C4ISR Forward ...

A Vision for the Future

NRaD

A CORPORATE INITIATIVES GROUP DOCUMENT

July 1997

Our Strategic Objective

Promote our C4ISR Vision of the Future

Our Strategic Intent

A key element in the 1997 NRaD Strategic Plan is the strategy to "develop and articulate an integrated vision for C4ISR." The responsibility for this was assigned to the Corporate Initiatives Group (CIG), an NRaD interdepartmental team charged with articulation of long-range, coordinated activities that promote our primary corporate missions. The publication of this document and subsequent briefings and brochures fulfill this assignment. The vision contained in this document has my full support and that of your Executive Board. It crosses all of our Department boundaries and focuses on interdepartmental thinking and teaming. Its scope is NRaD wide.

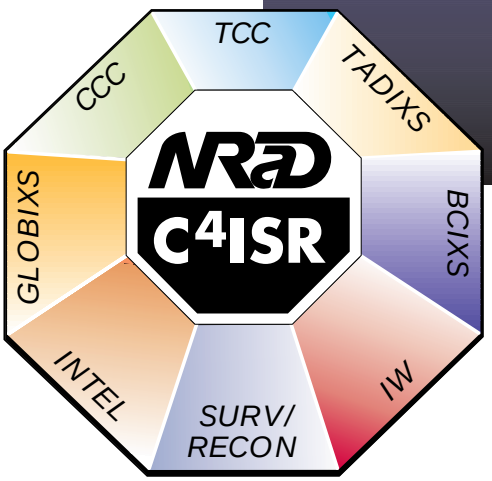
I urge you to read this document in its entirety, take it aboard and integrate it into your thinking and planning. My desire is to get us all on course toward the achievement of the vision by incorporating its tenets into our programs, our marketing efforts, our innovations, and our technology explorations.

Executive Officer

Team Members

Leader: Vic Monteleon

Jim Aitkenhead
Jerry Dufeck
Clancy Fuzak
Mary Gmitruk
Sue Hearold
Richard North
Lynn Parnell
John Roese
Hal Smith
Skip Thaeler
Frank White



Contents

The Goal
2

The Changing Environment
3

Information—The Heart of the C4ISR Vision
4

Set a Course—Acquisition to Understanding via Our Corporate Initiatives
7

9 *Dynamic Interoperable Connectivity*
12 *User Pull/Producer Push*
14 *Distributed Collaboration*
18 *Consistent Situation Perception*
20 *Information Warfare*

The C4ISR System of Systems—Attributes
22

NRaD's Approach to C4ISR Evolution
30

The Goal

C^{4}ISR, looking forward to the 21st Century, must have as its overriding goal, to provide our warriors the tools necessary to achieve information dominance over all real and potential enemies. That is a big order. It means that our C^{4}ISR system must provide the right people the right information at the right time in the right context to successfully prosecute any mission, including:

- Peacetime operations/engagements
- Deterrence and conflict prevention
- Local and theater hostilities

—singly, or as part of a joint or coalition force.

While ensuring that our warriors have the best information obtainable, the C^{4}ISR system must assist in the denial of information to any and all real and potential adversaries. In short, our C^{4}ISR system must help cut through the "fog of war," while at the same time, intensifying that fog to our enemies.

Good commanders find ways to win. That is what makes them good. The best systems in the world will not make a poor tactician or strategist good, nor will they enable them to win decisive battles. Just as the acquisition of more capable ships, aircraft, and weapons assures us no automatic victory, having the "best" C^{4}ISR does not assure success. Certainly, effective C^{4}ISR is a necessary condition for effective warfighting, but in and of itself it is insufficient to guarantee military success. However, optimal C^{4}ISR will lead effective commanders to optimal decisions and success.

Our overall vision is achieving dominant C^{4}ISR—supporting effective commanders by reducing the fog of war for them while increasing it for the enemy. The goal of this document is, foremost, to provide NRaD's scientists, engineers, and managers a coherent insight into that vision so that we can understand how each of our tasks supports realization of the vision.

Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C^{4}ISR)—Integrating disparate units and functions into coordinated operational capabilities.

Information Dominance—Providing the warrior sufficient and timely information and associated tools to plan and execute effectively while denying—through both active and passive means—the enemy adequate information on which to plan and execute effectively.

The Changing Environment

Forward bases are being lost because of shrinking budgets and growing nationalism. The lack of a superpower threat and economic considerations have forced the Pentagon to rethink roles and missions. During the Cold War, Navy thinking was based on defense. The tactical world was seen as a set of defensive warfare mission areas. Anti-submarine warfare, anti-air warfare, and anti-surface warfare were the "hot ticket" items. Amphibious warfare and mine warfare were given secondary attention. With the demise of the Soviet Union, thinking began to change—from forward basing to forward deployment—from "anti-warfare to pro-warfare," that is, *pro*mote our national objectives, *pro*vide forward presence, *pro*ject force as needed, and, finally, *pro*tect our own forces (which includes all the earlier "anti's").

Deployed Navy and Marine expeditionary forces are critical, in this age of resurgent nationalism, to prevent nationalistic brushfires from escalating into raging international forest fires. The watchwords are "first on station," and whether it is Rwanda, Somalia, Bosnia, Haiti, or Iraq, the Navy must be ever vigilant and ever prepared. C^4ISR is a key ingredient in that preparation.

According to Admiral Jay L. Johnson, Chief of Naval Operations, and General Charles C. Krulak, Commandant of the Marine Corps, there are four basic tenets to international security in today's multi-polar world: *prevention, deterrence, crisis resolution,* and *war termination.* The concept is to "win" early and cheaply—to resolve crises before they escalate into major confrontations. Navy and Marine expeditionary forces can provide a powerful psychological calming or deterrent effect, unconstrained by diplomatic or territorial imperatives, during times of potential crisis. The key to prevention is our forward presence. It is also the key to deterrence. However, to achieve true deterrence *both sides* must know that our forces have the information necessary to get the job done, and that deployed forces and their superiors, up to and including the National Command Authority, have a consistent view/perception of the emerging situation and the necessary forces and will to carry out any required action. The cost savings of deterrence are nearly impossible to calculate. The savings, though, are real and are measured in human lives saved as well as dollars not spent. Crisis resolution must occur early, as a result of decisive action. The value of Navy and Marine expeditionary forces is almost inestimable. They do not require the permission of foreign governments to be on scene. The U.S. can employ these forces to take unilateral action to defuse a crisis, using whatever force is necessary to protect our national interests. Good examples of this were the Tomahawk strikes against Iraqi land targets to reinforce the "no-fly zone," and the use of naval air and missile strikes to convince warring Bosnian factions to negotiate. When flashpoints occur, it will be necessary for U.S. and allied forces to terminate the hostilities as quickly as possible. The Navy and Marine Corps presence can buy valuable time until more permanent forces can be made available.

Central to this role for the Navy/Marine team is information. Having an advantage over an adversary in timely, relevant, and correct information provides great leverage—Desert Storm tank battles are a recent military example. We call this advantage *information dominance*. Information dominance ensures that our forward-deployed forces can act with the best information at hand. *Nearly everything we do at NRaD is related, in some way, to developing and maintaining information dominance.*

Information—
The Heart of the C4ISR Vision

C4ISR is both a process and a system, or more correctly, an aggregate of systems. The process has to do with what we do and how we do it. The "system" is the worldwide network of individual hardware elements and software tools that support the decision-making process.

In the simplest terms, the process is about people making decisions in a distributed, multi-mission environment—in sufficient time to have a positive impact on the outcome of an operation. The elements of the process follow an information timeline, in the order listed on the next page. The "it" refers to relevant information.

Transforming Raw Data into Critical Understanding

Data are useful only if transformed through a process of "distillation," in which vast amounts of raw material (data) are distilled, analyzed, combined, and fused into information and ultimately into small but valuable portions of understanding.

Get It—Information is acquired through the use of non-organic and organic surveillance and reconnaissance resources and is acquired from local and remote operational and intelligence databases. Strategies of user pull and producer push are used to ensure that the right data and information go to the right individual at the right time.

Protect It—In the technologically driven world in which we live, tools and techniques to confuse, spoof, and destroy our information bases are readily obtainable. Potential and real enemies can be expected to try to cause our critical information systems to fail just prior to and during crises. We must have procedures in place to thwart such attempts. At all costs, we must ensure the integrity of our C^4ISR system and the information contained within it.

Analyze It—The major function of operational intelligence, after data and information collection, is to develop operational meaning from that information. The rapid and accurate analysis of information to obtain military relevance is key to winning the information war and is a critical piece of the C^4ISR process.

Use It—Knowledge and understanding are used to make command decisions (for example, selection of courses of action, and force assignment/resource management).

Share It—The information contained in the C^4ISR system is of little use unless it is shared among levels in the chain of command. Appropriate communications and networking, along with collaborative tools, allow such sharing to occur. It is more than merely "getting the word out," or in Navy parlance, "passing down the line." It requires sharing up, down, and laterally across the chain of command, with the goal of all relevant players achieving a common and consistent understanding.

These processes must operate continuously while we attempt to deny our adversaries the ability to accomplish them. We must also execute our decision cycle faster than our opponent in order to force him into a reactive posture.

Our vision for the future is to build a C^4ISR system of systems that provides all of these elements. The system that we envision allows users to acquire or access all necessary data. It provides tools to support analyses that transform data into information and knowledge. It provides mechanisms for using and sharing the knowledge to assess alternatives and to build consistent understanding. It protects all the processes and information, and it allows/facilitates disruption and denial of similar processes and information of hostile parties. Beyond these elements, the envisioned system *supports virtual organizations, operating out of virtual spaces and command centers anywhere, each accessing distributed information bases.* A tall order? The multi-polar world and the advancing rate of technology demand no less.

