CHAPTER IV
INFORMATION SUPERIORITY

A. DESCRIPTION

Information Superiority (IS) is defined by the Chairman, Joint Chiefs of Staff (CJCS) in Joint Vision 2010, as "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." To ensure that our forces can acquire, verify, protect, and assimilate the information needed to effectively neutralize and dominate adversary forces, IS must combine the capabilities of command, control, communications, and computers (C^4); intelligence, surveillance, and reconnaissance (ISR); and information operations (IO). Achieving IS increases the speed of command, preempts adversary options, creates new options, and improves the effectiveness of the selected options. The result is an ability to increase the tempo of operations and to preempt or blunt adversary initiatives and options (Reference 10).

Command and control (C^2) is described as the "exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission" (Reference 11). The C^2 process involves gathering information, assessing the situation, identifying objectives, developing alternative courses of action, deciding on a course of action, transmitting orders that can be understood by recipients, and monitoring execution (Reference 12). This requires maintaining a seamless, robust network linking all friendly and multinational forces and providing common awareness of the current situation (C^4). The ISR component of IS provides near-real-time awareness of the location and activity of friendly, adversary, and neutral forces throughout the battlespace infosphere. For the purposes of this document, C^4 and ISR are referred to collectively as C^4ISR. The term *information operations* (IO) encompasses a variety of defensive and offensive activities, including the use of digital weapons against digital targets anywhere in the battlespace (Reference 10).

The term *information system* includes information, information-based processes, information hardware and software systems, and computer-based networks either individually or in combination. It should be noted that information superiority is a dynamic arena. Doctrine, policy, and taxonomy must evolve as quickly as the supporting technology. This chapter describes the relevant key technology initiatives to joint warfighter requirements, but is not representative of the entire spectrum of warfighter IS roles and missions.

Other Joint Warfighting Capability Objectives (JWCOs) also contain key programs and technologies that support the IS needs of the warfighter. Although Information Superiority is an enabler to all the JWCOs, four of them are particularly closely aligned with IS: Combat Identification (Chapter VI), Joint Readiness and Logistics (Chapter IX), Electronic Warfare (Chapter XI), and Protection of Space Assets (Chapter XIV).

The mission space relevant to U.S. national security is expanding and becoming more complex. The United States, as the only superpower, has a key role to play in the post–cold war era. Our roles and responsibilities are somewhat different from those we had during the cold war. Some important differences affecting military organizations and operations have already

manifested themselves. The first is the increasing importance of operations other than war (OOTW), in which military organizations are being tasked to do a wide variety of nontraditional missions, from humanitarian relief to peace enforcement. Second, while these differences stem from geopolitical considerations, other changes in the mission space are driven by technology. Third, an entirely new form of warfare may emerge, known as *information operations*. Finally, asymmetrical forms of warfare have become significantly more potent with the increased lethality and accessibility of weapons of mass destruction (WMD).

Information Superiority is essential to achieving virtually all the other joint warfighting capabilities in the 21st century battlespace. Information superiority also requires an ability to protect the information collection, processing, exploitation, and dissemination capabilities of the United States and its multinational partners. In addition, commercial advancements are being made available to friends and foes alike at lightning speed. It will be the U.S. DoD S&T policy to ensure that all military systems have sufficient open architectures to facilitate adding the latest and most effective technology as it becomes available with a plug-and-play capability.

B. OPERATIONAL CAPABILITY ELEMENTS

Warfighters of the future must be able to respond rapidly and effectively, with little or no tactical warning, to a wide range of uncertain threats. These threats include conventional forces, WMD of increasing technological sophistication, and many other adversarial forces of increasing capability. At the same time, there is a decreasing likelihood of the presence of large number of forward-based U.S. forces in a particular theater of action. An effective U.S. response is likely to require interoperation and sharing of resources with allied other coalition forces in the face of these threats. The Chairman of the Joint Chiefs of Staff's *Joint Vision 2010* (Reference 4) calls for the rapid deployment of forces capable of engaging an enemy on arrival and sustaining operations with a minimal logistics tail in the area of operations, as well as the immediate execution of noncombat missions.

All of this challenges our most basic assumptions about command and control and the doctrine developed for a different time and a different problem. One of the most enduring lessons derived from the history of warfare is the degree to which fog and friction permeate the battlespace. The fog of battle is about the uncertainty associated with what is going on, while the friction of war is about the difficulty in translating the commander's intent into actions. Much of the fog of war, or what is referred to today as a lack of battlespace awareness, has resulted in our inability to tap into our collective knowledge or to assemble existing information, reconcile differences, and construct a common picture. Equal emphasis needs to be placed on developing a current awareness of both friendly and enemy dispositions and capabilities, and in many cases, emphasis on neutrals needs to be increased, as became evident in Bosnia. Traditionally, the responsibilities for each of these interrelated pieces of battlespace awareness have been parsed or allocated to different organizations, resulting in significant barriers to pulling together a common picture, The rest of the problem is a lack of coverage resulting from limited-range sensors and their ability to discriminate.

Achieving this capability demands significant advances in our ability to deliver the right data and information at the right time in the desired format to commanders at all levels, to use that data and information to develop superior knowledge of the battlespace in real time, and to employ that knowledge effectively in planning and executing operations. To achieve and maintain force dominance in the 21st century, the emphasis on information technology development must shift from a platform-centric to a network-centric approach. Network-centric warfare

(NCW) is defined as the information superiority–enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace. The shift to an open-architecture, network-centric focus will allow the joint warfighter to achieve greater agility in responding to changes in threat and exploiting continuing advances in technology (Reference 10).

The goal of IS, as illustrated in Figure IV–1, is to enable the development of new concepts of operation that will ensure operational dominance of the battlespace. This is accomplished through the three JV2010 IS challenges of information transport and processing (ITP), battlespace awareness (BA), and information operations (IO); and a fused, assured information infrastructure, referred to as the Global Information Grid (GIG). The Joint Staff C4 Directorate, as JV2010 IS Coordinating Authority, developed the GIG as the structure for implementing IS. Based on the Advanced Battlespace Information System (ABIS) study (Reference 13) completed in 1996 and the Defense Science Board's Integrated Information Infrastructure (III) initiatives, the IS challenges of BA, IO, and ITP provide the means of achieving the IS capabilities needed by the warfighter. Additionally, the GIG provides the organization, architecture, and goal-concept that enables the DoD/service/agency chief information officers (CIOs) and others to effectively and efficiently manage the department's information technology (IT) resources and assets. These challenges depend on end-to-end, global, flexible, assured access to information and information systems provided by the GIG for implementation. The GIG provides the means for achieving IS, the key enabler of JV2010. These capabilities are significantly more advanced and bandwidth intensive than the initial capabilities of the Global Command and Control System

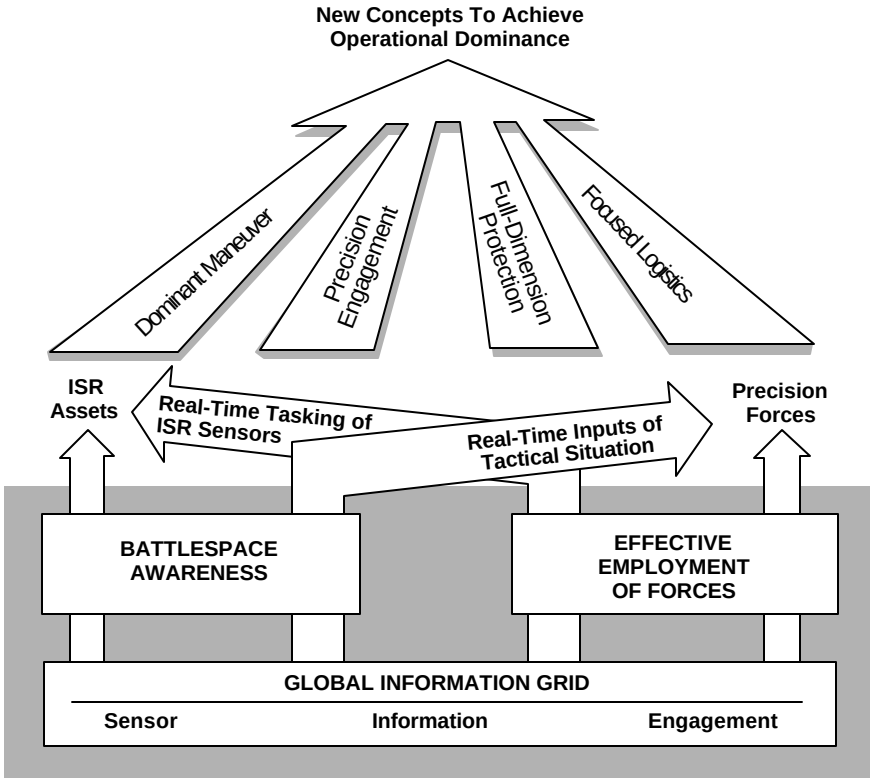

Figure IV–1. Concept—Information Superiority

(GCCS) and those successfully demonstrated in the Bosnia Command and Control Augmentation (BC^2A) program. Initial segments of these capabilities were demonstrated in DARPA's Information Superiority Demonstration 98 and 99.

The necessary improvements that must be accomplished to achieve the goal of Information Superiority are described by the *Task Force XXI Army Warfighting Experiment Integrated Report: Modeling of Opportunities* (Reference 14). Some of the quantitative factors that this report highlighted are (1) a decrease in the development of division plans from the current average of 72 hours to a goal of 12 hours to complete, (2) a decrease in the time for a call for fire from 3 minutes to 30 seconds, and (3) a decrease in the time required for a deliberate company attack from 40 minutes to 20 minutes. Additional factors such as significant reductions in the average decision cycle time, significant reductions in the number of attack assets that need to be scrambled, improvement of kill ratios, and reductions in friendly and allied losses are also required. Information Superiority provides the primary mechanism for achieving these improvements.

