i><b>Information Infrastructure</b></i>	<b>Stovepiped:</b> Vertically Integrated Inflexible Imbalanced	<b>DII/COE:</b> Mission Oriented More Secure Command and Control-Oriented Interoperability	<b>Integrated Information Infrastructure:</b> Secure, Adaptable Supports COTS Balanced Bandwidth Access





1. Deputy Secretary of Defense and the Chairman, Joint Chiefs of Staff issue policy supporting primary attributes of future logistics modernization goals, reflecting CJCS doctrine, component joint combat support requirements, and best commercial practices (such as changing the process, not the commercial software), with associated time table for implementation
2. USD(A&T) through Deputy Undersecretary of Defense for Logistics lead a collaborative effort across DoD to develop “To-Be” operational and system logistics architectures by 2000
3. USD(A&T) through Deputy Undersecretary of Defense for Logistics, in concert with the DoD Chief Information Officer and the logistics leaders of the components, create a portfolio of community capabilities in accord with these architectures to include the following:
  - Accelerate the application of Simulation Based Acquisition
    - Establish formal programs for Simulation Based Acquisition and selected capabilities from the Advanced Logistics Program.
    - Synchronize these programs so they use the same model of logistics operations, creating the Simulation Based Lifecycle Management approach.
    - Focus SBA on improving the agility and reliability of existing systems via modernization through spares and other upgrades.
    - Require program offices to use SBA in conjunction with integrated development environments linked by the product data mediation services mentioned below.
  - Examine ALP to identify those planning and execution capabilities which can be extracted and developed for immediate fielding
  - Immediately transition those portions of ALP to a Joint Program Office led by a component Executive Agent and fund to field a worldwide capability for CINC J-4s
  - Corporate mediation services for product and transaction data
    - Establish corporate data mediation services for product and transaction data that:
      - Restructure and focus initiatives such as JCALS, JEDMICS, JTAV, GCSS, and
      - Rationalize them with existing capabilities such as those of the Defense Automatic Addressing Service Center
    - Ensure that these services:
      - Provide easy access to authoritative, quality data in component supply chains, and
      - Be focused on supporting validated requirements of joint or inter-component automated applications
    - Through a combination of quality and accessible product/transaction data, achieve the goals of:
      - Effective configuration management of fielded systems,
      - Getting the right part to the customer when it is needed

- Common industry and user interfaces
  - Establish joint and common industry/user interfaces to facilitate efficient partnering with industry for product support.
  - The industry interface should be thought of as a *commercial transaction set* which allows DoD officials to oversee the performance of their industry partners while also serving as a product data interface for sharing engineering information.
  - The common user interface would be a combination of standard integrated electronic technical manuals for maintenance access to product data, and standard browser conventions for access to component supply chains with a common look and feel, regardless of the source of supply.
- Logistics Decision Support
  - Establish and utilize logistics decision support to enable the logistics leadership of the components and joint community to measure progress toward agreed upon strategic goals for the support of military operations, and for achieving commercial-strength efficiencies comparable to those of leading commercial examples.

#### 4. Component Initiatives and Roles

- Each component should be responsible for developing its portions of the overall operational and system architectures and for modernizing its supply chain in accordance with them.
- Supply chain modernization should employ *unmodified* COTS application software wherever possible.

#### 5. Policy on COTS software

- Use of COTS application software is only feasible if components change their business processes to accommodate the software and not the reverse. In the commercial world, such an approach works only when supported actively by corporate leadership.
- In DoD, policy from the Secretary of Defense that requires maximum use of commercial software, changing business processes to accommodate it, and continuous, strong leadership support for process change, would be the right top-level message.
- This policy from the Secretary should be augmented by a USD(A&T)/DoD CIO review of the technical standards and management processes governing application software acquisition. This review should result in mediating barriers to successful COTS application implementation such as current DII/COE rules on segmentation.
- A way to conduct this review would be to designate an emerging COTS logistics software acquisition program as the model and develop new standards and procedures for that acquisition.

## 6. Portfolio Management Approach

- To ensure that limited resources are focused on needed change, the logistics community should implement portfolio management processes to govern all of the funds expended on logistics information technology.
- Each component would have its own portfolio of supply chain applications but would follow its portfolio management processes with common attributes across DoD.
- These processes should ensure that:
  - Funds expended on changes to existing systems are limited to ONLY those improvements that would NOT be more cost-effectively implemented via modernization programs.
  - Formal requirements for modernized component supply chains be minimized, limited to those dictated by either the functional requirements of joint combat operations or the technical requirements of good information management, such as:
    - Total asset visibility, networked architectures, security
    - Compliance with commercial transactions standards policy
    - No wholesale/retail barriers
    - Support for corporate performance metrics, management data generated automatically as a by-product of operations,
    - Automatic receipt of materiel that closes all associated logistical and financial transactions
- Demonstrations and prototypes, such as the Logistics ACTD, are “mainstreamed,” that is, they are only undertaken if, when successful, one or more components will implement them in their supply chains.
- Investments not justified by specific functional improvements are justified by measurable reductions in the time and cost of improvement generally.
- Resources are focused on those investments which will achieve or enable the greatest improvement in logistics’ contribution to combat operations or savings in the cost of logistics support.
- Investments in information infrastructure (computing environments and communications) are separate from investments in applications and justified by the aggregation of applications supported. These infrastructure investments comprise the Integrated Information Infrastructure portfolio.
- Opportunities for new joint applications, community services, or common applications are identified, the requirements validated, executive agents assigned, and products delivered under acquisition discipline.
- Expenditures result in an acceleration of logistics process improvement.

