Planning Satellite Reconnaissance To Support Military Operations

Thomas Behling and Kenneth McGruther

"By the time the military determines intelligence requirements to support its new doctrine, it may be too late to influence decisions about the very intelligence support systems upon which the doctrine depends."

Thomas Behling is Deputy Director of the Office of Architectures, Assessments, and Acquisition at the National Reconnaissance Office. **Kenneth McGruther** is a policy consultant to that office.

The views expressed in this article are those of the authors and do not reflect official policies or positions of the Department of Defense, the NRO, or the CIA.

The nation's intelligence agencies face a dual challenge: how to come to grips with presidential tasking to become more directly supportive of current military operations, while also adjusting to a new national military doctrine that is still being developed. The presidential order was issued in 1995. The new military doctrine, Joint Vision 2010, was issued in 1996 and amplified in 1997 in a document called "Concepts for Supporting Joint Operations." Meanwhile, the global planning structure to replace the Cold War paradigm, including the role the Intelligence Community (IC)[1] should play, still is unfolding.

The fundamental premise of *JV2010* is that the operational commander will enjoy *information superiority*—the ability to see and hear virtually everything of importance in any engagement. It may be a decade or more, however, before the military sufficiently understands the implications of the new doctrine to impose the associated intelligence requirements for targeting, damage assessment, simultaneous operations, and the like.

This raises some difficult problems. Our current generation of satellites is reaching obsolescence and will have to be replaced within the next 5 to 10 years. Given design and development lead-times, decisions about the next generation of reconnaissance satellites are being made now. As a result, by the time the military determines intelligence requirements to support its new doctrine, it may be too late to influence decisions about the very intelligence support systems upon which the doctrine depends. Commanders using the new doctrine would have to do so using reconnaissance satellites extrapolated from the intelligence needs of the early 1990s.

Two other problems compound this situation. The first is the rapid development of commercial space and the increasing likelihood that our ability to use space freely will become threatened. US success in Operation Desert Storm stemmed in large part from our superior information predicated on spaceborne intelligence. Iraqi access to similar data sources was virtually denied. Today, three different US companies plan to launch commercial imagery systems before 2000 and are offering data from and access to these systems to a wide range of governments and commercial interests. By 2010, at least 10 nations will have their own imagery systems with resolution to 1 meter or less. Once others begin to take advantage of spaceborne intelligence technology, at a minimum there will be a narrowing of the gap we enjoyed in the Gulf war. As others come to understand the space reconnaissance business, covert military operations such as General Schwartzkopf's "Hail Mary" maneuver probably will become far more difficult to keep secret.

Second, the awareness that accompanies access to space will bring with it inevitable incentives to deny the use of space to others in time of conflict or crisis. In the worst case, interdiction could include attacks on our satellite reconnaissance systems or

the ground infrastructure that supports them. Because of policy decisions dating back to the Eisenhower administration, there has been a general assumption that use of space was available to all and that conflict in space was unthinkable. But, following a major Service war game in early 1997, Secretary of Defense Cohen was told by those who had played the Blue (US) side National Command Authorities, "Future adversaries will seek to reduce our information dominance.... It is to their advantage to render any [of our] space systems useless, thereby giving them parity in space which ultimately gives them asymmetric advantage."[2]

It is now public information that conflict in space is increasingly an issue in major war games. Space defense has been a topic on CBS's "Charles Osgood Show." *Aviation Week and Space Technology* has devoted increasing attention to space as a potential battleground. There have been open forums dealing with our space vulnerability, such as one that was sponsored by the Institute for Foreign Policy Analysis on Capitol Hill in October 1997. The US Space Command has declared that its primary mission in the future will be space control, rather than merely supporting other commands.