The IS challenges described above are evolutionary enhancements of the ABIS study, which defined three operational capability elements within each of the three broad operational capability areas. The following provides a summary of the ABIS study results:

- *Global battlespace awareness—information acquisition, precision information direction,* and *consistent battlespace understanding.* These capabilities allow the joint warfighter to control and shape the pace of the battle by providing commanders with a broader perspective and better intuitive feel of the local battlespace, including the environmental conditions and operational situation.
- *Effective employment of forces—predictive planning and preemption, integrated force management, and execution of time-critical missions.* These capabilities allow the joint warfighter to plan and execute operations in a manner that achieves an overwhelming effect at precise places and times.
- *Global Information Grid (encompassing what was formerly referred to in the ABIS study as the C^4ISR Grid)—universal transaction services, distributed environment support, and high assurance of services.* The GIG allows the joint warfighter to rapidly adapt to changing situations and environmental conditions and to attack high-priority targets throughout the battlespace. Information Superiority empowers lower echelon force elements by widely distributing the commander's intent and the information needed for timely and effective execution. Because these capabilities inevitably degrade in the course of battle, a key objective of IS is to enable commanders to plan for this eventuality, to identify and protect essential capabilities, and to reconfigure information flows and supporting C^2 structures to meet changing needs. This high degree of flexibility is achieved by a network-centric approach to the integration of current and future sensor, information, and engagement grids into a single GIG.

Additionally, the joint warfighter must have a superior defensive information operations (DIO) capability to defend information systems from both deliberate and accidental disruptions, intrusions, manipulations, and corruptions. This gives the joint warfighter a credible deterrent across the full spectrum of conflict, ensures information superiority, and permits the conduct of operations without effective opposition. Figure IV–2 represents a conceptual view of the DIO environment. This operational capability is of increasing importance as information technology becomes more widely available throughout the world.

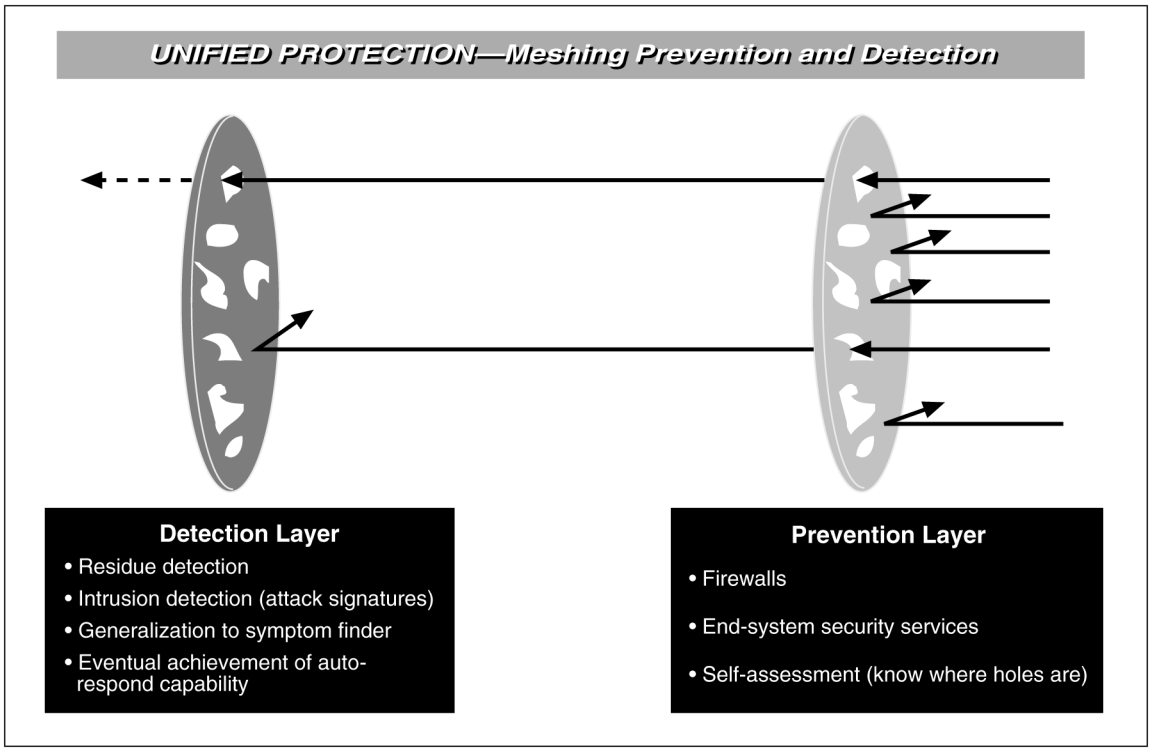

Figure IV–2. Concept—Defensive Information Operations

The DIO technology base must support joint warfighter requirements in DIO as well as effective management of the sensor, information, and engagement grids that compose the GIG. DIO operational capabilities include information assurance, operations security, physical security, counterdeception, counterpropaganda, counterintelligence, and electronic warfare (EW). DIO ensures timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes. Four interrelated processes support DIO: information environment protection, attack detection, capability restoration, and attack response. Additionally, critical DIO operational capabilities are included under assurance services as part of the GIG. Effective C^4I has been integrated into various other capability areas as appropriate.

Global Battlespace Awareness. Global battlespace awareness includes the operational capability to acquire and assimilate information about the position and movement of global friendly, adversary, and neutral forces, and about the global geospatial situation, including the undersea, surface, air, and space environment in which they are or could be deployed. This by necessity includes environmental issues such as weather, chemical and biological dispersion, etc. It also includes the capabilities to provide a common view and understanding of the situation of tactical and supporting forces across the global battlespace, from joint force commanders to individual shooters. The effective integration of global battlespace awareness within a federated system will provide the warfighter with an all-encompassing view of the local battlespace and of current and projected operational conditions, and an enhanced ability to identify and localize features of the battlespace in the face of degraded environmental conditions and hostile countermeasures. More than 400 different mission and functional software applications currently support the Joint Task Force (JTF) commander. This global view will support and enhance the warfighters' intuitive feel for situations and command options.

The specific operational capabilities necessary to achieve global battlespace awareness are as follows:

- *Information acquisition*—the provision of sufficient, timely, and high-quality surveillance, reporting, target designation, and assessment information on enemy, friendly, and U.S. units, events, activities, status, capabilities, plans, and intentions to ensure that joint or multinational commanders have dominant local battlespace knowledge and understanding.
- *Precision information direction*—the capability to dynamically control and integrate global information and direct it to both tactical and supporting C^4ISR resources for targeting, weaponeering, mission preview, battle damage assessment (BDA), and combat assessment to maintain the ability for the on-scene commander to exploit and shape the local battlespace. This also includes the integration and synchronization of information into up-to-date mission products to be delivered just in time to the warfighter, anytime, anywhere.
- *Consistent battlespace understanding*—the capability to elevate the level and speed of the warfighter's cognitive understanding of enemy, friendly, and geospatial situations, and to maintain consistency in that view across tactical and supporting multinational forces and the global battlespace.

Effective Employment of Forces. With information superiority, commanders will be able to exploit their superior understanding of the battlespace to shape and control the conflict. Specific operational capability elements are as follows:

- *Predictive planning and preemption*—the ability to be proactive in the planning process in order to avoid direct confrontation (by employing alternative means), to be prepared to react and exploit opportunities when direct confrontation must occur, and to shape expected actions in order to stay within an enemy's decision cycle and keep him out of ours.
- *Integrated force management*—the capabilities needed to achieve the dynamic synchronization of missions and resources from components and multinational forces located anywhere.
- *Execution of time-critical missions*—the ability to provide processing languages, interface characteristics, and linkages that enable rapid target search and acquisition, battle coordination and target selection, handoff, and engagement for the prosecution of time-critical targets.

The Global Information Grid. The GIG will support global connectivity with flexible, rapidly configurable network services, intelligent assistance to facilitate universal user access to both raw and fused information, and assured services in stressed environments. The GIG will provide:

- A single, secure grid providing Information Superiority to DoD and the intelligence community.
- Flexible, seamless, end-to-end C^4ISR capabilities.
- Direct support to the command structures and additional support for time-critical, short-duration mission tasks such as "sensor–decision-maker–shooter" integration and support.

The services of the GIG are conceptually separate from command structures, disseminating global battlespace awareness to users when they need it and in the form that they need it to facilitate the collaborative planning and execution of joint and multinational operations. Achieving connectivity and flexibility across geographical dispersed, heterogeneous systems will also allow the creation of "virtual staffs" that expand and augment the capabilities of in-theater forces with collaborative services, reach-back capabilities, and reduced local footprint. The GIG scalability provides the capabilities for joint, high-capacity, netted operations and the necessary information/bandwidth needed on demand.

The critical operational capabilities of the GIG are:

- *Universal transaction services*—the capability to provide warfighters and their systems the ability to exchange data and understand information, unimpeded by differences in connectivity and national language, on a "just-in-time" basis, regardless of location.
- *Distributed environment support*—the mechanisms and services required to allow the warfighters to craft their C^4ISR information environments from the full set of assets connected through the GIG, including the ability to establish distributed virtual staffs and task teams.
- *High assurance of services*—high-quality services that warfighters must have, when needed, to meet dynamically changing demands and defend against physical and IO threats. This includes adaptive network management that anticipates changing requirements, and DIO operational capabilities of information assurance, operations security, counterdeception, counterpropaganda, counterintelligence, EW, and SIO.

C. FUNCTIONAL CAPABILITIES

Achieving critical IS operational capability elements will require significant advances in numerous functional capabilities to manage the acquisition, simultaneous processing, and parallel dissemination and presentation of information in an assured and secure manner, and to effectively integrate mission planning functions. The complexity of the information must be condensed and synthesized to an understandable level for the joint warfighter. This will require additional research and development (R&D) in cognitive science and human computer interface to allow the user to comprehend the situation. Additionally, new training mechanisms such as advanced distributed learning (ADL) will have to be provided to ensure the operational competence of the soldier, sailor, or airman in effectively using these new capabilities.

