

## **Chapter 1**

# **Defense Software Overview**

---

## Contents

<b>1.1 Software’s Role in A Dangerous World</b> .....	1-3
<b>1.2 Software and Future Warfare</b> .....	1-4
1.2.1 Joint Vision 2010: Information Superiority .....	1-4
1.2.2 Software Wargaming and Future Warfare .....	1-5
1.2.3 Army Vision 2010: Digital Battlefield.....	1-6
1.2.4 Navy IT-21 .....	1-7
1.2.5 Marine Corps: Operational Maneuver .....	1-7
1.2.6 Air Force: Global Engagement .....	1-8
<b>1.3 Budgets And Increasing Software Demands</b> .....	1-9
1.3.1 Decreasing Budgets.....	1-9
1.3.2 Modernization Budget Shortfalls .....	1-10
1.3.3 Software: The Force Multiplier.....	1-11
1.3.4 DoD Software Spending: Growing Demands.....	1-11
<b>1.4 Software: The Invisible Component</b> .....	1-13
<b>1.5 Software-Intensive Defense Systems</b> .....	1-14
<b>1.6 DoD Software Domains</b> .....	1-16
1.6.1 Weapon System Software .....	1-16
1.6.1.1 Embedded Software .....	1-17
1.6.1.2 C3 Software .....	1-17
1.6.1.3 Intelligence Software .....	1-18
1.6.1.4 Other Weapon System Software .....	1-18
1.6.2 Automated Information System Software .....	1-19
1.6.2.1 Simulation and Modeling Software.....	1-19
1.6.2.2 Artificial Intelligence .....	1-20
<b>1.7 References</b> .....	1-21

---

## 1.1 Software's Role in A Dangerous World

*“The superior ability of the United States warfighters to obtain, process, analyze, and convey information is our most powerful weapon on the battlefield. It is a cornerstone of our military strategy captured in Joint Vision 2010. Our superiority in information technology enables the United States to carry out a two MRC [major regional conflict] scenario with significantly reduced end-strength.”* — Deputy Secretary of Defense James J. Hamre [HAMRE98]

The U.S. is the world's peacekeeper, provider of humanitarian assistance, and counterterrorist policeman in an increasingly dangerous world. Jacques S. Gansler, Under Secretary of Defense for Acquisition and Technology, described the volatile world environment in a speech to the Precision Strike Association.

*“The end of the Cold War has brought great changes in the threat to our security. Today, we are much...more concerned with a whole host of potential enemies, ranging from terrorists and transnational organizations to rogue nations, whose intentions are highly unpredictable and, therefore, in many ways much more difficult to defend against.”* — Deputy Secretary of Defense James J. Hamre [HAMRE98]

The National Defense Council Foundation, an Alexandria, Virginia-based organization, monitors conflicts and the political, military, socioeconomic threat environment worldwide. It reports that, *“[i]n 1997, the conflict count was at 67, a bump up from the total of 64 last year.”* [NDCF97] The following characterizes the modern threat.

*“The dissolution of a monolithic adversary paves the way for a host of possible threats to U.S. interests that require rapid and flexible responses...Terrorism will continue to be a considerable problem...[and] terrorists likely will concentrate on technologies encompassing communications, sophisticated conventional weapons, and weapon disguise technologies ...While the employment of advanced and exotic weapons is less likely, their availability is increasing...The growth of international drug cartels continues and promises greater instability...[which] in turn can lead to clashes with neighboring countries...[A]bout two dozen countries are pursuing development or acquisition of nuclear, biological, or chemical weapons...[and] [t]he number of nations that possess operational theater ballistic missiles...could double to 10 by the year 2010.”* — Robert K. Ackerman [ACKERMAN97]

To counter this threat, the U.S. military is counting on the acquisition of software-intensive weapon systems and equipment needed to conduct multiple, concurrent contingency operations worldwide. These systems must be flexible and modifiable to perform in *any environment*. They must be deployable in situations where adversaries do not try to match us plane for plane, ship for ship, or tank for tank. Instead, they use *asymmetric* means of engagement, such as nuclear, biological, or chemical weapons, information warfare, and large numbers of low-cost cruise and ballistic missiles. In this context, software is the most formidable weapon we possess, as it is easily adaptable to respond to a volatile threat. The warfighter needs more and better software systems to monitor, — detect, assess, alert, and combat forces intent on disrupting an already precarious world order.

The warfighter relies on software for virtually every operation, including strategic and tactical operations; sophisticated weaponry; intelligence, surveillance, and security efforts; and strategic

mobilization and readiness. Indeed, virtually every operation that supports the warfighter is software-dependent, including routine business functions such as financial, personnel, logistics, and contract management. DoD's reliance on software-intensive systems is illustrated by the fact that it has over:

- 1.5 million computers (of which 827,000 are personal computers),
- 28,000 software systems (of which 11% are mission-critical),
- 10,000 computer networks,
- 88,000 communications systems, and
- 100,000 facility support systems (e.g., security and medical support systems). [HINCHMAN97]

---

## 1.2 Software and Future Warfare

In the future, U.S. forces will experience a transition from warfare of attrition, where opposing sides try to destroy the other's force structure, to reconnaissance/strike warfare. Opposing sides will try to destroy and out-perform the other's software-intensive systems. This will involve the use of precision, smart weapons, delivered from long range to minimize battlefield casualties. Future U.S. dominance depends on our ability to obtain and distribute real-time automated battlefield awareness (knowledge) in-theater, among the Services and our allies. This requires investments in software systems that can link major weapons platforms to field command units and in the technology needed to support those systems. [ERWIN98]

*“Knowledge in the form of an informational commodity indispensable to productive power is already, and will continue to be, a major — perhaps the major — stake in the worldwide competition for power. It is conceivable that the nation-states will one day fight for control of information, just as they battled in the past for control over territory, and afterwards for control over access to and exploitation of raw materials and cheap labor.” — Jean François Lyotard, 1979 [LYOTARD79]*

---

### 1.2.1 Joint Vision 2010: Information Superiority

In his *FY98 Report to the President and Congress*, Secretary of Defense (SECDEF) William S. Cohen explained that,

*“Out to the mid-term future, the initial template for our future force will be “Joint Vision 2010.” It is built on an integrated “system of systems” that aims to give our forces total battlespace awareness, as well as the capability to maneuver and engage the enemy at the times and places of our choosing throughout the entire battlespace. This system of systems will integrate the laptop, the microchip, the microwave, the videocam, the satellite and the sensor. It will connect the cockpit, the quarterdeck, the control panel and the command post and link the shooter to the commander to the supplier.” [COHEN97]*

In **Joint Vision 2010**, the Chairman of the Joint Chiefs of Staff presents a strategic plan for the next century premised on the superior application of software-enabled technologies. The *Joint Vision* explains how traditional military concepts of maneuver, strike, protection, and logistics will be leveraged by software-intensive systems to achieve *information dominance*. It states that

*“How we respond to dynamic changes concerning potential adversaries, technological advances and their implications, and the emerging importance of information superiority will dramatically impact how well our Armed Forces can perform its duties in 2010.” [JCS96]*

Joint Vision 2010 states that through *information superiority* U.S. forces will be able to achieve full spectrum dominance:

- Dominant maneuver,
- Precision engagement,
- Focused logistics, and
- Full-dimensional protection.

