Order Code RL31425

Military Transformation: Intelligence, Surveillance and Reconnaissance

Updated January 17, 2003

Judy G. Chizek
National Defense Fellow
Foreign Affairs, Defense, and Trade Division

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
17 JAN 2003	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Military Transformation: Intelligence, Surveillance and Reconnaissance	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Congressional Research Service Library of Congress 101 Independence Avenue, SE Washington, D.C. 20540-7500**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**33**	

Military Transformation: Intelligence, Surveillance and Reconnaissance

Summary

The Department of Defense (DOD) indicates it is undertaking a major alteration in its capabilities, from a force designed to fight the Soviet Union to one tailored to 21st century adversaries including terrorism. This shift has been prompted by the perception of a changing threat and improved technology, especially information technology. As the military services attempt to increase the agility and versatility of their weapon systems, they also see a need to increase the capabilities of military intelligence, surveillance and reconnaissance (ISR) to support the new weapon systems and operating methods against these new threats.

To judge whether service activities are likely to help the military "transform," the head of DOD's Office of Force Transformation, retired Vice Admiral Arthur Cebrowski (U.S. Navy) has proposed three criteria–whether the proposed capability can communicate and operate easily in conjunction with the other services, whether it helps the military develop new methods of warfighting, and whether it will be useful against a wide range of threats. In addition, ISR activities should, in the aggregate, provide a world-wide perspective of the threat, "fuse" all types of intelligence into one picture, access extensive details about the enemy, and monitor specific targets for long periods of time.

All of the services are planning ISR programs which exhibit at least some attributes of transformation. Many observers believe military ISR has already achieved some transformation, as shown in the war in Afghanistan by the military's ability to detect a target and destroy it within minutes. The military's ability to move intelligence quickly has improved dramatically. However, many observers are concerned that analysis may be lagging behind. Proposals to make revolutionary changes in analysis include using contractors to produce competing unclassified analyses, developing artificial intelligence capabilities for database work, and establishing more operations analysis centers.

The military intelligence community is supported by the national intelligence community, which even before the September 11 attacks was under intense scrutiny. Therefore, the aspects of the national intelligence community's operations in which Congress has expressed interest directly affect the quality of military intelligence. In addition, DOD's plans for improving its ISR capabilities raise potential issues for Congress with regard to cost, the balancing of potentially competing efforts to improve the flow of intelligence and the quality of the data, and the support of military leadership. Finally, the consequences of the military's role in homeland defense, and intelligence community reform may generate concern. Discussion of these issues is provided as background as Congress considers ISR programs as part of defense and intelligence authorization and appropriations legislation. This report will not be updated.

Contents

Note: This update of CRS Report RL31425, originally published on May 31, 2002, was prepared by Richard A. Best, Jr., Specialist in National Defense in the Foreign Affairs, Defense, and Trade Division. Questions concerning the Report may be directed to him at 202-707-7607.

Military Transformation: Intelligence, Surveillance and Reconnaissance

The Defense Department (DOD) indicates it has embarked on a huge effort, labeled "transformation," to dramatically shift from a force prepared to fight the Soviet Union to a force suitable for 21st century adversaries, including entities who conduct or are otherwise associated with terrorism. A key component of this transformation is DOD's Intelligence, Surveillance, and Reconnaissance (ISR) capability.[1] If ISR does not meet the needs of the 21st century force, much of the effort to shift to new kinds of forces and modes of operation could be wasted. Although the war in Afghanistan, Operation Enduring Freedom, has been widely cited as proof that DOD is successfully transforming,[2] Congress remains concerned that ISR capabilities may not be able to meet the needs of military force unless they also undergo significant change, particularly in the areas of Human Intelligence (HUMINT), analysis, and integration with the services' networking initiatives.[3] This paper will address ISR transformation from an unclassified perspective. Some aspects of ISR transformation can only be discussed in classified fora and are therefore omitted.

