NETWORKING THE NAVY

A MODEL FOR MODERN WARFARE

Lexington Institute

NETWORKING THE NAVY
EXECUTIVE SUMMARY

The U.S. military is in the midst of a far-reaching transformation driven mainly by new information technologies. The same innovations that are revolutionizing global commerce and culture are also changing the way in which America wages war. Many of the ideas about how military transformation should unfold originated in the Navy, in a conceptual framework that has come to be known as "network-centric warfare."

The latest refinement in Navy thinking about network-centric warfare is an initiative called Forcenet (or "FORCEnet" in naval parlance). Navy leaders describe Forcenet as the "glue" that will hold their scattered warfighting assets together in the information age — a resilient web of wireless links reaching from the seabed to geosynchronous orbit that can continuously connect the Navy's warfighting communities with each other, and with the rest of the joint force.

That sounds like a simple task, but in fact it is the most challenging system-integration effort any government agency has ever undertaken. The Navy describes six overarching goals of Forcenet: comprehensive, timely information for weapons and sensors; a "distributed and collaborative" command-and-control system; dynamic, resilient networks; adaptive and automated decision aids; "human-centric" technology and processes; and sophisticated information-warfare tools.

The technical standards and specifications for achieving such goals are very complex. In simple terms, though, Forcenet seeks to leverage recent investments in what might be called the three "R's" of information-age warfare — the richness of sensors, the reach of networks and the relevance of fused, multi-source information. If the many cutting-edge programs in these areas can be integrated in a common architecture, the gains in military performance should be truly revolutionary.

The design philosophy of Forcenet emphasizes flexibility and cooperation. Flexibility is afforded by open architectures, modular components, common standards, and other features that mimic the user-friendly environment of the Internet. Cooperation is reflected in the Navy's determination to fashion a network that seamlessly links to all organic, joint and national assets. This will enable the Navy to avoid duplicating the investments of other services while maximizing interoperability in wartime.

Because Forcenet is a realignment of existing efforts rather than new technology, it is inexpensive. Its annual budget is expected to be less than a tenth of the $300 million the Navy currently spends every-day. Nonetheless, by tearing down barriers to effective warfighting and efficiently leveraging all investments in new technology, it has the potential to transform warfighting. Among the existing Navy programs that offer some hint of what it can deliver are the Cooperative Engagement Capability, the Distributed Common Ground/Surface System, the Tactical Exploitation System, and the Advanced Hawkeye surveillance aircraft.

This report was written by Dr. Loren Thompson of the Lexington Institute and reviewed by the members of the Naval Strike Forum.

The history of the U.S. Navy has coincided with the most productive period of technological innovation in human experience — a period generally thought to have begun during the Enlightenment of the 18th Century. It is no exaggeration to say that there have been more technological breakthroughs in the past two hundred years than in the previous two million. Fortunately for the Navy, and for America, the values of freedom and tolerance embraced by the Founding Fathers were uniquely suited to sustaining an era of unprecedented progress.

However, America's aspiration to be a world leader in this period of rapid change has imposed a heavy burden on its armed forces. They must maintain a powerful global presence that adapts readily to new challenges without draining economic resources essential to other facets of national success. One way the services have sought to do this is by continuously assimilating new technologies that provide a warfighting advantage over foreign militaries. Such investments require a small portion of national wealth (about one percent) while enabling U.S. forces to dominate developments in many different regions — despite facing adversaries with superior mass and positioning.

Over the last hundred years, the Navy has repeatedly reinvented itself by embracing innovations such as the submarine, sea-based aircraft, nuclear power and digital electronics. Today, at the beginning of a new century, another wave of innovation is sweeping the Navy. It is the nascent age of networking — an era in which the sea services will become comprehensively interconnected, not merely among their various warfighting communities but with every outpost and asset in the entire military establishment.

It sounds simple, but no military force has ever before undertaken such a task. If it succeeds, every facet of naval warfare will be transformed. In the process, U.S. military power will become more flexible and effective and economical. The other military services — the Army, the Air Force and the Coast Guard — are following the same path, but it is a path first defined within the Department of the Navy. That is where the notion of network-centric warfare initially emerged, and where it is now finding most sophisticated expression in an initiative called Forcenet.

The purpose of this study is to concisely describe the content and meaning of a networked Navy. The study begins by exploring the evolution of ideas about military power in the information age, and then traces how the Navy has translated those ideas into programs. It identifies the key challenges in building a resilient network, and the systems that are likely to figure most prominently in a successful outcome. Finally, it explains why Forcenet may be the defining military innovation of this generation.

THE EVOLUTION OF JOINT CONCEPTS

During the 20th Century, U.S. defense efforts were driven by three successive waves of danger: imperialism, which produced World War One; fascism, which produced World War Two; and communism, which spawned two generations of tension known as the Cold War. When the latter threat collapsed in the late 1980s, U.S. policymakers were uncertain as to how national defenses should be reorganized. They were wary of excessive demobilization, but the nation had never before maintained a large military establishment in the absence of major threats.

By the late 1990s, though, a consensus began to emerge that the nation should replace its traditional, threat-based military preparations with a "capabilities-based" posture centered on information technologies. The first official document to fully reflect this consensus was Joint Vision 2010, prepared by the Joint Chiefs of Staff in 1996. JV 2010, as it came to be known, set forth the organizing concepts for how U.S. military power should be recast by the end of the following decade.

JV 2010 constructed a "conceptual framework" of four overarching goals — dominant maneuver, precision engagement, full-dimensional protection and focused logistics — that it said collectively would enable U.S. military forces to dominate the spectrum of conflict in the next century. All four goals were grounded in a requirement for "information superiority," which the document defined 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."

The Joint Chiefs acknowledged that information had always been critical to military success, but asserted that emerging technologies made it feasible for U.S. forces to apply information much more effectively, dissipating the "fog" of war. New technologies could be used to integrate the previously disconnected and duplicative operations of the services, producing a more unified and agile force capable of achieving devastating effects without the necessity for protracted, sequential massing of assets. The Joint Chiefs proposed a series of "transformations" that would realize their vision of information-age warfare within 15 years.

The 1997 Quadrennial Defense Review embraced the information-centric framework of Joint Vision 2010 as a "template" for future military preparations. The final report of the QDR, released in May of 1997, stated "The key to success is an integrated 'system of systems' that will give [U.S. forces] superior battlespace awareness, permitting them to dramatically reduce the fog of war." It continued, "This system of systems will integrate intelligence collection and assessment, command and control, weapons systems and support elements."