Achieving this full spectrum dominance means continuing to build an integrated, complex set of software systems (especially a common command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) architecture) to achieve dominant battlespace awareness. [QDR97]

---

## 1.2.2 Software Wargaming and Future Warfare

While the art of wargaming has been around for hundreds of years, software models and simulations are providing critical insights and analytical perspectives heretofore impossible to achieve. DoD is using software to wargame, predict, and plan for a range of possible threat scenarios and plausible outcomes up to the year 2020 and beyond. As Gen. Howell M. Estes, III, (USAF retired), former chief of U.S. Space Command, explains,

*“Wargames are critically important...to address real policy issues that need to be straightened out. Certainly, in the space business, [wargames] have much improved understanding of the critical nature of [space] systems.” [ESTES98]*

National-level software-intensive wargames have become a primary mechanism for regional commanders, the Pentagon, congressional, White House, State Department, Federal Emergency Management Agency (FEMA), and national intelligence organization decision-makers to explore critical national issues, such as:

- Information operations and information warfare;
- “*Network-centric*” warfare;
- Space control;
- Logistics and mobility;
- “*Asymmetric*” warfare;
- Interagency links to ensure achievement of the right “*effects*;”
- Military force reorganization to meet future defense needs; and
- Reorientation of major acquisition programs from “*platform centric*” to “*network-centric*” doctrines. [SCOTT98<sup>3</sup>]

Three major wargames (called “*Title-10*” games) are service-level with roles and missions defined by U.S. codes, sometimes involve 1,000s of players, including high-level military officers and civilian leaders. Title 10 wargames include the following. [SCOTT98<sup>1</sup>]

- **Army Wargaming.** Army After Next is a comprehensive initiative to better understand the nature of warfare 30 years into the future and provide insight into today's development efforts. It is laying the research foundations necessary for assessing the effects of increased mobility, lethality, and maneuver. In 1997, this wargame showed that if U.S. satellites are destroyed early in a conflict, ground forces quickly will become immobilized. [SCOTT98<sup>1</sup>]
- **Air Force Wargaming.** Global Engagement is exploring transitioning from an air-and-space force to a space-and-air force through a long-range planning process, which has identified new operational concepts and their implementation. For example, wargames confirmed the value of protecting space assets and identified the effectiveness of using both a suborbital military space plane and expendable launchers to quickly replenish orbital sensors lost during attacks. [SCOTT98<sup>1</sup>]
- **Navy Wargaming.** At Sea Fleet Battle Experiments are exploring future naval warfare concepts, from rotational base issues to asymmetric capabilities and responses. Experiments are being designed to integrate real-world training with technological advances, innovative operational concepts, and emerging software-intensive systems. Their effects on fleet capabilities and future requirements are also being evaluated. For example, Navy is using wargames to assess the operational effectiveness of certain design features being considered for its next generation aircraft carrier.
- **Marine Corps Wargaming.** Applying nonlethal and other innovative technologies, as well as software algorithms from other disciplines, such as the natural sciences, to military art and science are being investigated.
- **Joint Wargaming.** The 1998 Joint Land, Aerospace, and Sea Simulation (JLASS 98), held at the Air Force Wargaming Institute, was the fifth in a five-year series. It included students from all service war colleges, the National Defense University, and the Industrial College of the Air Force (ICAF). The game covered warfighting issues such as: deployment of joint forces to a conflict region; force employment and sustainment; intelligence, mobilization, and theatre force requirements; and logistics. Players fought with future weapon systems such as the Joint Strike Fighter, the F-22, the Airborne Laser, and missile interceptors. [SCOTT98<sup>2</sup>]

---

### 1.2.3 Army Vision 2010: Digital Battlefield

Army Vision 2010 implements Joint Vision 2010 and the concepts identified in Force XXI through the Digital Battlefield. According to David Borland, Deputy Army Chief Information Officer (CIO), with the Digital Battlefield,

*“[E]veryone on the battlefield can interact at any time using all the tools necessary to convey thoughts, orders, or plans to any system, mounted or unmounted, on the battlefield in real-time.”*  
[BORLAND97]

Borland also explains that the Army is pursuing the acquisition of software-intensive systems *“capable of growth for new requirements and technologies compliant with the Joint Technical Architecture”*. [BORLAND97]

The Army's current efforts are aimed at enabling today's soldiers and combat systems with information technology and other software enhancements while beginning long-term research and development efforts. For example, the Experimental Force (EXFOR) is a digitized, heavy

force testing program that identifies and evaluates new operational concepts, organizational designs, advanced technologies, doctrine, and tactics.

By leveraging radical advances in information technology, software-intensive advanced weapons, and platform speeds at the tactical and operational levels, the Army intends to ensure that land power remains a strategically decisive 21st Century warfighting element. [QDR97]

---

## 1.2.4 Navy IT-21

The Navy's *Information Technology for the 21st Century (IT-21)*, implements the *Joint Vision* strategy by defining the use of information system technologies to establish a clear linkage between command, control, communications, computers and intelligence (C4I) and naval warfare. IT-21 serves as the foundation for "*network-centric*" warfare that shifts focus from operations of individual ships and systems to C4I networks that link platforms and weapon systems, or in other words, link sensors to shooters.

Navy has embraced the concept called "*network-centric warfare*." It is the enhanced massed effect of widely dispersed, robustly networked sensors, command centers, and forces. Combining forward presence with network-centric combat power, the Navy seeks to decisively close timelines, alter initial conditions, and head off undesired events before they start. The sea will be used to gain advantage over the enemy, while naval precision engagements will employ sensors, information systems, software-intensive precision guided weapons, and lethal forces to attack key targets. Naval *full-dimensional protection* is an initiative to address the spectrum of threats and provide information, air, and maritime superiority, theater air and missile defense, and naval fire delivery. [QDR97] Automated Information Systems (AIS) and software-intensive technologies will integrate fleet-service, joint-service, theater, and national sensors with weapon systems and platforms.

---

## 1.2.5 Marine Corps: Operational Maneuver

Marine Corps *Operational Maneuver from the Sea* is an initiative to develop a tactically adaptive, technologically agile, opportunistic, and exploitative force. AIS will be used to coordinate what the Marine in the foxhole sees through his binoculars with the appropriate force needed. It will convert targets into aimpoints, and translate aimpoints into required mapping functions, identify the most effective weapons for each target, assign the appropriate ordinance or missile, and prioritize targets among weapons and platforms. Following weapons launch, automated processes will provide a reliable engagement assessment. [WALSH97]

The Marine Corps' future focus is on the enhancement of the individual Marine and his or her ability to win in combat. Their Combat Development System focuses on generating the most effective combination of innovative operational concepts, new organizational structures, and emerging software-intensive technologies. Through the five-year *Sea Dragon* program, the Marines have developed an extensive experimentation plan divided into three phases, each culminating in an Advanced Warfighting Experiment:

- **Hunter Warrior** examines Naval power projections in a dispersed, non-contiguous littoral battlespace, enhanced fires and targeting, C4I, and the “*single battle.*”
- **Urban Warrior** is a two-year effort to explore operations in urban, near urban, and close terrain.
- **Capable Warrior** investigates virtual and live forces. It comprises operational level deception and maneuvering in response to a crisis, combined with the objective of containing or obviating an incipient major theater war.