These developments are a particular concern at the National Reconnaissance Office (NRO), which has the mission of developing and operating the nation's imagery and signals intelligence satellites. The manner in which the NRO, and the broader IC which it serves, respond to these challenges will be critical to our national warfighting capability over the next two decades. In Desert Storm, we were fortunate to have the time to

"Satellite systems and information systems have to be built from the ground up with a fuller appreciation of the needs of the military."

build up our in-theater force structure and to use our intelligence satellites to serve operational needs. In the future, we may not be so fortunate. Consequently, both satellite systems and information systems have to be built from the ground up with a fuller appreciation of the needs of the military. The NRO cannot do it alone; increased cooperation and mutual understanding between the IC and operating forces are becoming essential.

A number of specific issues have to be faced. Should we build a satellite primarily to support the policymaker, or the military operator? What priority should be given to satellite system defense, including onboard countermeasures? How does the advent of widespread commercial remote-sensing satellites affect our strategy for using space? Who, and which systems, get priority in a period of declining budgets? These questions demand answers. Incremental thinking and evolutionary development probably will not get us there.

The time may have arrived to develop an IC-wide concept of operations, if not a formal doctrine, to provide general guidance for systems planning, budgeting priorities, and ongoing operations. To this end, a Joint Intelligence Operations Directorate might be created within the IC to give focus to integrating daily operations with military doctrine, planning, operations, and training. If, as *JV2010* avers, information superiority is the linchpin of future US military doctrine, it would seem that the IC should have a more central role in the military planning process, perhaps coordinated through the new position of Assistant Secretary of Defense for Command, Control, Communications, and Intelligence in the Office of the Secretary of Defense. The IC also has to continue to recognize the equity already invested in it by the national policymaking community, and to continue providing support for both long-range planning and crisis management.

The New Military Doctrine

The major difference in the nation's new military doctrine is that it is based on speed, rather than attrition. That is, the ability to make better operational decisions more swiftly, to move forces more rapidly in both a strategic and tactical sense, and to do both far more quickly than any adversary will enable us to use smaller, more agile forces more effectively than any prospective foe and to resolve any situation before it gets out of hand. Thus, *JV2010* stresses rapid and flexible maneuver, precision engagement from afar, and focused, just-in-time logistic support instead of large logistic bases. But underlying the ability to make more timely and better decisions is the assumption that we will have accurate and timely information.

A whole vocabulary has been created to capture the essence of this premise. *Sensor to shooter* implies that intelligence data will be fed directly to the operator holding the trigger of the gun, bomb-release, or missile (if not to the weapon itself). *Dominant*

battlespace awareness refers to the ability of the operational commander to have the big picture in sufficient detail to make both broad operational plans and real-time tactical decisions. *The revolution in military affairs* refers to this new form of information-based warfare. *Network-centric warfare* refers to the gridlike network system that will make this information readily available.[3]

Somewhat disingenuously, *JV2010* simply posits that superior, real-time, target-quality information will be available. Behind the jargon lie several key assumptions. The primary one is that everything of significance about the battlefield will be collected, fused, transmitted, and made available to the commander and that he then will be able to exploit that data to make faster, better operational decisions. Other assumptions are: command organizations will be "flattened" to create more direct connectivity between the commander and the operating unit; individuals at much lower levels will have operational decisionmaking authority; and communications systems will be sufficient to carry all this information.

These basic underlying assumptions themselves warrant further consideration. Information superiority will not just happen because of our superior technology. For example, in the Navy's annual major war game last summer, GLOBAL-97, which was the first major effort by the military services to examine *JV2010* at the operational level, it became evident that information superiority is not a "given" but must itself be an operational objective. In short, military planning and operations have to be optimized to use superior information, and to obtain, defend, and maximize it in both an absolute sense and relative to any adversary.

It behooves the intelligence world and the operating forces to get together and be sure that requirements and capabilities are in harmony.

How that will happen is yet to be determined. In some sense, the military is willing to leave it to the IC, figuring that is their business. But a system designed by intelligence experts, rather than military operators, would most likely be based on the information that can be provided, and it could be ignorant of what information is actually needed for operational decisionmaking.