ISR Background

Definitions

The Department of Defense defines intelligence as "information and knowledge obtained through observation, investigation, analysis, or understanding."[4] Surveillance and reconnaissance refer to the means by which the information is observed. Surveillance is "systematic" observation to collect whatever data is available, while reconnaissance is a specific mission performed to obtain specific data. For the purposes of this paper, the distinctions between intelligence, surveillance, and reconnaissance are not important unless specified–ISR is used as

---

[1] Secretary of Defense's Transformation Study Group, *Transformation Study Report*, April 27, 2001, p. 23. [http://www.defenselink.mil/news/Jun2001/d2001062transexec.pdf]

[2] See, for example, National Public Radio interview with Major General (retired) Perry Smith and Richard Hallion, *Morning Edition*, November 21, 2001; and Daniel Goure, "Location, Location, Location," *Jane's Defence Weekly*, February 27, 2002, http://jdw.janes.com.

[3] U.S. Congress, 107th Congress, 1st session, Committee of Conference, Intelligence Authorization Act for Fiscal Year 2002 H.Rept. 108-328, December 6, 2001, p. 18.

[4] Department of Defense, *Joint Publication 1-02, DOD Dictionary of Military and Associated Terms*, 12 April 2001, as amended 15 Oct 2001, p. 214.

a shorthand to refer to the system of collection assets and analysts which brings information about the enemy or potential enemy to the decision-maker, whether that decision-maker is a top general in Washington, DC or a soldier on the ground facing an armed attacker.

Sources

Another shorthand commonly used by the military services and the intelligence community refers to the source of any given piece of intelligence. Intelligence which comes from a person observing it is called Human Intelligence, or HUMINT. Intelligence derived from photographs and other imagery is called Imagery Intelligence, or IMINT. Intelligence obtained from electronic signals such as communications is called Signals Intelligence, or SIGINT. Finally, intelligence derived from other technically measurable aspects of the target, such as vibrations or hyper-spectral emissions, is named Measurement and Signatures Intelligence, or MASINT.[5] These terms are important, as they help characterize the basic structure of the intelligence community.

Military Intelligence Community

The Central Intelligence Agency (CIA), State Department, Department of Energy, Department of Justice, and Department of Treasury all contribute to the intelligence picture available to the military.[6] However, most intelligence used by the military comes from the Defense Intelligence Agency (DIA), which produces some HUMINT, MASINT and a large portion of the Defense Department's strategic, or long-term, analysis; the National Security Agency (NSA), which produces most SIGINT; and the National Imagery and Mapping Agency (NIMA), which produces most IMINT. The services themselves also produce all types of intelligence for the community.

Transformation Background

Today's security environment appears to be quite different from the environment of only ten years ago. Major shifts in both the threat to our national security, and the technologies available to us and our potential adversaries, seem to have occurred. In response, the military services have plans to change their ISR capabilities to meet the new environment effectively.

---

[5] For further explanation and discussion of the types of intelligence sources, see Richard A. Best, Jr., *Intelligence Issues for Congress*, CRS Issue Brief IB10012.

[6] Department of Defense, Joint Publication 2-02, National Intelligence Support to Joint Operations, 28 September 1998, p III-2.

Changed Environment

Most of today's military equipment and organization was originally designed to fight the Soviet Union. A common scenario was that the Soviets and their Warsaw Pact allies would attempt to occupy all of Western Europe, using large numbers of tanks and aircraft to sweep through Germany on their way to the rest of the continent. Defense against such an assault was perceived to require heavy weapons such as tanks, fighter and bomber aircraft, and aircraft carriers. However, the Warsaw Pact has collapsed and a similar threat has not emerged. Instead, the security environment looks significantly different compared to 1989. DOD's 2001 Quadrennial Defense Review (QDR) points out that we "cannot predict with a high degree of confidence the identity of the countries or the actors that may threaten (our) interests and security." The QDR explains DOD's perception of the changed threat by stating that the U.S. is no longer physically protected by distance from its adversaries. It sees a "broad arc of instability" from the Middle East to Northeast Asia, where non-state entities whose activities are damaging to U.S. interests (drug traffickers, terrorists, etc.) are growing in strength and finding safe-haven in weak and failing states. In addition, new technologies (especially information technologies and those related to chemical, biological, radiological, nuclear, or enhanced high-explosive weapons) are increasingly within the reach of potential adversaries, and warfare may extend to space and cyber space.[7]