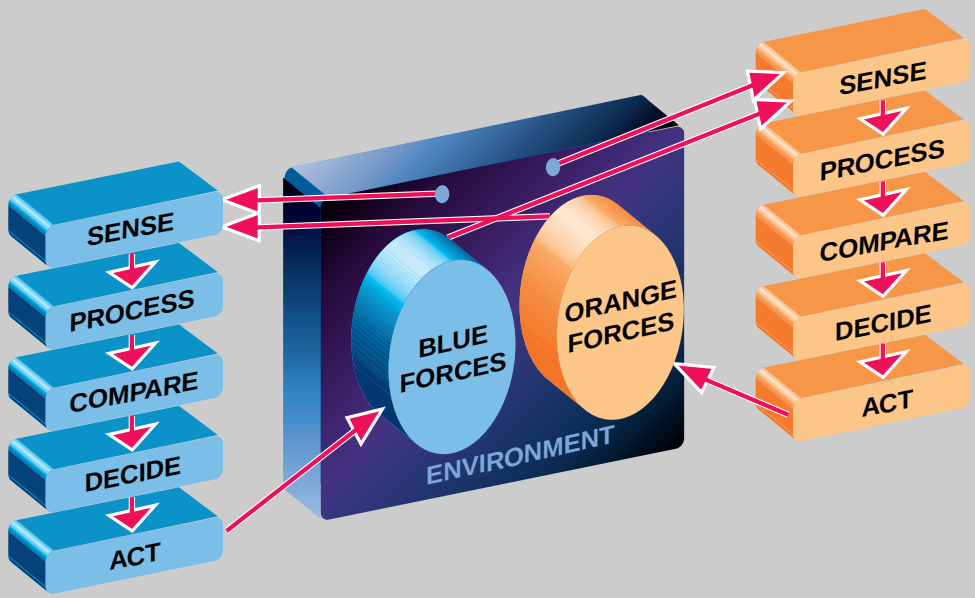
The C4I Decision Cycle

In the late 1970s, Dr. Joel Lawson, then Technical Director of the Naval Electronic Systems Command, devised a sketch of the command process as it applies to military forces. A simplified version of his concept for two opposing forces is shown below. The diagram suggests two command "cycles," one executed by blue and one by orange.

Each side performs a sensing function to "sample" the "system" (composed of the environment, our own and opposition forces, and neutral elements in an area of interest), gathering information on natural factors such as terrain and weather, and on all aspects of friendly, neutral, and hostile or potentially hostile elements. Next, the various sensor outputs are combined with other available information to form a perception of the current situation. This perceived state is then compared with a desired state as established by higher authority. The results of the comparison are inputs to a decision process in which alternative courses of action intended to alter (or perhaps maintain) the state are evaluated, and a course of action is selected. Finally, actions are taken which direct forces (and sensors). The actions alter the state of the system, and the cycle is then repeated.

Clearly this is not a simple feedback control process, since both blue and orange are attempting to alter the system state in their favor. It is also multidimensional, with multiple interactions. It is nonlinear, nonsequential, incomplete, and replete with conflicting indicators. The time to execute the command control cycle becomes critical in any warfare situation. It is highly desirable for blue to be able to manipulate the system more quickly than orange can respond, so that orange's decisions, based on poor information, are also poor—that is, benefiting blue. This implies that quality is a factor in the cycle time. The objective in terms of decision-cycle time is to execute a high-quality cycle—one that brings the system closer to the desired state—quickly.

A primary goal of command is to control the tempo of operations. Initiative in battle rests with the commander who controls the "OPTEMPO"; he will call the shots and force his adversary into a reactive mode. Acting "inside" the adversary's decision cycle—executing high-quality cycles more quickly than the adversary—is a necessary step in controlling the OPTEMPO.



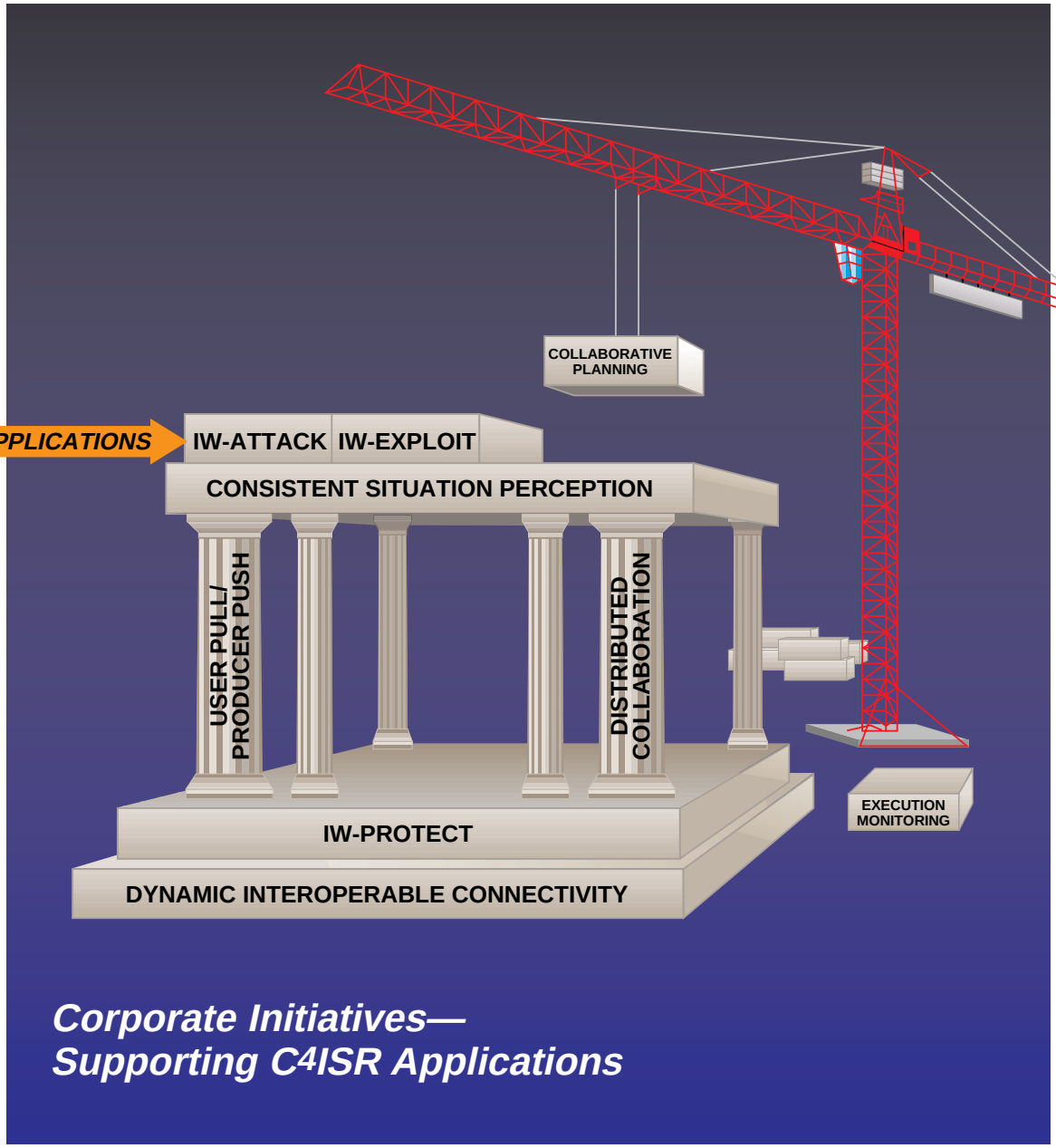
Set a Course—Acquisition to Understanding via Our Corporate Initiatives

At NRaD, we build the systems, develop the hardware and software, and integrate the pieces necessary to win the information war and achieve information dominance. Information dominance is central to modern warfare—it creates a military advantage as tactically significant as numerical end strength. Information dominance provides the warrior sufficient and timely information and associated tools to plan, observe, assess, and execute effectively, while denying—through active and passive means—the enemy adequate information on which to plan and execute effectively.

The course to information dominance is through effective C^4ISR. NRaD's vision—making information dominance a reality—is based on achieving five interrelated objectives, or Corporate Initiatives. Our first initiative, *Dynamic Interoperable Connectivity*, will provide assured connectivity, on demand, in user-selected formats, to any desired locations in the "infosphere," the worldwide grid of military databases, fusion centers, national resources, and commercial information. Given this fundamental capability, our second initiative, *User Pull/ Producer Push*, will use that connectivity to access strategically located database servers and anchor desks and provide users, at all levels, with key information. Our third initiative, *Distributed Collaboration*, will provide the tools necessary for warriors and their commanders to agree on a wide range of command-related issues. Our fourth initiative, *Consistent Situation Perception*, will facilitate a consistent tactical understanding, or consistent perception, of the operational situation. Our fifth initiative, *Information Warfare*, will protect our information resources while denying our enemy the information needed to implement aggressive actions.

The course to information dominance is through effective C^4ISR. NRaD's vision—making information dominance a reality—is based on achieving five interrelated objectives, or Corporate Initiatives.

C^4ISR requirements for operational forces derive from the roles and missions assigned to those forces, the force composition, force capabilities, and operational doctrine. Operational C^4ISR depends on an underlying command structure. To support operations, our system capabilities must span the entire range of roles, missions, organizational structures, and politics, or any subset of these.



The five NRaD Corporate Initiatives form the core capability for information dominance. The Corporate Initiatives are interdependent—all five are required as a set in order to provide the operational command with the tools needed for successful command and control:

- Without Dynamic Interoperable Connectivity, User Pull/Producer Push is not assured.
- Without User Pull/Producer Push and Distributed Collaboration, Consistent Situation Perception within a defined battlespace cannot be achieved.
- Without the first four initiatives, planning and replanning of operations cannot take place, nor can those plans be executed in time synchronization.
- Without protective Information Warfare, these initiatives and our ability to perform command and control can be lost.