The QDR report cited several "critical enablers" of next-generation warfare, including "a globally vigilant intelligence system," "global communications," and "superiority in space." In December of 1997, a congressionally-chartered body of independent experts called the National Defense Panel issued a counterpoint to the QDR findings that implicitly endorsed the JV 2010 framework while asserting a need for greater urgency in transforming the force. The panel noted in particular the importance of using space-based systems and information operations to combat "asymmetric" (unconventional) threats.

In 2000 the Joint Chiefs of Staff released an updated version of their doctrinal vision that confirmed the precepts of JV 2010 while emphasizing the role of networks in future warfighting. The new document, Joint Vision 2020, reflected the ferment among entrepreneurs and intellectuals as the Internet rapidly infiltrated every facet of commerce and culture. Joint Vision 2020 appropriated a concept developed by the Navy, "network-centric warfare," to capture the core feature of next-generation warfare.

The basic idea behind network-centric warfare was that military performance could be hugely improved by connecting all the sensors and weapons of the joint force in a resilient information network — a network any warfighter could access as needed. By sharing the same timely and comprehensive information resource, including tools capable of quickly merging and manipulating data from many sources, warfighters could escape the spatial and organizational isolation that had dogged them throughout history. A key

requirement of this vision was that U.S. forces have information technology and skills superior to those of adversaries, so that they could operate more quickly and precisely.

Joint Vision 2020 called for a "global information grid" that could tie together every asset of the U.S. military establishment in a web of high-capacity, instantaneous, multimedia communications. That was a tall order, but one which seemed to speak directly to America's technological strengths and global responsibilities. When the administration of George W. Bush conducted its own Quadrennial Defense Review in 2001, the transformation priorities it settled on closely matched the information-centric ideas of its predecessors. Not only did the new administration stress the centrality of networks in future warfare, but it exhibited a strong sense of urgency about military transformation long before the atrocities of 9-11 underscored the need for change.

NAVY NETWORKING CONCEPTS

Many of the concepts today driving the networking of U.S. military forces originated in the Navy. In 1990, long before network-centric warfare became a central feature of joint doctrine, the Navy established a program called "Copernicus" to assimilate emerging information technologies. As Chief of Naval Operation Jeremy Boorda later explained it, "Copernicus is the Navy's initiative to make command, control, communications, computers and intelligence (C4I) systems responsive to the warfighter; to field these systems quickly; to capitalize on advances in technology; and to shape our doctrine to reflect these changes."

The admirals managing Copernicus understood that information technologies had the potential to revolutionize military operations, and therefore promoted their systematic application across the entire range of Navy roles and missions. Not only could information technologies enhance the speed and precision of naval warfare, they argued, but the technologies

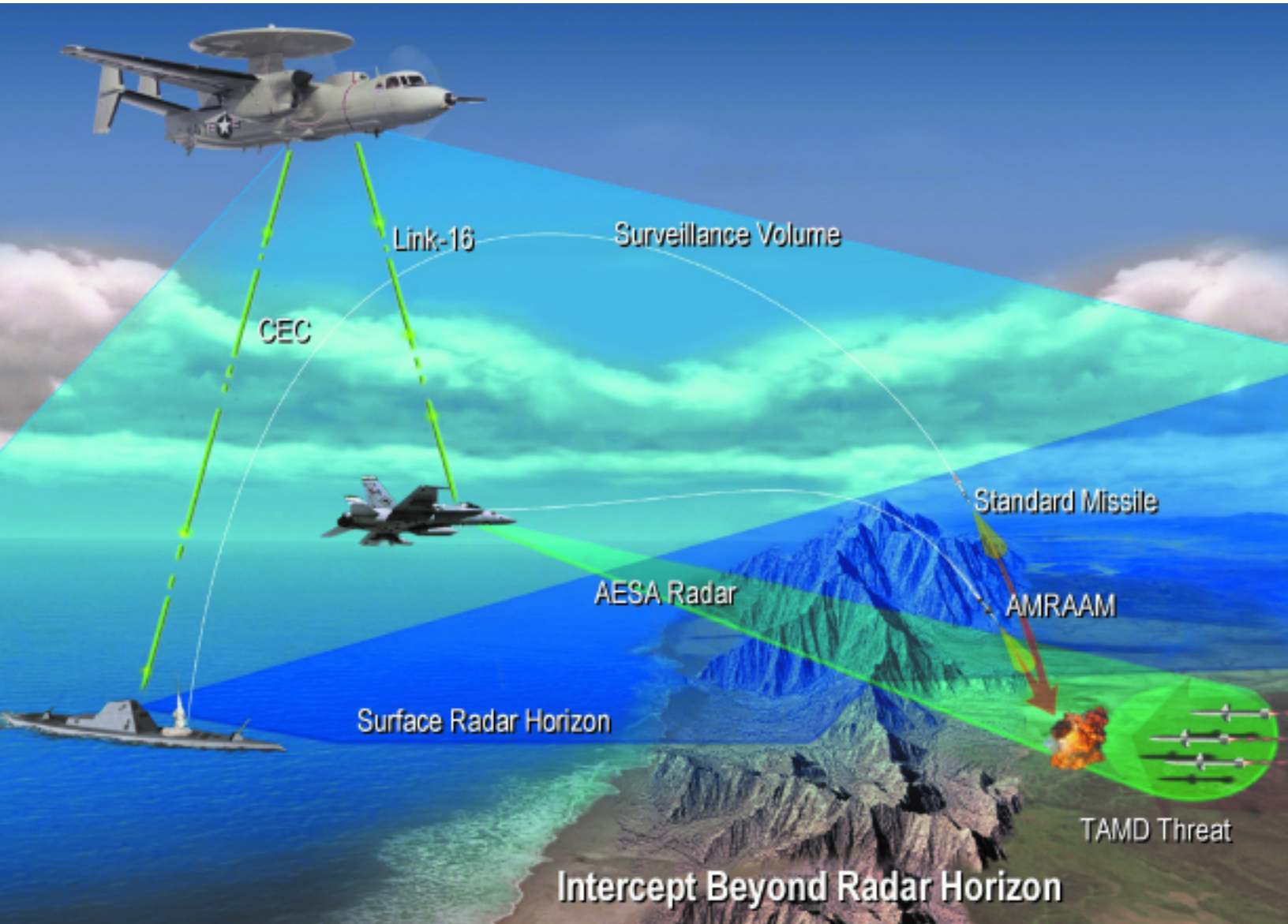
Milstar satellites can securely transmit air tasking orders in six seconds.

could be employed to impede the effectiveness of enemy forces by denying access to critical data. Copernicus also anticipated the increasing emphasis on joint operations in later years by insisting that Navy information architectures be fully interoperable with those of other services.