Outside observers, including other members of the national intelligence community, generally agree with DOD's characterization of the threat. Concern over surprise, deception, increasingly diverse threats, weapons of mass destruction, the Middle East, and Asia, appears consistent. Some add that non-state actors with new technology may undermine nation-state control in many countries. This could exacerbate the effects of environmental deterioration and disaster, increasing the probability that the U.S. would feel compelled to deploy its military forces to stem a resulting humanitarian crisis.[8]

In sum, many analysts believe the U.S. is now faced with "asymmetric warfare," in which means such as drug-trafficking, terrorism, and biological warfare would be used to attack our interests. The events of September 11 appear to confirm the judgement that the threats of the future are unlikely to look like the threats of the past. Because these are means that the United States would not choose to employ itself and which bear no resemblance to the old Warsaw Pact tank assault scenario, some believe the U.S. military is currently ill-prepared to deal with them.

In addition to the changed threat, the U.S. military along with the rest of society also has experienced major changes in the technologies available. The huge increases in both information processing technology, including data collection and storage, and communications technologies such as increased bandwidth and

---

[7] Department of Defense, *Quadrennial Defense Review Report*, September 30, 2001, p. 3.

[8] Gregory F. Treverton, *Reshaping National Intelligence for an Age of Information*, Cambridge University Press, Cambridge, UK, 2001, p. 28. See also Bruce D. Berkowitz and Allan E. Goodman, *Intelligence in the Information Age*, Yale University Press, New Haven, CT, 2000, pp. 5-11.

networking, appear to be able to completely change the way military forces are equipped, organized and employed.[9]

Definitions

Based on these changes in both the threat and in available technology, DOD states it must "transform." Transformation in the context of large organizations such as the Defense Department is generally recognized as a process of radical change involving technology, organization, and concepts of employment. Another term used in military theory which also expresses the idea of transformation is "revolution in military affairs." However, even within DOD there are at least two competing perspectives on what constitutes "transformation." Some personnel define transformation as a discontinuous or leap-ahead change.[10] This view supports those who believe it is necessary to move money, manpower, and particularly patterns of thinking ("doctrine") away from current weapon systems and methods to entirely new technologies and procedures. They perceive that resources are being wasted on the older systems, and the only way to accomplish change is to do so in a radical way. The Navy's shift in the 1920s and 30s from the battleship to the aircraft carrier as its centerpiece weapon system could be considered an example of a leap-ahead change, even as the battleship remained in service until the 1980s. The Army's plan to replace its tank force in favor of much lighter vehicles and other technologies may be seen as an attempt to achieve similar change.[11]

Others tend to define transformation as incremental change using current or modernizing technologies in new ways, with an end result of radical improvement over time. They express concern that the future is unknown; if DOD cuts out proven capabilities for new ones, those new capabilities may not match the currently unforeseen threat any better than today's technology. A proven technology, however, may be able to be adjusted to meet that unknown situation. These officials point to examples such as the change in the military's ability to attack targets from the air, comparing Operation Desert Storm against Iraq in 1991 to Operation Enduring Freedom against Afghanistan in 2001. Nearly every weapon system which was used in Afghanistan had also been used in Iraq in 1991. However, improved communications, procedures and the Joint Direct Attack Munition (a standard 2000 lb bomb which can be guided using Global Positioning System technology) allowed B-52 bombers to attack targets which were very close to friendly military personnel

---

[9] See, for example, Michael L. Brown, "The Revolution in Military Affairs: The Information Dimension," *Cyberwar: Security, Strategy and Conflict in the Information Age*, edited by Alan D. Campen, Douglas H. Dearth, and R. Thomas Gooden, AFCEA International Press, Fairfax, VA, 1996, pp. 32-52; Bill Keller, "The Fighting Next Time," *New York Times Magazine*, March 10, 2002, p. 32.

[10] Gail Kaufman and Gopal Ratnam, "U.S. Navy Releases Broad Transformation Outline," *Defense News*, April 15-21, 2002, p. 8.