Dynamic Interoperable Connectivity

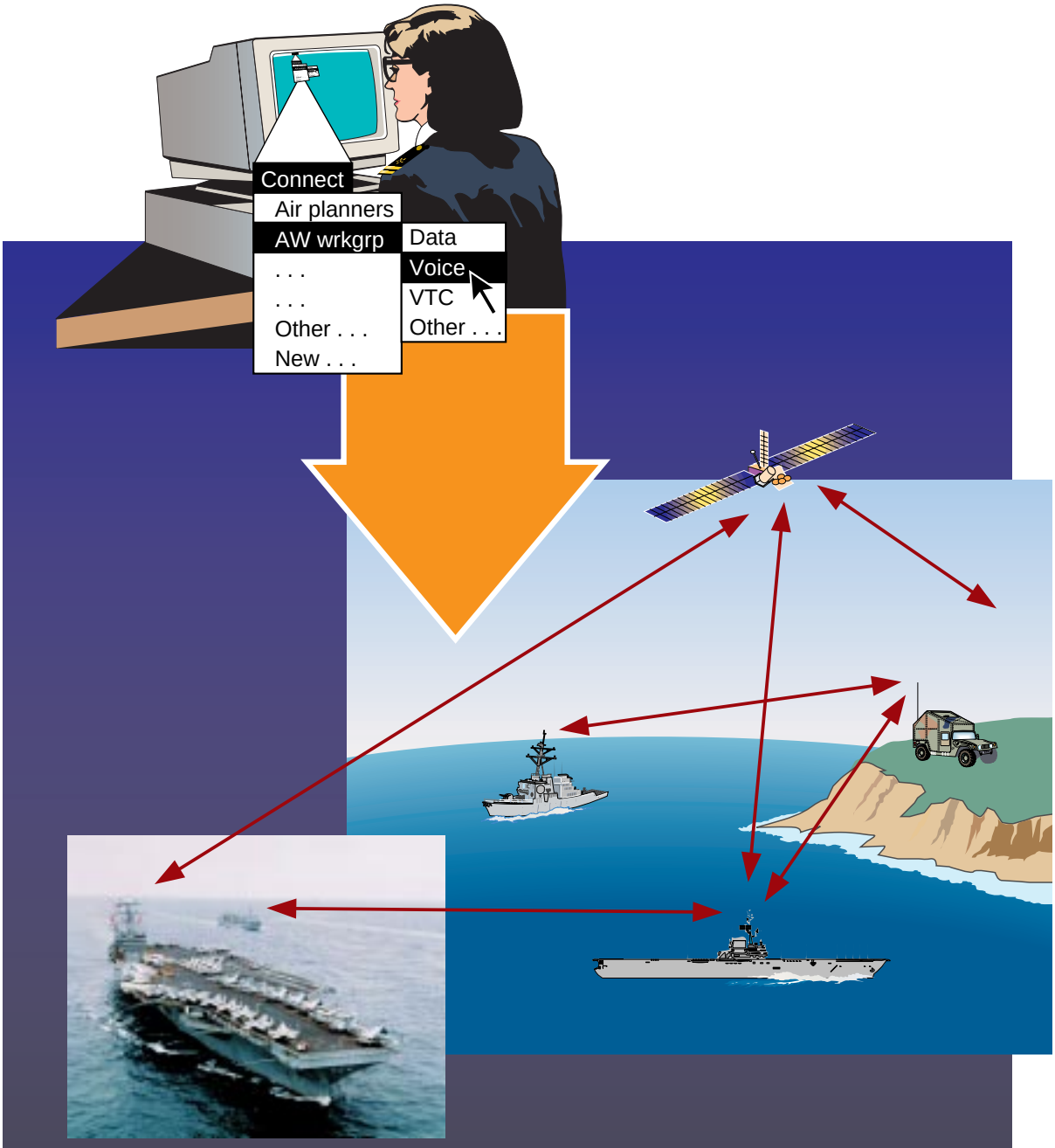
Dynamic Interoperable Connectivity is the conduit for all data and information, whether that information moves 15 feet or 15,000 miles. The Dynamic Interoperable Connectivity initiative aims to ensure that the warrior has reliable and secure access to all needed information. Now and for the foreseeable future, the number of possible connections and the capacities of those connections between mobile nodes will fall short of total user demands. Therefore, the command organization must provide dynamic mechanisms for allocating available resources to users based on mission and operational needs.

Timely information availability is critical to command and warfighting processes. The methods of information sharing—what is needed and when it is needed—are determined by the user. Therefore, users must control connectivity.

Not all connectivity users are people. Machines also must exchange data. Connectivity supporting machine data exchange has been accepted Navy practice for the four decades since the introduction of the Naval Tactical Data System and Link 11. Connectivity can involve any number of people and machines, in various locations, as required to accomplish a task.

Now and for the foreseeable future, the number of possible connections and the capacities of those connections between mobile nodes will fall short of total user demands.

Dynamic connectivity is flexible, supporting the time-varying needs of users. But it is also economical, supporting the sharing of resources. The telephone is a useful analogy. Telephone connections are dynamic, with all resources, from user handsets through physical links and central switches, shared among many users. This allows a given set of resources to provide service to many more users than could be supported by dedicated static resources. In addition, many users are part of a multi-user community that requires connectivity functions. Yet each user seldom performs all the functions, all the time. When only part-time participation is required, tracking time-shifting task assignments appropriately not only provides better use of bandwidth but reduces workload and improves efficiency for each user.

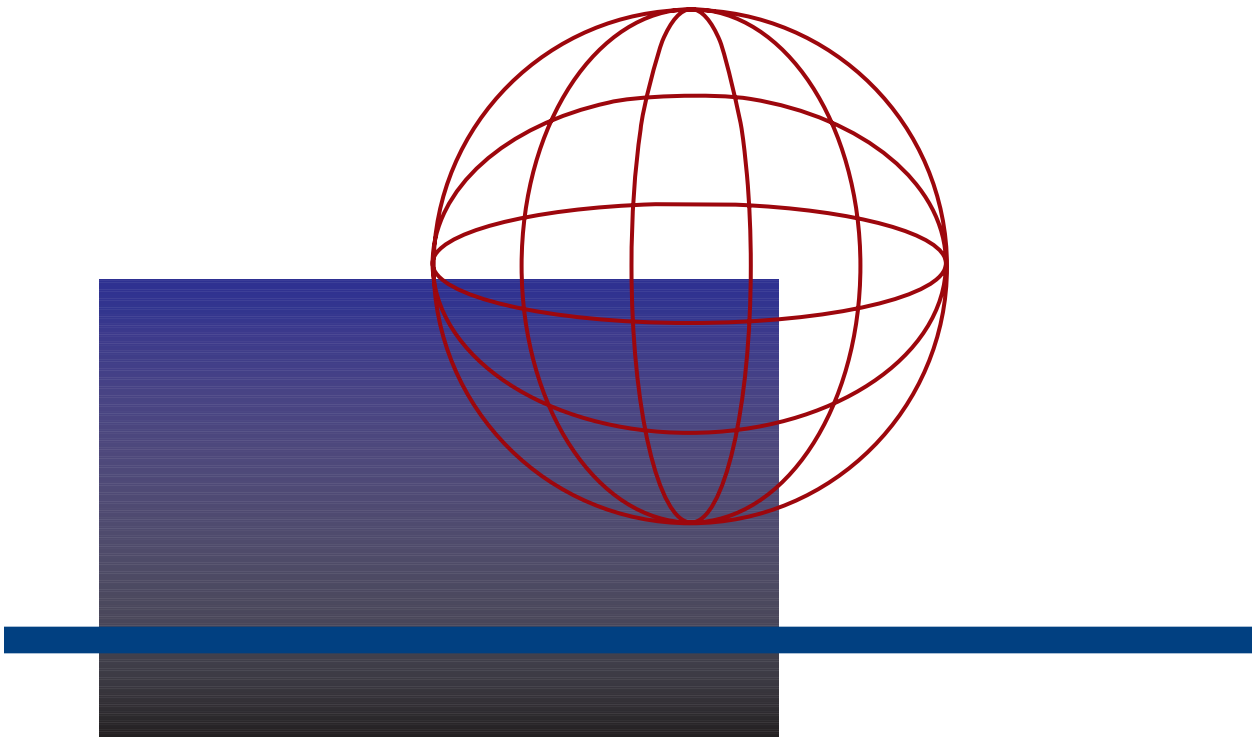


Dynamic Interoperable Connectivity is user-demand responsive in connectivity (endpoints), information format, quality of service, throughput, and real time.

Connectivity is required between mobile naval nodes, among both fixed installations and mobile naval forces worldwide, and with non-naval locations worldwide. The non-naval locations include other Services; other U.S. Government installations, facilities, and nodes; allied forces and locations; commercial and educational entities; and even hostile forces under some circumstances. These connectivities require varying levels of security, timeliness of connection establishment, timeliness of information transfer, duration of the user–user interaction, robustness against unintentional or intentional disruption, information integrity or accuracy, covertness, and simultaneity (conferencing).

Interoperability is critical. Users define connectivity in support of common activities. When the community of users extends beyond Navy boundaries, interoperability based on the standards of the larger community is required. Supporting interoperability demands the ability to exchange information and commands between users. This in turn places demands on all of the underlying procedures, processes, and hardware at every level. Interoperability implies a common (human or machine) language, common security methods and shared “keys,” common protocols, and common modulation formats or methods. Where these items are not shared in common, translation mechanisms must be provided.