---

## 1.2.6 Air Force: Global Engagement

*Global Engagement: A Vision for the 21st Century Air Force* is the Air Force vision for air and space warfare through the year 2010. It calls for maintaining and improving capabilities through quality personnel, integrated global battlespace awareness, and advanced command and control technologies. Air and space superiority will provide all U.S. forces freedom *from* attack and freedom *to* attack. Air Force precision engagement capabilities will enable the reliable application of selective, simultaneous force against specific targets. This will achieve desired effects with minimal risk and collateral damage. Air and space-based assets will contribute to U.S. *information superiority*, and agile combat support will allow combat commanders to improve force responsiveness, deployability, and sustainability.

The Air Force has established six battle laboratories to implement this vision. The concepts validated in the labs will be assimilated into Air Force organization and doctrine, as well as training and acquisition efforts. The six labs include the following areas of concentration:

- Unmanned aerial vehicles,
- Information warfare,
- Air expeditionary forces,
- Space capabilities,
- Battle management command and control, and
- Force protection. [QDR97]

On 14 June 1996, Secretary of the Air Force, Sheila E. Widnall, addressed the National Press Club in Washington, D.C. She talked about hosting a conference on modeling and simulation for the other service secretaries. They flew to the Joint Training and Simulation Center at the U.S. Atlantic Command near Langley Air Force Base, VA, a battle lab for training joint force commanders and their staffs. This battle lab’s software systems gives commanders the ability to explore options, see the logical consequences of decisions, and see how an intelligent adversary might respond to various decisions. Windall explained that,

*“At that command center we can conduct an exercise integrating real decision-makers working against a simulated enemy force — and real aircraft flown on training ranges thousands of miles away against simulated adversaries — using modeled weaponry so we can get a look at how these new weapons will affect our capabilities.”* [WINDALL96]

---

## 1.3 Budgets And Increasing Software Demands

---

### 1.3.1 Decreasing Budgets

The disappearance of the traditional monolithic adversary with identifiable threats has brought about a demand for less defense-related spending. However, we now face a legion of lesser potential adversaries with widely varied capabilities, goals, and battle environments. To meet a more diverse mission with a smaller budget requires greater efficiency in the use of our resources. This means replacing manpower with automation, and large forces with smaller forces, more carefully directed by accurate information. Software-intensive systems allow us to do accomplish more with fewer resources. Using a single aircraft with a smart bomb to attack a target carefully selected from appropriate intelligence information costs much less than sending in multiple aircraft with multiple conventional weapons to neutralize a minimally-defined target area. Software-based systems will continue to receive an increasing share of reduced budgets because they allow weapon systems to be more flexible and effective at an overall lower cost.

*“The need for U.S. military forces to adapt to new and more diverse military missions is matched by the requirement to meet these challenges within the constraints of available resources. The concurrent explosion in new technologies offers opportunities to innovatively assess new ways of addressing these issues...Information Age Technologies will provide warfighters with a breadth and depth of information unparalleled in military history. Using this information to enhance the command and control of precision strike weapons will provide U.S. forces with capabilities which have never before been available.”* — SECDEF William S. Cohen [COHEN97]

Undersecretary Gansler explains that the 21<sup>st</sup> Century warfare environment requires extensive modernization of current systems by taking advantage of rapidly changing software-intensive technologies (e.g., adding Digital Battlefield capabilities to older systems). [GANSLER98<sup>1</sup>] According to Gansler,

*“Our acquisition team must provide the warfighter with the full protection of superior weapons and total information superiority in the battlespace. To achieve total information superiority, we must incorporate advanced information systems into every weapon we acquire.”* [GANSLER98<sup>2</sup>]

The 1997 **Report of the Quadrennial Defense Review (QDR)** details a plan to increase procurement funds to prepare for future challenges and upgrade aging military systems. Modernization involves automating older platforms with software systems to bridge the gap until new platforms are developed to implement the Joint Vision 2010 framework. Table 1-1 lists the FY99 budget requests submitted to the Congress for major defense modernization programs.

Army	FY99-FY03
Ammunition	\$6.6 B
Trucks/Support Vehicles	\$5.5 B
M1A2 Tank Upgrade	\$3.2 B
Longbow Apache Helicopter	\$2.8 B
Navy	FY99-FY03
F/A-18E/F Aircraft	\$15.0 B
DDG-51 Destroyer	\$14.1 B
New Attack Submarine	\$7.5 B
LPD-17 Amphibious Transport Dock Ship	\$6.5 B
V-22 Tiltrotor Aircraft	\$5.8 B
Air Force	FY99-FY03
C-17 Airlifter	\$13.4 B
F-22 Fighter	\$11.7 B
CV-22 Tiltrotor Aircraft	\$1.7 B

Table 1-1. FY99-FY03 Major Defense Modernization Programs [DBFY99]

### 1.3.2 Modernization Budget Shortfalls

Shrinking procurement funds, dwindling forces, and expanding missions are compounding modernization challenges for acquisition managers within defense structure and budget downsizing. According to Under Secretary Gansler,

*“We have dropped our procurement account by 70% over the last 10 years and must now apply vast new resources to modernization — perhaps \$10 to \$30 billion a year more — in order to provide the dollars we need to maintain total superiority in the future battlespace.”* [GANSLER98<sup>1</sup>]

The FY99 defense budget authority was \$270.5 billion. As listed on Table 1-2, the FY99 budget includes \$48.7 billion for the procurement of more weapon systems, which is projected to reach \$63.5 billion in FY03. [DBFY99] In constant FY99 dollars, the defense budget has dropped 32% since the end of the Cold War. Spending on new equipment procurement is down by 50%. Active duty personnel have declined in numbers by nearly 33% since the Berlin Wall fell. While active troops and spending have been dramatically reduced, the commitments overseas have skyrocketed. The Army, for example, was involved in 10 major deployments between 1950 and 1989. Since 1990, it has deployed troops in 27 major contingencies — a 16-fold increase. [SKIBBIE98] The Navy and the Air Force have experienced similar increases in their security commitments, with 38 joint service deployments since 1990.[WOOD98]

	BUDGET AUTHORITY				
	FY99	FY00	FY01	FY02	FY03
QDR Goal	\$49.0 B	\$54.0 B	\$60.0 B	\$61.0 B	\$62.0 B
FY99 Budget	\$48.7 B	\$54.1 B	\$61.3 B	\$60.7 B	\$63.5 B

Table 1-2. DoD Procurement Budget FY99 to FY03 [DBFY99]

### 1.3.3 Software: *The Force Multiplier*

Under austere budget constraints, DoD is using software as a force multiplier. Software increases the capabilities of warfighters by arming them with powerful, smart weapons and decision support tools. It gives them the flexibility to adjust to previously unknown threats. It allows them to do more with less; and it increases the effectiveness of our service men and women through information superiority. Thus, our fighting forces are depending on the defense acquisition corps to equip them with software-intensive systems that have the character, disposition, capability, usability, interoperability, maintainability, and flexibility needed to fight and win.

### 1.3.4 DoD Software Spending: *Growing Demands*

As a single entity, DoD is the world's largest consumer of software goods and software-related services. DoD, the Defense agencies, and military services information technology (software, hardware, and support services) budgets for fiscal year FY98, as reported to Office of Management and Budget (OMB), are summarized on Table 1-3. [McCONNELL97]

FY98 IT BUDGET (Billions)	
DoD	\$10.2 B
DoD Agencies	\$3.4 B
Air Force	\$2.3 B
Navy	\$2.2 B
Army	\$2.0 B

Table 1-3. DoD FY98 IT Budget [McCONNELL97]

OMB does not require that DoD report what it spends on software embedded in weapon systems and in command, control, communications, and intelligence (C3I) systems classified as National Security Systems (NSS). [Defined below.] However, the GAO explains that, "*The Department of Defense...has estimated it spends \$24 billion to \$32 billion annually for software embedded in weapon systems.*" [HOENIG97] The median of those two figures added to the total of what DoD spends on software for other purposes is illustrated on Figure 1-1. Personnel include government hardware and software engineers, systems analysts, computer programmers, and technicians. Software budgeted for automated information systems (AIS) and C3I systems, not classified as NSS, includes software for administrative and operational purposes. (NSS AIS systems that support weapon systems are included within the weapon system budget numbers.) Support services include non-NSS software services not provided by government personnel.