Because Information Superiority has taken on a more global context, capabilities are needed for automated natural language understanding and foreign language translation of messages and documents. The ever-expanding volume of foreign and domestic message traffic places an additional burden on the systems needed to store, maintain, search, and retrieve data. R&D to advance the engineering of large databases is also needed to improve the capability to manage huge amounts of data. In fact, as the GIG continues to evolve, a focus on total-life-cycle systems engineering is needed to achieve end-to-end performance. Additionally, intelligent agent research that addresses the added complexity and the dynamic and distributed nature of our battlespace requires us to be able to anticipate, adapt, and actively seek ways to support both our users and the systems that they employ. Current intelligent agent research addresses software components that are able to perform complex assignments with a high degree of autonomy and sensitivity to task context and operational environment. The agents must be able to learn from

their experiences, communicate and cooperate effectively with both people and other software agents, and move from place to place within the GIG as required.

Table IV–1 provides a mapping of the IS functional capabilities to the operational capability elements and broad operational capabilities.

Table IV–1. Functional Capabilities Needed—Information Superiority

Functional Capabilities	Operational Capability Elements								
	Global Battlespace Awareness			Effective Employment of Forces			Global Information Grid		
	Information Acquisition	Precision Information Direction	Consistent Battlespace Understanding	Predictive Planning and Preemption	Integrated Force Management	Execution of Time-Critical Missions	Universal Transaction Services	Distributed Environment Support	High Assurance of Services
1. Intelligence Processing and Broadcast	●		○	●	●	●			●
2. Intelligent, Distributed Mapping, Charting, and Geodesy (MC&G)	●		●					○	
3. Collaborative Situation Assessment and BDA			●		●	●			●
4. Collection and Distribution of Weather and Environmental Conditions	●		●	●					
5. Common Understanding and Representation of the Battlespace	●		●	●	○				
6. Consistent Situation Projection		●	●	●					
7. Mission Rehearsal and Embedded Training		●			●	○			
8. Command Projection and Sharing of Commander's Intent		●		●	●				
9. Support for Simultaneous, Coordinated Operation					●				
10. Repair and Consumables Management	○		○	●	●	●	●		○
11. Joint Force Automated Battle Rules of Engagement					●				
12. Theater Intelligence Processing and Broadcast	●		●						●
13. Shared, Distributed Collaborative Planning		●	○	●	●	●		○	
14. Rapid, Accurate BDA	●	●				●			
15. C4ISR System Management	●				●	●	○		
16. Force Status and Execution Management	●		○		●	●			
17. Parallel Dissemination of Intelligence/BDA	●					●			●
18. Rapid, Accurate Automated Targeting	○	●	●		●	●			
19. Automated Mission and Weapon-to-Target Pairing	○					●			
20. Seamless Connectivity						○	●	○	
21. Space Assets	●	●	●	●	●	●	●	●	●
22. Automatic Adaptive Information Conditioning							●		
23. Location-Independent Addressing, Both Stationary and "On the Move"	●						●		
24. Flexible, Adaptive Access Control						○	●		
25. Support for Heterogeneous Users and Interfaces								●	
26. Knowledge-Based Access, Retrieval, and Integration of Information						○		●	
27. Distributed, Collaborative Processing						○		●	

Table IV–1. Functional Capabilities Needed—Information Superiority (continued)

Functional Capabilities	Operational Capability Elements								
	Global Battlespace Awareness			Effective Employment of Forces			Global Information Grid		
	Information Acquisition	Precision Information Direction	Consistent Battlespace Understanding	Predictive Planning and Preemption	Integrated Force Management	Execution of Time-Critical Missions	Universal Transaction Services	Distributed Environment Support	High Assurance of Services
28. Massive, Heterogeneous Distributed Information Management						○		●	
29. Automated Intelligent GIG System Management						●		○	●
30. Service Extension and Modular "Plug and Play"									●
31. Information Consistency, Integrity , Protection, and Authentication	●					○			●
32. Access Controls/Security Services								○	●
33. Service Availability							●	○	●
34. Network Management and Control						○	●	○	●
35. Damage Assessment	●						●		●
36. Reaction (Isolate, Correct, Act), Including Recovery and Reconstitution									●
37. Vulnerability Assessment and Planning	●						●		●
38. Preemptive Indication	●								●
39. Intrusion Detection/Threat Warning	●								●
40. IO and Spectrum Dominance Planning and Monitoring		●			●				
41. Synthesis of Complex Data and Information			●		●				
42. Large Database Engineering, Manipulation, Search, and Retrieval	●		●		●		●		
43. Realistic C4ISR Modeling and Simulation				●					
44. Text Understanding	●		●						
45. Foreign Language Translation	●		●		○				
46. Life-Cycle Systems Engineering									●
47. Satellite System Survivability	●	●	●	●	●	●	●	●	●

● Strong Support ○ Moderate Support

D. CURRENT CAPABILITIES, DEFICIENCIES, AND BARRIERS

Currently fielded information systems do not support the kind of robust, assured, and timely flow of accurate and relevant information needed to meet future joint warfighting needs. Operational practices limit flexibility and effective employment, even though ongoing DoD and individual service efforts such as the Defense Information Infrastructure (DII) (part of the National Information Infrastructure) and C4ISR Integration Task Force are making important improvements.

There needs to be a coevolution of doctrine, organization, training, materiel, leadership, and personnel (DOTMLP) as well as cultural changes to truly achieve the Information Superiority required for JV2010 and the Revolution in Military Affairs (RMA). Doctrine and organizational changes are needed to reflect the required network-centric integration of systems

and information. Leaders and personnel need to understand the capabilities, changes, and information available, as well as the changes needed in the acquisition and fielding of systems to achieve true integration, assurance, and interoperability. Joint Task Force integration into ever-changing allied/coalition/agency environments is forcing a need to reassess information and systems classification/security processes and applications. Joint training and education is necessary for every aspect of military operations, most importantly information systems, for all ranks.

The structure for C^4ISR remains divided along organizational and functional lines and is strongly tied to the hierarchical command structure, due in large part to inadequate capabilities for the automation of multilevel security. Even when information can be provided, it may be in a form that has been tailored and optimized for some other mission. These divisions, tied to a rigid framework of battlefield geometry, limit a commander's ability to assign sensors to priority targets and to dynamically retask high-value assets across missions and services in response to changing situations and opportunities. Furthermore, communications bandwidths and connectivity are inadequate to support the flow of data under conditions of peak demand.

"Stovepiping"—the operational fragmentation and end-to-end segregation of information flow by type, command structure, and mission—makes it difficult to acquire, process, and disseminate essential information across joint forces, and makes it virtually impossible to develop a common picture of the battlespace. The ever-increasing amount of foreign language message traffic further exacerbates this problem. In addition, the sheer volume and complexity of information are often overwhelming. Although there is a high degree of assurance (i.e., confidence in the integrity, confidentiality, and availability) associated with information received via stovepiped classified systems, there is less assurance associated with information received across heterogeneous systems.

Current C^4ISR systems provide only a limited ability to detect and monitor targets and events concealed in foliage, in structures, under ground, or in adverse weather or countermeasure environments. Rigid ISR systems and lack of visibility of independent tactical sensor tasking and coverage further limit our ability to manage and coordinate sensor assets for real-time operations.

DIO limitations include:

- Inadequate management of distributed information
- Countermeasures that are generally reactive to emergent IO rather than anticipatory
- Lack of predictive and anticipatory network management capabilities
- Limited IO sensors and processing capability for GIG self-defense
- Intrusion detection techniques that do not scale or that do not facilitate damage assessment or automated response.

A number of technological, organizational, operational, and programmatic barriers make it difficult to overcome these limitations. Nonetheless, existing capabilities are being applied in unique ways and are being extended to provide more effective means of network protection. Ranging from advanced access control systems to effective means of encryption of databases and transmitted information, tools are becoming available that help ensure the availability, integrity, and confidentiality of critical information for the joint warfighter. For example, the Air Force Research Laboratory ISSE GUARD program is addressing the problem of providing worldwide flexible, interoperable, high-assurance systems with multiple levels of security.

Technological advances alone are not sufficient. Traditional concepts of operation and rigid C^4ISR structures will need to change if the warfighter is to realize the benefits of advancing technology. Total-life-cycle systems engineering concepts must be developed and applied to achieve true plug-and-play integration of complex heterogeneous systems and protocols. Global battlespace awareness transcends individual service and organizational divisions and will require the effective integration of, and sustained commitment to, individual service and joint programs within a common architecture.

Table IV–2 provides a mapping of key technologies to limitations to functional and operational capabilities.