Some resources needed to support Dynamic Interoperable Connectivity are inherently limited. Spectrum must be shared among surveillance, navigation, identification, communications, command control warfare, and weapons systems. Physical space for communications equipment is limited, and today’s radio systems (cryptographic device, modem, transmitter/receiver, antenna coupler, antenna) are usually dedicated to a single user or group. A goal for Dynamic Interoperable Connectivity is to eliminate dedicated equipment and spectrum. Shared use of equipment and spectrum will increase efficiency, expand the number and types of users having communications access at any given time, and reduce costs. An additional goal of Dynamic Interoperable Connectivity is to reduce communications mutual interference.



User Pull/Producer Push

NRaD is developing new information technologies to provide the warrior, or user, with expertise and tools for making information dominance a reality. While these technologies enable advanced methods for information transfer and a digitized display of the battlespace, it is the user who thinks, plans, and executes a mission. Any technology improvement or solution must consider the user as the most important resource for any mission.

User pull is a capability that allows the warrior dynamic access to specific information needed for mission performance. Connectivity to the infosphere must seamlessly provide a timely response to the warrior's request.

Producer push allows command centers and intelligent sources to direct and inform the warrior with commands and data specific to his operation. With large volumes of data available, control of information flow is essential to avoid overwhelming the recipients. A filtering process is required to alert the user to critical incoming information. Anchor desks serve as a support information infrastructure at the command or functional level and control the volume of information distributed to the warrior. Equally significant, these desks provide for human interaction with the warrior.

The tools being developed for User Pull/Producer Push focus on display systems because they remain the primary interface to information. Research in human–system interface technology is rapidly evolving to make display tools simpler and more natural to use. Such tools include a compact warrior terminal, improved video/graphic capabilities, and intelligent search agents for accessing data sources in the infosphere. The design of these software tools and expert systems will allow the warrior to obtain, understand, and process the right information for his operation without requiring him to have knowledge of system architecture or connecting paths.

Any technology improvement or solution must consider the user as the most important resource for any mission.

While the concept of User Pull/Producer Push focuses specifically on the user, its realization is enabled by supporting technologies in surveillance, operational planning and execution, and network communications. Dynamic connectivity with the infosphere is essential for acquiring information on demand and conducting mission planning. This connectivity must allow interoperability among data systems and provide for time-critical and high-volume data to be received by the user at any time.

INFORMATION
EVERYWHERE

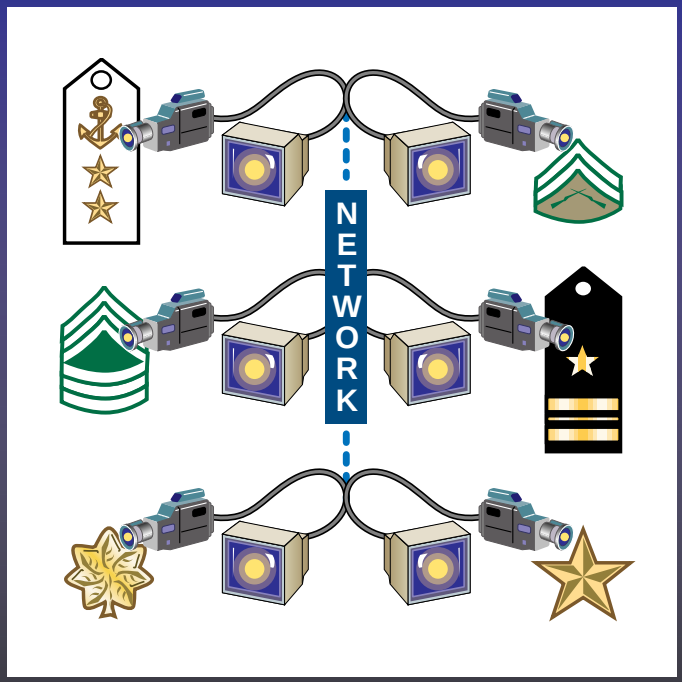
USERS
ANYWHERE

Distributed Collaboration

The Distributed Collaboration initiative envisions improved computer-based technologies that enhance the warrior's ability to conduct distributed, multi-echelon, multi-force C^4ISR at any level of conflict. NRaD is exploring technologies to provide a distributed collaborative work-space supporting situation assessment during uncertainty, continuous planning and replanning, execution monitoring, localized plan repair, and team decision-making.

Distributed Collaboration must support a varying operations tempo—from minutes to make a decision, to days for planning—anytime, anywhere, with a mix of Services, federal agencies, and countries. Collaboration must support not only warfighting but also operations other than war. Collaboration will be among peers and across operational expertise, up and down echelons, and across all critical functions; for example, operations, sensor management, and logistics. The size of groups may be a few individuals to teams of teams. Coordination and collaboration are much more complex and far reaching than it used to be.

The technological challenge in supporting new command and control concepts is to get the right information in a usable form into the hands of the warrior in a manner that allows for faster and more accurate situational assessment and response than the enemy can achieve. The goals of Distributed Collaboration are:

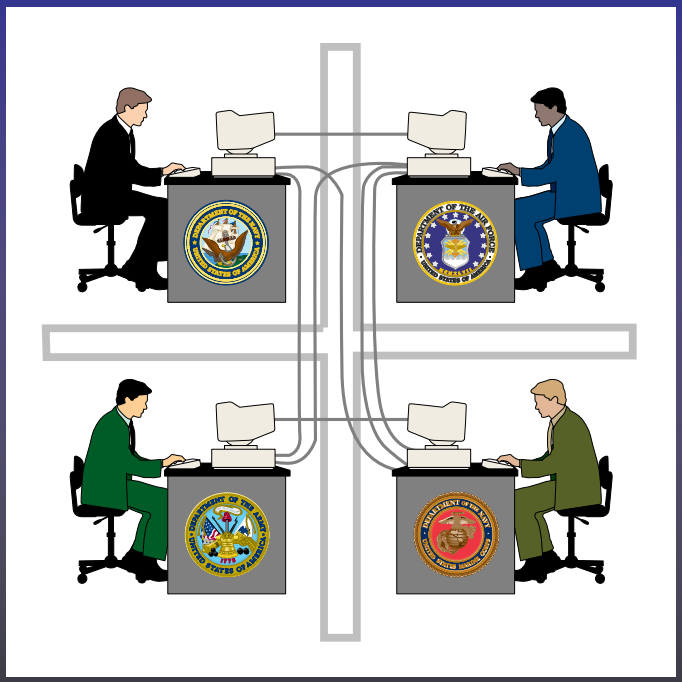


TOOLS AND CONNECTIVITY FOR COLLABORATION

- To collaboratively achieve understanding of the operational situation.
- To collaboratively plan early to gain advantage over the enemy's decision cycle.
- To command or operate from any location by deploying tailored force packages.
- To dynamically synchronize force operations by collaborative execution monitoring, repair, and integration of shared assets across echelons, missions, components, and coalition forces.

Collaboration allows for augmentation (for example, several planners doing the job in one day vice one person working many days), integration of multiple specialists' knowledge, and debate to reach a better decision. Collaboration requires trust, which develops with time, proximity, and shared experience. The sociology of cyberspace is embryonic in understanding how collaboration in a computer-mediated and abstracted reality will support the development of trust.

The initial technological support for collaboration was to replicate an office meeting for a physically distributed membership via videoconferencing, shared whiteboard, and presentation software. Such support is comfortable in its familiarity, including the ability to read body language. In a relatively relaxed pace of hours or days, Commanders-in-Chief tend to like this type of collaborative support. In the future, these distributed meetings will also be able to take advantage of information technology for smart information retrieval and analysis (intelligent agents), groupware decision support, and shared interactive 3-D and augmented displays.



TRANSPARENT INTERACTION

Ultimately, computer abstractions representing relevant attributes such as agency or specialty, and perhaps even “body language,” may more quickly and precisely convey interpersonal exchanges. Machine-mediated synchronous and asynchronous collaboration, as well as abstract representations of space, time, and people, will likely increase.

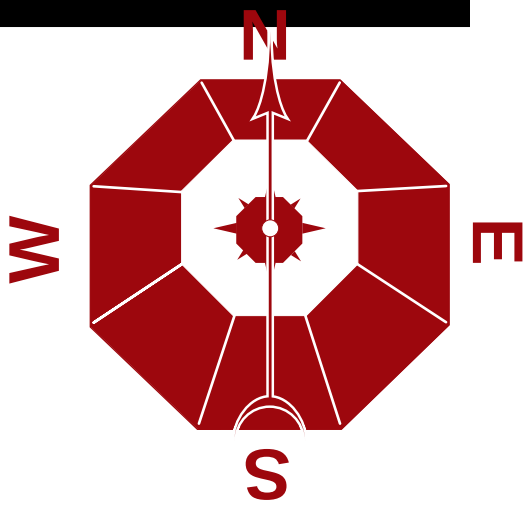
Warriors work within the more stringent time constraints of seconds to hours. They want the ability to rapidly access experts and relevant changing information, to contribute to and acquire an understanding of the situation, to instantaneously replan with all players as the situation requires, and to monitor and report execution. As noted in the User Pull/Producer Push section, any information or expert should be accessible. Collaboration tools add the capability to also share understanding and to decide and act in unison regardless of physical and organizational boundaries.

Distributed Collaboration provides an infrastructure for interaction that must become part of the Global Command and Control System (GCCS) and Joint Maritime Command Information System (JMCIS) core. This infrastructure must support the full range of applications from sensor collection to shooter execution as well as other operations management tasks such as planning and logistics.