At the core of Copernicus were four overriding goals: to provide a common tactical picture to all members of a naval force; to comprehensively connect them in a web of instantaneous voice and data links; to compress the steps involved in moving information from sensors to shooters; and to conduct information operations that would degrade enemy warfighting capabilities. The Navy adopted the phrase "network-centric warfare" to describe this nascent warfighting paradigm, because it stressed integration and communication over autonomy in conducting naval operations.

A handful of visionaries such as vice admirals Gerald Tuttle and Arthur Cebrowski were instrumental in developing the conceptual foundations of network-centrism. Its appeal within the Navy was enhanced by the need to formulate new concepts of operation suited to waging war in littoral areas. Outside the Navy, military leaders were impressed by the elegance of the network-centric vision, its relevance to the changing needs of the joint force, and its potential to leverage powerful technological forces unfolding in the commercial world.

Network-centric warfare requires seamless connectivity among warfighting systems.



The Navy's early embrace of network-centric warfare in part reflected its traditional style of operations, which entailed the continuous forward deployment of a distributed force far from U.S. territory or supporting infrastructure. The value of timely and reliable communications links in assuring the most effective employment of this scattered force stimulated Navy and Marine Corps leaders to think imaginatively about the meaning of the information revolution.

The resulting enthusiasm for change — far removed from the stereotypical conservatism of military organizations — was displayed in detail during deliberations for the 2001 Quadrennial Defense Review. The sea services advanced a coherent vision of joint warfare enabled by emerging technology that could cope with a world of diverse dangers. Not only did this vision acknowledge the importance of the other services, but it highlighted how Navy technology investments such as the Cooperative Engagement Capability (CEC) and Multifuctional Information Distribution System (MIDS) would bolster joint-force synergy. It was a strikingly ecumenical vision.

THE BIRTH OF FORCENET

The early years of the new millennium were tumultuous ones for the Navy and the nation. Shortly after the Quadrennial Defense Review was completed in summer of 2001, members of the Al Qaeda terrorist organization executed major attacks in New York and Washington. The United States responded with a hastily mounted campaign to destroy Al Qaeda cells in Afghanistan, dubbed Operation Enduring Freedom. Barely a year after that campaign was completed, a second campaign to topple the government of Iraq, Operation Iraqi Freedom, was launched.

The Global Hawk unmanned aerial vehicle combines long endurance with a large and versatile sensor package.

Navy and Marine Corps performance in the two campaigns proved that considerable progress had been made in accomplishing the goals of Copernicus and network-centric warfare. Sea-based forces executed strikes far more quickly and precisely than in any pre-

vious campaign, primarily because of continuous cooperation with other elements of the joint force. By depending on other services for intelligence and logistics, the Navy and Marines were able to penetrate deep into the interior of Afghanistan and Iraq, rapidly defeating numerically superior adversaries. The combination of better access to joint assets and greatly improved organic capabilities produced a true revolution in strike warfare.

There was little question that networking the force had greatly enhanced military performance. As Chief of Naval Operations Adm. Vernon Clark noted after the Afghan operation, "80% of Navy strike sorties attacked targets that were unknown to the aircrews when they left the carriers. They relied upon networked sensors and joint communications to swiftly respond to targets of opportunity." Clark viewed early victory in Afghanistan as vindication for the proponents of network-centric warfare, and in summer of 2002 he unveiled a bold new vision built upon the foundation of information technology and operations laid out a decade earlier by his predecessors.

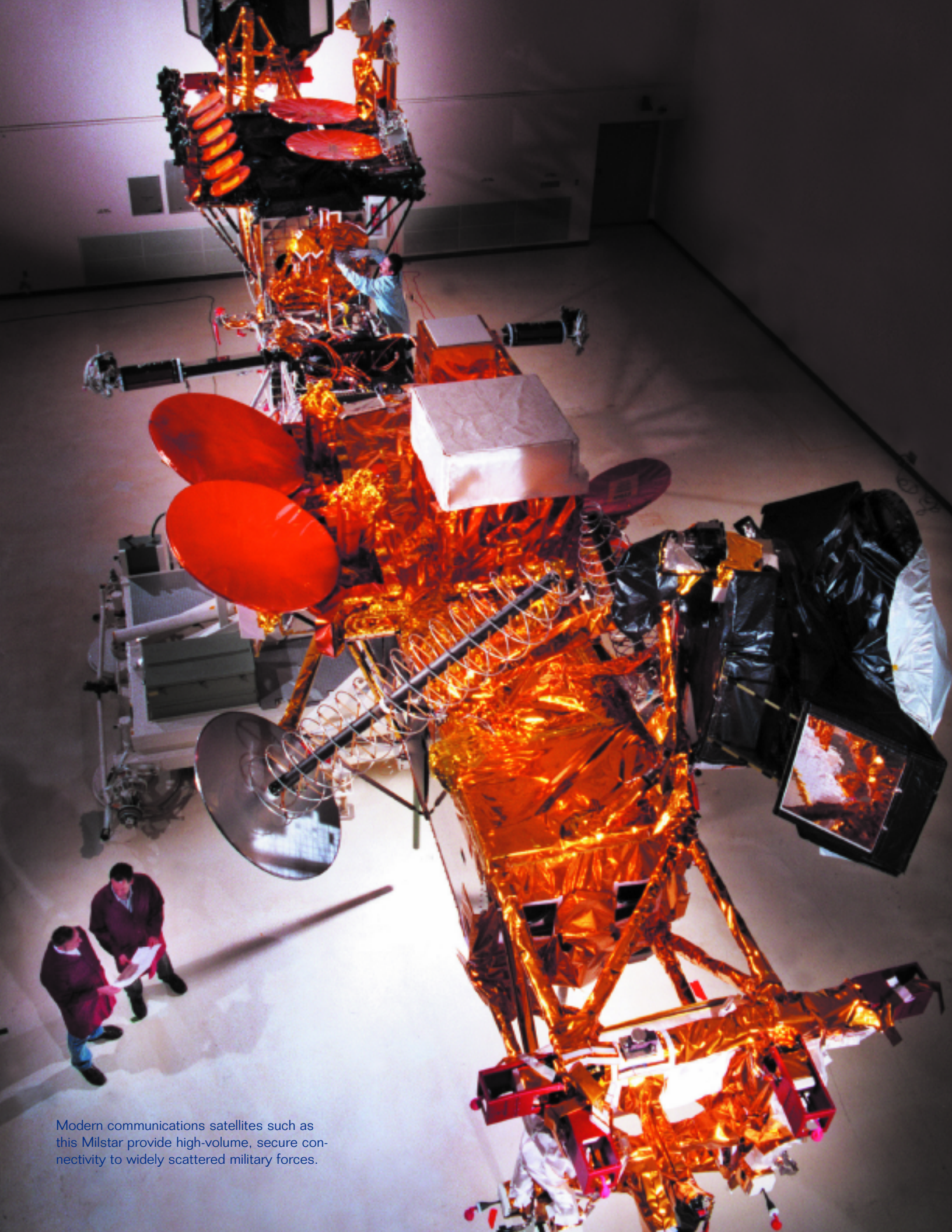
Clark's vision was called "Sea Power 21: Operational Concepts for a New Era." It was constructed to offer the clearest, most concise explanation of what warfighting advantages naval forces could provide in the information age. Clark described three overarching missions: "Sea Strike," the global projection of offensive power; "Sea Shield," the global projection of defensive power; and "Sea Basing," the global projection of sovereignty. The three missions were synergistic, in that decisive offensive force both depended on and contributed to defensive might, and both in turn required secure forward basing at sea.