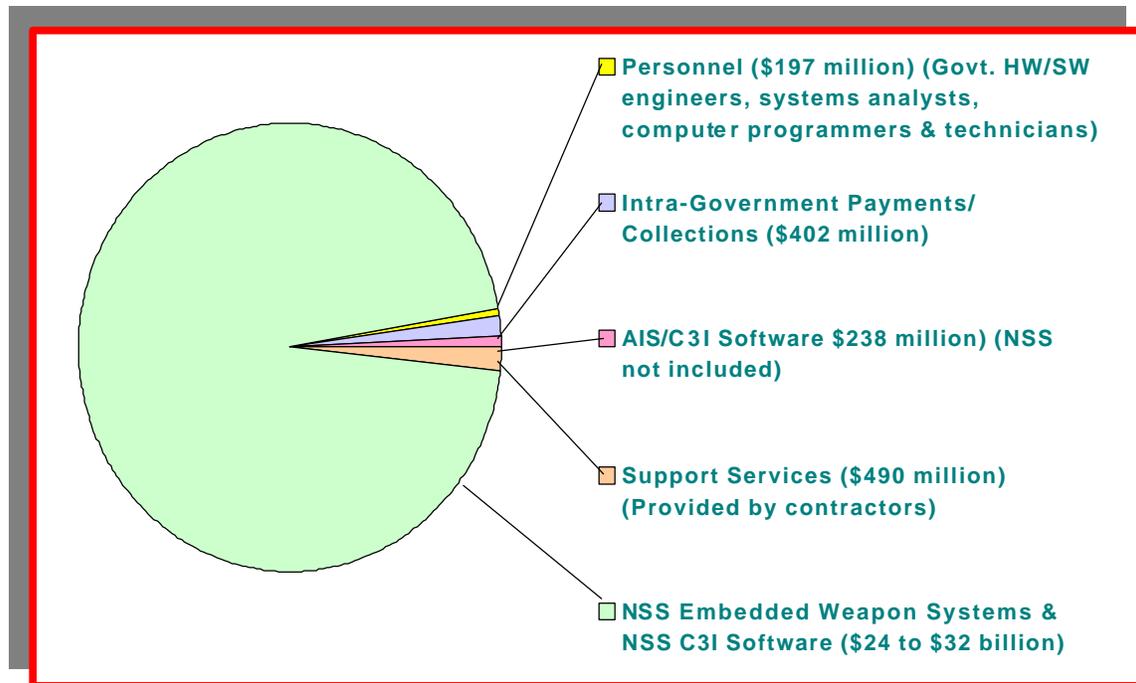


Figure 1-1. Composite DoD Annual Software Budget [BROWN97]

The responsibility for finding the funds to make up for Gansler's \$10 to \$30 billion modernization shortfall, in large part has been placed on you, today's acquisition managers. As you will learn in Chapter 3, *Statutory Framework Governing Software Acquisition*, the Revolution in Business Affairs (RBA), an initiative outlined in the 1997 **Quadrennial Defense Review**, is expected to create the revenues to support defense modernization needs. These monies will be generated by "reengineering" or "reinventing" DoD support activities. Sources of projected savings include:

- Reducing infrastructure,
- Acquisition reform,
- Outsourcing and privatizing,
- Implementing commercial/dual-use technologies and open systems,
- Reducing standards and specifications,
- Integrated process and product development, and
- Cooperative programs with allies. [QDR97]

In light of these plans for funding Defense modernization through improved management, there is widespread agreement — among DoD, the defense industry, and the Congress — that our process for determining weapon system requirements and acquiring software-intensive-systems often is costly and inefficient. One major problem stems from the wide-scale unpredictability of the acquisition process. In a speech to the 1993 Software Technology Conference, Salt Lake City, Utah, Lloyd K. Mosemann II, Assistant Deputy Secretary of the Air Force (Command, Control, Computers, and Support) astounded the audience by saying:

*“It might surprise you, or perhaps even shock you, for me to say that the Pentagon does not want process improvement, it does not want SEI Level 3, or reuse, or Ada, or metrics, or I-CASE, or architectures, or standards. What the Pentagon wants is predictability! Predictable cost, predictable schedule, predictable performance, predictable support, and sustainment — in other words, predictable quality.”* [MOSEMANN93]

---

## 1.4 Software: *The Invisible Component*

Software’s job is to tell the computer what to do and how to do it. Referred to as “*smart*” technology, software gives the computer its brains. Without software, a computer is just a box with a fan and a video screen. As Cetron and Davies explain, “*Without software to control it, all this hardware is just scrap metal, plastic, and highly purified sand.*” [CETRON97] Even many “simple” household appliances, such as microwave ovens, bread machines, washers, etc., would be useless without the embedded software they use for control.

Software has no mass — you cannot see, touch, feel, weigh, smell, or hear it. As such, software is often misunderstood, ignored, or confused with its hardware because it has no physical properties. People have trouble understanding something that is invisible, exists in an ethereal world of magnetic fields and electronic bits and bytes.

Theoretically, because it is intangible — it has none of the physical properties that cause physical systems to age and break down — it will never wear out. Also theoretically, software could last forever! Because software is intangible, it can be designed; but it cannot be built in any physical way.

Not only is software difficult to describe and comprehend in the traditional sense — software is hard to build. In 1985, David Parnas, an internationally renowned computer expert, explained that “*software is hard*” to build because it is inherently and necessarily complex. [PARNAS85]

Software pioneer, Frederick P. Brooks, Jr., explains that, “*Software entities are more complex...than perhaps any other human construct...Software systems have orders-of-magnitude more states than computers do...[Because] the complexity of software is an essential property,*” it does not lend itself to the simplification techniques found in other disciplines. [BROOKS87] For example, in mathematics simplified models of complex problems are often used as analytical tools. This does not work with software. The essence of software is that it achieves the solution of a complex problem by compounding its complexity (i.e., the algorithms defining a solution are exponentially more complicated than the real-world problems they solve). [GLASS91]

Software is a relatively new engineering field, whereas computer hardware engineering is much better defined and disciplined. Semiconductor evolution is so stable and mature, it is easy to predict where the technology will be two years from now — or even well into the next millennium. This is illustrated by, what has been dubbed *Moore’s Law*, after Gordon E. Moore, cofounder of the Intel Corporation. Moore’s Law states that processor performance and density (the number of transistors that can be packed onto a microchip), relative to their cost, doubles every 12 to 18 months. This phenomenal rate of productivity translates into a 100-fold improvement over the past decade, and a 10,000-fold improvement over the past 20 years. After 30 years of production, Moore’s Law stands firm.

In contrast, software evolution is always playing catch-up with its hardware cousin and is usually two years behind — if lucky. Once software is able to efficiently use the latest processing power (by then two years old), it sometimes takes another two years to work out all the bugs. And then, it's time to play catch up all over again.