Our vision of Distributed Collaboration requires technological enhancement to the collaborative infrastructure. A collaborative virtual environment is an interactive, computer-generated environment that supports multiple users both synchronously and asynchronously performing their jobs. The virtual multimedia workspace is a smart, virtual environment where one can integrate customized, automated work mechanisms with distributed human expert collaborative activities. A graphical, intelligent, multi-person cyberspace should support group decision-making, information retrieval, shared situational awareness, assessment, planning, and execution monitoring scalable to all echelons. Near-term implementations use commercial off-the-shelf Internet browsers with JAVA-based applets and multimedia graphics as the core. Within the workspace, warriors need an enhanced capability to continuously plan and replan operations. Required capabilities include:

- Shared plan representation linked to a central strategy with distributed, collaborative plan generation and refinement.
- Common, integrated map-based and logic/time-based plan presentation and interaction.
- Shared objective decomposition and concurrent plan development with conflict resolution.
- Proactive planning via modeling and simulation of options.

In addition, real-time, distributed object management capabilities and repositories for retrieval of plans and interactions are required.



The technological challenge in supporting new command and control concepts is to get the right information in a usable form into the hands of the warrior in a manner that allows for faster and more accurate situational assessment and response than the enemy can achieve.

Consistent Situation Perception

Consistent Situation Perception is the desired result of the processes of tasking, collecting, evaluating, disseminating, and displaying information for military use in all warfare areas. It encompasses the old “Who, What, When, Where, and Why” and adds several new features. Consistent Situation Perception is both a “process” and a “view.” The process involves getting the right information to the right people at the right time. The shared view is the common operating picture.

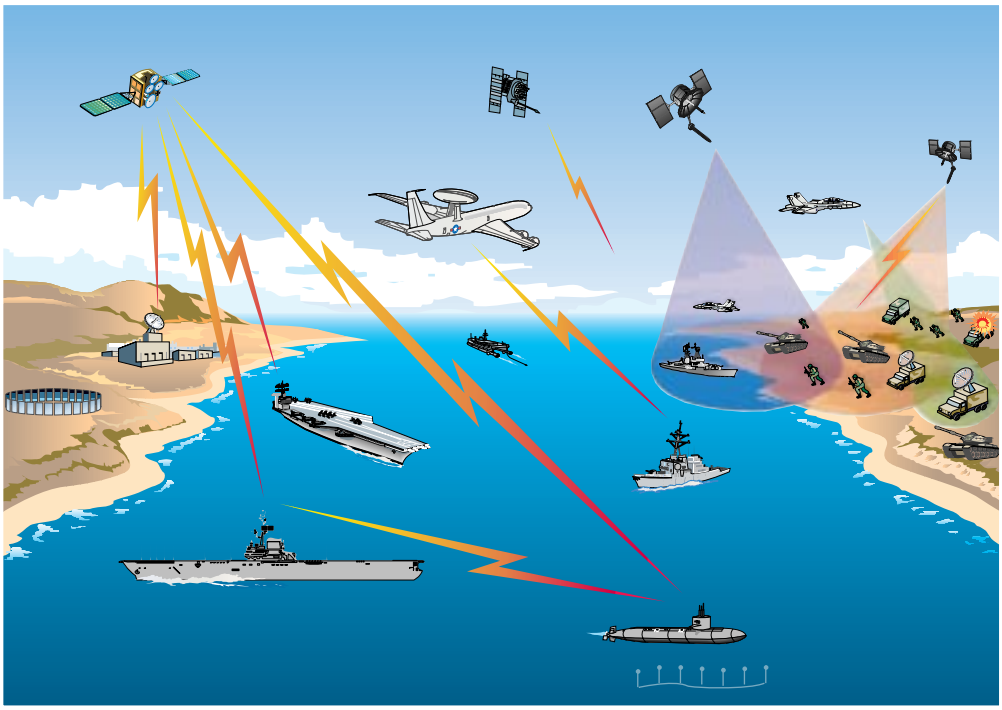
There are three thrusts for Consistent Situation Perception. The first thrust is development of new sensors to gather more data. The real emphasis here is that an increased volume of data and stronger fusion engines will yield more useful, accurate information. The second thrust is fusion of intelligence, surveillance, and reconnaissance data to produce the common operating picture. The third thrust is real-time management, display, and dissemination of the common operating picture.

The Consistent Situation Perception process is a continuum of national, theater, and organic sensor tasking, data collection, data fusion, data analysis, and dissemination of tailored information to users/decision-makers at all echelons of command. Inherent in the overall Consistent Situation Perception capability is a C^4 architecture that facilitates the timely delivery of information so that it can be used effectively.

Consistent Situation Perception is much more capable and yet more disciplined than its predecessors. The Consistent Situation Perception’s common operating picture is an interactive, scalable, 3-D, audio, and visual representation in a geographical/spatial format. Users/decision-makers can select and see past, present, or future projections of activity and tactical situations. Users can task sensors for data feedback that will meet tactical timeline requirements. Red, white, or blue ground, naval, air, space, and other assets can be selected and viewed individually or in combinations. Standard military symbology is used; however, functional symbology (a ship looks like a ship) can be selected. This feature is very useful in reconstructing historical events and briefings. Audio can also be selected and employed to complement certain video representations; for example, warning of hostile weapon system threat radius. Users can also use voice commands in lieu of point-and-click mouse commands. All-source and GENSER-releasable common operating pictures are generated automatically and simultaneously.

An additional data sort and view option is available in the common operating picture: (1) all data regardless of sensor source or accuracy or (2) accurate data only. Since data validity and accuracy are relative, quality parameters and data sensor type can be set by the user. For tactical warning applications, data display speed takes precedence; accuracy follows close behind. In non-tactical situations, the reverse is usually desired.

Along with the view, users have direct access to underlying textual information and the ability to interface “live” by voice conference or keyboard with distributed anchor desk experts. Instead of timely, accurate data, the real-world intelligence situation is often the paucity of data, spurious data, or conflicting information. Even though pattern recognition and modeling are also common operating picture features, it often takes a knowledgeable user to provide accurate estimates of activity when available sensors are not producing what is needed to fill the pattern or model.



Sensors, spanning the electromagnetic and acoustic spectra, monitor the total environment of natural and man-made events and objects. The sensors and other sources provide data on our forces, hostile forces, neutral elements, and nature. These data are fused and interpreted to form knowledge and understanding of events, trends, and intentions. When the resulting knowledge and understanding are shared appropriately, the result is Consistent Situation Perception.

Information Warfare

The Department of Defense (DoD) must be prepared for missions along the entire spectrum from peace to war, including military operations other than war, such as peace-keeping and humanitarian operations. These operations can be opposed by a wide range of adversaries, including State and non-State entities. To meet this challenge, DoD elements must be organized, trained, equipped, and supported to plan and execute Information Operations across the conflict spectrum.

Recently defined by the Assistant Secretary of Defense for C^4I, the goal of Information Operations (of which Information Warfare is a subset) is to secure peacetime national security objectives, deter conflict, protect DoD information and information systems, and shape the information environment. If deterrence fails, Information Operations becomes Information Warfare and seeks to achieve or ensure U.S. information superiority or dominance to attain specific objectives against potential adversaries as times of crisis and/or conflict arise. Like Information Operations, the goal of Information Warfare is to promote freedom of action for U.S. forces while hindering adversary efforts—to affect adversary information and information systems while defending one's own information and systems. Defending information systems is known generally as "information assurance"; this includes all means that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This also includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities and, in times of crisis or conflict, limiting or destroying information systems of a specific adversary or adversaries to achieve or promote specific objectives.

Focusing on the conflict portion of the Information Operations spectrum, Information Warfare promises to transform how wars are fought, just as air power once transformed the geography of warfare by extending the reach of conventional weaponry. Every point in the infosphere becomes a possible site of attack or counterattack. On the battlefield, information is the lifeblood of command and control. Military forces, in turn, are highly dependent on command and control for the effective application of combat power. This dependence creates opportunities to enhance our military power by directing offensive Information Warfare against an adversary's information-based systems, processes, and computing. Conversely, it creates vulnerabilities for our own command and control unless it is adequately protected from such attacks. The actions of a commander to realize the practical benefits of offensive and defensive Information Warfare on the battlefield comprise command control warfare (C^2W).

Integrated, mutually reinforcing plans and operations are an essential component of effective C^2W. Although C^2W is still a relatively new and evolving warfare area, it integrates several long-standing warfare disciplines, including electronic warfare, military deception, psychological operations, computer and information security, and operations security. Surveillance, intelligence, communication, and computing also are used to execute C^2W actions. The information warrior requires visibility into the total infosphere analogous to commanders' needs in other warfare areas to know about platform positions and movements, weapons use, and supply levels. Our own command and control systems will provide comparable visibility into Information Warfare actions and resources. Coordination among system developers throughout product life cycles contributes further to the integration of our capabilities across the three key

facets of C^2W: *Information Warfare–Exploit, Information Warfare–Attack,* and *Information Warfare–Protect:*

- *Information Warfare–Exploit* uses signals intelligence or other means to acquire information directly from an adversary. The products resulting from exploiting this information contribute to our commanders' situation perception and understanding, for use in follow-on C^2W actions or other operations.
- *Information Warfare–Attack* includes actions that deny, disrupt, or physically destroy command and control targets, with the intended effect of degrading the quality and tempo of an adversary's decision-making.
- *Information Warfare–Protect* defends against the exploitation of our own information by such means as encryption, firewalls, or physical isolation. Information Warfare–Protect also counters intrusions, misuse, deception, and other types of attack, preventively where possible, and otherwise through timely detection and containment of an attack and recovery from its effects.

NRaD's focus in supporting the DoD Information Warfare effort is the research, development, test, and evaluation of features of the information infrastructure, including automated information systems such as C^4 systems that serve the needs of the National Command Authority and operating forces under all conditions of peace and war. Within the total information environment, the information infrastructure includes the aggregate of individuals, organizations, and systems that collect, process, or disseminate information, including the information itself.