[11] Edward F. Bruner, *Army Transformation and Modernization: Overview and Issues for Congress*, CRS Report RS20787.

with little risk of hitting the friendly soldiers. This would not have even been considered in 1991.[12]

Transformation Criteria

Regardless of how transformation may be defined, retired Vice Admiral (USN) Arthur Cebrowski, the chief of the Defense Department's Office of Force Transformation, has identified some criteria by which military programs may be judged for their transformational qualities. His top criterion is that the weapon system or operating procedure be **interoperable**. Interoperability means that the system can function easily with a variety of other systems, including those from other services.[13] Other criteria Cebrowski has named are judgements as to whether the system helps the user to **change warfighting methods**, as opposed to merely improving existing methods; and whether the system can deal with a **wide range of threats**.[14]

Observers generally agree with Cebrowski's criteria. For example, Andrew Krepinevich, Executive Director of the Center for Strategic and Budgetary Assessments, also notes the requirement for interoperability and support to new warfighting methods, and discounts any hard and fast rule that a program must employ new technology to be considered transformational. At the same time, Krepinevich, along with some other observers, advocates the leap-ahead definition of transformation, and therefore would likely want to see larger changes in interoperability and warfighting methods than might Cebrowski.[15]

ISR Criteria

In addition to assessing the military services' ISR programs based on Cebrowski's informal criteria for transformation, it may be helpful to look at what ISR they will really need. Some commonly recognized characteristics include a **world-wide perspective, fusion, detail, and persistent surveillance**.[16]

The transformed force, much more than the Cold War force, needs a truly world-wide perspective derived from world-wide collection capabilities and in-depth analysis. During the Cold War, the threat from the Warsaw Pact was considered so great that military activity in other places often was considered inconsequential, or

---

[12] Goure, "Location."

[13] See Anthony W. Faughn, *Interoperability: Is it Achievable*, Center for Information Policy Research, Harvard University, October 2002, pp. 5-6.

[14] Gail Kaufman and Amy Svitak, "Pentagon Develops New Transformation Criteria," *Defense News*, March 11-17, 2002, p. 4.

[15] Andrew F. Krepinevich, "Defense Transformation," Testimony before the United States Senate Committee on Armed Services, April 9, 2002.

[16] Berkowitz and Goodman, pp. 112-123; Transformation Study Group, p. 30.

a "lesser included threat."[17] The intelligence community therefore put greater effort toward monitoring the Warsaw Pact than the rest of the world. Today, however, the threat may in fact come from within a country which appears quite non-threatening. For example, one former Central Intelligence Agency analyst notes that, in 1998, half of the foreign crises which demanded U.S. attention occurred in "lower-priority areas,"against which fewer analysts and collection resources had been allocated.[18]

Fusion refers to bringing together all types of intelligence to create one consolidated picture of the threat. As mentioned in the beginning of this paper, the various sources of intelligence form the basic structure of the intelligence community. That is, every piece of intelligence data is identified by whether it came from HUMINT, SIGINT, IMINT, or MASINT. In addition, these data are often kept in separate communications channels and databases designed to support the unique aspects of the data collected. A piece of imagery, for example, requires different bandwidth, software, and hardware for transmission than does a communications intercept, and they each fill completely different types of fields in a database. However, military forces cannot easily use separate HUMINT, SIGINT, IMINT, and MASINT data. They need one "fused" assessment of the threat. While this has always been true, the speed and precision with which the transformed force is expected to act makes this fusion even more desirable, as it presents information about the enemy in a timely, clear manner.

The transformed force may also seek more detailed information than before. First, given today's emphasis on precise application of force while mitigating risk to U.S. and civilian personnel, the intelligence required to employ destructive force such as a bomb or artillery round has increased. As adversaries hide within civilian populations or inside mountains, the once straightforward process of identifying potential targets has become much more complex. Once a target has been identified for destruction, the information required to successfully employ the weapon is increasing as target coordinates must be accurate to within a few feet in three dimensions. Even after a weapon is employed, the assessment of whether the target is destroyed, known as bomb damage assessment (BDA), has also increased in difficulty. In the Cold War, this was performed primarily by comparing "before" and "after" images of the target. If a target such as an enemy tank looked destroyed, with its turret blown off or smoke coming out of a gaping hole, then it probably was. Weapons used by the transformed force, however, may not cause that type of visible damage. Even in Operation Desert Storm against Iraq, precision-guided munitions made only small holes in Iraqi tanks as they penetrated and completely obliterated the insides. This damage, however, could not be seen from imagery. Other types of information, such as hyperspectral data which might detect whether the tank got very hot from internal explosions, are needed to make an accurate damage assessment. Second, as opposed to most Cold War scenarios, physical destruction is not the only effect the transformed force may be able to bring against the adversary. The military force may, for example, be able to accomplish its objectives by isolating an opposing