---

## 1.5 Software-Intensive Defense Systems

Software-intensive systems have forever changed the American military's concept of the battlefield. After Desert Storm, General Colin L. Powell, Chairman of the Joint Chiefs of Staff, wrote about his “*toolbox*” of software technology:

*“The Information Age has dawned in the armed forces of the U.S. The sight of a soldier going to war with a rifle in one hand and a laptop computer in the other would have been shocking only a few years ago. Yet, that is exactly what was seen in the sands of Saudi Arabia in 1990 and 1991.”*  
[POWELL92]

In contrast to the military hardware which it enables, our constantly changing arsenal of software distinguishes us from every other advanced military on the globe. Software-intensive systems give us the technological edge to compete and win in the ever-changing, volatile world environment.

In a speech on the role of software in modern warfare, Lieutenant General Robert H. Ludwig explained that, “*In Desert Storm men and machines went off to war with something the world has never seen...software.*” When modern weapon systems are referred to as being “*smart,*” it is because software provides their brains. For instance, by retrofitting them with smart software-intensive components, even the intelligence of “*stupid bombs*” can be raised. As Ludwig succinctly stated, the “*Fly-by-wire F-16C...without software,*” is nothing more than, “*...a 15-million dollar lawn dart!*” [LUDWIG92]

*“The most powerful weapon we possess is an invisible one — our software!”* — Alvin & Heidi Toffler [TOFFLER93]

From an historical perspective, the acquisition and management of software-intensive systems is a relatively new military endeavor. During the Vietnam War, the F-4 Phantom used virtually no software in its weapon systems and software was used sparingly in other defense applications. Back then, software-intensive systems were characterized by big workhorse main frames, occupying large rooms, using thousands of watts of electricity, tons of air conditioning, punched card inputs, with long overnight turnarounds. During the 1970s, the rapid evolution of sophisticated electronic circuitry gave us smaller processors producing more computing power for a fraction of the cost. These advances, compounded by more demanding requirements, dramatically increased DoD's software use. Figure 1-2 represents a summary of Air Force and NASA software system size growth between 1960 (Vietnam War) and 1995 (post-Gulf War).

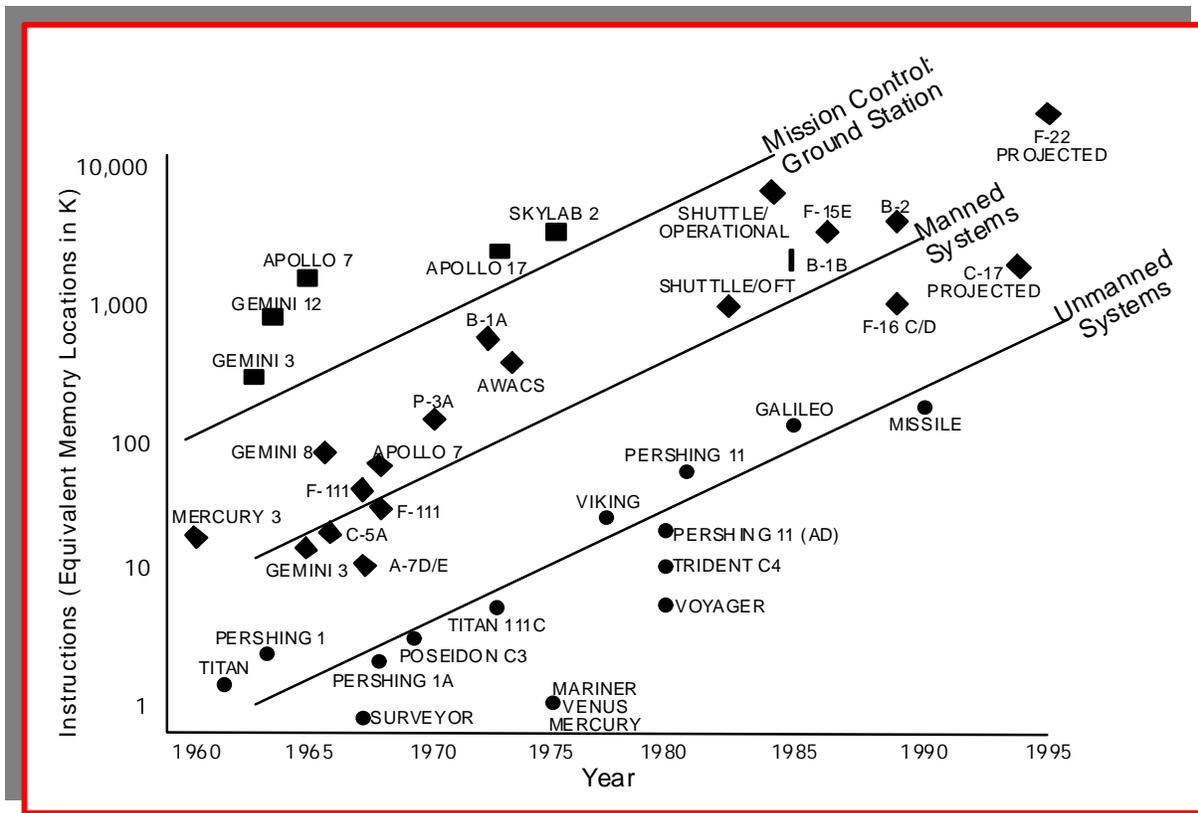


Figure 1-2. Software Systems Size Growth 1960 to 1995

Software is used to accomplish many functions formerly performed by specialized hardware, and in most cases, impossible with hardware alone. For example, software, more than any other system component, makes stealth technology possible. To cut down on its radar profile (or cross-section), the B-2 bomber has no vertical surfaces; e.g., it has no tail. Software controls all the aircraft’s directional stability. The automated flight controls on the F-117 stealth fighter are another example of how software enables stealth, as illustrated on Figure 1-3. [DANE90]



Figure 1-3. The F-117 is an Example of Software-Enabled Stealth [DoD Photo]

Over the years, the importance of software has escalated. For example, 80% of the F-22 Raptor's functionality is achieved by software, which comprised 30% of engineering and manufacturing development (EMD) costs. Software designed it, is helping build it, and will fly it. Lieutenant General Jim Fain, described software's importance when he said, *"The only thing you can do with an F-22 that does not require software is to take a picture of it" [and today even the camera is software-dependent!]* [FAIN92]

## 1.6 DoD Software Domains

The two major DoD software domains are Weapon System Software and Automated Information System (AIS) software. Despite the different operational requirements of weapon system and AIS software, both domains perform the same functions in that they each collect, record, process, store, communicate, retrieve, and display information stored in or input to computers. The guidance you find here is applicable to the acquisition and management of *all* software-intensive systems — whether weapons systems or automated information systems. Differences in the development or management of software within the two domains are the exception, not the rule, and will be brought to your attention as required. Software subcategories within the domains are shown in Figure 1-4.

