CHAPTER 8
INFORMATION SUPERIORITY AND SPACE

DoD is committed to taking full advantage of the opportunities provided by the Information Age by improving situational awareness and the ability to share this awareness to support new operational concepts and a knowledge-based workforce. To this end, the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)) also has been designated as the Chief Information Officer of the Department, and has been assigned responsibilities for space-related policy, acquisition oversight, and guidance.

INFORMATION SUPERIORITY

Information superiority is all about getting the right information to the right people at the right time in the right format while denying adversaries the same advantages. The United States enjoys a competitive advantage in many of the technical components of information superiority, but the U.S. also has vulnerabilities stemming from its increasing dependence on high technology. Experiences from Somalia to the Balkans have shown that low technology adversaries also can wage effective information campaigns, especially in urban environments.

Given that DoD information can be adequately assured, and the opponents' capabilities are appreciated, U.S. strengths in the information domain can be translated directly into competitive advantages by emerging network-centric concepts that are designed to leverage high-quality shared awareness. Moreover, the Department's financial, logistics, and acquisition practices can be improved significantly by the use of information technology and improved business practices. Thus, information superiority is reflected in both the Revolution in Military Affairs (RMA) and the Revolution in Business Affairs (RBA). These twin revolutions are mutually supportive.

IMPORTANCE OF INFORMATION SUPERIORITY

In the Information Age the opportunities and obstacles to achieving national security objectives will often be informational in nature. Information superiority is a principal component of the transformation of the Department. The results of research, analyses, and experiments, reinforced by experiences in Kosovo, demonstrate that the availability of information and the ability to share it significantly enhances mission effectiveness and improves efficiencies. Benefits include: increased speed of command, a higher tempo of operations, greater lethality, less fratricide and collateral damage, increased survivability, streamlined combat support, and more effective force synchronization. Kosovo also highlighted the shortage of assets for intelligence, surveillance, and reconnaissance and the need for more secure interoperability and information protection, especially within coalitions.

The ability to move information quickly to where it is needed and to create shared awareness provides an opportunity to develop new concepts of operation and approaches to command and control (C2) that are more responsive, provide greater flexibility, and increase combat power. To achieve their full potential, however, these new concepts and approaches need to be co-evolved with changes in organization, doctrine, material, personnel, and the like. New approaches to command and control include integrating the now separate and sequential processes for planning and execution and the capability for forces to be self-synchronizing. Based on a common understanding of the situation and the commander's intent, these forces are able to be more proactive and shape the battlefield, as well as to respond quickly in a coordinated fashion.

SPACE

Space is a domain like the land, sea, and air where military activities are conducted. Access to and use of space is central to DoD accomplishing its missions. U.S. joint forces successfully exploit space capabilities today across the spectrum of military operations. Space and space related activities enable detection of missiles inbound against the U.S. or its allies; enhance command and control of U.S. forces; target weapons; and forge worldwide deployments into a single, global force, able to deter and defend against major regional contingencies, engage in small operations, and lead peacekeeping operations. Unimpeded access to and use of space is and will remain a vital national interest. Space is now part of the tactical battlefield and its use is growing. U.S. forces can respond to crises faster and have fewer troops in harm's way because commanders can use space to reach back to CONUS bases for support. DoD needs to ensure its systems are interoperable and fully integrated across the land, air, sea, and space.

Space forces and space-based capabilities are integral to the deterrent posture of the U.S. armed forces. They help to ensure that preparations for and initiation of hostile actions will be discovered in a timely manner and they introduce an element of uncertainty into the minds of potential adversaries about whether they can achieve their aims. Space forces are critical to the ability of the United States to ensure the costs of the threat or use of force are unacceptable to potential aggressors. The deterrence of aggression and the defense of the United States and its allies will be strengthened by ensuring that adversaries cannot achieve an asymmetric advantage by countering U.S. space capabilities or using space systems or services for hostile purposes.

Space forces contribute to the overall effectiveness of U.S. military forces in the event deterrence fails. The high technology force multipliers provided by space systems enhance the combat power of military forces. The capability to control space, if directed, will contribute to achieving the full dimensional protection, battlespace dominance, and information superiority necessary for success in military operations. Space forces thus will enable the United States to compel an adversary to cease and desist from the pursuit of its aims through the use of necessary and proportional force.

Ensuring the freedom of space and protecting U.S. national security interests in the medium are priorities for space and space-related activities. U.S. space systems are national property afforded the right of passage through and operations in space without interference. In this regard, space is much like the high seas and international airspace. The political, military, and economic value of the Nation's activities in space, however, may provide a motive for an adversary to counter U.S. space assets. Purposeful interference with U.S. space systems will be viewed as an infringement on U.S. sovereign rights.

INFORMATION SUPERIORITY STRATEGY AND GOALS

ELEMENTS OF INFORMATION SUPERIORITY

Achieving information superiority requires organizing information to create knowledge and then providing that knowledge reliably and in a timely manner to decision makers. Information increases dramatically in value when combined into a coherent picture. However, this value is not realized until it reaches someone who can use it to create a shared awareness. Thus, the importance of interoperability—the ability of different organizations and systems to share and utilize information—is paramount. DoD must have a comprehensive approach to integrating the Department's information processes and to achieving interoperability across organizations and systems. Without it there will continue to be gaps and barriers that diminish the quality, quantity, and timeliness of information that is available for operations. Shared awareness allows for synchronized efforts. Thus, it is important not only that situation-related information is shared, but also that there is a capability for collaborative decision making and sharing of commander's intent, plans, and implementing actions. These create the conditions necessary to synchronize actions dynamically in response to developing situations and to take advantage of opportunities as they occur.

While the Information Age has created enormous opportunities, it has also created significant vulnerabilities for those who depend upon an uninterrupted flow of quality information to support operations. Protecting DoD information and information assets is a basic necessity. Protection and redundancy must be engineered in from the outset, not added on as an afterthought. Since information superiority is a relative concept, operations to disrupt, deny, degrade, destroy, and exploit an adversary's information and information processes are an integral part of achieving, maintaining, and leveraging information superiority.

PREREQUISITES FOR PROGRESS

There are three prerequisites for progress toward information superiority—innovation, co-evolution, and the achievement of a critical mass of information infrastructure (infostructure).

INNOVATION

Successful innovation depends on an understanding of the possibilities, the ability, and tools to experiment with new concepts and capabilities, recognizing at the same time that some innovations will fail. This involves the technical and operational communities, as well as opportunities for joint experimentation. Strong ties between the technical and operational communities provide warfighters with a better understanding of the capabilities and opportunities that emerging information concepts and technologies provide, and provide systems designers and developers with a better appreciation of operational requirements and environments. Experimental venues facilitate innovation by providing opportunities for discovery and capturing empirical data for analysis.

CO-EVOLUTION

Successful introduction of information technology must be accompanied by significant changes in business practices which are key to creating and leveraging information superiority. Therefore, concepts of operation, command approaches, systems, organization, and doctrine must co-evolve together and thus must be an integral part of DoD's investment strategy. The need for co-evolution must also be reflected in experimental venues. The force structure of tomorrow must take into account the requirements for human expertise, skills, and experience necessary to create and manage knowledge. Entering the 21st century, information technologies are advancing at unprecedented rates; DoD must be in a position to anticipate and leverage these technologies.

INFOSTRUCTURE AND TECHNOLOGY INVESTMENTS

A critical mass of protected information and information processing capabilities; trained personnel; and assured connectivity is needed so warfighters can gain hands-on experience with the power of information and the possibilities of networking. The achievement of information superiority is not a one-time milestone, but rather a continuing process of identifying the best that technology has to offer while adapting and integrating it to DoD needs.

MAKING INFORMATION SUPERIORITY HAPPEN

To ensure that the above prerequisites are in place, DoD is developing appropriate policy and oversight initiatives, actively pursuing opportunities to improve international cooperation in the areas of Command, Control, Communication, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) and space-related activities, partnering with industry, and working to anticipate and understand the implications of emerging information technologies.

POLICY AND OVERSIGHT

Current advances in information technology are redefining the way DoD does business, as well as creating new economic opportunities in the commercial sector. The enormous crop of technology available in recent years is the result of government-sponsored research and development investments in seminal research and technologies many years ago. Today's challenges include both investment choices for future technologies and insertion of current products into information superiority capabilities for the warfighter. Technology insertion, however, can be very disruptive unless it is accompanied by appropriate changes in enterprise organizations, procedures, training, and standards. To address these challenges, the Department is developing an information superiority advanced technology plan that provides guidance and focus to current and emerging DoD and commercial research and development. The Department has also strengthened ASD(C3I) involvement in oversight of Advanced Concept Technology Demonstrations (ACTDs). Finally, the Department has defined metrics for information superiority, and is planning a joint command and control experiment in 2001 centered on information presentation and comprehension.