---

[17] Berkowitz and Goodman, p. 114.

[18] John B. Gannon quoted in "Time for a Rethink," *Economist*, April 20-26, 2002, [www.economist.com].

commander electronically. However, creating or defending against this type of effect requires extremely specific intelligence.

The ability to continuously monitor a given target and provide immediate assessment of changes to it, known as persistent surveillance, is seen as essential to the transformed force's ability to defeat unconventional enemies like terrorists.[19] As has been seen in Kosovo and Afghanistan, detailed, long-term surveillance of a house or convoy, such as that provided by a Predator Unmanned Aerial Vehicle (UAV) or a special operator on the ground, is key to properly identifying all personnel in the target area and maintaining full awareness of all activities, hostile, friendly, or neutral. The assessment that the desired target is present and can be effectively struck must then be made and communicated to the striking force within seconds, so that the opportunity is not lost.

Some experts express caution about these characteristics. They assert that doctrinal writings about the transformed force assume perfect access to perfect intelligence, that training its personnel to rely on such intelligence will prevent them from learning initiative, and that reliance on perfect intelligence may keep the U.S. from acting in circumstances where it needs to act but, for whatever reason, its precision-guided munition or other high-technology asset cannot be used.[20] The U.S. intelligence community does not have eyes and ears everywhere in the world, and it does not have perfect vision into potential adversary minds. Transformation advocates, when asked, recognize the fact of imperfect intelligence and respond to this criticism by emphasizing the planned force's agility, in equipment and training, to overcome situations where intelligence is imperfect and respond quickly to the evolving circumstances.

DOD Plans for Future Forces

To assess the intelligence, surveillance and reconnaissance aspects of military transformation, it is useful to have a basic understanding of the military forces which the future ISR structure will be expected to support. This section explains, in general terms, DOD's plans for future forces, and provides greater detail on ISR programs. All of the services are planning their forces in light of the changed threat and new information technologies. In general, the changes are intended to increase the force's access to information, agility and versatility while maintaining or increasing its lethality.

OSD and JCS. The Office of the Secretary of Defense (OSD) and the Joint Chiefs of Staff (JCS) have multiple initiatives touted as supporting ISR. While neither organization procures weapon systems, they do have a voice in funding, research and development, operating methods supported, and joint organization.

---

[19] General Richard B. Myers, Chairman, Joint Chiefs of Staff, DOD News Briefing, December 11, 2001.

[20] For example, see Mark M. Lowenthal, "Grant vs. Sherman: U.S. Military Doctrine and the Future of Combat Leadership," Handel International Strategy Conference, available at www.nwc.navy.mil.

In November 2001, Secretary Rumsfeld established an Office of Force Transformation, headed by retired Vice Admiral Cebrowski, to monitor and push transformational ideas in the services. The office is staffed by approximately 18 uniformed and civilian personnel from all the services and 15 contractors, and focuses on five broad areas–strategy, concept formulation, technology and technological surprise, joint and service experimentation, and operational prototyping. The office intends to assess service plans with respect to these areas, and make recommendations to the services and OSD which identify gaps in DOD's capability to meet potential threats, increase efficiency, improve existing capabilities, and recognize outmoded paradigms which should be changed.[21] The OFT is studying Operation Enduring Freedom to determine whether there are completely different ways it could have been approached, and also seeking to provide seed money to service experiments which appear transformational.[22]