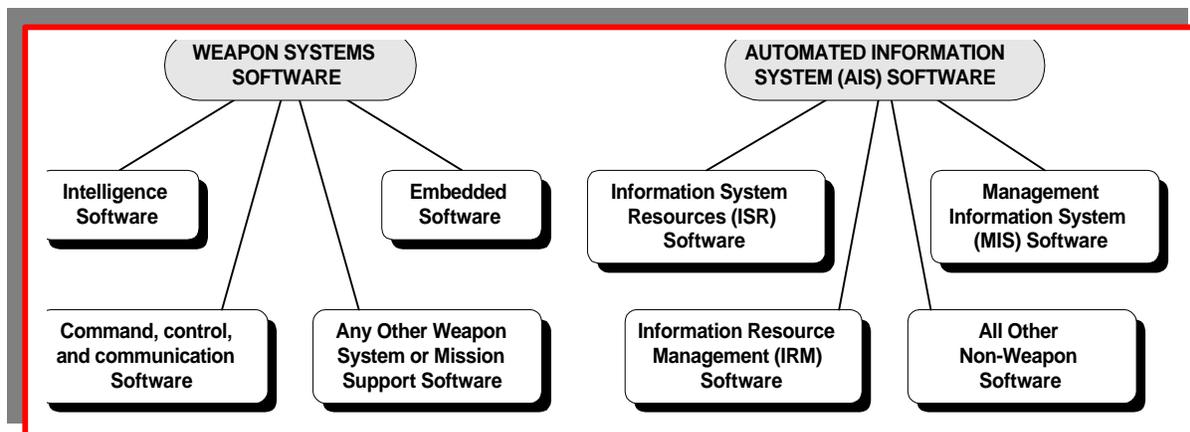


Figure 1-4. DoD Software Domains

### 1.6.1 Weapon System Software

Weapon systems include aircraft, ships, tanks, tactical and strategic missiles, smart munitions, space-launched and space-based systems, command and control (C2), and command, control, communications (C3), and intelligence (C3I) systems. Weapon system software is classified as embedded, C3, C3I, and all other software that supports or is critical to the weapon system's mission. Examples of weapon system software are the Aegis radar and fire control system and the software on the B-2 bomber. For example, B-2 bomber software must oversee and coordinate avionics functions, surveillance, electronic countermeasures, smart munitions, and intelligence systems.

### 1.6.1.1 Embedded Software

Embedded software is specifically designed into, or dedicated to, a weapon system as an integrated component of the total system. Embedded software functions as an integral part of the weapon system, and must be capable of satisfying the requirements for which it was designed or implemented; however, it does not readily support other applications without some form of modification. An example of embedded software is that contained within the electronic circuitry of a smart weapon. The pilot can activate the *go-no-go* function allowing him to *fire-and-forget* his precision guided missiles. He cannot access, control, or modify the onboard software that governs the munitions' radar, laser, infrared guidance sensors, or that activates the warhead. [HUEY91]

On the F-16, annual growth or modification for avionics, mission planning, or automatic test equipment software for all U.S. and foreign military sales aircraft is estimated at one million lines-of-code. While the F-16's embedded software components are very complex, they are only the tip of the software iceberg needed to develop and field this complex, software-intensive system, as illustrated in Figure 1-5.

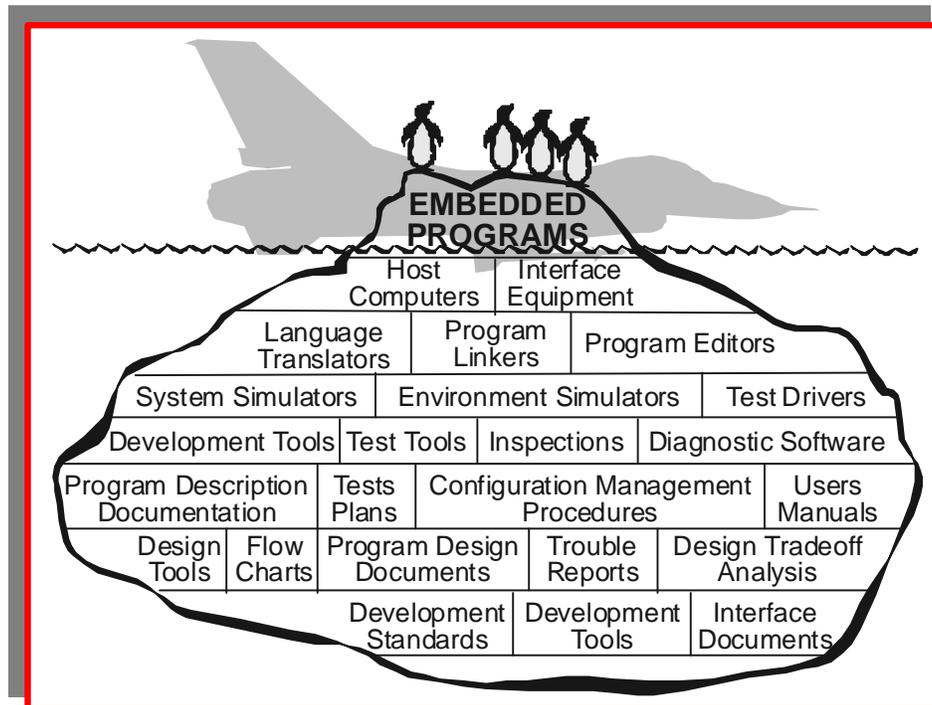


Figure 1-5. F-16 Embedded Software Iceberg

### 1.6.1.2 C3 Software

Command, Control, and Communications (C3) software is the category of weapon system software that communicates, assimilates, coordinates, analyzes, interprets information, and provides decision support to military commanders. Through advanced applications and computer technology, the C3 center aids commanders with their mission of exercising authority and giving direction to assigned forces. It provides instantaneous situational assessment, allowing for advantageous, timely positioning and decision-making.

### 1.6.1.3 Intelligence Software

Intelligence, often combined with a C3 system (C3I), plays an important role in times of conflict and national security emergencies. It also maintains efficiency and responsiveness in day-to-day military operations. Intelligence software provides fast, reliable, secure information giving continuity to tactical or strategic operations under all conditions. It is designed to be dynamic and adapt to rapidly changing environments. This software has the capacity for self-assessment through reliable warning functions that rapidly detect and react to threats or intruders. Intelligence software is found in command facilities and communications, surveillance, tracking and warning, navigation, and decision support systems. [WHITE80]

### 1.6.1.4 Other Weapon System Software

Associated with every weapon system, there is a variety of software that does not fall under the embedded, C3, or Intelligence categories. Nevertheless it is integral and absolutely essential. This software supports the weapon system and its mission. It includes software that performs mission planning, training, simulation, maintenance, battle management, system development, program management, scenario analysis, data reduction, configuration management, logistics, security, safety, quality assurance, and the testing of software and equipment. Examples of other weapon system software include the applications required to gather literally millions of data points. These data are generated during the ground and flight testing of any major developmental aircraft which is required to aid in extensive data analysis and reduction. Figure 1-6 illustrates the concept of other weapon system software. [DSMC90]