A solution probably can be found: our ability to collect, process, and communicate data is growing exponentially. *But without adequate understanding of operational needs, and without adequate links to the operators themselves, we could easily reach a dead end in the realization of JV2010. Consequently, it behooves the intelligence world and the operating forces to get together and be sure that requirements and capabilities are in harmony.* To do that will mean doing business differently.

Some Disconnects

Developing satellite architectures based explicitly on future customer needs is a departure from the past. Heretofore, technology itself was the pacer for developments. The NRO encouraged, and then took major gambles on, promising technologies (which to a substantial degree is why the United States now is far ahead of the rest of the world in its intelligence capabilities). Capabilities were then adapted to emerging national and, to a lesser extent, to military requirements. The NRO's ability to do so resulted from a combination of national willingness to take risks, the fact that NRO's programs were based primarily on performance and schedule rather than cost, and the low profile that organization enjoyed in the public budgetmaking process. Those circumstances are shifting, yet it will continue to be important that America keep the lead in information capabilities, along with its ability to use space effectively.

Given the changing circumstances, the best way to link future satellite designs to future military needs may be to press for technological innovation within a broad, qualitative understanding of future military needs. Maintaining our leadership in R&D is essential to continue to maintain America's advantages in space. Breakthroughs such as those in the past may not be necessary, and it may be fiscally prudent not to take the sorts of technological risks deemed necessary during the Cold War. But continued technological innovation will be vital to maintain the information dominance that we now enjoy, and upon which *JV2010* rests. As the National Defense Panel recently pointed out, that means some false starts will occur; major attempts at innovation rarely succeed on the first try. We cannot afford to play it safe, and the penalties for failure have to be minimized.

In groping for answers on how to deal with the new military doctrine, the IC has been asking specific questions of the military. For example, in an NRO-OSD Net Assessment–sponsored war game series called *Forward Focus*, the questions have been: What sort of information do you need under various conditions?

How do you want it packaged? How quickly do you need it? The answers given provide substantial insights. But these are small-scale and isolated efforts, and they do not yet reflect broad efforts to harmonize the views of the two entities.

In sum, without explicit and in-depth institutional linkages between emerging military doctrine and intelligence support system development, decisions about intelligence programs are likely to be based on outdated assumptions and current interpretations of requirements rather than on emerging doctrine, future force structures, and streamlined command organizations. While performance improvements will be achieved, national assets will not have been optimized for supporting military operations under the envisioned new style of such operations, and the information superiority on which the new military doctrine depends will not be realized.

An example that illuminates the point is the debate pertaining to imagery satellites between what is called *wide-area coverage* and *rapid revisit point coverage.* Since Desert Storm, most attention has been on how to support wide-area coverage of the battlefield. One reason is that it is easy to describe what is wanted from satellites in terms of area coverage: image a large area and then figure out what is there by looking at the details. Much attention has gone into developing systems that can provide this capability with a high degree of assurance. Wide-area coverage suffices for strategic purposes such as finding out who is building new sites or pieces of military equipment, or for fixing the battlefield—that is, taking periodic snapshots to determine the location and recent movements of large-scale forces. In such cases, rapid responsiveness is not critical. Using Desert Storm as the model, wide-area coverage demands would dictate the best satellite architecture for the future.

JV2010 suggests otherwise. Rapid maneuver and use of long-range precision ordnance presume access to precise, dynamic, real-time, target-quality data. In the realm of overhead reconnaissance, this means very rapid revisit point coverage would be the priority requirement—that is, the desire to look for specific targets and at designated locations, roughly as one uses a highly focused flashlight beam. To optimize resolution of imagery, however, satellites have to be in low orbits, where they cannot have access to one place on the ground for more than a few minutes per pass. So what they will be looking for has to be determined well in advance. Any last-minute changes in satellite tasking are difficult, if not impossible, to accomplish.[4]

As a result, the demands for responsiveness placed on imagery satellite systems are extreme. Moreover, timeliness has to be met without compromising the wide-area coverage needed to support the strategic warning needs of the National Command Authorities. Similar issues could be raised for SIGINT satellites. To adapt the architecture—not just the satellites but the entire C4ISR system[5]—will require a careful rethinking of everything from system design to intelligence concepts of operation. Some in the IC, for example, have emphasized the role of aircraft and unmanned aerial vehicles as future collection platforms for tactical reconnaissance. But these take time to fly to targets of interest, and, as recent events in Iraq have demonstrated, airborne systems create substantial political problems—as well as unacceptable risks in the case of manned aircraft—when overflights are tried short of full-scale war.