Table IV–2. Goals, Limitations, and Technologies—Information Superiority

Goal	Functional Capabilities	Limitations	Key Technologies
Global Battlespace Awareness			
Operational Capability Element: Information Acquisition			
Provide sufficient, timely, high-quality surveillance, reporting, target designation, and assessment information on enemy, friendly, and U.S. units, events, activities, status, capabilities, and plans/intentions to ensure that joint/multinational commanders have dominant battlespace knowledge.	Intelligence processing and broadcast Intelligent, distributed MC&G Repair and consumables management Theater intelligence processing and broadcast C^4ISR system management Rapid, accurate automated targeting Large-database engineering, manipulation, search, and retrieval Text understanding Foreign language translation Space assets	Limited coverage extent, quality, and continuity currency "Stovepipe" nature of systems/information by type, acquirer/dissemination Few systems have near-real-time (NRT) capabilities for responding to tasking and providing direct-continuing support to forces Limited capability to detect, identify, and monitor targets/events in foliage, in buildings, and under ground Lack of consistent displays at all levels Many capabilities can be denied by weather and countermeasures Manpower-intensive—little automation of integration/fusion, target detection, target ID, and BDA capabilities Manpower-intensive language and protocol translation Limited ability to rapidly store, search, and retrieve large volumes of sensor data	Small volume/weight, very high speed capacity processors and storage devices; application software that can be embedded with sensors/platforms Software applications for intelligent selection and following of coverage areas/targets Software applications for use with multiple data sources (including reference/databases) to enhance target detection, tracking, and designation (e.g., detecting changes) Visualization technologies Foliage-penetrating moving target indicator (MTI) and synthetic aperture radar (SAR) Near-simultaneous multispectral coverage (multispectral x 100s of bands) Passive/multistatic MTI/SAR Small-volume/weight, hyperspectral, rapidly deployable smart surface sensors Direct integration of Global Positioning System (GPS) with sensor outputs where appropriate Transfer/translation applications and storage devices/communications for NRT tactical aircraft sensors

Table IV–2. Goals, Limitations, and Technologies—Information Superiority (continued)

Goal	Functional Capabilities	Limitations	Key Technologies
Global Battlespace Awareness (continued)			
Operational Capability Element: Precision Information Direction			
Maintain the ability of the on-scene commander to exploit and shape the battlespace by dynamically directing and integrating (in accordance with operation, battle, and mission priorities) both tactical and supporting ISR resources for targeting, weaponeering, mission preview, BDA, and combat assessment.	Situation projection Mission rehearsal and embedded training Command projection Shared, distributed collaborative planning Rapid, accurate BDA Rapid, accurate automated targeting IO and spectrum dominance planning and monitoring Space assets	Limited response to battlespace changes; rigid ISR, lack of visibility into sensor tasking and coverage Sortie impact limitations, poor/slow BDA Limited comprehensive sensor tasking to support mission No just-in-time retargeting capability	Object-oriented, distributed, intelligent, and dynamic planning, scheduling, and target handoff Embedded, fault-tolerant, distributed modeling and simulation (M&S) for mission preview, rehearsal, and training M&S for full-spectrum dominance planning M&S for IO surveillance and planning Joint multisensor fusion, information fusion, and sensor cross-cueing providing a consistent battlespace picture Integrated cross-sensor tracking with unique target ID and real-time updates Smart systems for target and infrastructure identification, recognition, behavior, and change detection and BDA Distributed, collaborative, virtual planning in real time Rapid M&S for sensor coverage analysis
Operational Capability Element: Consistent Battlespace Understanding			
Elevate the level of our cognitive understanding of the enemy, friendly, and geospatial situation; maintain consistency in that view across tactical and supporting forces.	Intelligence processing and broadcast (from CONUS; fused NRT signals intelligence (SIGINT) and imagery; increased/fused sensor data in NRT) Intelligent, distributed MC&G Collaborative situation assessment and BDA Collection and distribution of weather and environmental conditions Common understanding and representation of the battlespace Situation projection Repair and consumables management Theater intelligence processing and broadcast Rapid, accurate automated targeting Synthesis of complex data and information Large-database engineering, manipulation, search, and retrieval Text understanding Foreign language translation Space assets	No common operational picture Inadequate information support for commander's decision needs Presently too much information without quality thresholds; not scaleable Text message intensive with no automated machine understanding Inadequate dissemination of understanding Intelligence preparation of the battlefield (IPB) of battlespace degrades when battle begins Inability to process multiple languages and protocols Lack of consistent displays at all levels	Joint multisensor fusion, information fusion, and sensor cross-cueing Mass storage of information Intelligent products to support decision making Common 3D integrated situation display with selectable detail and resolution Virtual reality (VR) situational displays High-rate broadcast Smart systems for target and infrastructure identification, recognition, behavior, and change detection and BDA Auto data validation and data validity tags Tailored search and retrieval of heterogeneously located information Intelligent self-aware agent for knowledge retrieval, filtering, sanitization, and deconfliction Improved data and uncertainty visualization management Real-time M&S for assessment and friendly/enemy course-of-action analysis (COAA) Automated natural language understanding Automated natural and computer language, syntax, and protocol translation Multilevel information security and information assurance Distributed, synchronized, large database

Table IV–2. Goals, Limitations, and Technologies—Information Superiority (continued)

Goal	Functional Capabilities	Limitations	Key Technologies
Effective Employment of Forces			
Operational Capability Element: Predictive Planning and Preemption			
Lean forward in the planning process to (1) avoid direct confrontation (by employing alternatives); (2) be prepared to react and exploit opportunities when direct confrontation must occur; and (3) shape the expected actions to stay within the enemy's decision cycle and keep him out of ours.	Intelligence processing and broadcast Collection and distribution of weather and environmental conditions Common understanding and representation of the battlespace Situation projection Command projection Repair and consumables management Shared, distributed collaborative planning Realistic C4ISR modeling and simulation Space assets	Automated planning systems not dynamic Wargaming not effectively integrated in C4ISR and cannot be used for online planning evaluation Sensor tasking and countermeasures are "reactive" to emergent IO rather than anticipatory Information search and retrieval can choke at times of peak demand Lack of distributed, consistent data at all levels	Object-oriented, distributed, intelligent, and dynamic planning, scheduling, and target handoff Embedded, fault-tolerant, distributed M&S for mission preview, rehearsal, and training M&S for full-spectrum dominance planning M&S for IO surveillance and planning Smart systems for target and infrastructure identification, recognition, behavior, and change detection and BDA Real-time M&S for assessment and friendly/enemy COAA Continuous sliding collaborative planning across battlespace Just-in-time mission package construction and delivery Smart nodal analysis and weaponeering Smart target/weapon pairing and update Easily deployable, evolvable, scaleable, plug-and-play architecture Cross-functional virtual teams
Operational Capability Element: Integrated Force Management			
Achieve dynamic integration of force operations by collaborative execution monitoring, repair, and retasking of shared assets across echelons, missions, components, and multinational forces (control of "coherent" joint/simultaneous operations to optimized, dynamic use of resources without preempting "intuitive" use).	Intelligence processing and broadcast Mission rehearsal and embedded training Command projection Support for simultaneous, coordinated operation Repair and consumables management Joint force automated battle doctrine Shared, distributed collaborative planning C4ISR system management Force status and execution management Rapid, accurate automated targeting IO and spectrum dominance planning and monitoring Space assets	Present coordination via rigid framework of battlefield geometry Limited ability to apply all assets to formulate and support coherent defensive situation Limited understanding of what needs to be done (strategy, commander's intent) and relationship of individual tasks to overall campaign objectives Manually intensive development of plans to support simultaneous operations Limited real-time insight into conduct of plan No responsive way to dynamically retask high-value assets across missions and services in response to changing situations and opportunities	Embedded, fault-tolerant, distributed M&S for mission preview, rehearsal, and training M&S for full-spectrum dominance planning M&S for IO surveillance and planning Real-time M&S for assessment and friendly/enemy COAA Intelligent nodal analysis and weaponeering Distributed, collaborative, and virtual situation awareness Dynamic shared war plan that deals with uncertainty Dynamic allocation of shared resources in real time Decision support to assess and replan consumables

Table IV–2. Goals, Limitations, and Technologies—Information Superiority (continued)

Goal	Functional Capabilities	Limitations	Key Technologies
Effective Employment of Forces (continued)			
Operational Capability Element: Execution of Time-Critical Missions			
Provide a real-time fused battlespace picture with integrated decision aid tools that ensures coordinated dynamic planning and execution of a broad spectrum of missions, from time-phased attack of fixed targets to reconnaissance of battle areas and prosecution of time-critical targets by integrated hunter-controller-killer assets. Provide processing and linkages that enable rapid target search and acquisition, battle coordination and target selection, handoff, and engagement for prosecution of time-critical targets.	Intelligence processing and broadcast Collaborative situation assessment and BDA Repair and consumables management Shared, distributed collaborative planning Rapid, accurate BDA C4ISR system management Force status and execution management Parallel dissemination of intelligence/BDA Rapid, accurate automated targeting Automated mission and weapon-to-target pairing Space assets	Slow decision and resource allocation process with respect to target cycle times Poor detection of fleeting target entities in crowded battlespace Slow, incomplete fusion process Best sensor information not incorporated Human-intensive BDA Targets appear after force package commitments, pop-up targets, movement cycles Execution status unknown Inability to counteract target reaction to threat and engagement Simultaneous pulls on sensors Insufficient connectivity Sensor management not tied to commander's intent	Intelligent nodal analysis and weaponeering Wideband communications and interconnectivity Real-time, cognition aiding displays Intelligent planning/decision support tools Data interoperability/synchronization Intelligent IPB process Fusion and integrated target tracking Automatic target recognition Advanced, adaptive, multilevel security (MLS) ISR management and integration tools Visualization technologies
Global Information Grid (GIG)			
Operational Capability Element: Universal Transaction Services			
Provide warfighters and their systems the ability to exchange and understand information, unimpeded by differences in geography, connectivity, processing, language, or interface characteristics on a "just-in-time" basis.	Repair and consumables management Seamless connectivity Automatic adaptive information conditioning Location-independent addressing Flexible, adaptive access control Service availability Network management and control Damage assessment Vulnerability assessment and planning Space assets	Information transport generally tied to C^2 hierarchy Lack of interoperability Unacceptable limitations on connectivity to tactical users Lack of adaptive conditioning of information to optimize services Users burdened with requirement to know network addresses Limited ability to support multiple levels of security and MLS, especially in multinational operations Limited capability to support continued operations during network partition	Real-time M&S for assessment and friendly/enemy COAA Intelligent nodal analysis and weaponeering Automatic target recognition Advanced, adaptive, intelligent MLS Adaptable tactical/mobile networking Rapidly deployable tactical fiber extensions Tactically extensible, high-rate, asymmetric mobile communications Advanced compression and coding abstracting for conditioning of information Dynamic reallocation of computing resources MLS secure commercial off-the-shelf (COTS)-based clusters Secure GPS Fault avoidance and recovery mechanisms

Table IV–2. Goals, Limitations, and Technologies—Information Superiority (continued)