But all three overarching missions depended on something else, too: a flexible and resilient web of communications that could unify the dispersed fleet of the future into a globally integrated fighting force. Adm. Clark called the resulting architecture "Forcenet," and described it as "an initiative to tie together naval, joint and national information grids to achieve unprecedented situational awareness and knowledge management." Said differently, it was the greatest system-integration challenge ever proposed in the history of warfare.

And the most promising. In effect, the Navy was once again taking the lead in exploring the full warfighting potential of emerging technologies. Just as Copernicus had anticipated later shifts in joint doctrine, so Sea Power 21 and Forcenet sought to define the next era in global military engagement. It would be an era in which traditional distinctions between strategic and tactical operations, air and surface operations gradually melted away to be replaced by a single integrated web of interactions stretching from the seabed to geocentric orbit. It was the birth of a new Navy, unlike any that had ever existed before.

FORCENET GOALS

Considering its pivotal role in Navy plans, Forcenet is a surprisingly inexpensive program. The service expects to spend about $20 million annually on it during the present decade — less than a tenth of the $300 million the Navy and Marine Corps spent every day in fiscal 2003. Forcenet is cheap because it is a conceptual breakthrough, not a new technology. In the words of a Navy report to Congress, "Forcenet is an enterprise alignment and integration effort. It looks across warfare mission areas to identify capabilities and efficiencies that would not be realized under the existing paradigm of individual stove-piped programs."



Modern communications satellites such as this Milstar provide high-volume, secure connectivity to widely scattered military forces.

Stove-piped in this context refers to the military tradition of reporting upward throughout hierarchical command structures. Like smoke rising up ducts from stoves, the various information flows generated by military sensors typically do not converge until they approach the top of the command structure. Organizational barriers impede the sharing of information across operational levels of activity unless it first flows upward and then back downward — in the process often getting garbled and delayed.

In conceptual terms, Forcenet cuts across arbitrary organizational and mission boundaries to assure timely access to useful information. Rather than designating command elements or functional experts who decide which information is shared with local units, the system enables those local units to pull whatever information they need off an internet-style utility that is comprehensive in scope, extremely precise, immediately available, and continuously updated. Analyses by the Chief of Naval Operations' Strategic Studies Group project huge gains in military performance if this model is correctly implemented.

However, effective implementation is challenging in both technological and cultural terms. Not only must dozens of sensor, communications, battle management and weapons programs (some of them outside the Navy) be integrated into a seamless architecture, but warfighters must be educated to use them in new ways. For example, the information generated by intelligence-gathering satellites, once unavailable to most warfighters in raw form, may become a routine resource for tactical operations.

Navy planners have identified six overarching requirements that Forcenet must satisfy if it is to realize the bold vision of information-age warfare set forth by the Chief of Naval Operations:

1. It must provide "multi-tiered sensor and weapons information" suitable for expeditionary operations, meaning operations conducted far from the American homeland and supporting infrastructure.

2. It must provide a "distributed, collaborative" command-and-control system that enables widely scattered forces to function continuously with common purpose.

3. It must provide "dynamic, multi-path and survivable networks" that are resilient and reliable under the most trying wartime circumstances.

4. It must provide "adaptive, automated decision aids" that enable warfighters to quickly organize, assimilate and act on information from many disparate sources.

5. It must provide "human-centric" technology and processes that can generate optimum results despite the constraints imposed by normal human behavior and capacities.

6. It must provide "information weapons" suitable for degrading enemy knowledge and compromising the information systems on which adversary actions depend.

An information architecture capable of delivering all these features under the stress of sustained combat would be unprecedented. It would facilitate fast-moving, surgical operations that no adversary could hope to match, much less surpass. Decisive effects would be generated through finesse rather than massed firepower, greatly enhancing both the economy and survivability of friendly forces.

The EA-6B Prowler is designed to deny adversary access to the radio-frequency portion of the electromagnetic spectrum.

FORCENET VALUES

Forcenet does not have a final goal in the sense of a fixed end-state at which point it will be considered completed. Within the context of capabilities-based planning that spawned Forcenet, major technology initiatives are assumed to evolve indefinitely in response to changing demands and opportunities. The systems and processes that satisfy the six requirements set forth in the previous section will change over time as new threats emerge, new technologies become available, and new operational concepts are embraced.

The absence of a concrete end-state may be unsettling for those accustomed to traditional acquisition programs, but it is the logical response to a period of unpredictable threats and rapid technological change. With so little certainty about future needs, the Navy has to keep its warfighting options open. Forcenet is the glue that will hold together the core warfighting capabilities of the Navy (to use a metaphor favored by Vice Adm. Richard Mayo), but it makes no final judgments about which systems should provide those capabilities. In fact, current design philosophy requires that the Forcenet architecture be independent of any particular sensor or weapon configuration.

Forcenet leverages investments in the richness of sensors, the reach of networks, and the relevancy of fused, multisource information. These "three R's" — richness, reach and relevancy — are the guiding principles in designing warfighting architectures for the

The Advanced EHF satellite will provide unprecedented information security, reliability, and carrying capacity.

(Opposite page)
The Advanced Hawkeye surveillance aircraft will have enhanced sensors and comprehensive connectivity.

information age. They are analogous with the three R's of industrial-age education (reading, writing and arithmetic), which provided standards for the exchange of information and the pursuit of new discoveries in an earlier era. In today's world, richness, reach and relevancy make possible a knowledge-enabled concept of warfighting that changes traditional notions about the significance of time and space.