INTERNATIONAL COOPERATION

The success of future military operations across the spectrum of conflict depends on the ability of the United States and its partners to exchange information quickly, unimpeded by technological barriers. Lessons from Kosovo indicate that the inability to share information in secure, interoperable ways can have adverse mission consequences. DoD is taking concerted action to inform other nations of its plans for the future and to seek opportunities for cooperative developments that will improve interoperability. Where appropriate, multinational fora such as the Multinational Interoperability Council, the NATO Consultation, Command, and Control Board and its subcommittees, the Combined Communications Electronics Board, the Quadrilateral C3 Senior National Representatives forum, the NATO Partnership for Peace Program, the Southeast Europe Defence Ministerial initiative, and the Quadrilateral International Cooperative Opportunities Group are used to engage allies and partners in a productive dialogue and to develop the necessary partnerships. The United States contributes to these efforts by providing technology for command and control, communications, and crisis management, as well as assistance with C3 architecture development and systems engineering. Specific examples of DoD's efforts during 2000 include the NATO Defense Capabilities Initiative (DCI), Year 2000 Outreach program, and initiatives in the areas of information assurance (IA), battlefield information collection and exploitation, and multifunctional information distribution. DoD engaged in international consultations on remote sensing cooperation and concluded agreements with Canada and Japan. DoD continued to support ongoing efforts to discuss national security space equities at the UN Conference on Disarmament and Committee on Peaceful Uses of Outer Space.

PARTNERSHIPS WITH INDUSTRY

DoD works closely with the U.S. defense industry to promote international industrial teaming and to keep the C3 community apprised of DoD plans and strategies for the future. The benefits of this closer relationship include increased chances for improving interoperability and broader markets, and increased competition leading to more affordable products and insights into the plans of the other nations. The establishment of partnerships between the defense space sector and the intelligence, civil, and commercial space sectors will serve to balance investments, enable the leveraging of scarce resources, and reduce the cost of acquiring, operating, and supporting operational space force capabilities. The Department led the successful effort to define licensing criteria for commercial radar, hyperspectral and second-generation electro-optical systems, finalized an interagency agreement on licensing of private remote sensing satellite systems, developed a government strategy on foreign remote sensing space cooperation, and assisted the National Oceanic and Atmospheric Administration (NOAA) on finalizing the Commercial Remote Sensing Licensing Regulations.

INFORMATION SUPERIORITY GOALS

One of DoD's principal information superiority goals during 1999 was to maintain the capability to execute its missions throughout the Y2K rollover. This commitment to the American people was met. The following goals are being pursued in parallel, though they are maturing at different rates.

CREATE AN INFORMATION SUPERIORITY TEAM

The foundation of all other goals is to attract, motivate, train, and sustain a world class team dedicated to creating and leveraging information superiority within DoD.

IMPLEMENT EFFECTIVE PROGRAMS FOR ESTABLISHING INFORMATION ASSURANCE AND CRITICAL INFRASTRUCTURE PROTECTION

The Department's defense in-depth strategy protects critical assets and processes needed for mission accomplishment through effective training and certification of personnel, improved security operations, public key infrastructure (PKI), an integrated attack sensing and warning capability, the capability to conduct computer forensics, and the ability to leverage IA and critical infrastructure protection (CIP) technology solutions. DoD must also develop policies to define the use of commercial products and ensure business practices keep pace with electronic capabilities. DoD must work with allies and coalition partners to protect information since, in an interconnected world, this translates into the ability to protect DoD's information and critical infrastructure.

BUILD A COHERENT GLOBAL INFORMATION GRID

The Global Information Grid is a major initiative that takes an enterprise view of DoD networking, computing, interoperability, and information assurance. It places emphasis on both the importance of information as a strategic resource and the need for greater compatibility of information technology with commander in chief (CINC), Service, and agency mission-critical operational processes.

ACHIEVE END-TO-END C4ISR INTEGRATION

An integrated joint and combined C4ISR capability is necessary to ensure that information will be available, relevant, accurate, protected, authenticated, and provided in a useful and timely manner.

PROMOTE THE DEVELOPMENT OF KNOWLEDGE-BASED WORKFORCE

Improved productivity in the Information Age depends, in large measure, upon the creation and maintenance of reusable knowledge bases; the ability to attract, train, and retain a highly skilled workforce; and core business processes designed to capitalize upon these assets. Central to this effort is the employment of a number of strategies aimed at optimizing information sharing, collaboration, and reuse.

STRENGTHEN DEFENSE INTELLIGENCE FOR THE 21ST CENTURY

Getting needed intelligence information to decision makers in a timely and useful manner is critical in achieving information superiority. Intelligence faces significant challenges to meet the requirements of the 21st century. The Department must revitalize and reshape the intelligence workforce. The Department faces personnel shortfalls in linguists, all-source analysts, human intelligence collectors, and cyber specialists. The Department must transform and streamline its intelligence processes across: tasking, collection, processing, analysis, exploitation, and dissemination to keep pace with the changing threat environment. The Department must strengthen its collaboration with industry, academia, and other non-traditional intelligence partners. The Department must address hard technological problems such as increased use of: deception and denial, more sophisticated commercial encryption, and fiber optic and cellular communications. The Department should place particular emphasis on integrating new SIGINT and MASINT technologies into intelligence capabilities.

STRENGTHEN INFORMATION OPERATIONS, SECURITY, AND COUNTERINTELLIGENCE

Foreign intelligence services and non-state actors are targeting the Department's secrets and critical program information. DoD is committed to countering such threats and protecting against trusted insider misconduct by updating policies and programs and developing a more aggressive posture to counter foreign threats and to protect against trusted insider misconduct. Further, DoD will rationalize security requirements to ensure secure information sharing among coalition partners while continuing to protect against the improper release of information. In so doing, the level of security awareness throughout DoD and its coalition partners will be increased.

PROMOTE ELECTRONIC COMMERCE AND BUSINESS PROCESS CHANGE

In order to realize the gains associated with Information Age technologies, DoD is committed to developing and implementing new ways of doing business that are designed to leverage the power of information. The Department is also committed to using electronic business/electronic commerce principles, processes, and technologies as the primary means of transacting its business.

FOSTER DEVELOPMENT OF AN ADVANCED TECHNOLOGY PLAN FOR INFORMATION SUPERIORITY

The convergence of disparate technologies into a package that has operational utility requires the development and implementation of a coherent plan. Therefore, DoD is developing an advanced technology plan for information superiority to rationalize investments, coordinate and leverage research, and focus efforts on high priority areas.

CREATING THE INFOSTRUCTURE

THE INFOSTRUCTURE VISION

The quality of DoD's infostructure will be a pacing item on the journey to the future. The ability to conceive of, experiment with, and implement new ways of doing business to harness the power of Information Age concepts and technologies depends upon what information can be collected, how it can be processed, and the extent to which it can be distributed. The ability to bring this capability to war will depend upon how well it can be secured and its reliability. DoD envisions an infostructure that is seamless with security built-in, one that can support the need for increased combined, joint, and coalition interoperability, leverages commercial technology, and accommodates evolution.

SEAMLESS AND COHERENT

To facilitate the end-to-end flow of information necessary to support network-centric operations, information processes must be transparent to users. DoD systems must transition from isolated stove-piped environments to a seamless and coherent infostructure. This requires the establishment of a Department-wide mechanism for gaining visibility into the many separate planning, budgeting, acquisition, operations, and maintenance activities that contribute to DoD's information systems and processes. DoD's Global Information Grid is designed to achieve this by creating a DoD-wide network management solution, comprised of enterprise network policies, strategies, architectures, focused investments, and network management control centers that bring order out of the current, highly fragmented Service-centric DoD information infrastructure.

BORN JOINT AND COALITION

Future operations will be joint, include reserve components and civilian specialists, and most likely will involve partnerships with other countries to form a coalition. Their effectiveness will depend not only upon the ability of DoD to share information and collaborate internally but externally as well. Therefore, interoperability must be considered a key element in all DoD operational and systems architectures. That interoperability must include the ability to overcome language and cultural barriers. Experience shows that after the fact interoperability fixes are costly, do not satisfy mission requirements, and create security problems. Success is achieved by incorporating interoperability from the start.

LEVERAGES COMMERCIAL TECHNOLOGY

The engine driving advances in information technologies is in the commercial sector. DoD benefits from the sheer size of the commercial marketplace for information technology which drives down the costs of off-the-shelf capabilities, fuels an unprecedented rate of improvement in cost/performance, and makes interoperability easier to achieve. As a result, DoD now can reap the benefits of private sector investments, saving scarce R&D dollars to invest in militarily significant areas that the commercial sector is not addressing. The downside is that the latest technology is now available to potential foes and allies alike.

SECURITY BUILT IN

Security, like interoperability, must be incorporated into systems designs from the beginning to be effective and affordable. Security must be co-evolved with approaches to interoperability since new/revised links among systems increases vulnerabilities. While DoD's continuing migration from analog to digital systems will facilitate efforts, there will always be legacy systems and systems that coalition partners use that lack adequate security. DoD is exploring approaches to deal with these exceptions; however, these will in all likelihood entail limiting the functionality and utility of these nonconforming systems.

ACCOMMODATES EVOLUTION

Change is the constant of the Information Age. DoD infostructure must be designed to accommodate rapid change as both requirements and technologies evolve. A comprehensive strategy that consists of appropriate architectures, standards, design principles, configuration management, and regression testing will be incorporated into DoD's infostructure processes.

INFOSTRUCTURE INITIATIVES

ARCHITECTURES FOR JOINT VISION 2020

An integrated national security architecture is being developed to eliminate unnecessary vertical stovepiping of programs, minimize unnecessary duplication of missions and functions, achieve efficiencies in acquisition and future operations, provide strategies for transitioning from existing architectures, and thereby improve support to military operations and other national security objectives. This integration effort includes the various sources of intelligence, surveillance, and reconnaissance capabilities. Thus, these communities will be able to more efficiently access and exploit information from multiple sources as well as to integrate the end-to-end intelligence cycle to provide timely, relevant information products.