Goal	Functional Capabilities	Limitations	Key Technologies
Global Information Grid (GIG) (continued)			
Operational Capability Element: Distributed Environment Support			
Provide all mechanisms and services required to allow warfighters to craft their C4I information environments from full set of assets connected through the GIG, including ability to establish distributed, virtual staffs; to share a common, consistent perception of the battlespace; and to construct distributed task teams among sensors, shooters, movers, and command posts.	Support for heterogeneous users and interfaces Knowledge-based access, retrieval, and integration of information Distributed, collaborative processing Massive, heterogeneous distributed information management Space assets	Limited ability to integrate processes across heterogeneous system domains Inadequate knowledge of navigation and retrieval for massive, distributed, heterogeneous systems Minimal capability for exploiting information within the network to provide users with knowledge and advisory cues Minimal capability to manage distributed information, especially in asymmetric and broadcast communication environments Limited flexibility and adaptability of information security for multinational operations Lack of interoperability	Tailored search and retrieval of heterogeneously located information Real-time M&S for assessment and friendly/enemy COAA Intelligent nodal analysis and weaponeering Multimode, multilingual interface services Heterogeneous multimedia conferencing Intelligent mediators and database management system tools Massive data storage and management Flexible information security for information exchange, access, and conferencing Visualization technologies
Operational Capability Element: High Assurance of Services			
Provide high-quality services to warfighters that will be available whenever and wherever needed; that can be adapted, scaled, and projected to meet dynamically changing demands; and that can be defended against physical and information warfare threats.	Automated intelligent C4ISR system management Service extension Information consistency Life-cycle systems engineering Space assets	Limited ability to support MLS, especially in multinational operations Lack of modular plug-and-play to allow adaptation of services and to project information-intensive support globally Lack of confidence that nonorganic assets will be available when needed Lack of predictive/anticipatory network management capabilities Lack of IO sensors and processors for GIG self-defense Limited ability to provide both capability and "hardness" Limited ability to effect design trades on a system-wide level	Intelligent nodal analysis and weaponeering Management tools for anticipatory services Tools for projecting and visualizing GIG capabilities in terms of projected operational needs Multilevel, adaptive information security IO surveillance and defense tools Software integrity validation Secure distributed systems

Table IV–2. Goals, Limitations, and Technologies—Information Superiority (continued)

Goal	Functional Capabilities	Limitations	Key Technologies
Global Information Grid (GIG) (continued)			
Operational Capability Element: High Assurance of Services (continued)			
Provide protection from deliberate or inadvertent unauthorized disclosure, acquisition, manipulation, modification, or loss of sensitive information under various complex security policies, using distributed open systems architectures and different security attributes.	Information consistency Access controls/security services Vulnerability assessment and planning Preemptive indication Intrusion detection/threat warning	Limited ability to support MLS, especially in multinational operations Countermeasures generally reactive to emergent IO rather than anticipatory Limited network discovery, management, security management, and expert systems capabilities Limited availability of trusted operating systems Vulnerabilities in application of COTS items Inadequate tools for validating system security and robustness Limited authentication and identification capabilities Inadequate automated intrusion detection techniques Inadequate data contamination recovery techniques	Secure firewalls and guards (B3 level) Dynamic reallocation of computing resources Intelligent network discovery, intrusion detection, and response capabilities MLS COTS-based clusters Trusted systems Malicious code detection tools Security analysis tools Security engineering for systems
Eliminate, or reduce to an acceptable level, the vulnerabilities that an adversary could exploit by obtaining information about friendly capabilities, limitations, and intentions.	Access controls/security services Reaction (isolate, correct, act) Vulnerability assessment and planning	Limited network discovery, management, security management, and expert systems capabilities Limited authentication and identification capabilities Limited ability to manage distributed information Limited classification management capability of data objects	Robust, adaptive, intelligent, context-based information distribution infrastructure Advanced high-speed protocol/ encryption and advanced key management for tactical and strategic networks
Ensure that information is sound and unimpaired.	Information consistency Access controls/security services Service availability Network management and control Damage assessment Reaction (isolate, correct, act) Vulnerability assessment and planning Preemptive indication Intrusion detection/threat warning	Limited ability to support MLS, especially in multinational operations Limited availability of trusted operating systems Vulnerabilities in application of COTS items Limited authentication and identification capabilities Limited classification management capability of data objects Limited scaleable encryption	Secure firewalls and guards (B3 level) MLS COTS-based clusters Trusted systems Advanced high-speed protocol/ encryption and advanced key management for tactical and strategic networks

Table IV–2. Goals, Limitations, and Technologies—Information Superiority (continued)

Goal	Functional Capabilities	Limitations	Key Technologies
Global Information Grid (GIG) (continued)			
Operational Capability Element: High Assurance of Services (continued)			
Provide early warning of potential attacks so as to (1) alert all defensive mechanisms; (2) initiate available, reactive measures; and (3) minimize or obviate attack effectiveness.	Damage assessment Vulnerability assessment and planning Preemptive indication Intrusion detection/threat warning	Limited predictive and anticipatory network management capability Limited IO sensors, processing, and reporting for GIG self-defense Inability of intrusion detection techniques to scale or to facilitate BDA or automated response	Intelligent network discovery, intrusion detection, and response capabilities Security analysis tools Secure GPS
Achieve an ability to continue to operate at some nominally acceptable level through attacks so as to avoid catastrophic failure of the system and endure into the postattack period for recovery or reconstitution or both.	Service availability Network management and control Damage assessment Reaction (isolate, correct, act) Vulnerability assessment and planning	Limited predictive and anticipatory network management capability Limited IO sensors, processing, and reporting for GIG self-defense Inability of intrusion detection techniques to scale or to facilitate BDA or automated response Limited IO damage assessment and damage control capability Limited capability to support continued operations during network partition	Dynamic reallocation of computing resources Intelligent network discovery, intrusion detection, and response capabilities Security analysis tools Fault avoidance and recovery mechanisms

E. TECHNOLOGY PLAN

Achieving Information Superiority and seamlessly integrating Information Superiority into warfighting operations will require both advances in technology and development of new operational concepts to exploit them. Table IV–3 maps IS DTOs to operational capabilities, while Figure IV–3 traces the flow of key technologies to operational capability elements. The volume on DTOs provides further information on demonstrations and DTOs. Figures IV–4 and IV–5 provide an integrated roadmap of key demonstrations and JWSTP DTOs. Note that the IS DTOs are closely linked with a number of DTOs in the JWCOs of Precision Fires (Chapter V), Force Projection/Dominant Maneuver (Chapter X), and Joint Readiness and Logistics, and Sustainment of Strategic Systems (Chapter XII); and the DTAP areas of Information Systems Technology (DTAP, Chapter III), Sensors, Electronics, and Battlespace Environment (DTAP, Chapter VII), and Human Systems (DTAP, Chapter IX).

The current JWSTP program includes a number of demonstrations that provide the basis for immediate improvements in global battlespace awareness and the integration of improved knowledge into mission planning and execution. These demonstrations also support new concepts of C^4ISR operation and improvements in the warfighter's ability to use ISR assets. These will demonstrate the value of information superiority to the operational forces and provide a strong foundation on which to build an effective long-term program to achieve the JCS's future warfighting vision. In addition, new C^4ISR capabilities and concepts will immediately begin to affect capabilities and concepts of operation in all other warfighting areas.

Table IV–3. Demonstration Support—Information Superiority

Demonstration	Operational Capability Elements: Global Battlespace Awareness: Information Acquisition	Global Battlespace Awareness: Precision Information Direction	Global Battlespace Awareness: Consistent Battlespace Understanding	Effective Employment of Forces: Predictive Planning and Preemption	Effective Employment of Forces: Integrated Force Management	Effective Employment of Forces: Execution of Time-Critical Missions	Global Information Grid: Universal Transaction Services	Global Information Grid: Distributed Environment Support	Global Information Grid: High Assurance of Services	Service/ Agency	DTO	Type of Demonstration: ACTD	ATD	TD
Robust Tactical/Mobile Networking							○	○	●	DARPA	A.02		X	
Integrated Collection Management ACTD		●								DIA	A.05	X		
Rapid Terrain Visualization ACTD	●		●							Joint	A.06	X		
Battlefield Awareness and Data Dissemination ACTD			●				○	○		DARPA	A.07	X		
High-Altitude Endurance Unmanned Aerial Vehicle ACTD	●								○	DARPA	A.10	X		
Counter-Camouflage Concealment and Deception ATD	●									DARPA	A.11		X	
Information Dominance (C^2 Protect and Attack for I/O ATD)				●		●			●	Army	A.12		X	
Satellite C^3I/Navigation Signals Propagation Technology									●	Air Force	A.13		X	
C^4I for Coalition Warfare ACTD					●		●	●		Army	A.23	X		
Information Operations Planning Tool ACTD		●		●					●	Air Force	A.25	X		
Information Assurance: Automated Intrusion Detection Environment ACTD	●								●	DISA	A.26	X		
Global Precision Surveillance: Discoverer II	●	●	●	○		○				Joint	A.27		X	
Space-Based Space Surveillance Operations ACTD		●			●					Air Force	A.28	X		
Personnel Recovery Mission Software ACTD		○				●				JSSA	A.30	X		
Human Intelligence and Counterintelligence Support Tools ACTD	●				○					Army	A.31	X		
Joint Continuous Strike Environment ACTD			●	●	●	●				Joint	B.07	X		
Theater Precision Strike Operations ACTD			●	●	●	●				Joint	B.25	X		

Table IV–3. Demonstration Support—Information Superiority (continued)