Two key offices for developing technology, the Advanced Systems & Concepts Office and the Defense Advanced Research Project Agency (DARPA), have strong track records in ISR development. For example, DARPA developed both the Predator and Global Hawk Unmanned Aerial Vehicles, then handed them off to the Advanced Systems & Concepts Office for further development as Advanced Concept Technology Demonstrations (ACTD). Although still in developmental status, both aircraft have contributed substantially to the war in Afghanistan.[23] Both offices appear to continue to consider ISR as a significant area for research. For example, of the 15 ACTDs which the Advanced Systems & Concepts Office established for FY2002, five are technologies which promise to improve the military's ability to collect data on enemy forces. Another may substantially improve the ability of commanders to control surveillance and reconnaissance assets over the battlefield. A final ACTD aims at new ways of analyzing intelligence.[24] DARPA is developing continuing advances in unmanned vehicles, a foliage-penetrating radar, an advanced ISR management program, and artificial intelligence for database analysis.[25] Its recently formed Information Exploitation office is specifically intended to work on improving the military's ability to identify a target on the battlefield and communicate that information quickly to a weapon system for destruction.[26]

---

[21] Vice Admiral (ret) Arthur Cebrowski, "Special Briefing on Force Transformation," *DOD News Service*, November 27, 2001. Also discussions with Col Donna Kenley, Office of Force Transformation, 18 January 2002.

[22] Bill Keller, "The Fighting Next Time," *New York Times Magazine*, March 10, 2002, p. 32.

[23] Bruce Rolfsen, "On-the-Job Testing," *Air Force Times*, January 21, 2002, p. 12.

[24] Deputy Undersecretary of Defense for Advanced Systems and Concepts website: [http://www.acq.osd.mil/actd/descript.html] as of March 18, 2002.

[25] Dr. Tony Tether, Director, DARPA, Testimony before the Subcommittee on Military Research and Development, Committee on the Armed Services, House of Representatives, June 26, 2001.

[26] John Markoff, "Chief Takes Over New Agency to Thwart Attacks on U.S.," *New York Times*, February 13, 2002, p. A27, col.1.

The Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD/C3I) has oversight of ISR concept development. It has divided ISR initiatives into five categories. First, as discussed above, are collection technologies. Second are efforts for interoperability and networking, ensuring that all intelligence available to one entity is also available to other entities working in the same theater.[27] A major contribution to this effort is ASD/C3I's coordination of the Distributed Common Ground System (DCGS). DCGS is an umbrella term for several systems tailored to individual service requirements. These systems are designed to receive and process HUMINT, SIGINT, IMINT, and MASINT data (all of which come in different forms and often on different networks), support analysis of the data, and distribute intelligence to their customers, both on the battlefield and at higher headquarters. DCGS is recognized as being extremely important to all of the services, and they are moving toward this single, integrated architecture.[28] ASD/C3I's third category for initiatives is persistent and responsive surveillance, with programs such as the Global Hawk long-endurance UAV, the Army's Aerial Common Sensor, and Space-Based Radar. Fourth, the office seeks new ways to use existing capabilities, such as getting imagery to be automatically tagged with all required geographic coordinate information. Finally, ASD/C3I is working on the communications technology needed to move the collected intelligence to its customers.[29]

Other than its work on DCGS, some ISR planners discount ASD/C3I work, noting that they coordinate directly with the other services without prompting from the OSD office, while ASD/C3I may push "one size fits all" solutions.[30] Some observers also believe that ASD/C3I has little actual authority, with the result that services continue to do what they think best for themselves. Most of ASD/C3I's power appears to come from its direct access to the Joint Requirements Oversight Council (JROC), which is chaired by the vice chairman of the Joint Chiefs of Staff.[31] The JROC validates major service programs as being either "joint" or not. Those programs which are not deemed joint enough are unlikely to receive funding. However, the current chair, Marine General Peter Pace, believes that the JROC is not

---

[27] Kevin Meiners, Director, ISR Systems, OASD (C3I), "OSD Perspective on ISR Needs and Initiatives," powerpoint briefing, March 06, 2002.

[28] William S. Cohen, Secretary of Defense, *Annual Report to the President and the Congress*, 2001, pp. 122-123. Also, discussions with service ISR planners.