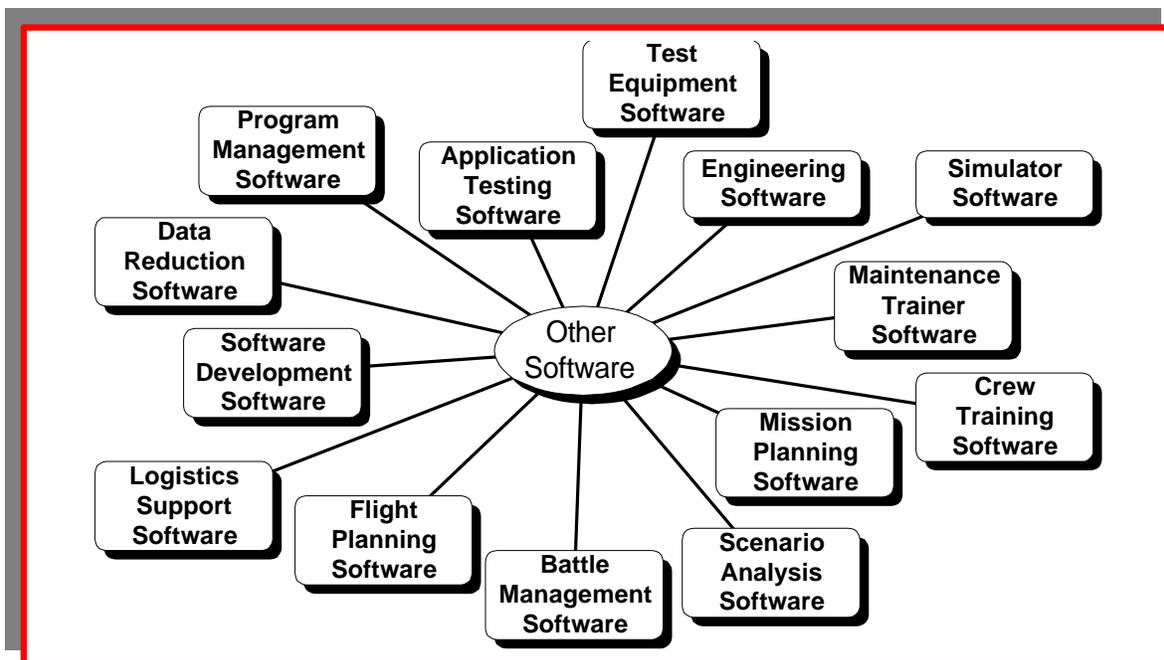


Figure 1-6. Other Weapon System Software (Not Embedded)

The Ballistic Missile Defense (BMD) program illustrates the extreme range of functional performance requirements demanded of other weapon system software. BMD software controls surveillance, tracking, target detection and prioritization, weapons assignment, weapons control

and guidance, system fault tolerance and fail-safe operations, network routing and management, security-access control, and damage assessment.

---

## 1.6.2 Automated Information System Software

While embedded systems relate to and interface with physical world entities, AIS systems relate to the information world and can have thousands of interfaces with other AIS systems. AIS software performs the functions of systems operations and support not associated with a weapon system. AIS supports administrative functions, such as accounting, payroll, finance, personnel, inventory control, mapping, and equipment and maintenance scheduling. An AIS can access multiple, large databases of information where applications restructure existing data in a way that facilitates administrative operations or management decision-making. This category (also called non-weapon system software) includes:

- Information System Resource (ISR),
- Automated Information System (AIS), and
- Information Resource Management (IRM) software.

DoD relies heavily on commercially developed products for AIS applications. However, you should remember that *security requirements cut across both weapon system and AIS software domains*.

Much of AIS software falls under the industry category of Information Technology (IT). IT includes a wide spectrum of products and services from computer electronics, computer hardware manufacturing, computer software, and software-related services. Over the past decade, industrial growth has shifted dramatically from computer electronics and computer hardware manufacturing to software products and software-related services.

A major initiative in the area of AIS is the Global Combat Support System program. This system will provide:

*“...total systems integration services and products to modernize standard Automated Information Systems (AISs) into integrated systems that are responsive to Air Force needs during times of war and peace.” [GCSS95]*

### 1.6.2.1 Simulation and Modeling Software

Software not only helps us fight and win, it enables us to train and wargame. Simulators used to train and models used by strategists, are enabled by software and sensors. DoD’s science and technology strategy places strong emphasis on synthetic environments using software systems for distributed interactive simulation. Software-intensive developments include:

- Automation and robotics;
- Aided or automatic target recognition; and
- Distributed command, control, and communications.

The fifth Navy Seawolf (a smaller, less expensive version than its predecessors) used simulation design software (a developed-in-house animation package) to test future stealth submarine design capabilities. Engineers assembled a software mockup of the Seawolf and analyzed its anticipated performance characteristics in a virtual undersea environment. Through software models, the Navy customer was able to take a cyberspace tour of the futuristic fly-by-wire vessel. Software enabled shock-level tests (anticipated effects of different types of impact damage) to be run on various Seawolf components. Where ruggedized, versus militarized, equipment can be used was determined. [ROOS95]

Simulation software also saves time and test resources. During full-scale engineering and manufacturing development (EMD), durability testing of the C-17 Globemaster airframe was completed in record time. Over 60,000 simulated flight hours were logged — the equivalent of two design lifetimes — of which more than 17,000 simulated flights were conducted — the equivalent of a 60-year operational life. Airframe loads simulating 25 different mission profiles, ranging from airdrops to short-field landings, were enacted by more than 260 software-intensive hydraulic actuators. Movement data were processed and analyzed from over 1,000 strain gauges and deflection monitors. Approximately 11% of the flight profiles were performed in the high stress environment of flight below 2,000 feet at speeds above 300 knots. Several weeks ahead of schedule, EMD testing requirements for the C-17 airframe specification were satisfied without leaving the ground. [SMITH94]

### 1.6.2.2 Artificial Intelligence

As Admiral James B. Busey, IV (USN) claims simulators relying on artificial intelligence (AI) software provide high density, fast, effective, and inexpensive ways for us to prepare the warfighter for possible far-flung encounters and unforeseen conflicts. He explains that in future wars there will be too much information, too widely spread, for any one individual (or single unit) to cope without the help of *intelligent* software systems. Artificial intelligence is based on the fundamental concept that software can process artificially sensed information, make optimal decisions based on this information and well-defined objectives, and translate those decisions into actions. [BUSEY95]

Where databases merely store information, AI systems use information. They treat data as knowledge — not just surface patterns — but meaningful information that has consequences and causes things happen. [HAYES93] DoD uses AI models and simulations during concept exploration for new or upgraded weapon systems acquisitions. It expands and evaluates the range of technical, operational, and system alternatives. It is also used for test and evaluation exercises and for planning and decision aids to expand the ability of commanders to train, plan, and employ their forces. [BUSEY95]