Demonstration	Operational Capability Elements: Global Battlespace Awareness: Information Acquisition	Global Battlespace Awareness: Precision Information Direction	Global Battlespace Awareness: Consistent Battlespace Understanding	Effective Employment of Forces: Predictive Planning and Preemption	Effective Employment of Forces: Integrated Force Management	Effective Employment of Forces: Execution of Time-Critical Missions	Global Information Grid: Universal Transaction Services	Global Information Grid: Distributed Environment Support	Global Information Grid: High Assurance of Services	Service/ Agency	DTO	Type of Demonstration: ACTD	ATD	TD
Extending the Littoral Battlespace ACTD			●		●	●		●		USMC	M.02	X		
Joint Cognitive Systems for Battlespace Dominance		○	●	○						Army, Air Force	HS.06			
Decision Support Systems for Command and Control	●	●	●		●	●	○	○		Navy	HS.21			
Consistent Battlespace Understanding			●							Army	IS.01			
Forecasting, Planning, and Resource Allocation				●						Army	IS.02			
Integrated Force and Execution Management				●	●	●				Army	IS.03			
Simulation Interconnection			●							Joint	IS.10			
Digital Warfighting Communications			○		○	○			●	Army	IS.23			
Intelligent Information Technology	●						●	●	●	DARPA	IS.28			
Information Presentation and Interaction			●		●					DARPA	IS.32			
Joint Force Air Component Commander			●	○	●	●				DARPA	IS.34			
Future Command Post Technologies	●			○	●					DARPA	IS.47			
Agent-Based Systems for Warfighter Support				●		●				DARPA	IS.48			
Smart Networked Radio	●							●	○	Army	IS.49			
Advanced Intelligence, Surveillance, and Reconnaissance Management	●									DARPA	IS.50		X	
Advanced Radar Processing From Airborne Platforms	●		●	●		●				Air Force	SE.03			
Automatic Radar Periscope Detection and Discrimination	●		●	●						Navy	SE.05			
Affordable ATR via Rapid Design, Evaluation, and Simulation	●									Army, Air Force	SE.19			
ATR for Reconnaissance and Surveillance	●									Joint	SE.20			

Table IV–3. Demonstration Support—Information Superiority (continued)

Demonstration	Operational Capability Elements: Global Battlespace Awareness: Information Acquisition	Global Battlespace Awareness: Precision Information Direction	Global Battlespace Awareness: Consistent Battlespace Understanding	Effective Employment of Forces: Predictive Planning and Preemption	Effective Employment of Forces: Integrated Force Management	Effective Employment of Forces: Execution of Time-Critical Missions	Global Information Grid: Universal Transaction Services	Global Information Grid: Distributed Environment Support	Global Information Grid: High Assurance of Services	Service/ Agency	DTO	Type of Demonstration: ACTD	ATD	TD
Advanced Focal Plane Array Technology	●		○							DARPA	SE.33			
Optical Processing and Interconnects	○	○	○						●	Air Force	SE.35			
High-Density, Radiation-Resistant Microelectronics						●		○	●	DSWA	SE.37			
Microelectromechanical Systems	○								●	DARPA	SE.38			

● Strong Support ○ Moderate Support

The IS DTOs listed in Table IV–3 also cover a wide range of initial IO needs. For example, Information Dominance (A.12) will provide an electronic attack capability against advanced communications in use today as well as those that are being further developed as recognizable potential threats in future conflicts.

The following is a summary of the Information Superiority DTOs:

- *A.02, Robust Tactical/Mobile Networking*, will develop the technology to provide a high-bandwidth, robust, multimedia, theater-level communications networking infrastructure that can be rapidly deployed to support military operations. This will include the demonstration of new mobile routing cellular/personal communications services, over-the-horizon connectivity for isolated and rapidly maneuvering forces, and the ability to exchange multimedia data through an Internet-like network. As a result, interactive sessions or imagery transfers on the battlefield will take place in seconds rather than in minutes or hours, even under the most stringent user demands.
- *A.05, Integrated Collection Management ACTD*, will provide an initial capability for dynamic retasking and will demonstrate integrated collection management (ICM) of signals intelligence (SIGINT) and imagery intelligence (IMINT) from national and theater sensors. This will include providing tasking-level data and status feedback to the JTF, dynamic integrated tasking of sensors from all-source strategies and cross-cueing of collection assets, and tasking inside friendly and enemy operating cycles in less than 24 hours, with an ultimate goal of 2–4 hours.