DEFENSE ENTERPRISE COMPUTING CENTERS (DECCs)

DECCs, based in the continental United States, process combat and combat support requirements for warfighters deployed around the world. DoD has substantially reduced the cost of this processing by modernizing and consolidating 194 Service and Defense Agency Information Processing Centers into five Defense Enterprise Computing Centers with 14 DECC detachments providing regional and local computing and information technology support.

GLOBAL INFORMATION GRID (GIG)

GIG is an enterprise view of DoD networking, computing, interoperability, and information assurance consisting of a globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The end goal is a secure, robust, integrated, and interoperable architecture that is effectively managed to help achieve information superiority.

To implement the GIG, the CIO will provide a sound set of principles; use the DoD CIO Executive Board to address critical enterprise IT issues; develop an integrated, synchronized architecture to manage complexity and diversity, and ensure an enterprise approach; and implement processes to enforce compliance with architectures and policies.

A critical element of an integrated architecture is a common set of technical standards. The DoD Joint Technical Architecture (JTA) identifies the minimum set of standards and guidelines to be used when acquiring all new systems or upgrading existing ones. Since the JTA contains a large number of standards a web-accessible JTA is being developed to facilitate consistent selection of applicable standards.

GLOBAL COMMAND AND CONTROL SYSTEM (GCCS)

GCCS is a warfighter-oriented system and is the single joint command and control (C2) system for the Chairman, Joint Chiefs of Staff. GCCS supports the National Command Authorities (NCA) and subordinate elements in conducting synchronized operations from dispersed locations. GCCS allows commanders in chief (CINCs) and joint task force (JTF) commanders to maintain dominant battlefield awareness through a fused, integrated, near real-time picture of the battlespace. It provides them with integrated imagery and intelligence situational awareness, indications and warnings, collaborative planning, course of action development, and intelligence mission support. In FY 2000, GCCS released several new mission applications and baseline updates, migrated selected GCCS applications to the NT environment, and developed/fielded embedded training tools for GCCS applications and new modules of the Readiness Assessment System.

SPECTRUM MANAGEMENT

The use of high technology weapons, satellite and ground communications, radio navigation, surveillance, and satellite control systems continue to increase the Department's reliance on assured access to the electromagnetic spectrum and the need for a more integrated approach to spectrum allocation. DoD fielded a standard automated system to assist warfighters with frequency management and spectrum allocation, developed a system to determine risks of electromagnetic environmental effects on ordnance, established a process for preparing and coordinating DoD positions to support international spectrum decisions, revised acquisition policies to ensure that the electromagnetic spectrum is considered during system development or procurement, and developed a common costing process model to analyze effects of spectrum reallocations to DoD. Although the Department successfully defended spectrum critical to national security during the International Telecommunication Union 2000 World Radiocommunication Conference, the Department of Commerce has since advised that certain bands vital to DoD operations continue to be at risk for reallocation. Bands used by DoD satellites are especially at risk since viable satellites already in orbit are major capital systems that cannot be refitted to use alternate bands of spectrum.

GLOBAL COMBAT SUPPORT SYSTEM (GCSS)

GCSS provides real-time logistics support to the warfighter across DoD for transportation, supply, maintenance, engineering, personnel, force health protection, acquisition, and finance functions needed to support and sustain the operational requirements of CINCs, JTFs, NCA, Service components, and Services. Sustaining investments in technology and in the transformation of logistics business processes will continue to improve the United States' ability to capture essential data elements at the source, transforming them into actionable information thereby compressing the decision-making cycle and improving the readiness posture.

GCSS CINC/JTF

The GCSS CINC/JTF is being deployed to CINCs to meet current operational requirements. In FY 2000, GCSS CINC/JTF developed the capability to provide field commanders with an integrated logistics view of resources across the battlespace and in the support pipeline.

DEFENSE INFORMATION SYSTEM NETWORK (DISN)

DISN is DoD's consolidated global enterprise-level telecommunications infrastructure. Worldwide DISN implementation provides an information transport infrastructure to DoD locations around the world, wherever the Department's missions take its people. Accomplishments during FY 2000 include the uninterrupted transition of the DISN to Y2K compliance and operation as well as the expansion of network and computer protection policies started in FY 1999.

JOINT WORLDWIDE INTELLIGENCE COMMUNICATIONS SYSTEM (JWICS)

The Defense Intelligence Agency (DIA) provides the Defense and the Intelligence Community worldwide Top Secret Sensitive Compartmented Information (SCI) communications via JWICS. This high-speed multimedia communications system provides critical 24-hour-a-day, 7-day-a-week intelligence operations support that includes data, voice, and video teleconferencing. Accomplishments during FY 2000 include the uninterrupted transition of the JWICS network to Y2K compliance and the beginning of the modernization of the network to Asynchronous Transfer Mode (ATM).

DEFENSE MESSAGE SYSTEM (DMS)

DoD's primary means of messaging communications (AUTODIN) is being replaced by DMS—a flexible, commercial-off-the-shelf network-centric system. DMS provides multimedia messaging and directory services using the underlying network and security services of the GIG.

JOINT INTEROPERABILITY TEST COMMAND (JITC)

JITC reduces risk to the warfighter by ensuring compatibility, integration, and interoperability throughout the life cycle of DoD National Security Systems/Information Technology Systems (NSS/ITS). During FY 2000, JITC certified U.S. forces' platforms for Tactical Data Information Link (TADIL) A/B/J conformance, completed TADIL interoperability certification/validation tests, conducted the DoD Interoperability Communications Exercise (DICE) employing over 20 systems, and provided solutions to CINC's operational interoperability problems.

PROTECTING DOD'S INFORMATION INFRASTRUCTURE

DoD integrated protection initiatives are needed to ensure that its cyber and physical infrastructures perform as necessary for the execution of DoD missions.

CRITICAL INFRASTRUCTURE PROTECTION (CIP)

As DoD transitions to a network-centric enterprise, interdependencies become increasingly important. It is necessary to fully understand the connectivity and interdependencies of DoD infrastructures that interface with commercial infrastructures on base, off base, within the U.S., and overseas. These infrastructure services support critical military activities and, if disrupted, could seriously affect the operational readiness and availability of U.S. military forces. While the commanders focus on protecting their critical infrastructures within their operational environments, DoD's CIP program focuses on defense-wide infrastructure services, including financial, information, logistics, transportation, space, personnel, health, public works, command and control communications, intelligence and surveillance, and emergency preparedness.

The Department continued to use the approach validated during its Y2K experience. Specifically, the operationalization of critical infrastructure protection by focusing on CINC identification and review of operation plans and mission areas, identifying required critical infrastructures and assessing vulnerabilities based on required capabilities. In support of this effort, DoD continued to develop standardized assessment protocols for cyber/physical, on/off-base integrated vulnerability assessments, and tested the protocols in a series of balanced survivability assessments. Regional assessments were conducted of the Pacific Northwest DoD sites and supporting commercial and DoD infrastructures. Host nation critical infrastructure assessments were also conducted for the CINCs, OSD, Services, and DoD agencies, so they could take effective actions to facilitate contingency planning and ensure continuity of operations as part of the Department's global Y2K efforts. Working with several allies, DoD conducted international table-top exercises to identify the most pressing issues to be addressed to ensure interoperability across the spectrum of DoD operations.

ASSURANCE

Assuring the information U.S. forces need when they need it means DoD's programs, policies, and procedures are developed to ensure the availability, integrity, authentication, confidentiality and non-repudiation of all its data, information, and knowledge as it is collected and disseminated across the Global Information Grid. This vision provides the focus for the Department to create a secure and reliable infostructure (information infrastructure) and supports an integrated approach to developing requirements, acquiring systems, and programming for the future force.

Defense-in-depth is the strategy the Department developed to assure the readiness of its infostructure. Defense-in-depth provides for a layered defense aimed at deterrence, protection against attacks or disasters, detecting and defeating attacks, and reconstituting its infostructure if required. It recognizes that people, operations, and technologies are the critical components of this strategy and it is the synergy between these elements that ultimately creates the level of assurance DoD requires to successfully complete its missions.

In 2000, the Department continued to build toward a robust IA program by focusing on activities that target identified shortfalls in people, operations, and technology. After completing a comprehensive review of its IA/IT Management skill sets, DoD has implemented several actions to improve the management of its IA/IT workforce focused on standardizing training and certification. In addition, completion of DoD computer investigations training facility will help us build and maintain an expert IA workforce.

Improving operations for IA saw DoD complete the establishment of the DoD Computer Forensics Lab (DCFL) late in 1999 and in March of 2000 DoD strengthened its responsiveness to computer attacks by instituting a comprehensive Information Assurance Vulnerability Alert (IAVA) program. This combined with the employment of "Red Teams," interdisciplinary teams that are threat-based opposing forces used to expose and exploit the information system vulnerabilities of friendly forces, helped to significantly strengthen the Department's IA posture and defenses against cyber attack.

Key IA policies were crafted for the GIG, computer network defense (CND) and encryption export standards which will help guide DoD toward a more assured operating environment in the future. In August 2000, DoD PKI policy was updated to incorporate use of smart card-based hardware tokens beginning December 2000. This will allow migration to more robust PKI-based network access control mechanisms and a more robust protection of sensitive data, particularly on mission critical information systems.