---

## 1.7 References

- [ACKERMAN97] Ackerman, Robert K., “Military Intelligence Expands Collection and Analysis Focus: The Difficulty in Predicting Future Roles or Adversaries Mandates Greater Information Gathering and Analysis,” *Signal*, Armed Forces Communications and Electronics Association, Fairfax, Virginia, October 1997.
- [ALSOP98] Alsop, Stewart, “A Software Junkie Rejects Windows 98,” *Fortune*, 20 July 1998.
- [BORLAND97] Borland, David, as quoted by Joshua A. Kutner, “U.S. Success in Future Battlefield Hinges on Information Advantage,” *National Defense: NDIA’s Business & Technology Journal*, December 1997
- [BROOKS87] Brooks, Fredrick P., Jr., “No Silver Bullet: Essence and Accidents of Software Engineering,” *Computer*, April 1987.
- [BROWN95] Brown, Lori Hylton, Christopher Johnson, and William Warlick, *Global Competitiveness of the U.S. Computer Software and Service Industries*, U.S. International Trade Commission, June 1995.
- [BROWN97] Brown, Linda, “Category 43 FY96 Budget Authority Exhibit,” OSD/C3I, 24 January 1997.
- [BUSEY95] Busey, ADM James B., IV, “Battlefield Technologies Muster in Synthetic Arenas,” *SIGNAL*, July 1995.
- [CETRON97] Cetron, Marvin and Owen Davies, Probable Tomorrows: How Science and Technology Will Transform Our Lives in the Next Twenty Years, St. Martin’s Press, New York, 1997.
- [COHEN97] Cohen, William S., **Annual Report to the President and the Congress**, Government Printing Office, Washington, D.C., April 1997.
- [DANE90] Dane, Abe, “Black Jet,” *Popular Mechanics*, July 1990.
- [DBFY99] “**Department of Defense Budget for FY 1999**,” Press Release No. 026-98, U.S. Department of Defense, The Pentagon, Washington, DC, 2 February 1998.
- [DSMC90] Caro, Lt Col Isreal, et al., Mission Critical Computer Resources Management Guide, Defense Systems Management College, Fort Belvoir, Virginia, 1990.
- [ERWIN98] Erwin, Sandra I., “Forging First-Rate Forces Requires Up to \$30B Annual Funding Boost,” *National Defense: NDIA’s Business and Technology Magazine*, National Defense Industrial Association, Arlington, Virginia, July-August 1998.
- [ESTES98] Estes, Gen. Howell M., III (USAF retired), as quoted by William B. Scott, “Wargames Revival Breaks New Ground,” *Aviation Week & Space Technology*, 2 November 1998.
- [FAIN92] Fain, Lt. Gen. Jim, (USAF) as quoted by Lt. Gen. Robert H. Ludwig (USAF), “The Role of Technology in Modern Warfare,” briefing presented to the Software Technology Conference, 14 April 1992.
- [GANSLER98<sup>1</sup>] Gansler, Jacques S., “**Affordable Weapons Systems; A Design For The Future**,” Speech presented to the Precision Strike Association Annual Programs Review, Fort Belvoir, Virginia, 19 May 1998.
- [GANSLER98<sup>2</sup>] Gansler, Jacques S., “**Modeling and Simulation: A New Way To Address Environmental Concerns**,” Speech Presented to the Environmental Security Modeling and Simulation Conference, Alexandria, Virginia, 5 May 1998.
- [GCSS95] **Global Combat Support System**, March 1995
- [GLASS91] Glass, Robert L., Software Conflict: Essays on the Art and Science of Software Engineering, Yourdon Press, Englewood Cliffs, New Jersey, 1991.
- [HAMRE98] Hamre, DEPSECDEF John J., “**Information Systems: Y2K & Frequency Spectrum Reallocation**,” Statement before The Senate Armed Services Committee, Washington, D.C., 4 June 1998.
- [HAYES93] Hayes, Patrick J., “Is Artificial Intelligence Real?: Absolutely — and Vital for Riding the Rising Tide of Information,” *Washington Technology*, 9 September 1993.

- [HINCHMAN97] Hinchman, James F., *High-Risk Series: Information Management and Technology*, Letter Report, GAO/HR-97-9, United States General Accounting Office, Washington, DC, February 1, 1997.
- [HOENIG97] Hoenig, Christopher, **Managing Technology: Best Practices Can Improve Performance and Produce Results**, GAO/T-AIMD-97-38, Information Resources Management Policies and Issues Accounting and Information Management Division, United States General Accounting Office, Washington, DC, 31 January 1997.
- [HUEY91] Huey, John and Nancy J. Perry, "The Future of Arms," *Fortune*, 25 February 1991.
- [JCS96] **Joint Vision 2010**, Chairman Joint Chiefs of Staff, Department of Defense, The Pentagon, Washington, DC, 1996.
- [JOHNSON98] Johnson, Susan Tinch, and Jack A. Bobo, *Software Workers for the New Millenium: Global Competitiveness Hang in the Balance*, National Software Alliance, Arlington, Virginia, January 1998.
- [KEMERER97] Kemerer, Chris F., "Software: Reusable Asset" *InformationWeek*, 22 September 1997.
- [LUDWIG92] Ludwig, Lt Gen Robert H., "The Role of Technology in Modern Warfare," Speech presented to the Software Technology Conference, 14 April 1992.
- [LYOTARD79] Lyotard, Jean François, "Introduction," *The Postmodern Condition: A Report on Knowledge*, 1979.
- [McCONNELL97] McConnell, Bruce, as quoted by Bob Brewin, "IT Spending Remains Flat," *Federal Computer Week*, 17 March 1997.
- [MOSEMANN93] Mosemann, Lloyd K., II, as quoted in *Ada Information Clearinghouse Newsletter*, Vol. XI, No. 2, August 1993.
- [NACS92] "A National Strategy for Semiconductors," The National Advisory Committee on Semiconductors, February 1992.
- [NDCF97] "The NDCF World Conflict List," National Defense Council Foundation, Alexandria, Virginia, 1997.
- [PARNAS85] Parnas, David Lorge, "Software Aspects of Strategic Defense Systems," *American Scientist*, September-October 1985.
- [POWELL92] Powell, GEN Colin L., "Information-Age Warriors," *Byte*, July 1992.
- [QDR97] **Report of the Quadrennial Defense Review**, U.S. Department of Defense, The Pentagon, Washington, DC, May 1997.
- [ROOS95] Roos, John G., "New and Newer Submarines: As Seawolf Prepares to Prowl the Depths, A Likely Successor Already Roams — In Cyberspace," *Armed Forces Journal INTERNATIONAL*, July 1995.
- [SCOTT98<sup>1</sup>] Scott, William B., "Wargames Revival Breaks New Ground," *Aviation Week & Space Technology*, 2 November 1998.
- [SCOTT98<sup>2</sup>] Scott, William B., "JLASS Wargame Challenges Players' Real-Time Battle Skills," *Aviation Week & Space Technology*, 2 November 1998.
- [SCOTT98<sup>3</sup>] Scott, William B., "'Title-10' Games Shape Policies," *Aviation Week & Space Technology*, 2 November 1998.
- [SMITH94] Smith, Bruce A., "Downsizing to Deepen As Backlogs Shrink," *Aviation Week & Space Technology*, 14 March 1994.
- [STRASSMANN97] Strassmann, Paul A., *The Squandered Computer: Evaluating the Business Alignment of Information Technologies*, The Information Economics Press, New Canaan, Connecticut, 1997.
- [SILVESTRI97] Silvestri, George T., "Employment Outlook: 1996-2006; Occupational Employment Projections to 2006," *Monthly Labor Review*, U.S. Department of Labor, November 1997.
- [TILLET98] Tillett, Scott, Colleen O'Hara and Daniel M. Verton, "**Agencies' IT Spending Nears \$30B in Fiscal '99**," *Government Computer News*, 18 May 1998.
- [TOFFLER93] Toffler, Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century*, Little, Brown, and Company, Boston, 1993.

- [WALSH97] Walsh, Edward J., “Naval Mission Planning Built Around Information Systems,” *National Defense: NDIA’s Business & Technology Journal*, December 1997.
- [WHITE80] White, Eston T., Defense Organization and Management, National Defense University, Washington, D.C., 1980.
- [WIEBNER98] Wiebner, Mike, “Global Government Partners: Tech Firms Jockey for Lucrative Foreign Contracts,” *Washington Technology*, 16 July 1998.
- [WINDAL96] Windall, Secretary Sheila E., “Visible and Invisible Capabilities,” Speech presented to the National Press Club, Washington, D.C., 14 June 14 1996.
- [WOOD98] Wood, Lt. Gen. C. Norman (USAF Ret.), “High Technology Is Essential to Reviving Our Defense Force,” *Signal: Official Publication of the Armed Forces Communications and Electronics Association*, November 1998.