In fact, for all the emphasis on optimizing satellite and airborne collection for battlefield support, there are, or at least there should be, some major cautions about moving too quickly or singlemindedly to do so. One is that the support which Intelligence, Surveillance, and Reconnaisance (ISR) systems need to provide to the military may not only be what the military calls "Intelligence Preparation of the Battlefield" for locating targets; it also may encompass enemy intentions and orders of battle, as well as detailed and highly focused requirements, something more akin to looking for needles in haystacks.

As to the last of these, intelligence systems optimized to support the military on the conventional battlefield may not be particularly well suited to the tailored and highly specific data that need to be collected on given individuals and fixed points. Specific, highly focused intelligence on such problems as movement of terrorists or elements of potential weapons of mass destruction, as well as drug trafficking and piracy, are important features of the post–Cold War era of national security for both the military and the national policy customer.

It is also obvious that the military will not be the sole recipient of data gleaned through national sensors. Civilian policy officials still are, and probably always will be, the primary day-in and day-out customers for satellite-generated material.

While operational information, such as locations of combat units and

their movements and emissions suggesting imminent attack, is key to military commanders in the field, national policy customers are more interested in longer term strategic warning: which countries provide likely threats, what are their intentions, and what force capabilities are they developing or are they likely to develop in the future? In those cases, long lead-times, more focus on intentions than on immediate capabilities, and an entirely different way of putting together the picture are required.

All this is compounded by the fact that the customer list for overhead imagery is growing, and as awareness of the value of our national systems spreads, the national customer demand on those systems is likely to keep increasing. Through civilian authorities, NRO systems supported assessments in national emergencies such as the Northridge, California earthquake and Hurricane Andrew. In a Federal Emergency Management Agency interactive exercise in 1996 involving a potentially catastrophic earthquake along the New Madrid Fault underlying the Mississippi River, participants learned about the information that NRO assets could provide to help them quickly understand the situation they had to deal with. As a result, the NRO was one of the first places those same state participants turned for information in major floods that subsequently occurred in the central United States. *Aviation Week* went so far as to advocate that "reorientation of intelligence to support 'public agents' [that is, nongovernmental organizations, corporations, and even individual citizens who pursue international political, social, and economic objectives] may be the key to the transformation of the Cold War Intelligence Community."

"The customer list for overhead imagery is growing, and as awareness of the value of our national systems spreads, the national customer demand on those systems is likely to keep increasing."

With all these considerations in mind, *our national intelligence sensor systems probably should not be designed solely with the evolving military doctrine in mind, nor is direct military control of national assets the solution.* Alternative solutions are needed because of the array of customers for national systems and the wide range of their intelligence needs. But there is more: there is a fundamental distrust by the military that in a pinch it really will have access to national sensor information to the extent needed.

The cultural and doctrinal views of senior military commanders encourage the continuation of building indigenous military systems and developing operational plans based on an implicit assumption that national systems cannot be depended on. There are several reasons for this, including inadequate hooks to accept intelligence from national systems, old-fashioned service parochialisms, and, above all, the discomfort military commanders experience when they have to depend on assets they do not control. As a major study of lessons learned in Desert Storm put it, "Combat units are most comfortable and practiced at integrating their weapons with intelligence and targeting sensors which are organic." Or, in the words of one Army field commander, "I would be begging for coverage, and that is not acceptable."