In place of a static force structure or end-state, Forcenet fosters a culture of change underpinned by core values. These values are expected to endure for many years, regardless of how military threats or technologies may change. Six values seem to be most fundamental to the Forcenet concept:

1. Precise and timely information will be an indispensable enabler of military success for the foreseeable future; the Navy must continuously assimilate new information technologies because key adversaries are likely to do so too.

2. The Navy cannot achieve sufficient warfighting leverage from its technology investments unless it makes maximum use of the information resources available in other services; rather than duplicating the capabilities of those services, the Navy should invest in organic systems only when it can add value to the joint force or believes non-Navy assets may be unavailable in wartime.

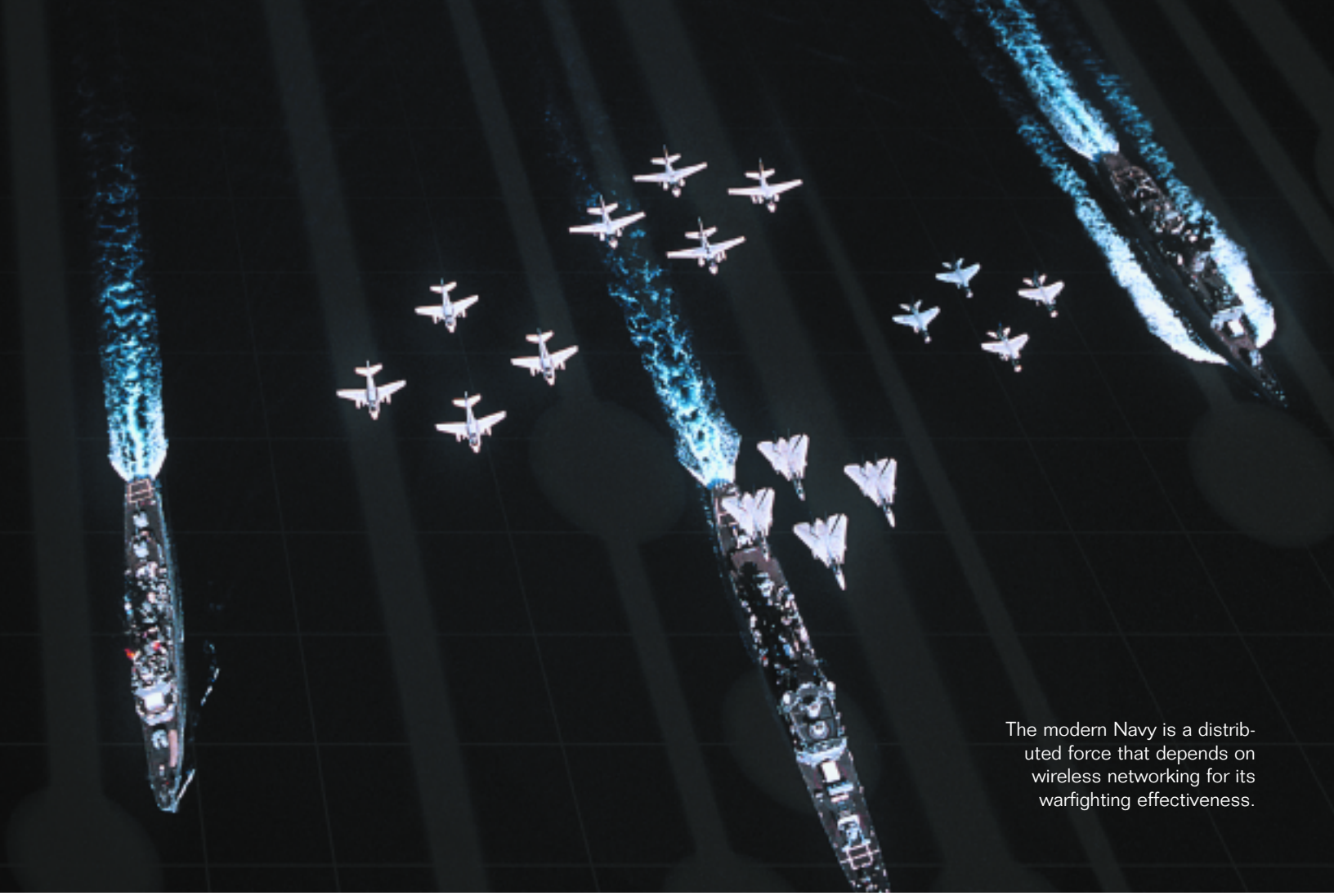
3. The need to exploit diverse information resources from different warfighting communities and services dictates an emphasis on interoperability; unless information flows utilize common language and interface standards, it will be impossible to obtain critical information in a timely fashion.

4. The preferred approach to facilitating joint cooperation and interoperability is to rely on modular, open architectures that can be continuously upgraded and adapted; the commercial world offers a model for how such architectures can be implemented quickly without compromising network security.

5. An internet-style system in which users pull what they need off the network rather than having it pushed down by remote authority is well-suited to the emerging operational environment; as long as they are adequately equipped and trained, local users are usually the best judges of what information they require from across the joint network.

6. There is no substitute for realistic experimentation in assessing the potential advantages and vulnerabilities of new information technologies; unless new concepts and technologies are rigorously tested, they may erode rather than enhance the Navy's warfighting capabilities.

What these values amount to is an ecumenical, open-minded approach to military modernization far removed from the organizational insularity of past years. A Navy that once thrived on autonomy and tradition now proposes to make its warfighting effectiveness dependent upon cooperation with other services. Ultimately, it may relinquish signature missions and weapon systems to concentrate on those activities where it has a demonstrable comparative advantage. Thus, rationalization of service roles and missions is an inescapable consequence of the Forcenet vision.



The modern Navy is a distributed force that depends on wireless networking for its warfighting effectiveness.

KEY PROGRAMS

Forcenet will be implemented using a "spiral" development model, meaning that progressively more capable increments will be fielded over time. Given budgetary constraints and technical challenges, it may take a decade or longer to fully realize the synergies associated with network-centric warfare. However, the Navy has already made considerable progress in assimilating the benefits of information technology. A handful of programs stand out as harbingers of how Forcenet will transform the sea services.