The C4ISR System of Systems—Attributes

Admiral William A. Owens, U.S. Navy, (Ret) made the following observations in his landmark paper, "The Emerging System of Systems":

> *The most profound implication of the new era, with the collapse of the Soviet Union, goes almost unnoticed. It is, namely, that the basic rationale for defense planning has shifted from threat to capability and from liability to opportunity.*
>
> *Now, we are freer to think in terms of shaping the future . . . we must design military forces more specifically in terms of their political purposes. In short, we must rebuild an intellectual framework that links our forces to our policy . . . .*
>
> *Each of the military services has wrestled with these issues over the past few years. Much of what they are saying to themselves runs in parallel. Read the flagship pronouncements of each of the military services: the Army's descriptions of Force XXI, the Navy's "Forward . . . From the Sea," the Air Force's "Global Reach, Global Power," and the Marines' "Operational Maneuver . . . From the Sea." The visions they sketch are remarkably similar. Each points toward the capacity to use military force with greater precision, less risk, and more effectiveness. Each relies on three areas of technology:*
>
> - *Intelligence, Surveillance, and Reconnaissance (ISR).*
> - *Advanced command, control, communications, computers and intelligence (advanced C4I).*
> - *Precision Guided Munitions (PGMs).*
>
> *The interactions and synergism of these systems constitute something new and very important . . . it is the creation of a new system of systems.*

We can and must rise to the challenge of producing the overarching, integrated C4ISR system on which the success of our warriors and the effectiveness of their weapons so critically depend.

A number of attributes are desired in the C4ISR system of the future. The list of these attributes is open-ended. Attributes can be added as they are identified, and as technology permits their realization. The attributes discussed below—*user-centric and intuitive, integrated, interoperable, seamless, consistent and scalable, adaptable/configurable/tailorable,* and *survivable*—represent the set of what appears to be achievable based both on the current baseline of systems in the operational world and the state of current and emerging technology.

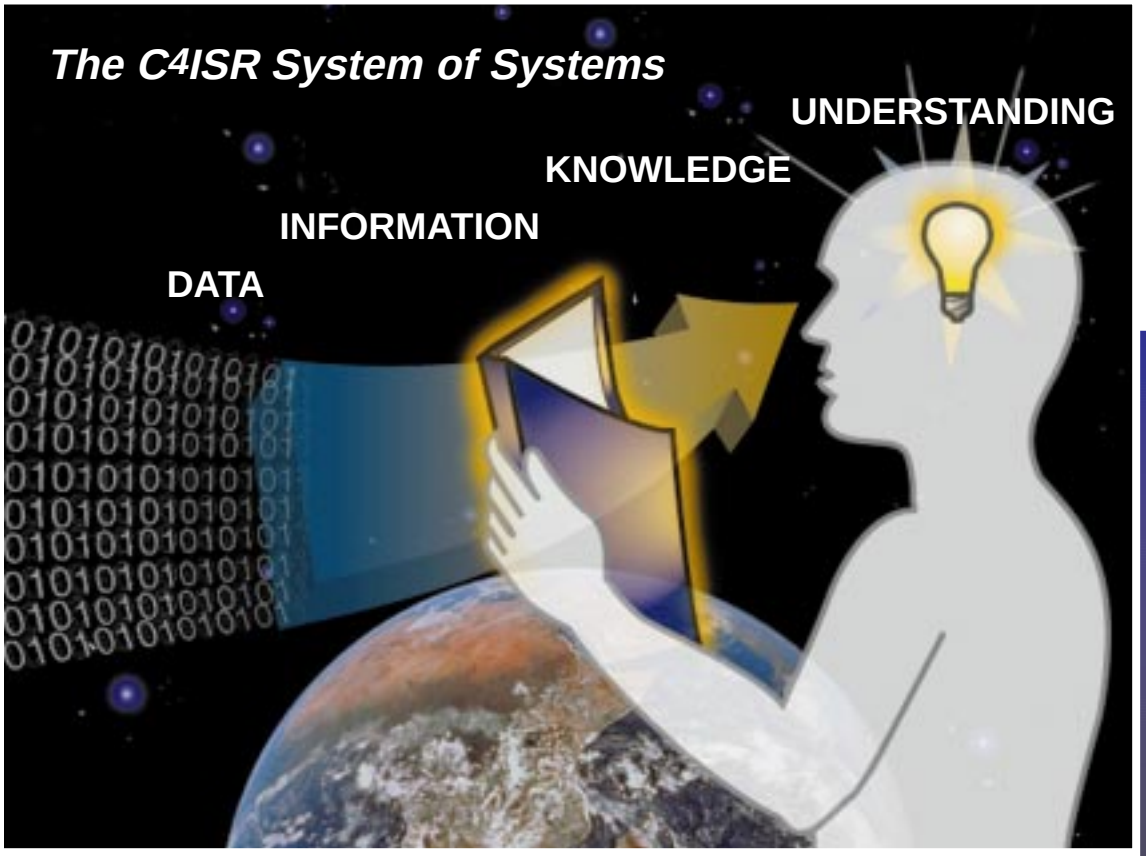
User-Centric and Intuitive—*User-centric* means that the C4ISR system of systems will be built for and focus on the needs and requirements of users at all operational levels of command. This is not a new concept. However, there has been criticism recently from deployed forces that the wide array of advanced communications and intelligence systems (for example, as used in Bosnia) has helped the higher echelons of the chain of command while the on-scene combatants have not received the benefits of new technologies. The user-centric attribute of the emerging C4ISR system of systems acknowledges that technological benefits must be provided to users at all echelons, from top to bottom, if we are expected to fight more

effectively, and win. To make this happen, the entire C^4ISR architecture will be reviewed. As a result, some adjustments may be necessary. Bandwidths may be increased and/or adjusted in certain areas, obsolescent equipment replaced, and new equipment issued to those echelons and units that need modern C^4ISR to enhance their efficiency and survivability in the battlespace.

In view of the extremely rapid pace of technological development, the growing challenge for DoD and commercial C^4ISR theorists and technologists is to involve users/decision-makers throughout the systems development process so that they can (1) understand the breadth and scope of the emerging technologies, (2) visualize applicability of the technologies to real-world C^4ISR situations, and (3) provide a continuum of substantive input into the creation of the C^4ISR system of systems.

Interestingly, acknowledging *user-centric* as one of the main attributes of the C^4ISR system of systems also means that capability and power are shifting inexorably toward functional users.

Ergonomics is the study of equipment design aimed at reducing operator fatigue and discomfort. As a design characteristic of the C^4ISR system of systems, “intuitive” can be described as mental ergonomics, meaning that the system will consider and incorporate features that will make it physically and mentally easier to operate. Compared to earlier computer systems, it should reduce or eliminate mental stress and “cyberphobia,” even with novice users. To accomplish this, the C^4ISR system of systems must be logical, functional, and robust. A goal is to make it so innately “friendly” that users will not need formal instruction in its operation and usage. Overall, the purpose of the *user-intuitive* attribute is to make the system operate on a level of convenience and performance such that virtually anyone can use it.



Supporting the user is a worldwide system of systems containing all the information necessary for him to gain knowledge and achieve understanding.

Integrated—"Integrate" is commonly defined as "to make into a whole by bringing all parts together, or to unify." Within the context of the C4ISR system of systems, *integrated* means, in essence, that every component and all echelons can be electronically joined, connected, or networked to provide rapid access to the information, service, or point of contact required by a user.

C4ISR integration goals will permit connectivity that is defined by communities of users, not by distances or physical communications media. It might involve two users in adjacent offices or compartments connected by copper wire (perhaps a person operating a work station, and a database), or it might involve many users throughout the region working on a common problem connected by a mix of submarine fiber optics, wire lines, and satellite radio links—for example, a group of sensors, processing algorithms, databases, and analysts tracking surface ships in the Pacific Ocean.

The integration effort encompasses all sensors: naval, air, ground, and space forces; joint forces; and allied military resources. Service components and DoD organizations are performing the necessary analysis and system engineering in order to implement the integration objectives found in the evolving C^4ISR architecture documents such as “Copernicus,” “Sonata,” “C^4I for the Warrior,” and “Forward . . . From the Sea.”

Interoperable—Joint Chiefs of Staff Pub 1-02 provides two definitions of *interoperable*, both of which are applicable to the evolving C^4ISR system of systems:

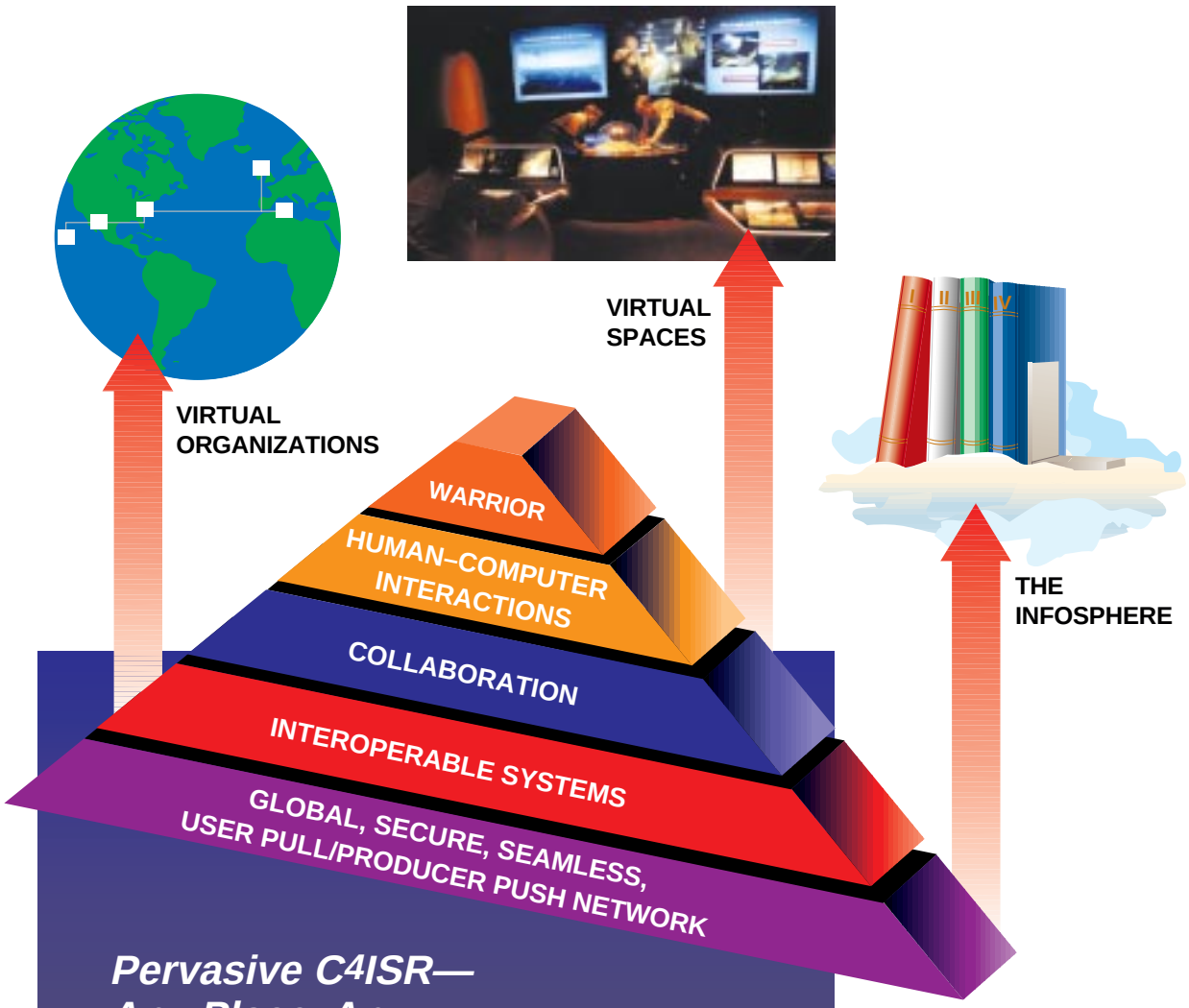
> *The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together.*
>
> *The condition achieved among communications–electronics systems or items of communications–electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users.*

Interoperable also implies a basis of commonality.

The U.S. Services (joint forces) must operate together effectively if we have to fight. Warriors cannot fight separately and expect to win, particularly in an era of reduced military manpower and austere DoD budgets. Interoperability is further amplified in terms of operating in concert with friendly and allied forces. In the future, we must be able to participate fully as part of a formal multinational response or as part of “ad hoc” coalitions forged to react to short-notice crisis situations similar to Desert Storm. Participation in both NATO Standing Naval Forces and in a variety of exercises with the navies, air forces, and land forces of coalition partners around the Pacific rim, Norwegian Sea, Arabian Gulf, and Mediterranean basin also provides solid foundations for sustaining interoperability with our friends and allies. Additionally, the outreach to the former Warsaw Pact countries in the NATO Partnership for Peace program is building both solidarity and interoperability. We have already made progress in expanding and intensifying our cooperation in Eastern Europe with exercises such as the BALTOPS and BREEZE series with units from Bulgaria, Estonia, Latvia, Lithuania, Poland, Romania, Russia, and Ukraine.

The building blocks of the C^4ISR system of systems include common language (human or machine), common input data formats, common protocols, common processing, common modulation formats or methods, standardized output reporting, and common security methods and shared “keys.” Where these items are not shared in common, translation mechanisms must be provided, as noted in the Dynamic Interoperable Connectivity section. Overall, this is a difficult and expensive task, particularly when other countries are included in the matrix. Often, these countries have manpower to offer, but lack the training and funding necessary to make them technological partners in the efforts.

Programmatically, interoperability as a C^4ISR system attribute is also important. The opportunities to capture new technologies already funded by other services, industry, or allies can greatly leverage our investments, with a corresponding opportunity for reducing program cost.



Pervasive C4ISR—Any Place, Any Time Frame, Any Organizational Structure

Resting on the foundation of a global, protected network of information servers, the C4ISR capability we envision will provide the best information to our warriors, and the support tools to most effectively use that information to our fullest advantage in the execution of any or all missions.

Seamless—Seamlessness is a particularly important attribute in the dynamic operations of the Consistent Situation Perception and User Pull/Producer Push concepts. *Seamless* is defined here as electronic connectivity transparency. Operationally speaking, this means that users need not be concerned with how to get information or where it is located. Systemic, procedural, and administrative boundaries around functional disciplines will, in effect, disappear to the user. Seamlessness will support interdisciplinary interactions between battlespace sensors, communications, and weapons systems. The seamless attribute is applicable to joint and combined forces, all echelons of command, and multi-level security. System communications protocols and interface standards will continue to be invoked; however, the seamless attribute will permit this to be accomplished automatically and with great speed. Practically speaking, this means that users/decision-makers can focus more on information and task and less on the connectivity and process when obtaining information.

The attributes represent the set of what appears to be achievable based both on the current baseline of systems in the operational world and the state of current and emerging technology.

Consistent and Scalable—*Consistent* is defined as uniform and applies primarily to the common operating picture. It means that the uniformity of the common operating picture's data content and information presentation will be clearly understood across all echelons of command. In effect, this will get all users/decision-makers "on the same sheet of music."

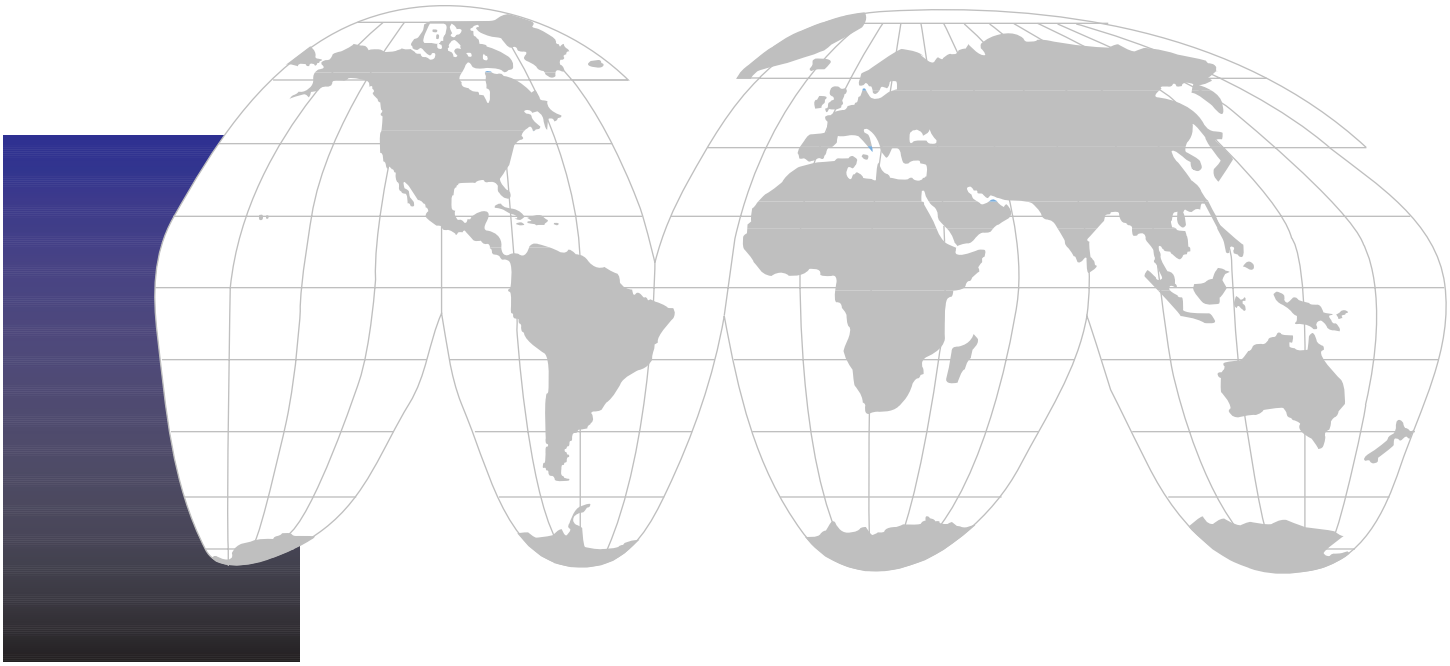
Scalable is defined as flexible in size, modular, or distributed and means that both the Consistent Situation Perception process and the common operating picture can be sized or scoped to fit the particular situation in which it is being applied. Starting from a global perspective, the Consistent Situation Perception/common operating picture can manage data and information in decreasing subsets of time, space, composition, tasking, and echelons of command down to the level of unique, individual C^4ISR users/decision-makers.

Adaptable/Configurable/Tailorable—From a C^4ISR user's viewpoint, *adaptable/configurable/tailorable* means that the system, in supporting both the Consistent Situation Perception and the common operating picture, will be totally responsive to the user's unique requirements for information to support specific missions, tasks, or functions. This attribute will encompass the entire spectrum of time, space, sensor tasking, data accuracy, and data classification for U.S. and friendly/allied forces.