Until and unless a process is developed which will ensure that national systems can be relied on, such as time sharing, task sharing, or building sufficiently flexible systems so that all customers can be supported simultaneously, this deep-seated military instinct is unlikely to change. Yet these views are maintained at a high dollar cost because of the redundant capabilities that result. If there is to be any hope of changing that situation, the IC must improve its understanding of, and cooperation with, military operations, and vice versa.

Finally, future intelligence linkages to military support have to be framed with a broad understanding about potential risks to space operations. Otherwise, we risk blundering into a destabilizing situation in which the disadvantaged side in a given crisis, feeling desperate, resorts to irrational means to deny us the use of space, or at least of space-derived data. Realistic, if not extraordinary, threats need to be included in the process by which future satellite systems are designed, assessed, built, and operated. If warranted, protection concepts could be designed into the NRO's satellite architectures.

In a related sense, there are significant policy issues associated with this emerging threat of warfare in space that have not yet been adequately addressed. These issues are as broad and significant as those faced with the advent of nuclear weapons in the 1950s, and they demand the same sort of analytic and philosophical rigor and innovative thinking as was

done in that era by Herman Kahn, Henry Kissinger, and others. This is not a technological or military problem. All aspects, however, affect how the NRO designs the next several generations of the nation's intelligence satellite.

Determining Future Intelligence Needs

How can military commanders become more comfortable with depending on national assets to provide them with the information they need when they need it? The effort to articulate these needs has to begin now, and some specific ways in which the IC traditionally has operated need to change. The reality is that there now exist two major approaches to how future generations of national satellite systems should be designed. One is "same, but better": wide-area coverage, support for national strategic warning, and perhaps substantially more coverage by changing the mix of collectors. The other approach is what *JV2010* envisions: a fused, integrated, joint, and responsive intelligence picture that directly supports the warfighter.

Using past practice to determine which road to take is not helpful. Typically, requirements for intelligence satellite systems have been developed by focusing on some aspect of the threat, or by positing future scenarios and then asking for inputs on how much and what sort of coverage would be needed to support related military operations. Target sets are compiled, total volume and capacity performance are determined from the inputs, and these are validated, filtered, reviewed by the Services and the CINCs, and finally codified. Candidate systems are evaluated based on their ability to satisfy these "agreed" requirements.

"To use today's process for determining the next generation of satellites would be like trying to drive down a road looking only in the rearview mirror."

But, given the contemplated changes in our military doctrine, to use today's process for determining the next generation of satellites would be like trying to drive down a road looking only in the rearview mirror. That this is a fundamentally reactive process should be no surprise. It was never designed or intended to account for whether military forces would operate differently 10 to 20 years hence, because there was no fundamental change in military doctrine during the Cold War. With the advent of a new military doctrine, however, determination of ISR requirements, and the systems needed to fill those requirements, has to become anticipatory rather than reactive.

War games, such as those sponsored by the Service war colleges, and games developed specifically by the NRO and OSD, have been found to be a useful crystal ball. Key insights pertaining to ISR that have emerged from these various games include the following observations:

- Future military success will depend on our ability to expedite the fusion-analysis-dissemination loop, collect intelligence on new threats, provide near-continuous coverage of high-interest targets, and maintain an adequate strategic warning capability, all for the purpose of facilitating decisionmaking by the military commander.

- Devising measures for understanding and assessing the relative importance of "battlespace awareness" to engagement outcomes will be crucial in making asset acquisition, deployment, and employment decisions.

- ISR capabilities have to be included on CINC Integrated Priority Lists (annual submissions of top requirements for future military warfighting capability). One way to make sure they can get there is by ensuring that ISR assessments are included in warfare assessment models and that ISR interactions can be independently assessed for operational impact.

- Streamlining the flow of intelligence from sensor systems to operators will require flatter command structures, more autonomy to forward-operating forces, and commensurate revisions in training, doctrine, and command.

- However good our ability to collect against specific battlefield operations, it is still necessary to prepare the battlefield by learning about our adversary's intentions in addition to enumerating capabilities and selecting targets.

- An adversary that feels itself disadvantaged because of America's dominant ability to use space may opt to "level the playing field" by attacking our ISR systems, either in space or on the ground.