SECURITY

DoD security missions and programs must work in widely diverse security environments—from the office to the foxhole occupied by warfighters from other countries. In response to a rapidly evolving security environment, the Department is pursuing an active security paradigm. Active security integrates traditional security missions and programs with the Department's defense-in-depth and risk management strategies. The active security paradigm also provides visibility into the Department's numerous missions and programs that protect its assets. The approach focuses on consistent department-wide assessments of the risks and resources needed to counter threats. The increased visibility resulting from these assessments permits security officials to collaboratively assess what protective measures are most appropriate to manage the evolving risks caused by new and emerging threats in an increasingly complex global environment.

COUNTERINTELLIGENCE

The counterintelligence (CI) challenges facing DoD are both dynamic and global in scope. To confront these challenges proactively, DoD worked with their CI counterparts in the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA) to develop a new strategy called CI 21. To make CI 21 a reality, authority will be vested in a CI Board of Directors, chaired by the Director, FBI, and composed of the Deputy Secretary of Defense, the Deputy Director, CIA, and a senior official from the Department of Justice. The Board will appoint a National CI Executive who will serve as the Nation's leader for CI with full access to all sensitive CI activities. This new leadership schema will give DoD unprecedented ability to protect its secrets and leverage the capabilities of all national CI forces.

In addition, DoD will form a new Joint CI Center (JCIC) which will provide the same strategic focus and unity of effort for support to the combatant commands. This concept was developed and tested during the Kosovo conflict, and was found to be highly successful. This initiative will build on the base of an existing small Joint CI Support Branch, and will be able to support several contingency operations simultaneously.

DoD will continue to expand support to critical technology protection, and enhance support to force protection and combating terrorism efforts. The new Joint CI Training Academy (JCITA) will be brought to full operational capability and the innovative Joint CI Analysis Group (JCAG) will be brought to initial operational capability.

ENABLING THE WARFIGHTER

Information superiority for the warfighter requires that the right information is collected, processed, protected, and distributed to create shared awareness of the battlespace and that the necessary tools are in place to facilitate command and control of forces.

INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (ISR)

Over the next decade, DoD is implementing an Intelligence, Surveillance, Reconnaissance Integrated Capstone Strategic Plan (ISR-ICSP) to provide integrated and responsive ISR capabilities operating in a collaborative enterprise and assuring the delivery of timely, relevant information for the NCA and joint/combined forces. Initiatives are underway to improve information infrastructure, operations/ISR integration, air/space integration, ISR integration, interactive collection management, collectors and new capabilities, and multiple intelligence collaboration. This emphasis on integration of national/theater/tactical sensors, commanders, and shooters will enable U.S., allied, and coalition forces to strike rapidly and decisively at extended ranges against time-critical targets.

DoD is also focused on the development of new ISR systems and selective modernization of current systems. Several initiatives underway that facilitate the use ISR capabilities include the publication of summary documents, the use of C4ISR support plans, study and analysis efforts, and emphasis on ISR support to time-critical targeting operations. Additionally, the Joint Chiefs of Staff have completed several complementary studies which qualified and quantified ISR shortfalls, resulting in the near-term reallocation of ISR assets among the CINCs, and identified long-term ISR requirements. JCS has restructured its Joint Warfighting Capabilities Assessment (JWCA) process, that will strengthen its role in requirement formulation and approval for ISR systems. Based on Kosovo lessons learned, additional emphasis has been placed on time-critical targeting and battle damage assessment.

IMAGERY INTELLIGENCE

Senior Initiatives. DoD is continuing to progress toward the next generation Imagery Intelligence (IMINT) capability by modernizing airborne platforms like the U-2, fielding improved sensors, and fielding of the Global Hawk Unmanned Aerial Vehicle (UAV). The Advanced Synthetic Aperture Radar System (ASARS) Improvement Program (AIP) for the U-2 fleet will improve all-weather, day/night imaging capability to provide increased area coverage, improved imagery resolution for target detection and identification, geolocation accuracy sufficient for precision-guided munitions (PGMs), and a moving target indicator (MTI) capability. Improvements in the Senior Year Electro-Optical Reconnaissance System (SYERS) include incorporating a multi-spectral imaging capability (MSI) and improving sensor resolution at longer ranges, geolocation accuracies, and area coverage. AIP and SYERS Pre-planned Product Improvement (P3I) will significantly improve combat capability and enhance the warfighter's ability to detect and prosecute time critical targets (TCTs); a critical shortfall identified by Kosovo lessons learned. These systems will also help to provide the ISR capabilities needed to support military operations in urban terrain. Technology and some equipment from the AIP and SYERS P3I will also be applied to Global Hawk sensor improvements along with accelerated platform improvements.

Future Imagery Architecture (FIA). With the award of FIA, the Department has made significant progress implementing the next generation satellite IMINT capability. In addition, the Department has restructured the Radar Technology Improvement Program (RTIP) for multi-platform application including

Joint Surveillance Attack Radar (JSTARS) and Global Hawk. The Department is also promoting the use of commercial imagery satellite capability in conjunction with national collection assets and associated value-added products and services.

Studies. The Department is factoring the results of ISR studies into Service and agency modernization programs. The MTI/IMINT Fusion Study identified requirements and opportunities for integrating MTI capabilities from various platforms as well as integrating and cross cueing MTI data with imagery. The ongoing Decision Support Center Multi-INT Fusion Study will identify and characterize the improvements associated with integrating multiple intelligence service information needs.

Tasking, Processing, Exploitation, and Dissemination (TPED). One of the major operational challenges for imagery support to warfighters is TPED infrastructure improvements. Efforts underway include developing and integrating FIA interfaces, providing a balance of imagery and geospatial investment and ensuring that baseline capabilities include the highest priorities. The National Imagery and Mapping Agency (NIMA) is managing TPED improvements to fully exploit national, airborne, and commercial imagery. Resources were added beginning in FY 2001 to meet increased demand for precise geolocation, reduced decision cycle timelines, and greater processing capability. NIMA, the Department of Defense, and the Community Management Staff, continue to implement the guidance set forth by the Deputy Secretary of Defense and the DCI to provide the necessary TPED infrastructure.

SIGNALS INTELLIGENCE (SIGINT)

The National Security Agency (NSA) completed both an internal and external study of the agency and initiated an effort to transform the Unified Cryptologic System to meet Unified Cryptologic Architecture for 2020 goals. NSA's internal response to the changing intelligence environment is documented in the NSA Business Plan. The Intelligence Community (IC) and DoD are fully engaged in NSA's transformation and committed to ensuring current readiness capabilities are appropriately risk-managed during the modernization.

Evolutionary upgrades to the Integrated Overhead SIGINT Architecture (IOSA) will ensure a durable satellite collection capability. Furthermore, efforts to revitalize the field of Electronic Intelligence (ELINT) reached a critical stage with the publication of a community-vetted strategy for future investment/ reinvestment and an ELINT Business Plan that was delivered September 29, 2000. In collaboration with the IC and DoD, the Director, NSA (DIRNSA) will establish a Community ELINT Management Office (CEMO), to be jointly staffed and resourced and it will serve as the primary advocate for the ELINT enterprise and its strategy. The CEMO will be chartered to oversee ELINT architectures and perform human resource and program assessments by having visibility into all ELINT programs across the IC and DoD. To institutionalize the importance of interoperability, NSA created the National Tactical Integration Office (NTIO) to better address issues of national-tactical interoperability and collaboration within the Unified Cryptologic System.

MEASUREMENT AND SIGNATURE INTELLIGENCE (MASINT)

DoD, in cooperation with the IC, continues to improve U.S. MASINT capabilities. The first increment of a projected six-year increase in the resources assigned to the Central MASINT Organization was initiated in FY 2000. The focus of the first year was on improving support to joint military operations through the creation of MASINT operations and production coordination elements. In addition, the implementation of standardized processes and procedures will more efficiently address the needs of MASINT users. DoD is placing particular emphasis on strategies and techniques to strengthen MASINT TPED and increase analytical depth, particularly in the arenas of advanced synthetic aperture radar (SAR), radio frequency MASINT, acoustic collections, multi/hyperspectral information, and missile and nuclear/chemical/biological warfare counterproliferation. There is also an IC-wide effort underway to fully integrate MASINT capabilities into the DoD DCGS architecture.

MISSILE DETECTION/MISSILE WARNING

The Department continues to move forward with replacing the proven theater and strategic missile warning Defense Support Program satellites with the greatly improved Space-Based Infrared System (SBIRS). SBIRS is a complex systems-of-systems program, requiring full integration with both national and theater missile defense programs, as well as infrared technical intelligence, space surveillance, battlespace characterization, and theater CINC MASINT support programs. The greatly improved performance of the SBIRS architecture will significantly enhance not only missile defense programs, but also a wide variety of other mission areas.

Although there have been some delays in fielding the new consolidated SBIRS ground architecture, the first SBIRS-High satellites remain on schedule for launch in FY 2004. In addition, the SBIRS-High high elliptical orbit sensors remain on schedule for a FY 2002 delivery to their host satellites. Finally, SBIRS-Low will baseline its operational requirements and complete a system requirements review in 2001, with first launch planned for FY 2006.