58
AG

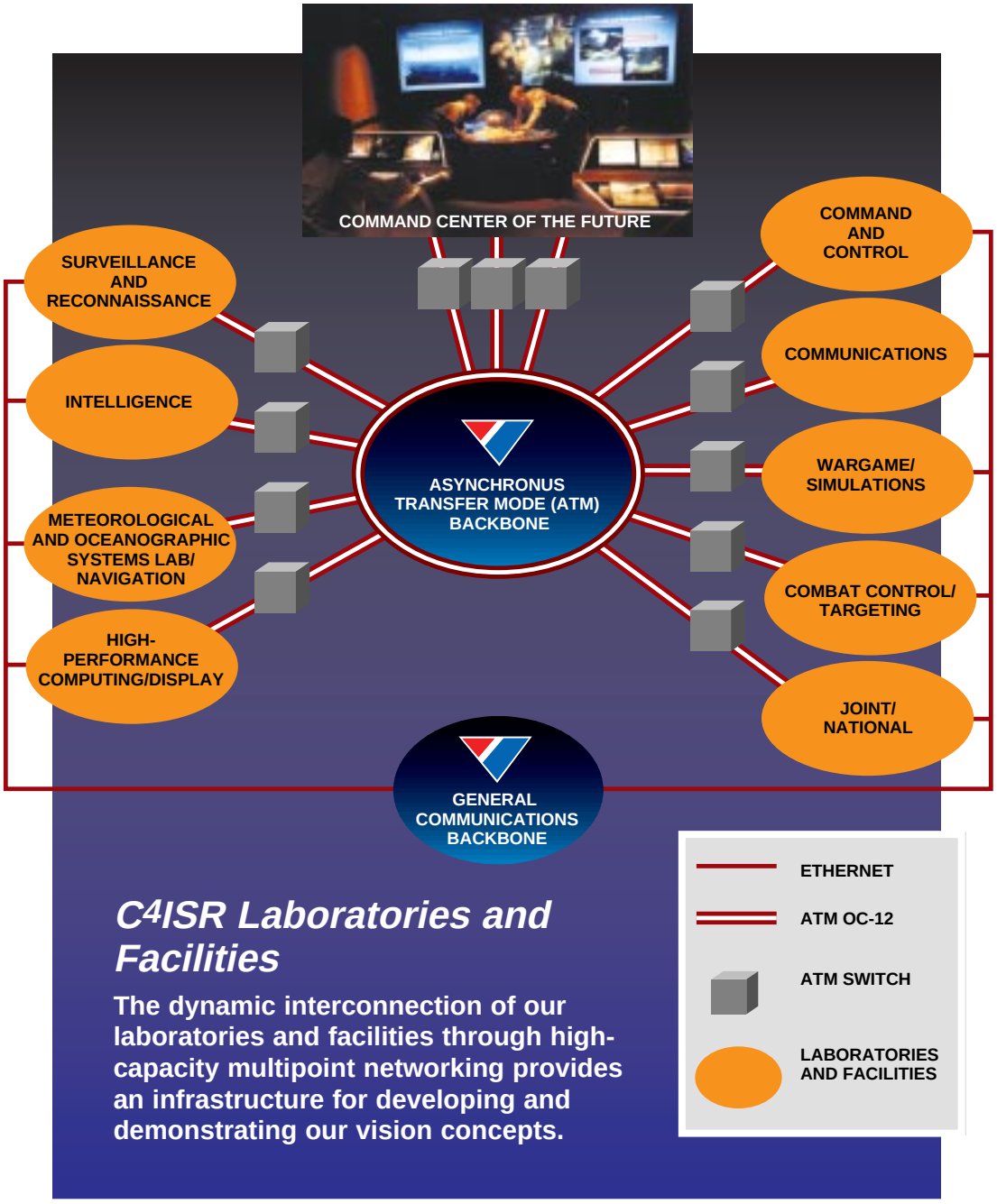
Survivable—Survivability can be regarded as a matter of a system's life or death or as a matter of upgrading by degrees. The C^4I portion of the C^4ISR system of systems is being conceived and implemented with non-developmental item hardware, commercial off-the-shelf hardware and software, and government off-the-shelf software components in an open-systems architecture. As such, *survivable* is being defined more in terms of life and death and the total replacement of inoperable system components with new (spare) components rather than incremental improvement or on-site repair. Comprehensive MIL-SPEC-type survivability will also continue to be considered and applied to C^4I systems and system components, but on a selective basis, and only when necessary.

There is a relationship between the growing emphasis on commercial sourcing and the total replacement of system components for survivability. First, commercial computer system costs have been reduced by about 50% over the past decade while military systems' costs have remained virtually unchanged. In many instances, it now costs less to swap-out the entire component than it does to support a DoD parts and maintenance infrastructure. Furthermore, because technology continues to change so rapidly, and previous methods of procurement caused excessive delays, some of the military systems deployed in the battlespace today are obsolete in terms of capability. Technology is moving too fast not to use commercial off-the-shelf components. Commercial off-the-shelf hardware trends include component standardization, miniaturization, modularization, and simplification. Typically, these are features desired in military systems too. There are, however, pros and cons to this situation. On the positive side, not all military systems need to be MIL-SPEC. On the negative side, a growing reliance on commercial sourcing means that DoD has relinquished a certain amount of production and logistics control and configuration management; that is, will the new components be in the warehouses when we need them?



NRaD's Approach to C4ISR Evolution

NRaD is uniquely qualified to provide the expertise and tools to allow the warrior to achieve information dominance. Almost every NRaD project deals with acquiring data, transforming data into information, using information to operate, or moving data and information from where they reside to where they are needed. *NRaD is at the cutting edge of technologies to support the processes of transforming data into information; information into knowledge; and knowledge into understanding.*



C4ISR Laboratories and Facilities

The dynamic interconnection of our laboratories and facilities through high-capacity multipoint networking provides an infrastructure for developing and demonstrating our vision concepts.

Our great strength at NRaD is our unique work across the spectrum of C^4ISR. This work ranges from basic research through prototyping and fully produced systems and to life-cycle support of fielded systems. Furthermore, NRaD's facilities, laboratories, and fleet communications capabilities allow our engineers and scientists to replicate an operational environment unachievable in the commercial world. Only at NRaD can the pieces of the overall C^4ISR system be integrated and tested in both laboratory and operational contexts. We are aggressively applying our unique expertise and capabilities to the central element of future naval warfare—information dominance.

NRaD's importance in C^4ISR lies in the fact that we are an integral part of the U.S. military infrastructure, and in the breadth of our program base, our corporate personnel expertise, our corporate memory, our unique laboratories and facilities, our connectivity to operational commands and other Centers, and our demonstrated ability to integrate components and subsystems into a greater whole. We will team with other DoD activities, industry, and academia to transform technology into effective tools for the warrior.

NRaD's approach to the development of C^4ISR systems embraces the concepts of evolutionary acquisition, coupled with a strong commitment to standards-based architecture. The development process is a continuous sequence of *visioneering, prototyping, demonstrating, integrating,* and *evolving* all the components of our C^4ISR systems.

Visioneering—This is the process of conceiving ideas for the application of emerging technology to C^4ISR, and then translating those ideas into models. We can then imagine how those models might be used in a command setting to give a decided boost in military operational advantage. NRaD's Command Center of the Future, in large measure, exists to demonstrate these models and to create an interest in our customers in moving them to the next stage. We at NRaD have the potential to be visionaries. Any idea, no matter how far-fetched, deserves to be looked at. We owe it to ourselves to be continually on the lookout for these ideas, knowing that there is a clear command intention to exploit the promising ones.

Prototyping—The next step in the process is to develop a working example of the model so that it can be shown in the context of C^4ISR. Prototyping is being conducted at NRaD and needs that C^4ISR context. For prototypes to be "sold" to customers, their relevance to mainstream C^4ISR programs must be demonstrated. The Navy's Exploratory Development (6.2) and Advanced Development (6.3a) communities must embrace this. The next step, namely that of demonstrating the prototype in an operational/command center environment, must be an integral part of the exploratory/advanced development process.

Demonstrating—There are many opportunities to demonstrate our prototypes, and the number of these is increasing. The Joint Warfare Interoperability Demonstration (JWID) is a good vehicle to showcase our emerging technology in a joint operational setting. Fleet and joint exercises also provide good exposure of our demonstrations to the operating forces, but care must be taken not to interfere with the primary objectives of the exercises, such as readiness and training. If done in an operational setting in the context of operational scenarios, demonstrations can provide excellent means for acquiring fleet/operational feedback prior to "hardening" the design for delivery and integration.

The Approach—How We Get There

We will provide effective tools for the warrior by applying our networked C4ISR laboratories and test facilities in a dynamic evolutionary sequence of "concept-to-reality" engineering and development.

Integrating—When a decision is made to proceed with an addition or upgrade to an element of the C^4ISR system, integration and associated testing must occur in a laboratory setting that replicates, as much as possible, the operational one. A successfully integrated component will not adversely affect the performance of the total system when placed under operational stress. The environment and stresses applied during the testing must be as "worst case" as can be replicated in order to ensure that unanticipated second-order effects will not upset system performance.

Evolving—Evolution completes the development cycle for a new concept. Once the element is successfully integrated, two parallel processes must occur. The first is the review and analysis of system performance/operational effectiveness by the warriors themselves. Feedback must be given to the development community on a periodic basis. Armed with knowledge of both deficiencies and suggestions for improvement, our thinkers can get busy conceiving revolutionary ideas that lead to additional cycles of development.

In this document, we have charted the course to the destination of optimal C^4ISR. The course is set toward the horizon of information dominance, and the stars by which we intend to navigate are described by our corporate initiatives. As we move forward, we will continue to work toward achieving our goal of dominant C^4ISR.

This is our vision.

This is our future.

Naval Command, Control and
Ocean Surveillance Center
RDT&E Division
San Diego, CA 92152–5001

Reviewed and approved by
Executive Officer/
Base Operations Manager
NCCOSC RDT&E Division

TD 3001
July 1997

Approved for public release;
distribution is unlimited.

A Product of the Technical Information Division (TID)