- Consequently, operational success in the theater will depend on our

ability to retain and defend our space-based ISR, communications, and navigation capabilities.

- Space-based threats may be difficult to overcome, unless and until we specifically design better protection schemes into spacecraft designs and reconnaissance architectures.

In addition to these emerging trends, conclusions from the first three games of the *Forward Focus* war game series endorsed the need for more agile intelligence about specific events or activities, contravening the traditional and widely held understanding that what is primarily needed is wide-area coverage in order to "fix the battlefield" once per day. Specifically:

- The time available within which to plan (that is, between the request and the time to act) was the most critical variable in determining the specifics of intelligence that need to be provided.

- Wide-area coverage was necessary, but not sufficient, for the sort of operations envisioned by *JV2010*.

- In ambiguous planning situations, such as those associated with war avoidance and crisis management, the demand tends to increase for more in-depth, higher quality knowledge on a more complex range of objectives as well as target sets.

- In combat situations, military operators placed a higher value on responsiveness to tasking against a small and discrete set of targets than on detailed information that would require more time to deliver.

Reports from the field suggest that the NRO has come a long way . . . since Desert Storm in terms of providing direct support to operating forces. But the deep-seated concerns of senior military operators persist.

A final important insight that arose from the *Forward Focus* series was that, in cases where players were presented with preconflict crisis avoidance and military contingency planning situations, *they deemed it much more important to understand an adversary's intent and behavior than just to react to his initiatives.* If this is valid, then military intelligence support will have to be much broader than just target location and identification. This notion contravenes *JV2010's* subtle implication that merely detecting an event or target and recognizing a few characteristics may be sufficient, and that understanding an adversary's intent and plans need not be an explicit design goal.[6]

Toward Some Solutions

The IC is going to have to demonstrate its ability to deliver. To some extent, it has to: demonstrate a willingness to relinquish direct operational control of national satellite and airborne systems in exercises as well as for operational support; supplement national support systems by providing commercial imagery directly to the military commander; and build sufficient flexibility into its satellites and information support systems so that all customers can be served based on their need.

Reports from the field suggest that the NRO has come a long way in just the few short years since Desert Storm in terms of providing direct support to operating forces. But the deep-seated concerns of senior military operators persist. What seems to be needed is some sort of "partnering" arrangement to achieve related but not identical missions, using common systems, and a mutual understanding of both needs and capabilities. An IC-wide "concept of operations" to parallel how the military uses doctrine seems unavoidable.

The NRO has to think innovatively about how to satisfy the need of military commanders while also continuing to service its national customer base. Conceptual solutions are needed as well as improved technological capability. But conceptual solutions imply more than just a single-agency approach: a broader consensus needs to be reached among the various members of the IC on how they are to operate in concert to service their collective customers.

This requires Community-wide thinking to develop a common framework—what the military would call a "Concept of Operations." At this point, the issues are too broad and the Community too diverse and stovepiped. But successful precedents do exist. The Navy, for example, evolved from a stovepiped set of autonomous members driven by technology developments in the 1970s to a coherent organization based on a unified strategic planning and force development approach under what it

called the Maritime Strategy in the 1980s.

The foregoing illustrates the complexity of integrating *JV2010*, with emerging Service capabilities, and underscores that the development of new ISR capabilities will require taking some pragmatic steps before *JV2010* can become reality. This is all the more important, given other ongoing changes that include the changing national security environment, the advent of the possibility of warfare in space, the burgeoning use of space for commercial purposes, and the growing dependence of national policy customers on our national intelligence systems.

Specifically, we recommend the following to start to deal with these complex issues:

- Consideration should be given to chartering an institution of intelligence strategy and operations specifically to help anticipate uses of intelligence as it relates to evolving national strategy and future military operations—a Joint Intelligence Operations Directorate. This might operate along the lines that TRADOC does for the Army. It might be an adjunct to the National Defense University. Within its charter would be developing strategies for the operational uses of intelligence; determining future doctrine requirements for ISR and helping translate them into system requirements; assessing offensive strike versus force defensive needs; improving understanding of the value of ISR to combat campaign-level analysis by incorporating ISR into campaign-level assessment models; and engaging in the necessary dialogue about the linkage of space warfare and national sensor systems as it relates to framing policy options, strategies, doctrine, and operational patterns.