## 7. Policy on business rules for logistics data interchange

- DoD should establish a compatible logistics architecture with appropriate definitions and related measures to assure interoperability at the technical level.

- Deputy Undersecretary of Defense for Logistics should issue policies that result in reinvigorating the process for achieving agreements on the business rules governing the interchange of logistics data among DoD components.
- This policy should ensure that joint programs such as those included under Simulation Based Lifecycle Management are equal claimants in accessing data from component supply chains.
- This policy should also ensure that business rules agreed to by components are implemented expeditiously by setting forth expected schedule target guidelines.

#### 8. Policy on Modular Open Systems Approach

- Deputy Secretary of Defense and VCJCS should issue policy mandating use of the Modular Open Systems Approach on all new and retrofit acquisition programs in order to address the problem of diminishing manufacturing sources, reduce the logistics footprint, and facilitate interoperability between systems. This should apply to all acquisition programs, not just information technology systems.

#### 9. Policy on Information Assurance

- Deputy Undersecretary of Defense for Logistics, in conjunction with the DoD Chief Information Officer, should issue policy on logistics information assurance. This policy should guide the levels of protection and investments required in the protection of logistics information.
- Computer-to-computer communications must be secure. The policy should cover the procedures governing the granting of personnel access.
- Similarly, this policy should guide the interaction between components and the joint logistics and operations communities to assure adequate priority is assigned to logistics traffic.
- In acquiring security protection for unclassified information, DoD should consider acquiring commercial services as opposed to integrating or modifying commercial security products internally.
- An approach which has the DoD as one customer of a commercial enterprise serving multiple corporate and government entities may provide needed protection more quickly than internal approaches and mitigate problems of scalability.

---

## ANNEX F. GLOSSARY



---

## ANNEX F. GLOSSARY

<b>ACC</b>	Architecture Coordination Council
<b>ACTD</b>	Advanced Concept Technology Demonstration
<b>ALP</b>	Advanced Logistics Program
<b>ASD(C<sup>3</sup>I)</b>	Assistant Secretary of Defense (Command, Control, Communications and Intelligence)
<b>BW</b>	Biological Warfare
<b>C<sup>4</sup>ISR</b>	Command, Control, Communications, Computers and Intelligence, Surveillance, and Reconnaissance
<b>CINC</b>	Commander-in-Chief
<b>CJCS</b>	Chairman, Joint Chiefs of Staff
<b>COE</b>	Common Operating Environment
<b>COTS</b>	Commercial Off-The-Shelf
<b>CRAF</b>	Civil Response Air Fleet
<b>DARPA</b>	Defense Advanced Research Projects Agency
<b>DCI</b>	Director, Central Intelligence
<b>DDR&amp;E</b>	Director, Defense Research and Engineering
<b>DII</b>	Defense Information Infrastructure
<b>DLA</b>	Defense Logistics Agency
<b>DSB</b>	Defense Science Board
<b>GCSS</b>	Global Combat Support System
<b>GEO</b>	Geostationary Earth Orbiting
<b>GPS</b>	Global Positioning System
<b>III</b>	Integrated Information Infrastructure
<b>IR&amp;D</b>	Independent Research and Development
<b>ISR</b>	Intelligence, Surveillance and Reconnaissance
<b>JCALs</b>	Joint Computer-Aided Acquisition and Logistics Support
<b>JDAM</b>	Joint Direct Attack Munition
<b>JEDMICS</b>	Joint Engineering Data Management Information and Control System
<b>J-ROFs</b>	Joint Rapid Response Operations Forces
<b>JSEO</b>	Joint Systems Engineering Organization
<b>JT&amp;E</b>	Joint Test and Evaluation
<b>JTA</b>	Joint Tactical Architecture
<b>JTAV</b>	Joint Tactical Asset Visibility
<b>JTRS</b>	Joint Tactical Radio System
<b>LAN</b>	Local Area Network
<b>LEO</b>	Low Earth Orbiting

<b>LOCAAS</b>	Low Cost Autonomous Attack System
<b>LPD</b>	Low Probability of Detection
<b>LPI</b>	Low Probability of Intercept
<b>MEO</b>	Medium Earth Orbiting
<b>MRC</b>	Major Regional Conflicts
<b>OODA</b>	Orient-Observe-Decide-Act
<b>OSD(PA&amp;E)</b>	Office of the Secretary of Defense for Program Analysis and Evaluation
<b>PKI</b>	Public Key Infrastructure
<b>R&amp;D</b>	Research and Development
<b>RSOI</b>	Reception, Staging, Onward-movement and Integration
<b>RSTA</b>	Reconnaissance, Surveillance, and Target Acquisition
<b>S&amp;T</b>	Science and Technology
<b>SBA</b>	Simulation Based Acquisition
<b>SIGINT</b>	Signals Intelligence
<b>SSTOL</b>	Super Short Take-Off and Landing
<b>TRANSCOM</b>	United States Transportation Command
<b>UAV</b>	Unmanned Aerial Vehicle
<b>USD(A&amp;T)</b>	Under Secretary of Defense for Acquisition and Technology
<b>USJFCOM</b>	United States Joint Forces Command
<b>VCJCS</b>	Vice Chairman, Joint Chiefs of Staff
<b>VISA</b>	Voluntary Intermodel Service Agreements
<b>VTOL</b>	Vertical Take-Off and Landing