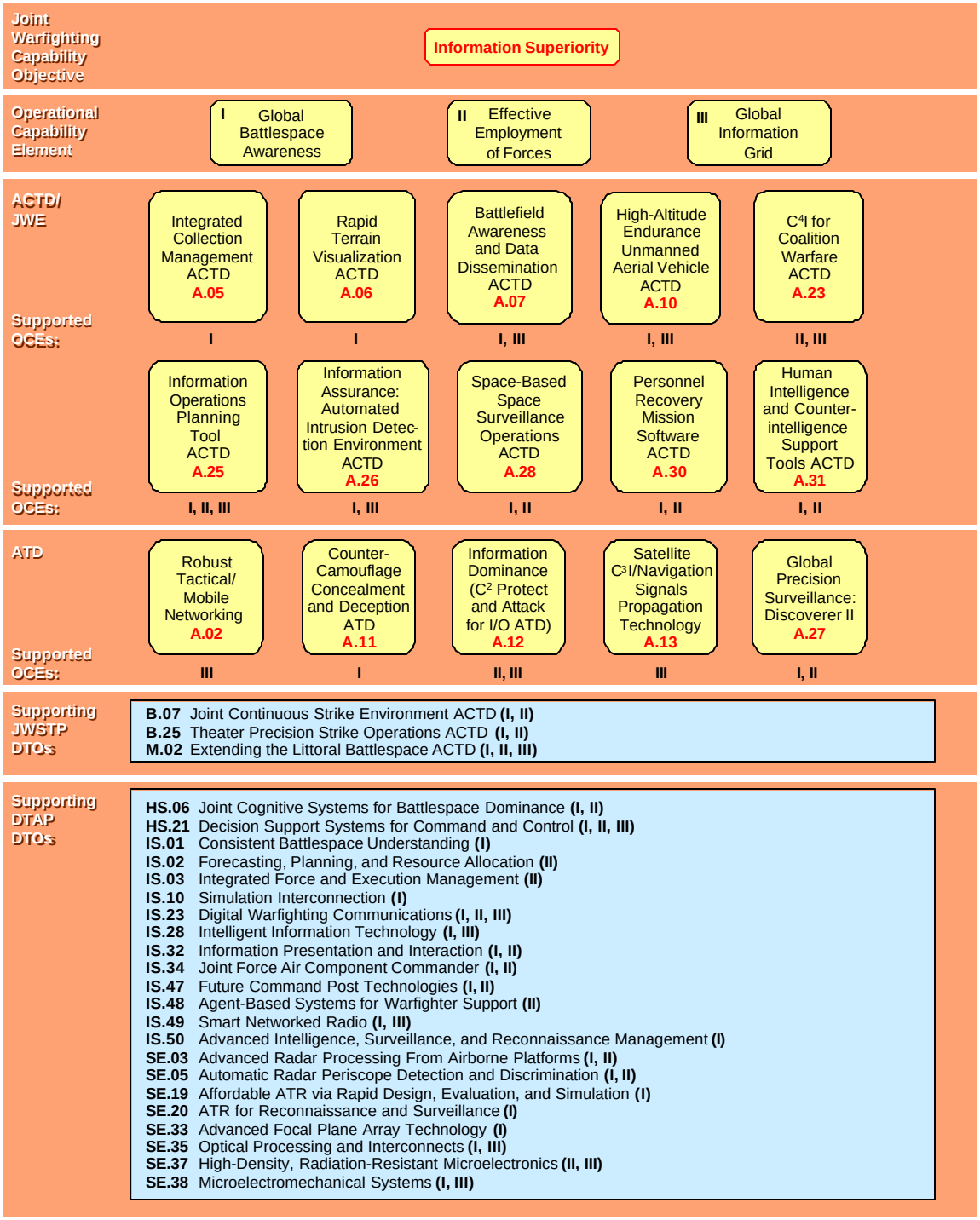

Figure IV–3. Technology to Capabilities—Information Superiority

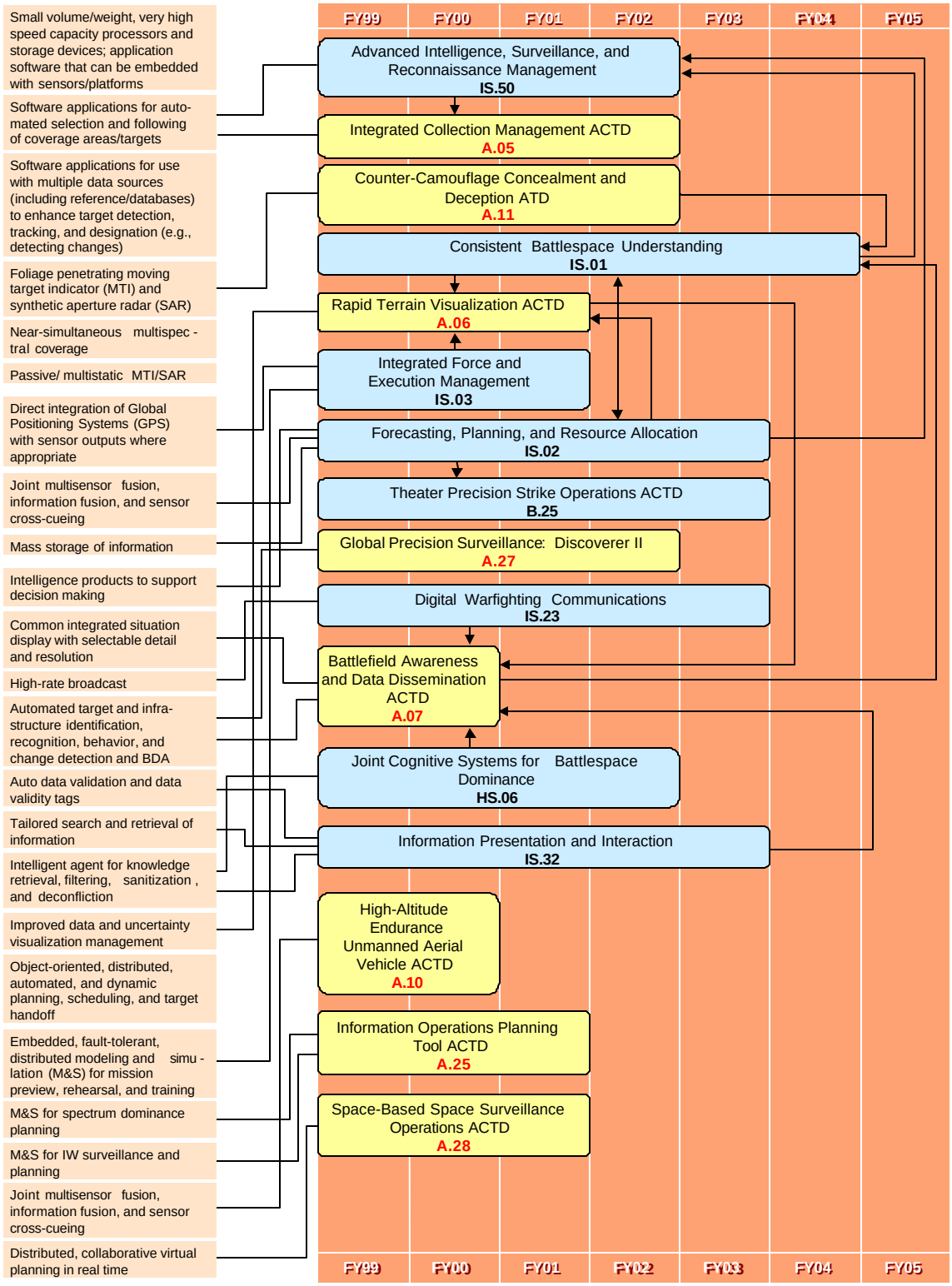

Figure IV–4. Roadmap—Information Superiority, Global Battlespace Awareness OCE

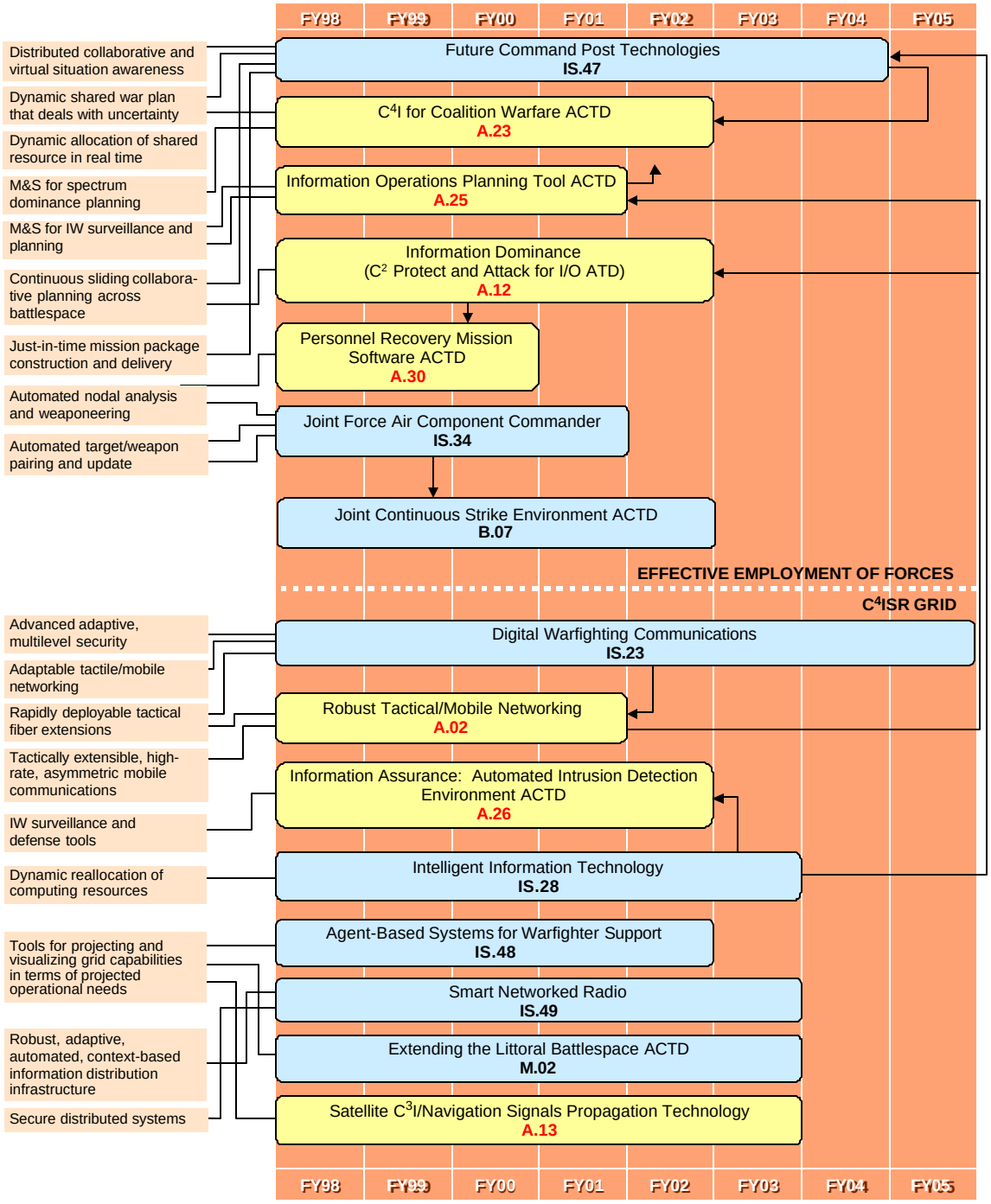

Figure IV–5. Roadmap—Information Superiority, Effective Employment of Forces, and Global Information Grid OCEs

- *A.06, Rapid Terrain Visualization ACTD,* will develop and demonstrate the rapid collection and generation of high-resolution digital terrain elevation data using imagery from aircraft and space platforms and the use of these data to generate terrain feature data and map backgrounds. This will enable the JTF commander to integrate terrain databases with current situation data, including intelligence, C^2, logistics, and weather.
- *A.07, Battlefield Awareness and Data Dissemination ACTD,* will provide the capabilities for forward warfighters to access and utilize very large information products that were previously inaccessible, and to seamlessly integrate these products with emerging 3D visualization applications. It will also provide information profiling services that will allow users to specify and control the flow of information into their forward sites, policy management services that allow commanders to manage information flows, and wideband delivery services that allow these services to operate across high-bandwidth broadcast links.
- *A.10, High-Altitude Endurance Unmanned Aerial Vehicle ACTD,* will develop and demonstrate a joint, adverse-weather, long-endurance, wide-area, day/night reconnaissance and surveillance capability in both a low-observable and conventional configuration. This will provide the joint warfighter with continuous, broad-area battlefield surveillance that has real-time connectivity to existing service exploitation centers.
- *A.11, Counter-Camouflage Concealment and Deception ATD,* will provide the warfighter the ability to detect and classify targets obscured by foliage and tactical deception techniques. A concept of operations (CONOPS) will be developed that will use this class of sensors on the Predator and Global Hawk unmanned air vehicles, and integrate the image exploitation capability from the battlefield into the semiautomated IMINT processing Common Imagery Ground/Surface System (CIG/SS) architecture developed under the recently completed DTO A.09.
- *A.12, Information Dominance (C^2 Protect and Attack for I/O ATD),* will develop, integrate, and validate hardware, software tools, tactics, techniques, and procedures that will secure the systems and networks of the Army's Tactical Internet and the First Digitized Division. This will provide new operational capabilities in the areas of advanced network access control, secure tactical network management, auditing, intrusion detection, and response mechanisms. It will also develop attack tools, techniques, and applications that will be integrated into existing or emerging intelligence and electronic warfare systems.
- *A.13, Satellite C^3I/Navigation Signals Propagation Technology,* will provide reliable real-time specifications and forecasts of ionospheric conditions and disturbances, and their effects on communications, surveillance, and navigation systems, including the Global Positioning System (GPS). This will allow radio frequencies, modulation schemes, data rates, and other system parameters to be set to match what the prevailing ionosphere will allow. Timely, reliable, advance warnings of disruptive ionospheric (scintillation) disturbances will allow operators time to adjust system parameters to mitigate those effects and, if necessary, switch to backup systems to ensure uninterrupted C^3I operations.

- *A.23, C^4I for Coalition Warfare ACTD,* will allow the U.S. Army to achieve message- and data-replication-based interoperability between its C^2 systems and those of its allies at corps through battalion level. Key technologies to be integrated include an internationally standardized data model, international preformatted messages (based on NATO standards), message parsing software, and an internationally developed data replication mechanism.
- *A.25, Information Operations Planning Tool (IOPT) ACTD,* will support the planning, development, synchronization, deconfliction, and management of an information operations campaign integrated between a joint HQ staff and the CINC components. The ACTD will also show how modeling and analysis tools with connectivity to current intelligence databases and a reachback capability to a garrison force can support the development of target recommendations and optimized courses of action aligned with CINC information operations taskings against an integrated air defense system.
- *A.26, Information Assurance: Automated Intrusion Detection Environment (IA:AIDE) ACTD,* will develop a capability to address the question, Are our information systems under attack? IA:AIDE is an effort to develop an initial "cyber radar" to detect coordinated attacks on the military information infrastructure. The program will provide an integrated suite of capabilities to detect attacks; provide data reduction, correlation, and visualization; and perform network operations.
- *A.27, Global Precision Surveillance: Discoverer II,* will reduce the risk and cost of a Space-Based Radar (SBR) system through the development of small satellite systems for theater surveillance with the flexibility for real-time tasking. Significant life-cycle cost reductions are a goal. The objective system would provide theater-wide day/night all-weather access, near-continuous surveillance, global precision targeting, direct theater tasking/downlink, and worldwide precision digital terrain elevation data (DTED) collection.
- *A.28, Space-Based Space Surveillance Operations (SBSSO) ACTD,* will develop the associated tasking, scheduling, and formatting procedures and demonstrate end-to-end space-based space surveillance. This will provide the space control community the opportunity to assess the overall operational utility of space-based space surveillance sensors compared with traditional ground-based space surveillance systems. This demonstration will serve as a pathfinder to advance required military CONOPS for future space systems like the Space-Based Infrared System low-earth-orbit constellation demonstration/validation and objective spacecraft. This new capability will also help ameliorate a capacity deficit in space surveillance observations by performing as a contributing sensor to the Air Force Space Surveillance Network (SSN).
- *A.30, Personnel Recovery (PR) Mission Software ACTD,* will support the migration from a paper-based PR response to an integrated Global Command and Control System (GCCS) software suite with a point-and-click mission interface. The end result will be an integrated hardware/software suite with specific data and applications to support joint search and rescue centers in performance of the PR mission.
- *A.31, Human Intelligence and Counterintelligence Support Tools ACTD,* will demonstrate, integrate, and assess tools to enhance HUMINT offensive (forensic intelligence) and defensive (force protection) missions. This capability will enhance

targeting (sources and facilities), improve overt and sensitive collection, and improve dissemination of information.