- All Flag Officers, either in their mandatory introductory Capstone course or in the Joint Flag Officer Warfare Course taught at Maxwell Air Force Base, should be provided an expanded module having to do with the operational dimensions of ISR in military planning and operations.

- War gaming and modeling should continue to be used extensively at various levels to explore the importance of space-derived intelligence data and the means of ensuring its collection and delivery.

- The NRO should continue to participate in and support the major Service war games.

- The NRO should open a dialogue with other IC members and with the CINCs and military services about how direct operational control of national reconnaissance assets can be passed to the operational commander, how this can be exercised, and how it would work in wartime, along with research into what this would mean to system parameters. Clear lines of responsibility would need to be developed for this effort, which might lead to the establishment of a J-3-like position for managing and operating satellite reconnaissance systems, as well as other platforms, to support crisis or military operations.

- The NRO should encourage and participate in a national public dialogue about the implications of space becoming a future battlefield.

- Assessment tools such as models, simulators, and demonstrators should be developed to evaluate futuristic concepts of operations rather than old ways of doing business. Measures of Effectiveness for the value of information and time have to be incorporated into assessment models. To that end, the NRO should work with others in the IC and in the US Space Command to build new families of models that would be more useful in assessing the operational impact of activities in an era when information, time, and forces and weapons are important.

- Finally, the IC needs to develop a "concept of operations" that provides a common-sense view of what it is about, how it does its work, and how its various components work in harmony to provide better support to all of its customers.

The era in which multiple intelligence agencies, operating autonomously and behind the "green door" of security cloaks and classified budgets, can apply the latest and greatest technology in a fiscally unconstrained manner is over. The overriding requirement for intelligence in joint military operations also means that the IC has to coordinate more directly everything from DoD budget decisions to development of military concepts of operations. The operational aspects of obtaining and analyzing intelligence, as well as exploiting it in future operations, cannot be assumed away. A new era in national security planning, centered around information superiority and its thoughtful application, has begun.

NOTES

1. The IC generally refers to the CIA, DIA, National Reconnaissance Office, NSA, and National Imagery and Mapping Agency, along with the intelligence offices within the military services and some civilian agencies. Their collective activities are coordinated, albeit not directed, by the Director of Central Intelligence and are overseen by the President.

2. Richard Armitage and David McCurdy, two senior policy advisers, played the National Command Authority in the January 1997 war game *Army After Next*. They felt strongly enough about what they experienced that they co-drafted a letter to the Secretary of Defense advising him about the impending risks having to do with our use of space in a crisis.

3. The term was placed into the lexicon by VAdm. Arthur Cebrowski, the Navy's Director for Command and Control, Communications, Computers, and Intelligence, Surveillance, and Reconnaissance.

4. Satellites can be placed in geosynchronous orbit—at an altitude of about 22,000 nautical miles—where they essentially stay in the same place relative to a point on Earth. While these satellites can perform missions such as missile warning, communications, and weather reporting, they are too far away to have the resolution required for militarily useful imagery.

5. The term refers collectively to "Command and Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance." Over the past two decades, these various functions tended to be merged into one overarching concept. Recently , however, a movement has been growing to separate intelligence components (ISR) from Command and Control, Communications, and Computers; the jury is still out on what Defense Department organizational changes will result.

6. The December 1997 report by the Congressionally chartered National Defense Panel, which the Secretary of Defense endorsed, challenged the Defense Department to broaden the range of contingencies for which force structure is planned. The report highlighted, for example, concentration on homeland and WMD defense and low-level conflict in addition to projection of conventional forces into various theaters.

Center for the Study of Intelligence
Washington, DC 20505