PLATFORMS

Manned Airborne ISR Assets. A high tasking level has been maintained for manned airborne ISR assets throughout 2000, supporting a full range of peacetime and contingency operations. The U-2 fleet improvements continue with upgrades to sensors and aircraft. Initial deliveries for the U-2 ASARS Improvement Program (AIP) sensor with MTI and SYERS P3I electro-optic/infrared (EO/IR) sensor with multi-spectral imagery capability are scheduled for delivery by early FY 2001. The RC-135 Rivet Joint fleet has been expanded from 14 to 16 aircraft, upgraded to a common baseline configuration providing additional communication capability and connectivity to improve warfighter support to theater operations. A third RC-135 Cobra Ball aircraft was delivered, giving the Department a 50 percent increase in airborne MASINT platform capability. Re-engining began on the entire fleet of RC-135 aircraft with an estimated completion date of FY 2005. The EP-3 fleet will be expanded by one additional platform in FY 2001. Additionally, the fleet is scheduled to receive the Joint SIGINT Avionics family (JSAF) modification and Common Data Link (CDL) upgrade. The Army's RC-12 Guardrail 2000, the Guardrail Common Sensor (GRCS) System #2, began fielding in FY 2000. GRCS #2 extends the capability of the airborne Communications Intelligence (COMINT) and SIGINT sensors and introduces a modular, open architecture that is Joint Airborne SIGINT architecture compliant. The system will also incorporate the Communications High Accuracy Location System-Exploitable (CHALS-X) system for precision geolocation of communications emitters. The RC-7 Airborne Reconnaissance Low-Multifunction (ARL-M) #5 rolled out in mid FY 2000. There are currently two configurations of the ARL system: ARL-COMINT (ARL-C) configured with a conventional communications intercept and direction finding payload; and ARL-M with IMINT, COMINT, and moving target indicator/synthetic aperture radar (MTI/SAR) subsystems. In recognition of the importance of MTI/SAR data to the military mission, the RTIP development was separated from the JSTARS Boeing 707 platform to allow for multi-platform development applications. A platform-independent radar design will allow maximum flexibility in designing a scaleable, modular solid state sensor at the cutting edge of technology and employable on manned and UAV platforms.

DoD expects to continue fielding additional tactical reconnaissance assets. These systems include the Marine Corps F/A-18D Tactical Airborne Reconnaissance System (ATARS) and the Navy's FA-18F Shared Reconnaissance Pod (SHARP). SHARP will replace the Navy TARPS when the F-14 platform is phased out beginning in FY 2003. SHARP will also be produced for the Marine Corps F/A 18D to initially augment and possibly replace the ATARS force structure.

UAV Assets. The Department is in the process of developing a UAV roadmap. This roadmap plans to capture each Service's vision toward bringing their respective UAV systems into the force. The Global Hawk High Altitude Endurance UAV completed the Military Utility Assessment phase (MUA) of its advanced concept technology demonstration (ACTD) and is now making the transition to a formal acquisition program. During the MUA, the Global Hawk demonstrated its long endurance and ISR imagery capability during many military exercises and demonstrations including a flight from Florida to take imagery off the coast of Portugal and then return. A demonstration with Australia, including a round trip flight from CONUS, is also planned for mid-FY 2001. The Predator Medium Altitude Endurance UAV continues to perform admirably in its support of Bosnia and Kosovo peace-keeping operations and has accumulated over 20,000 flight hours. Of the 12 Predator systems procured, the Air Force has now taken delivery of 8 systems. In addition, the Air Force has taken delivery of two prototype laser designators for Predator and plans to equip the Predator fleet with the laser designators in the future. The Army selected the Shadow 200 as its tactical UAV to support the ground maneuver brigade commander. The Shadow 200 is presently in Low Rate Initial Production (LRIP) with a 44-system program procurement objective. Initial operating capability (IOC) is planned for FY 2003. The Navy and Marines selected the FireScout vertical takeoff and landing tactical UAV to support their operations ashore and afloat. The FireScout is in development and its program procurement objective is 23 systems. IOC is FY 2003. The legacy Pioneer UAV systems will continue to be supported until replaced by FireScout in FY 2003. The U.S. Joint Forces Command is fielding the Tactical Control System Joint Operational Test Bed System to explore and develop joint interoperability concepts among the various UAVs.

Space Assets. Both classified and unclassified space assets continued to provide a broad range of support in peacetime, crisis, and conflict. The ability of space systems to provide access to any region on the globe, and provide total continuous coverage for such mission areas as navigation and missile warning make them a cornerstone of U.S. defense forces. The Department supports the contribution of space systems through closer integration with airborne and terrestrial systems for seamless intelligence, surveillance, and reconnaissance collection along with augmentation by commercial systems, particularly commercial imagery. U.S. Space Command and the Intelligence Community have improved their coordination in defining future space program requirements and remain the focal points for user needs.

GROUND/SURFACE SYSTEM SUPPORT

The DoD has adopted a multi-source ISR integration strategy for the JTF and below called the Distributed Common Ground System (DCGS). The scope of the strategy is to migrate ground TPED to a common interoperable baseline. This baseline assures joint ISR interoperability, facilitates multi-INT, multi-source collaboration and tasking, and the integration of air with space ISR operations. DCGS is designed to operate in three modes: forward deployed, split-based, and reachback. Its employment configuration is driven by the Joint Task Force Commander's requirements. Joint interoperability and multi-INT ISR are the DCGS objectives. To achieve these objectives ASD(C3I) orchestrates the DCGS as a cross-service, cross-agency strategy. The results have led to a distributed architecture used by the Air Force in support of Operation Allied Force and multiple examples of shared use of ISR processing equipment built by one service but used several times across the Services. Common Imagery Ground/Surface Systems (CIGSS) has established core components necessary for all service ground/surface systems to achieve interoperability. This has resulted in a common data link, and common imagery processor, as well as use of imagery exploitation support systems and the imagery product libraries as community standards. The Army-designed tactical imagery system has been adopted by the Navy and forms the basis of the Air Force's approach to ISR battle management. The Department is testing and certifying joint interoperability of the Services ground/surface systems. The goal is that any service ISR platforms/sensors should be interoperable with any services ground/surface systems. Results to date are increased interoperability and the need to transport fewer and smaller systems to the battlefield at a reduced total cost.

COMMUNICATIONS

SATELLITE COMMUNICATIONS

The Department's military satellite communications future architecture includes satellites, terminals, and control subsystems and will provide users with three general classes of service: protected, wideband, and narrowband. Satellite communications is an indispensable enabler of timely battlespace awareness, command and control, and information dissemination in a global arena. DoD approved strategy to transition from current systems to future architecture includes leveraging commercial satellite communications to the maximum extent possible while recapitalizing fixed and mobile ground terminals to use new satellites and spectrum bands, and to improve their capacity, protection, and spectrum-use efficiency.

Protected communications services are survivable to ensure warfighter command and control at all levels of combat. The strategy for protecting communications initially called for launching four Milstar II satellites by 2002, followed by the more capable Advanced Extremely High Frequency system in 2006. However, because the third scheduled Milstar II lauch failed, the first Advanced Extremely High Frequency satellite will be launched in 2004 and operate initially in Milstar II mode.

Wideband communications services rapidly move large quantities of C4I information including intelligence products, video, imagery, and data. DoD's wideband strategy is to launch the two remaining Defense Satellite Communications System satellites supplemented by Global Broadcast Service payloads on Ultra-High Frequency Follow-on (UFO) satellites. Two Defense Satellite Communications System (DSCS) satellites were launched in 2000. Three wideband gapfillers will be launched starting in 2004 to reduce the growing gap between tactical wideband requirements and capabilities. A more capable commercial-like advanced wideband system is envisioned starting in 2008.

Narrowband communications services provide networked multi-party and point-to-point narrowband links to tens of thousands of rapidly moving warfighters. DoD launched its last UFO satellite in 1999 and plans to supplement the constellation with a satellite in 2003 to maintain the system through 2007. In 2007, the Department plans to replace UFO with the Mobile User Objective System.

The DoD Teleport project expands on the Standardized Tactical Entry Point (STEP) program begun in the early 1990s. STEP was created to counteract operational deficiencies associated with the lack of pre-positioned Defense Information System Network (DISN) services and the use of non-standard equipment suites, which were revealed during Operation Desert Storm. Currently, the STEP program provides access to DISN services via X-band DSCS. Limited to X-band, STEP cannot meet the growing warfighter needs. Current and projected warfighter requirements also call for support in the Ultra High Frequency (UHF), Extremely High Frequency (EHF), commercial (L, C, Ku, and Ka), and military Ka frequency bands. Consequently, the DoD Teleport will provide the joint warfighter extended satellite communications (SATCOM) capability and DISN services access for worldwide operations.

COMMAND AND CONTROL

JOINT TACTICAL RADIO SYSTEM (JTRS)

DoD continues to enhance tactical communications to provide secure, survivable, and interoperable systems for joint and combined operations of conventional forces. JTRS was initiated to provide the standard for affordable, high capacity, scalable, interoperable tactical radios to replace all of DoD's current radio inventory, avionics upgrades, appropriate satellite terminals, and personal communications equipment. With the development and publication of the Software Communications Architecture (SCA) and software waveforms, the Services will be able to acquire a family of affordable, scaleable, high-capacity, interoperable radios. JTRS will provide the operational forces with an upgraded communications capability for more effective battlespace management and interoperability among Command, Control, Communications, Computers, and Intelligence (C4I) Systems supporting the warfighters' goal of realizing a fully digitized battlespace.