[29] Meiners briefing.

[30] Discussions with service ISR planners, January-March 2002. Some observers perceive the Joint Signals Avionics Family (JSAF) as an example of ASD/C3I trying to get one box to fit all services' needs. JSAF was intended to provide one sensor for the Army's Aerial Common Sensor, the Navy's P-3 replacement aircraft, and the Air Force's U2, Rivet Joint, and Global Hawk aircraft. The program was cancelled when the contractor could not meet some of the technological requirements, and the Army is attempting to salvage key aspects of it, with greater freedom to adjust requirements. See "Stenbit Offers Army a Chance to Manage Piece of Joint SIGINT sensor," *Inside the Air Force*, March 8, 2002, http://www.insidedefense.com

[31] Thomas Hawkins, *Defense Budget: Role of the Joint Requirements Oversight Council*, CRS Report 97-346 F.

playing a significant role in the transformation of the armed forces, and advocates a greater role in identifying and pushing development of new capabilities.[32] If Pace or his successors succeed in shifting the JROC from a simple validation role to a more pro-active one, this may also increase ASD/C3I's control over the future of ISR.

Joint Forces Command (JFCOM), established in 1999, is another organization which some defense experts believe has the potential to aid military efforts toward transformation and ISR integration.[33] This unified command has the charter to run major force experimentation and improve interoperability among the services, and has been working several ISR-related initiatives.[34] Its Joint Interface Control teams, consisting of communications specialists as well as special software and hardware, are reportedly improving communications among intelligence sources in Afghanistan.[35] JFCOM is testing a new analytical capability known as Operational Net Assessment this year. This system of databases, analytical tools, and networks claims to fuse intelligence and other data in an interagency environment.[36] DOD's new Unified Command Plan, which divides warfighting responsibilities among various commanders, may improve JFCOM's ability to support transformation. The plan emphasizes JFCOM's experimentation and interoperability duties while it moves responsibilities for homeland defense on land and sea from JFCOM to the newly created Northern Command.[37]

Do the Office of the Secretary of Defense and Joint efforts in ISR support transformation, according to Admiral Cebrowski's criteria? Taken together, they do appear to be helping improve interoperability while supporting changes in the way warfare is conducted against a wide range of threats. The DARPA and Advanced Systems & Concepts Office projects promise to provide some of the detailed intelligence sought, as well as improve persistent surveillance. ASD/C3I's leadership of DCGS could result in significant improvements in providing fused assessment to warfighters. Observers generally point to strengthening the JROC and JFCOM,

---

[32] Kerry Gildea, "Pace Calls for More Proactive JROC Process," *Defense Daily*, April 10, 2002, p. 4.

[33] For example, Andrew Krepinevich, executive director, Center for Strategic and Budgetary Assessments, supports the establishment of JFCOM, but believes the field exercises it runs and other aspects of its work could be more revolutionary. See Lisa Troshinsky, "JFC's 'Millenium Challenge 2002' Won't be Tough Enough: Analyst," *Navy News Week*, vol.DW22 No. 18 (April 30, 2001), [http://www.kingpublishing.com/publications/dw].

[34] General William F. Kernan, U.S. Army, statement before the Senate Armed Services Committee, April 9, 2002.

[35] JO2 Michael Wimbish, U.S. Navy, "USJFCOM-grown concept key to success in Afghanistan," Joint Forces Command Public Affairs, February 14, 2002.

[36] JO2 Michael Wimbish, U.S. Navy, "Joint Experiment will Test Information Linkage," Joint Forces Command Public Affairs, [http://www.jfcom.mil/About/experiments/mc02/ona.htm], undated article accessed May 1, 2002.

[37] Donald H. Rumsfeld, Secretary of Defense, "Special Briefing on the Unified Command Plan," Department of Defense Public Affairs, April 17, 2002.

particularly their influence on military spending, as ways to increase OSD's and JCS's abilities to guide military transformation.