The program most frequently cited is the Cooperative Engagement Capability (CEC), a system that combines information from widely scattered sensors to generate a composite picture of the airspace around a naval expeditionary force. CEC is a first-generation glimpse of the changes that Forcenet will facilitate. The system processes and fuses radar data from Aegis warships and E-2C Hawkeye surveillance planes to create precise "tracks" of nearby aircraft. This continuously updated picture, which includes navigational and identification-friend-or-foe information, is digitally linked to command computers and defensive weapons to provide unprecedented protection against airborne threats. Eventually, CEC-type networks will leverage information from every deployed system in the fleet and the broader joint force, allowing weapons to be used with maximum effect. For example, a warship may be able to employ weapons against hostile aircraft before on-board sensors can see it, because the warship has received information from off-board sources that provide a more detailed and comprehensive picture.

The antenna arrays on aircraft carriers reflect how critical information collection and connectivity are to joint warfighting.

The Cooperative Engagement Capability is a striking example of how networking can enhance the efficiency of weapons platforms. Once fully fielded, it will change the way warships are designed and deployed. A next-generation architecture is under development that will extend the coverage of CEC beyond the Navy by increasing transmission capacity and facilitating interfaces with systems such as the Army's Enhanced Position Location Reporting System. Some Navy proponents of CEC believe it is a suitable foundation for a joint composite tracking network — in other words, an integrated air-defense network that all the services can share.

A second program that reflects the goals and values of Forcenet is the Navy's version of the Distributed Common Ground/Surface System (DCGS). DCGS is a family of systems being pursued by all the military services to integrate and exploit intelligence from many different sources — tactical, theater-wide and national. One objective of Forcenet is to facilitate the flow of vital intelligence and reconnaissance data across mission and service boundaries. The movement of such information has been impeded in the past by organizational barriers and security concerns, depriving warfighters of critical insights.

DCGS will ameliorate this problem with an internet-style resource that utilizes open architectures and common interface standards. Anyone with the requisite skills and security clearances will be able to access timely intelligence that has been merged from multiple sources, including spy satellites. Traditional distinctions between types of intelligence and sources will become progressively less important as the services seek to generate the most useful and complete picture of what is known at any given moment for warfighters. And in characteristic Forcenet fashion, what information DCGS delivers will be driven by local needs rather than remote edict.

A third effort fully attuned to the Forcenet philosophy is the Navy's variant of an Army program called the Tactical Exploitation System. TES-N (as the Navy version is designated) would be a key component in the Joint Fires Network conceived to coordinate mis-

sile and gun fire against surface targets. The fires network uses off-the-shelf information systems to target and deconflict munitions originating from multiple platforms in support of forces ashore. But its success hinges on rapid exploitation of multisource intelligence, and TES-N provides a tool for accomplishing this task.

TES-N enables Navy tactical commanders to receive and utilize imagery from a broad range of sources, including photo-reconnaissance satellites, U-2 spy planes and Global Hawk unmanned aerial vehicles. In addition, it can combine processed imagery with signals intelligence generated by electronic eavesdropping systems such as the Air Force's RC-135 Rivet Joint aircraft to create a detailed picture of potential targets. Like CEC and DCGS, TES-N eliminates arbitrary barriers to the tactical exploitation of critical intelligence, enhancing the precision and economy of naval firepower.

Yet another precursor of Forcenet is the E-2C Hawkeye surveillance and communication aircraft, which first debuted in 1973. The latest variant of E-2C, called Advanced Hawkeye, provides a model of how the

The Prowler electronic warfare aircraft is likely to play a central role in information operations.

Forcenet philosophy would reconfigure existing programs for huge gains in performance. The Navy is developing a digital upgrade of the Hawkeye's surveillance radar that would enable it to detect and track missiles operating over land despite electronic clutter and enemy jamming. This is a necessary improvement to protect forward-deployed and allied forces from overland cruise and ballistic missile threats.

But even as it adapts its surveillance capabilities to new operational demands, the E-2C is acquiring a range of other features likely to make it a key node in network-centric warfare. First, it will be equipped with the MIDS (Link-16) tactical datalink that allows rapid exchange of target information with weapons platforms. Second, it will host the Cooperative Engagement Capability, not only feeding target data into the network but also serving as an airborne relay to greatly extend its reach. Third, it will carry the sophisticated Joint Tactical Radio System being acquired by all the services. Advanced Hawkeye thus is destined to be a core asset in the Forcenet architecture.

Dozens of other programs will eventually be subsumed under the Forcenet mantle, ranging from the EA-18G next-generation jamming aircraft to the Broad Area Maritime Surveillance (BAMS) system to be hosted on the Global Hawk long-endurance aerial vehicle. What all of these programs have in common is the potential to leverage emerging information technology in pursuit of greatly enhanced situational awareness, agility and precision. The ultimate product is a transparent battlespace readily dominated by joint forces across the spectrum of conflict from peacekeeping to special warfare to conventional combat.

SPACE "BACKBONE"