COMMON DATA LINK AND J-SERIES TACTICAL DATA LINKS

The common data link is DoD's primary wideband data link standard to support air-to-surface transmission of radar, imagery, video, and the sensor information from manned and unmanned aircraft. The DoD's J-series family (of Link-16, Variable Message Format, Integrated Broadcast Service, and Link-22) of low rate tactical data link standards is critical for battlefield awareness for joint and coalition forces. The Joint Tactical Data Link Management Plan is the vehicle overseeing Service migrations to achieve an integrated, predominant, joint forces capability by 2005.

SINGLE INTEGRATED AIR PICTURE (SIAP)

SIAP provides the warfighter the ability to better understand the battlespace and employ weapons to their designed capabilities. SIAP will support the spectrum of offensive and defensive operations by U.S., allied, and coalition partners in the airspace within a theater of operations (e.g., attack operations, suppression of enemy air defenses, air and missile defense, intelligence preparation of the battlefield). SIAP is accomplished through a combination of materiel and nonmaterial improvements.

SIAP is not the end-state—it is part of a larger construct that must be engineered so it can easily migrate toward, and support, a coherent tactical picture. As such, it is recognized that SIAP supports joint forces air component commander (JFACC) mission areas involving the tactical employment of airpower. An incremental approach is needed to develop and implement improvements to command and control of existing systems and the integrated architectures within which these systems operate while SIAP is being developed.

DIGITIZATION

The Army continues on the road to a digitized force employing information technologies to acquire, exchange, and employ data throughout the battlespace. The Army is equipping the First Digitized Division (the 4th Infantry Division at Fort Hood, Texas) and will equip the First Digitized Corps by the end of 2004. Army Division XXI efforts encourage innovation and have resulted in a new design for heavy divisions that reduces manpower platform requirements and combat platforms in the maneuver battalions while increasing lethality and survivability.

JOINT SURVEILLANCE TARGET ATTACK RADAR SYSTEM (JSTARS)

JSTARS is an airborne platform equipped with a long-range, air-to-ground surveillance system designed to locate, classify, and track ground targets in all weather conditions and provide targeting and battle management data to all operators, both in the aircraft and in the ground station modules. Aircraft deployed as part of NATO Allied Force operations met high operating tempo requirements, and provided time-critical information to operational decision makers and combat aircrews. Two E-8Cs were deployed in support of Kosovo operations and data from the 93rd Aircraft Wing reflects outstanding JSTARS performance—83 of 86 combat support sorties were accomplished with launch reliability of 99 percent, mission effectiveness of 96 percent, and mission capability rate of 80 percent. Production efforts were equally successful with all aircraft on or ahead of schedule.

COMBAT IDENTIFICATION

Combat identification is the process of attaining an accurate, real-time characterization of potential targets in a combatant's area of responsibility so as to allow the use of weapons or other tactical options. It is essential for overall battle management, operational effectiveness, and reducing fratricide and collateral damage. Systems employed for combat identification include those using cooperative (i.e., radio frequency question and answer) and noncooperative (e.g., analysis of radar return characteristics) methods, as well as methods which rely on radio reporting of friendly units' geographical positions over a network. DoD's current focus is on improving interoperability between the Services, improving combat identification between ground vehicles, and improving combat identification for close air support and deep strike aircraft missions—while leveraging advances already made in combat identification for air defense. A combat identification Capstone Requirements Document is scheduled for completion in FY 2001.

STRATEGIC COMMAND, CONTROL, AND COMMUNICATIONS

DoD continues to maintain survivable and enduring command and control of nuclear forces and weapons. Numerous efforts are underway to sustain and modernize these systems. A strategic C3 modernization planning effort was initiated to explore the utilization of complex information technologies and look at a cohesive C3 approach towards the modernization of the nuclear and senior leadership communication systems, National Missile Defense, and strategic information operations for the 2000 to 2020 timeframe. A Senior Leadership Communications System Executive Management Board was formally established to address information requirements of the Department's senior leaders. Correcting Year 2000 problems and developing contingency planning processes to manage the Year 2000 transition was a high priority and was successful.

PERSONNEL RECOVERY

The directive on Personnel Recovery, June 30, 1997, states that bringing home those who have put themselves in harm's way is one of the highest priorities of the Department of Defense and a moral obligation. Current DoD efforts in this regard are focused on improving Personnel Recovery capabilities for information management, critical communications links, evader location, and intelligence support. This year the Department also issued a revision to the original June 1997 DoD Directive on Personnel Recovery. This revision to the Department's first effort to provide policy oversight over personnel recovery matters, realigns DoD executive agency for recovery from the Air Force to Joint Forces Command, thus reinforcing the joint nature of recovery operations and emphasizing the need for all Services, not just the Air Force, to maintain a robust recovery capability.

INTEGRATION AND INTEROPERABILITY

JOINT AND COALITION INTEROPERABILITY

DoD continues its development of an integrated architecture leading to a Global Information Grid (GIG). The GIG will support warfighters and all other DoD users with a fully integrated information service that is reliable, secure, cost effective, and interoperable. Efforts continue in coalition interoperability as well. The Mulitnational Interoperability Council was formed in October 1999 and has begun work in improving coalition information interoperability. The major focus of this multinational forum is to address coaltion interoperability impediments in the areas of doctrine, policy, procedures, and information sharing. The Council is led by the Joint Staff Director of Operations.

C4 SUPPORT PLANNING

Understanding the C4I infrastructure support requirements for future weapon systems and information systems is critical to ensuring information superiority throughout the battlespace. DoD components develop C4I Support Plans (C4ISPs) for each acquisition program, identifying interoperability and C4I support requirements for each joint/combined military mission and function that the new system will support. During 2000, C4ISPs were prepared for new programs (e.g., Global Hawk) and for programs approaching full rate production and deployment (e.g., F/A-18 E/F and MV-22). Through these plans, requirements are matched against planned infrastructure capabilities to identify where investment schedules must be changed, or technical approaches must be modified.

The operational and system architecture views and the information exchange requirements (IERs) in C4ISPs build upon the architecture and IER data that must now be included in operational requirements documents (ORDs). Architecture-based tools such as the Joint Mission Area Analysis Tool facilitate cross-program assessments of C4I requirements and capabilities, and enable the Department to more effectively identify major system dependencies and manage correction of shortfalls. Revision of both Defense Acquisition System policies and procedures and Joint Staff guidance on requirements generation has now put in place the process to directly link operational requirements (including interoperability Key Performance Parameters) in the ORD to derived support requirements in the C4ISP, and to interoperability testing based on mission outcomes and assured delivery of information from sensors to shooters.

JOINT COMMAND AND CONTROL INTEGRATION/INTEROPERABILITY GROUP (JC2I2G)

JC2I2G was formed in FY 1999 as a result of defense acquisition reform studies directed by Section 912c of the National Defense Authorization Act for Fiscal Year 1998. In FY 2000 the JC2I2G helped create three CINC Interoperability Program Offices (CIPOs) and one Joint Forces Program Office (JFPO). Each CIPO office is co-located at one of the three Service system commands (Army Communication and Electronics Command, Navy Space and Naval Warfare Systems Command, and Air Force Electronic Systems Command. Each CIPO provides engineering advice and assistance in solving CINC integration/ interoperability issues for an assigned group of CINCs. The JFPO integrates issues and solutions horizontally across the CIPOs and the CINCs.

JOINT C4ISR DECISION SUPPORT CENTER (DSC) AND MODELING AND SIMULATION (M&S)

DSC completed a number of studies to leverage integrated and interoperable C4ISR to improve combat effectiveness. In FY 2000, the DSC analyzed C4ISR impact on asymmetric warfare, multi-intelligence fusion performance, GIG support to CINC requirements, and interoperability with coalition/allies. M&S tools are critical to the success of DSC studies, and the DSC provides DoD leadership in the development of robust information superiority components of the Department's M&S toolset. During 2000, additional funds were provided to accelerate the development of several ongoing M&S activities. The goal of this initiative is to ensure an M&S framework that can perform realistic technical assessments of current and proposed C4ISR systems and measure their military contribution in the context of current and evolving operational concepts.

INFORMATION OPERATIONS (IO)

Information operations support the objectives of the National Security Strategy by enhancing information superiority and influencing foreign perceptions. In conflict, IO enables information superiority by protecting the integrity of the United States' command and control, and common operating picture, while skewing, or degrading, an adversary's situational awareness. The Department's emerging concept for IO will be the basis for aligning strategy and policy across DoD. When approved, the strategic concept will guide and integrate IO policy, organization, and implementation and the research, development, and acquisition of IO capabilities. Program adjustments will be made as appropriate.

Support functions such as intelligence are integral to IO. To this end, the Intelligence Community, and DoD in particular is adapting or developing new intelligence policies and plans, capabilities, systems, and organizations to meet the current and projected needs of IO, as well as to provide critical and timely information that will assist the Department in force protection.

The Department is pursuing numerous actions to better implement IO. For example, DoD established a Defense IO Council (DIOC) and aligned the computer network defense (CND) and computer network attack (CNA) missions under USSPACECOM.

The DIOC oversees and coordinates the Department's efforts to develop policy and capabilities to support IO. This included a security review of all classified programs that support the development of IO capabilities to ensure they are properly and appropriately safeguarded, yet visible to the warfighter. The Department also conducted a broad area review of IO to develop a resource and capability baseline. This baseline provides the DIOC a basis for aligning, prioritizing, and integrating various efforts to operationalize IO in a more coherent and efficient manner. In tandem with the security review, ASD (C3I) is revising the Department's Security Classification Guide on IO, and will soon begin a revision of the Department's IO policy.