Near-term demonstrations will provide a basis for further improvements in tactical integration, real-time management of C^4ISR, and dynamic retasking of forces; and for better integration of concurrent planning and execution at the system level in the 2000–2005 timeframe. The prototype GIG capabilities demonstrated in the near term will begin to evolve into the type of massive, heterogeneous, distributed, and responsive information services environment envisioned in the ABIS study's long-term objectives.

Further advances and demonstrations are required for the 2000–2010 timeframe to ensure the availability of information superiority, and the secure and effective services that the warfighters will need in future conflicts. The Information Systems and Technology DTOs cover a number of longer term objectives, discussed in the *Defense Technology Area Plan* (Reference 3). These DTOs will demonstrate IS capabilities in support of new operational concepts to achieve overwhelming effect across the full spectrum of dominant maneuver, precision engagement, full-dimension protection, and focused logistics capabilities. Transitions from demonstrations associated with DTOs into fieldable systems integrated with a common architecture are critical to providing the joint warfighter with these technical capabilities.

F. SUMMARY

The programs described above will demonstrate and evaluate a wide range of potential IS improvements over the next 3 to 5 years. Realizing the incremental improvements that lead to the JCS chairman's revolutionary vision of overwhelming dominance in the battlespace will require a continuing long-term commitment not only within the S&T program but also to integrating these capabilities into systems. A similar commitment is required to continually reassess and update operational concepts, doctrine, and tactics in conjunction with changes in technology and threat. These efforts, coupled with the projected continued doubling every 2 years of the performance of the underlying information system hardware, should result in significant incremental improvements in the warfighters' visibility and command of the battlespace, as well as in the availability of accurate, detailed sensor-to-shooter information (see Figure IV–6).

Between now and the year 2002, improvements in force employment capabilities will be based in large part on better target recognition and timely attack, improved C^2 early in the campaign, the insertion of a defensive IO capability, and an improved information environment for collaborative work. Global battlespace awareness will be improved by providing a consistent situational picture and an ability for the integrated tasking of SIGINT and IMINT capabilities. Improved awareness capabilities will support tactical needs and provide real-time sensor information directly to shooters. C^4ISR grid capabilities will be improved to support more rapid configuration of tactical networks (including nodes for mobile users) with enhanced abilities to integrate and distribute information securely in a broadly heterogeneous environment.

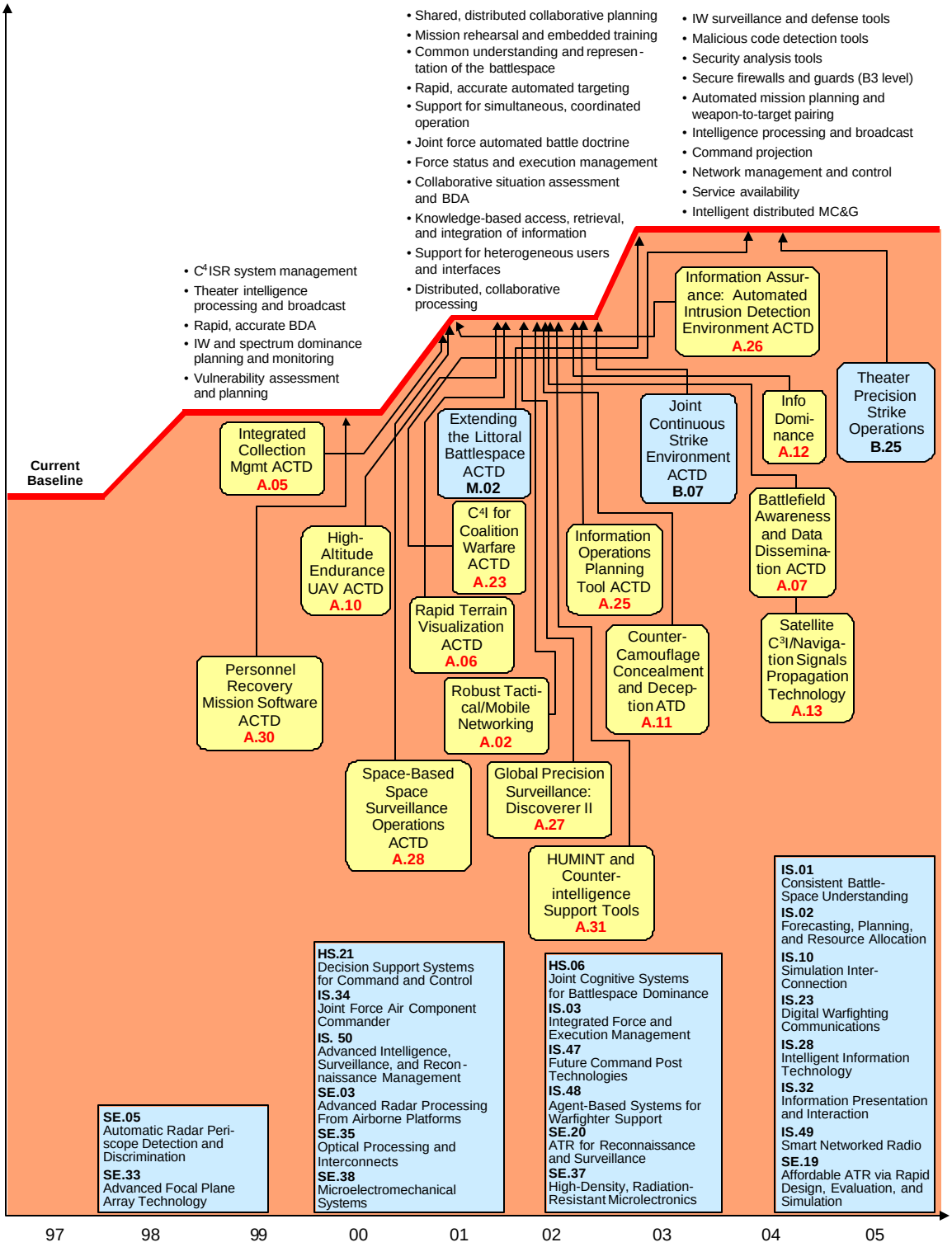

Figure IV–6. Progress—Information Superiority

In the longer term (2002–2012), the continued evolution of operational concepts and the availability of new technologies will provide a basis for the full development of the GIG concepts. Further improvements in force employment capabilities will be possible through wider dissemination of each commander's intent. Improved intelligent tools for local decision making, coupled with better status information and an ability to forecast likely future options and contingencies, would enhance the ability of commanders at all levels to reason from ambiguous information and to tailor force and mission packages to meet the needs of an ongoing conflict. Global battlespace awareness capabilities will be enhanced by continuously projecting friendly and enemy moves and their likely outcomes, by adaptively supporting cognitive functions of diverse users, and by providing tailored information for mission execution when and where it is needed. GIG capabilities will be made more robust by advances in adaptive network management and information warfare, and by providing end users with an ability to tailor and adapt their information environment and access to information.

Information operations is a relatively new joint warfighting area that is integrated into all three IS broad operational capability elements. Near-term capabilities will internetwork warfighters at the tactical level, improve the security and reliability of distributed databases, and provide improved protection techniques. Midterm capabilities will take advantage of high-bandwidth, encrypted links to internetwork warfighters at varying levels of security, and provide a suite of IO planning tools and effectiveness models. The successful advancement of these technologies will ensure the availability, confidentiality, and integrity of information by providing the warfighter with a robust, adaptive, intelligent, context-based information infrastructure and suites of tools to protect friendly information systems, while adaptively managing our own information management services.

It is important to recognize that the information warfare threat is real. IO capabilities, at various levels, are widely available throughout the world. DoD systems, particularly those that are unclassified, are currently vulnerable. While a concerted, coordinated attack against DoD interests would require considerable resources, significant focused damage to DoD information systems is already possible. The S&T community takes this threat seriously and will continue to focus funding on key technologies that support the joint warfighter IO requirements.

These recommended DTOs take fully into account commercially available technology and often utilize such technology. However, even with the continued capability improvements of commercial information systems, it will be a great challenge to meet the demand for greater bandwidth, processing throughput, and faster response time. In addition, unique technology will be required for capabilities needed only by the military. Also, in some areas, military capability is needed earlier than the commercial market has sufficient demand to justify.

While all the DTOs listed here are important critical components of the IS capability envisioned by *Joint Vision 2010*, they are insufficient. Out-year demonstrations will be needed to illustrate and validate additional advances. The emphasis in the out-year program will need to be on development and demonstration of essential intelligent, adaptable capabilities to ensure availability and security of services at all echelons and to support dominance in all types of conflict.

Information Superiority, with integrated information warfare capabilities, represents a new tenet in military doctrine. The appropriate investment in the supporting technologies will enable DoD to achieve military superiority through Information Superiority.