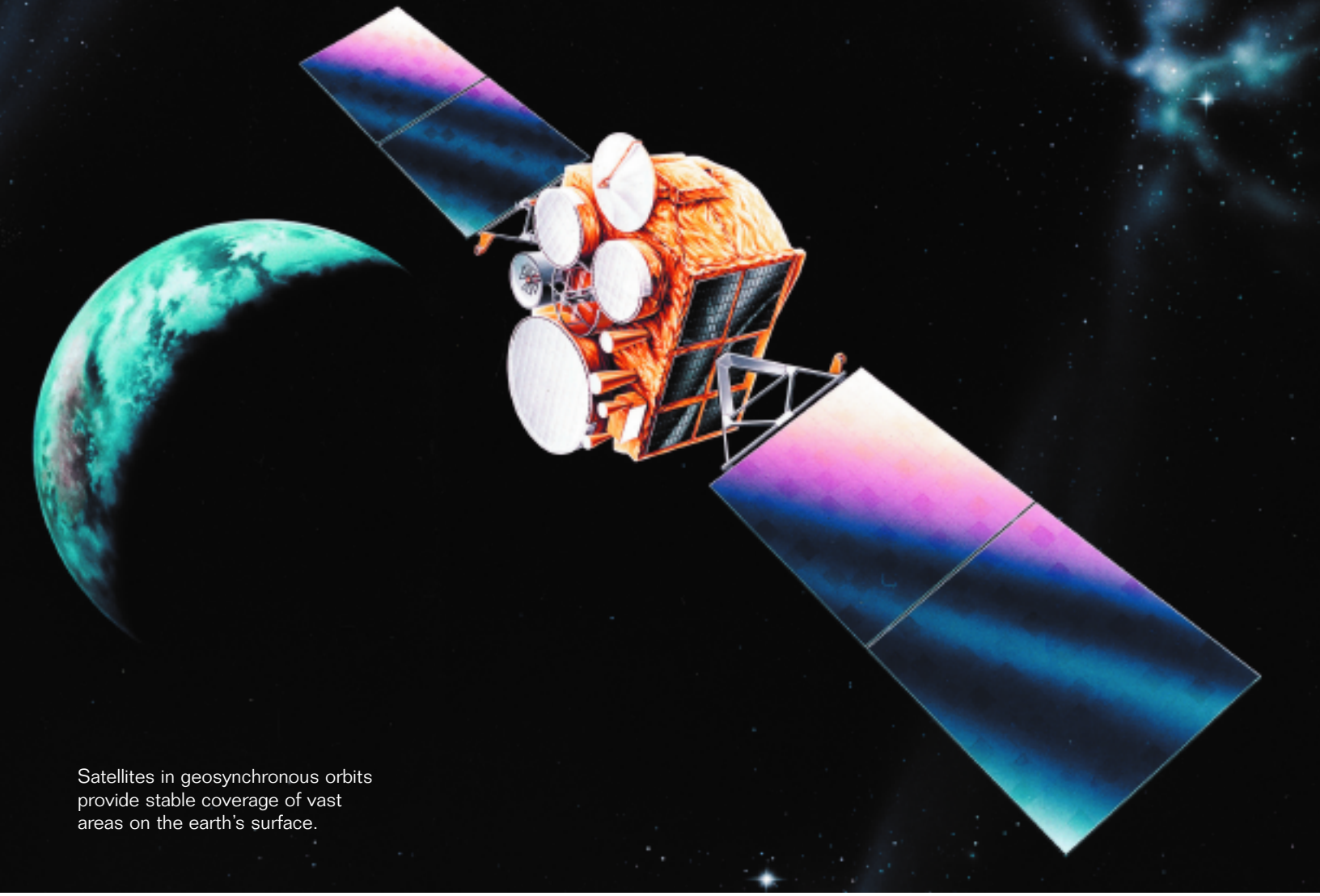
A core value of the Forcenet philosophy is that the Navy must learn to depend on other services for support in fields where it lacks competitive advantage. Nowhere is that principle more valid than in the case of space systems, a mission area for which the Air Force is lead service. According the Vice Adm. Richard Mayo, commander of the Naval Network Warfare Command, "space is the backbone of naval network-centric warfare, providing communications, precise timing, positioning, and battlefield characterization. Space also provides critical real-time intelligence, and surveillance information for naval combat operations." Mayo's command subsumes responsibility for implementing Forcenet and managing naval space activities.

The Navy has created a cadre of space experts who represent sea-service interests in government organizations overseeing space assets, such as the National Reconnaissance Office and the U.S. Strategic Command. This cadre is likely to play a central role in assuring effective fielding of Forcenet, because every facet of the envisioned architecture depends in some measure on orbital systems. There are five generic functions of military space systems that feed into Forcenet:

1. High-volume, secure global communications provided by constellations such as the Defense Satellite Communication System (DSCS) and Milstar II.

2. Imagery and electronic intelligence provided by the satellites of the National Geospatial Intelligence Agency and the National Security Agency.

3. Precise geolocational data for navigation and targeting provided by the 28-satellite Global Positioning System (GPS).



Satellites in geosynchronous orbits provide stable coverage of vast areas on the earth's surface.

4. Early warning of missile attacks provided by the Defense Support Program and its successor, the Space-Based Infrared System-High (SBIRS-H).

5. Detailed weather information provided by the Defense Meteorological Satellite Program and its successor, the National Polar-orbiting Environmental Satellite System (NPOESS).

All of the space systems supporting these functions are being enhanced in the current decade. For example, Cold-War photo-reconnaissance satellites and ground infrastructure will be replaced by the Future Imagery Architecture, which provides more frequent coverage of sensitive areas and faster dissemination of processed imagery. The existing collection of global-positioning spacecraft will give way to a higher power, more jam-resistant constellation that has the capacity to tailor the delivery of geolocational data depending on tactical conditions.

In terms of the implementation of Forcenet, the most important upgrades will be those transforming communications satellites. Orbital transponders are the main conduit through which the Navy maintains global connectivity. The resilience and carrying capacity of these systems thus are key determinants of what Forcenet can accomplish. In recent years, the Defense Department has achieved big gains in upgrading its space-based communications infrastructure. The carrying capacity of each DSCS satellite was doubled

to 8334 voice channels and 200 megabytes per second, while Milstar II transitioned from very low rates of data transmission to over a million bytes per second. An air tasking order that once took an hour to transmit via Milstar can now be sent in six seconds — with minimal likelihood of jamming or interception.

Both of these constellations will be replaced in the near future by even more capable systems. In the case of Milstar II, the next-generation Advanced Extremely High Frequency Satellite will provide a fivefold increase in the rate of secure data transmission and a sixfold increase in the number of terminals supported by each satellite. Over the longer term, a "transformational communications architecture" is expected to afford users internet-style flexibility in a very high-capacity, resilient communications network. The development of these new systems during the same period that Forcenet is being implemented gives Navy planners high confidence that the requisite bandwidth will be available.

A BOLD VISION

The basic notion of networking is not new. Networks have existed in an informal sense ever since the first human communities emerged in mankind's dim prehistory. What is different today is the speed, precision, capacity and reach of the most advanced networks. That is truly unprecedented — so much so that they are transforming civilization.

The Navy's long effort to assimilate the fruits of the information revolution was driven from its earliest days by a prescient awareness of what new technology could deliver to warfighters —friends and foes alike. From Copernicus to Forcenet, the Navy's leaders have consistently demonstrated that they are attuned to the underlying trends of the information age. It is a remarkable reflection on Navy culture that they chose to ride that wave, even though they knew it might mean the death of many cherished traditions.

Today, with Forcenet, the Navy has once again separated itself from the comfortable mainstream of conventional thinking. It is preparing to relinquish old missions and claim new roles based on an institutional consensus that change cannot be avoided and therefore must be embraced. Navy leaders will fight fiercely to defend the competencies in which their service excels, but they are prepared to be more ecumenical and interdependent than ever before. Indeed, they think their future success depends on it.

Vice Adm. Arthur Cebrowski, a key architect of Navy thinking about the future, told Aviation Week & Space Technology that "Network-centric warfare is not about technology. It is an emerging theory of war." What Cebrowski meant was that new technology creates possibilities, but it requires imagination and investment and institutional change to translate those possibilities into a military posture. Forcenet is precisely that — the operational construct and architecture that will make network-centric warfare a reality. It is a bold vision that provides a model for all warfighters in the information age.

Naval STRIKE FORUM

SENIOR ADVISORY BOARD

Admiral Stanley R. Arthur (Ret.)