USSPACECOM has been selected to be the supporting CINC for planning and coordinating all offensive and defensive computer network operations. In October 1999, the Joint Task Force for CND was realigned under USSPACECOM with the mission to monitor all DoD networks, provide tactical warning of orchestrated attacks, and coordinate their mutual defense. To carry out the CNA mission it assumed in October 2000, USSPACECOM is responsible for supporting the regional CINCs with capabilities to deny, degrade, or destroy an adversary's computer networks.

To support Presidential Decision Directive 68, *International Public Information (IPI)*, the Department has chartered a DoD IPI Committee to directly support the IPI Core Work Group at NSC. The function of this committee is to develop and coordinate DoD policy and plans to conduct international military information operations in support of IPI.

The Intelligence Community, and DoD in particular, are revising or developing new intelligence policies and plans, capabilities, systems, and organizations to meet the current and projected needs of IO, as well as to provide critical and timely information that will assist the Department in force protection. To assist in psychological operations (PSYOPs) and to help counter foreign propaganda, the Defense Intelligence Agency (DIA) has developed a Human Factors Analysis Center, and has assembled a panel for perception management threat analysis.

SPACE

SPACE CONTROL

The ability of the United States to access and utilize space is a vital national security interest because many of the activities conducted in space are critical to its national security and economic well-being. Potential adversaries may target and attack U.S., allied, and commercial space assets during crisis or conflict as an asymmetric means to counter or reduce U.S. military operational effectiveness, intelligence capabilities, economic and societal posture, and national will. Therefore, ensuring the freedom of space and protecting U.S. national security interests in space are priorities for the Department.

The mission of space control is to ensure the freedom of action in space for the United States and its allies and, when directed, deny an adversary freedom of action in space. The space control mission area includes: the surveillance of space; the protection of U.S. and friendly space systems; the prevention of an adversary's ability to use space systems and services, the negation of adversary space systems and services; and supporting battle management, command, control, communications, and intelligence. As the foundation for space control, space surveillance has received increased emphasis over the past year. A modernization plan and investment strategy has been developed to update the aging infrastructure, enhance the command and control structure, and evolve the system from a cataloging and tracking capability to space situational awareness system capability. There are also a number of prevention and negation efforts underway to include a space control technology development program that will support theater-level force protection through the development of capabilities that will have temporary and reversible effects on systems used for purposes hostile to U.S. national security interests.

NAVIGATION

The Global Positioning System (GPS) continues to provide the military with global, all-weather, continuous navigation, positioning, and timing data. The dual-use nature of the system also provides an ever-growing civil, commercial, and scientific user community with similar capabilities.

One of the greatest success stories of space as a force multiplier is GPS. Planners utilize GPS data to locate targets, develop the best attack and strike routes, and then program the information into precision weapons. Many of these same weapons utilize GPS for in-flight navigation updates. The ability to strike targets more precisely and from a greater range places fewer U.S. and allied personnel and equipment in danger, thereby reducing casualties. It is no longer necessary to calculate operations by the number of missions required to attack a target but rather by the number of targets that can be struck on each mission. Soldiers, sailors, airmen, and Marines rely on GPS for location as it enables them to navigate through both featureless deserts and extremely mountainous terrain. GPS enables CSAR efforts to swiftly locate and extract personnel in danger.

The currently planned GPS modernization program will add new military signals (known as the M-code) to Block IIR and IIF satellites as well as additional civil signals. Currently planned timelines call for adding the M-code to the last 12 Block IIR satellites along with an additional civil signal. The first scheduled launch with these expanded capabilities is planned to occur in 2003.

The Block IIF satellites will incorporate the third civil signal to support civil safety of life applications. Corresponding improvements in the ground control supporting infrastructure will also be implemented. The first scheduled launch of the enhanced Block IIF satellites is in the 2005–2006 timeframe.

At the direction of the President, Selective Availability (SA) was set to zero on May 2, 2000. Civilian users of GPS now receive position, velocity, and time information with no accuracy degradation. Since SA was discontinued, horizontal position errors of less than 10 meters have routinely been observed. This accuracy represents a nearly 10-fold improvement over that available to civil users when SA was activated.

The discontinuation of Selective Availability will continue to fuel the explosive growth of civil GPS applications throughout the world. The President's decision to discontinue Selective Availability was based upon a recommendation by the Secretary of Defense in coordination with the Departments of State, Transportation, and Commerce, the Central Intelligence Agency, and other Executive Branch departments and agencies. The decision acknowledged that worldwide transportation safety, scientific, and commercial interests could best be served by discontinuation of SA and was supported by the DoD's demonstrated capability to develop and deploy systems designed to selectively deny GPS signals on a regional basis when U.S. national security is threatened.

Because of the high demand for airspace and GPS access from the public and commercial sectors, increasingly sophisticated navigational equipment is required to ensure safety of flight in many areas of the world and successful military operations. The Global Access, Navigation and Safety (GANS) program upgrades and modernizes DoD capabilities to maintain compatibility with the civil sector. GANS addresses a wide range of issues, including the use of GPS in war and peace, precision landing, and global air traffic management.

SPACE LAUNCH

The effective use of space for military purposes requires reliable and affordable access. Current U.S. space launch systems differ only slightly from the ballistic missiles developed during the 1950s and 1960s, and are increasingly costly to use. The National Space Transportation Policy balances the efforts to sustain and modernize existing launch capabilities with the need to invest in the development of new, improved space transportation systems. DoD is the lead agency for improving today's expendable launch vehicle (ELV) fleet, including the requisite technology development. Table 8-1 illustrates the Department's spacelift highlights.

Table 8-1

Spacelift Operations[a,b]

	FY 1995	FY 1996	FY 1997	FY 1998	FY 1999	FY 2000	FY 2001[c,d]
Titan IV		4	4	4	2	3	2
Titan II				1	1	2	1
Atlas	12	7	8	6	5	5	4
Delta	3	8	11	12	10	5	9
Shuttle	7	7	8	5	3	3	8

[a] Government space launch operations for each expendable launch vehicle and DoD support to shuttle launches.

[b] During normal operations, the Air Force spacelift call-up capability is 90 days for medium lift vehicles (Delta, Titan II, and Atlas) and 180+ days for heavy lift vehicles (Titan IV). For emergency operations, the operational requirement documents for launch vehicles specify an emergency call-up of 45 days for medium launch vehicles and 90 days for heavy lift vehicles. However, current capability for acceleration of heavy lift indicates a 150 day call-up is more realistic (the Evolved ELV will reduce this period).

[c] Includes scheduled government space launches for each expendable launch vehicle and DoD support to shuttle launches.

[d] The FY 2001 maximum launch range rates are estimated at 48 for Eastern Range and 44 for Western Range.

The Department's objective is to reduce the launch costs while improving capability, reliability, operability, responsiveness, and safety. To achieve this objective, DoD initiated the Evolved ELV (EELV) program to replace current medium- and heavy-lift launch systems. Through this program, DoD is partnering with industry to satisfy both government and the international commercial market launch needs. EELV will reduce life-cycle costs, shorten launch timelines, and enable more DoD, civil, and commercial launches per year. The medium-lift and heavy-lift EELVs will have their first government flights in 2002 and 2003, with one and five scheduled launches, respectively.

The Department will cooperate with the National Aeronautics and Space Administration (NASA) in the development of technology, operational concepts, and flight demonstrations for the next generation of reusable launch vehicles that will replace the space shuttle.

SATELLITE CONTROL

Satellite control involves operations to deploy and sustain military systems in space. Table 8-2 summarizes the current number of on-orbit satellite systems and their primary missions. The Air Force Satellite Control Network (AFSCN) is the primary C2 support capability for DoD, the National Reconnaissance Office, civil, and allied space programs providing data processing, tracking, telemetry, satellite commanding, communications, and scheduling for over 100 satellites. The Naval Satellite Operations Center provides similar support for Navy satellite systems. The AFSCN global antenna network also provides unique launch/early orbit and anomaly resolution services. As a backup, Air Force Transportable Mission Ground Stations can provide mobile C2 capabilities for certain DoD satellites.

Table 8-2

Current On-Orbit Forces[a]

Capability	Navigation	Communications[b]	Missile Warning[c]	Environmental
On-Orbit	28	14	N/A	5

[a] Force levels shown are current as of December 8, 2000.

[b] Only includes Department of the Air Force satellites.

[c] Number of operational missile warning satellites is classified.

The Department's future satellite operations architecture establishes clear vectors to migrate satellite control into an integrated and interoperable satellite control network. The Department is working closely with NASA and NOAA in developing a strategy to transition from current and planned systems into the future (20+ years). This strategy establishes timelines to improve satellite operations efficiency, consolidate and enhance the ground infrastructure, and develop new ground communications standards. Additionally, the Air Force Center for Research Support (CERES) provides a full-service commercial off-the-shelf (COTS)-based system for controlling research and development satellites. CERES also serves as a C2 testbed, allowing military satellite operators and commercial vendors to test new commercial ground systems using DoD satellites.

METEOROLOGICAL SATELLITE CONVERGENCE

The National Polar-orbiting Operational Environmental Satellite System (NPOESS) is a Presidentially-directed tri-agency program between the Department of Commerce's National Oceanic and Atmospheric Administration, the Department of Defense, and NASA. The program is funded 50/50 between the Department and DOC and managed by a tri-agency Integrated Program Office which is responsible for planning, developing, acquiring, managing, and launching NPOESS. NPOESS is a converged satellite system that will replace the two separate previously planned polar-orbiting follow-on programs of the USAF and NOAA respectively. The goal of NPOESS is to provide the most advanced, accurate, and dependable environmental data to the warfighter, and to the many civilian users of the system via a single national system, while achieving cost savings over the separate previously planned follow-on programs. The NPOESS program is working with the European Organisation for the Exploitation of Meteorological

Satellites to cooperate on data sharing and explore other opportunities for future cooperation. The Department is working closely with NOAA and NASA to ensure that NPOESS continues to satisfy national security requirements.

RESEARCH AND ANALYSIS

There is much that remains to be known about creating and leveraging information superiority. DoD initiated the Information Superiority Investment Strategy program to provide an analytical framework and a body of empirical evidence to support C4ISR-related Quadrennial Defense Review analyses. DoD's C4ISR Cooperative Research Program is dedicated to advancing both the state of the art and practice of command and control. The program focuses on highly leveraged projects designed to better understand and measure shared awareness and self-synchronization, to develop and assess new approaches to command and control, to design experimental processes needed to co-evolve information-enabled mission capability packages, and to understand the challenges associated with coalition command and control.

The Department is conducting an integrated set of analyses designed to contribute to the development of a coherent, balanced C4ISR investment strategy. Information Superiority Investment Strategy (ISIS) analyses will establish explicit linkages among mission shortfalls, investment options, mission effectiveness, and fiscal implications. As a continuing process, ISIS plans to analyze the full spectrum of DoD missions and address each of the information superiority domains—intelligence, surveillance, and reconnaissance; communications; command and control/battle management; information assurance; information operations; and information technology.

INFORMATION MANAGEMENT INITIATIVES

GOVERNANCE

In view of the critical role information and IT play in the successful accomplishment of the Department's mission, DoD maintains an Information Technology Management (ITM) strategic plan to ensure that DoD IT investments have a strategic and mission focus. The plan is a key part of an end-to-end strategic planning process designed to guide all DoD organization elements in performing their ITM strategic planning and implementation and to help them identify and defend resources to optimize mission performance.

The DoD Chief Information Officer (CIO) Executive Board serves as the management body and focuses on resolving issues, ratifying policies, and prioritizing IT budget proposals. Information management and IT policies are being updated around the achievement of information superiority to more directly link IT with the mission and to accommodate the fast pace of technological advancements and statutory requirements. Over the last year, policies have been issued in such areas as the Global Information Grid, information management, information assurance, networks, software licensing, and electronic business.

ELECTRONIC BUSINESS (EB)

Information superiority will be supported by revamped business processes enabled by EB and knowledge management technologies and program initiatives. Access to combat support information will be accelerated, timely, complete, accurate, and increasingly paperless. This will expedite and increase information access and improve the quality of decision making. The application of EB principles is permitting the integration of Defense processes and evolution of a Defense enterprise capable of more fully supporting the warfighter.

KNOWLEDGE MANAGEMENT (KM)

KM is an emerging discipline that enables EB while focusing upon improving mission performance through strategic management of intellectual capital and knowledge resources. The emergence of supporting KM techniques and powerful web-based technologies for capturing, storing, retrieving, and sharing data and information and providing knowledge context, offers significant opportunities for achieving additional improvements in information superiority and the productivity of DoD EB processes. DoD is combining with EB to provide a critical synergy of complementary disciplines and technologies needed to achieve information superiority.

WORKFORCE MANAGEMENT AND TRAINING

Various initiatives are underway to attract, train, and retain a highly skilled workforce. These include programs that provide for scholarships for pursuit of education in shortage skill areas such as linguists and information technology. Within the DoD Intelligence Community there are civilian personnel initiatives that allow for higher salaries to attract and retain employees in critical skill categories where there are shortages.

Initiatives are underway to identify and track Information Assurance (IA) and IT professionals by definitive skill sets and ensure critical IA/IT management training is completed by individuals in key positions. Efforts are ongoing with other federal agencies on several projects ranging from updating Clinger-Cohen competencies to improving the processes for recruiting and hiring personnel, and allowing specialty pay for select IT skills in the Federal government.

The Information Resources Management College (IRMC) is the Department's flagship for information technology management training for senior managers, and offers a variety of information management courses. Its new Information Security/Assurance Certificate Program has been certified by the National Security Telecommunications and Information Systems Security (NSTISS) Committee as being compliant with the Information Systems Security Professionals standard, making IRMC one of only four schools in the Nation having this distinction. IRMC has been recognized as a National Center of Academic Excellence in Information Assurance, for meeting educational requirements of Presidential Decision Directive 63, "Critical Infrastructure Protection."

IT VISIBILITY AND OVERSIGHT

Section 8121 of the FY 2000 National Defense Appropriation Act for FY 2000 requires IT systems to be registered with and certified by the DoD CIO as to whether major automated information systems were in compliance with Clinger-Cohen Act requirements. Among other things, certification is based on analysis of alternatives, economic analysis, and performance measures, all of which relate to cost, risk, and return on investment.

The automated central registry, while proving useful in its own right, is being expanded to provide for a more integrated management view of DoD IT investments. DoD-wide concerns regarding information assurance, software acquisition oversight, global information grid, and enterprise software licensing will all be addressed through future registration updates. In addition, DoD has issued policies and initiated a formal oversight and review process aimed at providing DoD personnel at all levels with timely information on the progress of major information system investments.

FAMILY OF SYSTEMS (FoS) MANAGEMENT

Recent statutory requirements, including the Clinger-Cohen Act, mandated that DoD implement a process whereby IT investments were managed and evaluated based on specific, measurable contributions to DoD mission goals and priorities. To achieve this, the Department is beginning to manage and oversee its IT investments from a mission perspective by establishing FoS and IT portfolios. Trade-offs among investments will be made to the optimum benefit of the mission and benefits will be measured and evaluated in the context of their contribution to the overall success of the mission.

SOFTWARE ACQUISITION, DISTRIBUTION, AND MANAGEMENT

Under the DoD Enterprise Software Initiative (ESI), DoD is using software best practices to develop a DoD-wide business process for distributing and managing commercial COTS software. This initiative is saving money by aggregating requirements and leveraging DoD's buying power to achieve the most favorable terms and pricing for commercially available software and maintenance. The Department continues to achieve savings of 28 percent to 98 percent of General Services Administration pricing. Over the past year, customer orders have increased dramatically.

Several initiatives are underway to improve the quality of software in the Department. First, the identification of a core set of performance measures that will uncover root causes of software problems. Second, the analysis of opportunities for re-engineering software processes. Third, the realization of the need to ensure the security of software applications, as evidenced by DoD's initiation of a pilot program to analyze and mitigate the threats to software.

RECORDS MANAGEMENT

Records management promotes the sharing of vital information across the Department by assuring the capture, integrity, and retrievability of the thousands of official records generated yearly by the DoD. The DoD standard is the only one of its kind and has been endorsed by the National Archives and Records Administration (NARA) for federal-wide use. The standard has also been utilized by local/state governments as well as by the Canadian and Australian governments and is being considered for presentation to the American National Standards Institute/International Standards Organization (ANSI/ISO) communities for endorsement.

ACCOMPLISHMENTS

During the past year, many advances were achieved in furthering information superiority capabilities in the plans, policy, and programmatic areas. Through increased emphasis on leveraging the Planning, Programming, and Budgeting System much needed resources were obtained for programs critical to the success of the information superiority vision and, as a result, was able to increase funding for a number of critical programs. These accomplishments will help lay the foundation of a secure, interoperable infostructure with the addition of funds to:

- Implement a public key infrastructure.
- Expand defensive information operations.
- Establish a joint interoperability test and standards program.
- Expand the Joint Task Force—Computer Network Defense and develop a comprehensive approach to computer network defense.
- Build and protect the DoD infostructure.
- Complete the Global Positioning System.
- Ensure adequate intelligence support to the fused operations-intelligence common operational picture.
- Improve Electronic Intelligence capabilities.
- Build and maintain a SIAP capability.
- Increase future battlespace awareness by initiating the acquisition of Global Hawk and improved SIGINT capabilities.
- Enhance tactical imagery and provide a quick reaction capability.
- Initiate an end-to-end system of sensor tasking, information processing, exploitation, and dissemination of intelligence.
- Improve C4ISR support to Kosovo operations.
- Initiate a Capital Equipment Replacement Program to provide a significant increase in intelligence capability through state-of-the-art infrastructure across the security spectrum.
- Initiate a Measurement and Signature Intelligence (MASINT) Advanced Concept Program at four Joint Reserve Intelligence Centers.
- Ensure CINC warfighters' continued access to secure, adequate-capacity, up-to-date technology satellite communication systems that make efficient use of scarce spectrum resources.

CONCLUSION

Much progress has been made in reaping the rewards of advancing information technology. There is convincing evidence of the enormous potential of information superiority-enabled Network Centric Warfare and supporting network-centric operations. Yet, much remains to be done. Major challenges continue in the areas of interoperability, information assurance, and the achievement of a coherent infostructure to support DoD’s twin revolutions—the Revolution in Military Affairs and the Revolution in Business Affairs.