Admiral Leon A. (Bud) Edney (Ret.)

Dr. Roger E. Fisher

Admiral Huntington Hardisty (Ret.)

General Richard D. Hearney (Ret.)

Admiral David E. Jeremiah (Ret.)

Dr. Paul G. Kaminski

Admiral T. Joseph Lopez (Ret.)

Admiral Wesley L. McDonald (Ret.)

Vice Admiral Dennis V. McGinn (Ret.)

General Richard I. Neal (Ret.)

Admiral William D. Smith (Ret.)

Mr. David F. Stafford

Mr. John J. (Jack) Welch

WORKING GROUP

Vice Admiral Richard C. Allen, USN (Ret.)

Rear Admiral Philip Anselmo (Ret.)
Northrop Grumman Corporation

Rear Admiral Stephen H. Baker (Ret.)

Mr. William Buckey
Office of Governor Jeb Bush

Mr. Chris Caron
Office of Representative Tom Cole

Vice Admiral Daniel Cooper (Ret.)

Mr. Jim Dolbow
Office of Representative John Hostettler

Commander Lee B. Draper (Ret.)
ALPHA Technology

Vice Admiral Robert F. Dunn (Ret.)

Rear Admiral Richard Gentz (Ret.)

Rear Admiral John E. (Ted) Gordon (Ret.)
Alliant Techsystems

Vice Admiral Bat LaPlante (Ret.)

Mr. Loren R. Larson

Mr. Tom MacKenzie
Senate Armed Services Committee

Rear Admiral Daniel P. March (Ret.)

Vice Admiral John J. Mazach (Ret.)
Northrop Grumman Corporation

Mr. Ken Miller
Office of Representative Joseph Pitts

Rear Admiral Riley D. Mixson (Ret.)

Rear Admiral Kendell Pease (Ret.)
General Dynamics

Lieutenant General Charles Pitman (Ret.)
EFW, Inc.

Vice Admiral R. F. Schoultz (Ret.)

Rear Admiral James M. Seely (Ret.)

Mr. Kraig Siracuse
Senate Appropriations Committee

Mr. Jack Spencer
Heritage Foundation

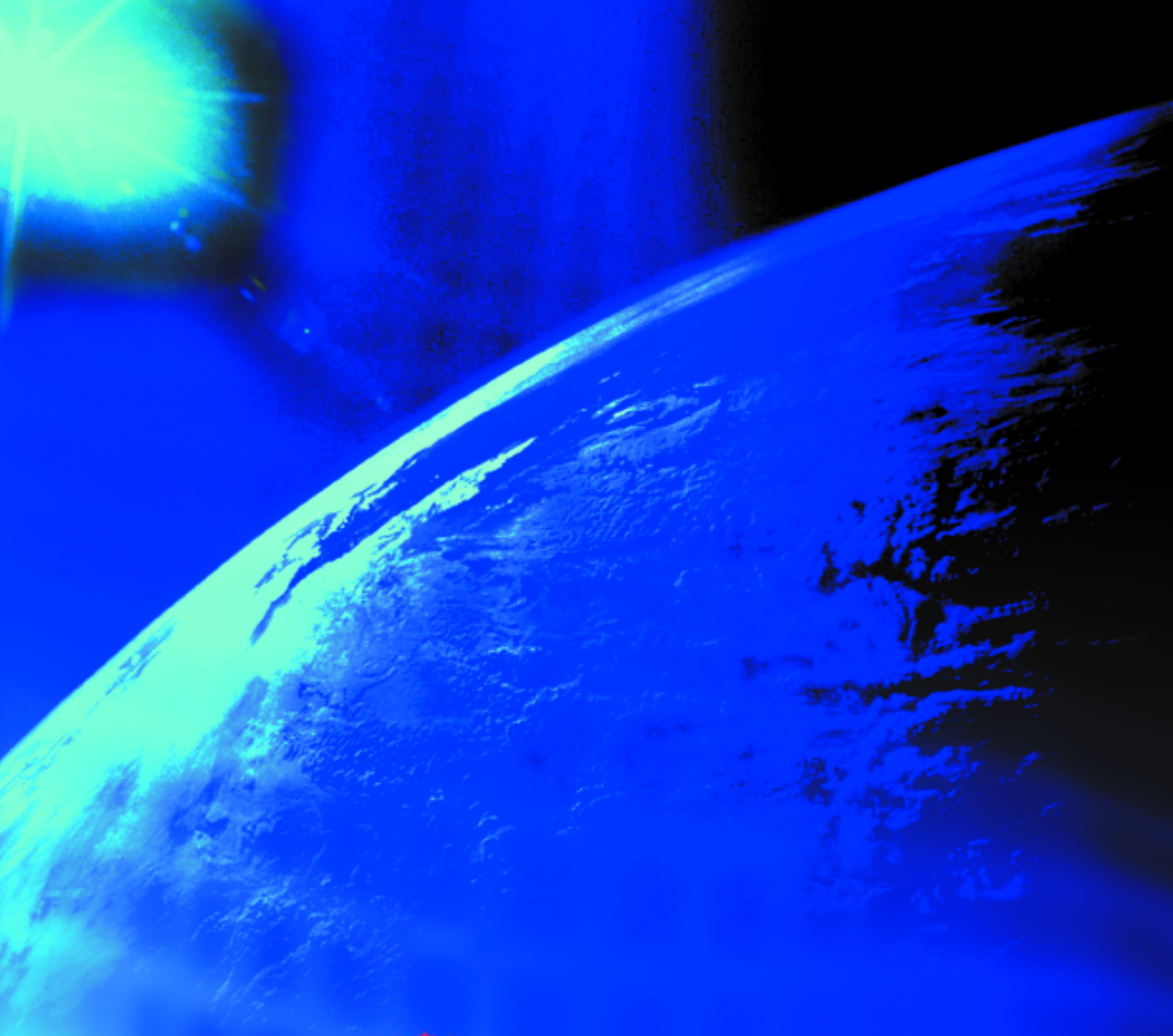
Ms. Jennifer Thompson
Office of Representative Robin Hayes

Dr. Scott C. Truver
Anteon Corporation

Lieutenant General William J. White (Ret.)

Vice Admiral Joseph B. Wilkinson (Ret.)

Rear Admiral Jay B. Yakeley III (Ret.)
Computer Sciences Corporation



Lexington Institute

1600 Wilson Boulevard • Suite 900 • Arlington, Virginia 22209
tel 703.522.5828 • fax 703.522.5837
www.lexingtoninstitute.org • mail@lexingtoninstitute.org

Printed in The United States of America November 2003