Army. The Army may be making the biggest force structure change of all the services, as it seeks to replace the M-1 tank as its centerpiece weapon system. It is designing the network-centric Future Combat System, an as-yet undefined combination of manned and unmanned vehicles, tied together with a comprehensive network, intended to be much lighter and therefore more transportable than today's weapon systems. This force will depend on the ability to detect enemy activity, share that information quickly, and defeat it before coming into close contact with an enemy.[38]

The Army's plans for ISR focus on interoperability. The Army recognizes that the majority of its intelligence needs are collected by other services and the national agencies. It therefore stresses being able to communicate with the other intelligence sources. However, exactly how it intends to accomplish that is still under development. Thus, at least some of the programs which will be needed to achieve Army objectives have not yet been defined. Technologically, research and development effort is focused on analysis tools, especially data fusion and validation. An apparently singular success in this area is the Pathfinder text analysis system, which is used extensively by the Army's National Ground Intelligence Center and is being incorporated into analysis systems throughout the military. This software is reported to be able to sort through 500,000 documents in just a few minutes, finding patterns, trends and statistics, and to have already contributed extensively to key decisions.[39] Key procurement efforts include the Distributed Common Ground Station, the Tactical Exploitation System for IMINT analysis, a Tactical Unmanned Aerial Vehicle (Shadow), a HUMINT analysis support system, the Aerial Common Sensor to replace the Guardrail and Airborne Reconnaissance-Low airborne reconnaissance systems, and the PROPHET ground-based sensor and jammer.[40] The Joint Tactical Terminal, a prototype radio system designed for interoperability to access several different intelligence broadcasts, has been deployed in Afghanistan with apparent success.[41]

Operationally, the Army says it is making major changes at the tactical level. It is forming Reconnaissance, Surveillance, Targeting and Acquisition (RSTA) squadrons to provide focused analysis to the brigade commander. Traditionally, this level of effort for collecting and analyzing intelligence occurs higher up the chain of command, at division and corps level. The shift to delivering high-quality, timely

---

[38] Roger Roy, "Army Seeks Smarter Future," *Orlando Sentinel*, January 13, 2002, p. 7. Frank Tiboni, "Future Concepts May Delay Army's WIN-T," *Defense News*, March 11-17, 2002, p. 8. For a more complete description of Army transformation plans, see Bruner, *Army Transformation.*

[39] "Pathfinder Puts Two and Two Together," *Jane's International Defense Review*, December 2001, p. 27.

[40] Interview with Mr. Pete Fisher, Army G2 office, February 08, 2002.

[41] Jeremy Singer and Frank Tiboni, "New Intel Devices Get Trial By Fire In Afghanistan," *Defense News*, March 25-31, 2002, p. 8.

intelligence directly to the smaller unit is a key aspect of why the Army believes it can operate some units successfully in combat without the armored protection an M-1 tank provides. These RSTA squadrons are expected to employ many of the technologies listed in the previous paragraph, particularly the tactical UAV, HUMINT analysis, ground sensors, and the DCGS for analysis and dissemination. The RSTA squadrons will place intelligence personnel trained to collect HUMINT forward to operate directly with tactical patrol elements, creating the potential to significantly increase the quantity and value of HUMINT to army operations.[42] A final planned change to army tactical intelligence operations is to allow every soldier, regardless of occupational specialty, to contribute his or her observations of battlefield activity to the intelligence network. How this will be manifested is not yet determined. If achieved, it will likely mean a vast increase in the amount of information available to the units, and a concurrent increase in the requirement for analysis while seeking to prevent information overload.[43]

Organizationally, the Army appears to have made fewer recent changes than other services. While both the Air Force and the Navy have in the past few years designated their senior intelligence officers as the functional managers for ISR, the Army does not have a focal point for ISR. The senior intelligence officer has some programmatic oversight, particularly for intelligence, but surveillance and reconnaissance fall under the purview of the operations officer.[44] Some observers believe this split in responsibility may slow the Army's ability to integrate all aspects of ISR not only with Army operations but with other service ISR capabilities.

Do the Army's activities in ISR support transformation? The Army's emphasis on interoperability, as well as its apparent major commitment to change the way it fights, seems to say they do, although there are still many questions to be answered concerning how the new army units will operate, including how they will use ISR. The RSTA squadron, incorporating most aspects of Army intelligence plans and promising fusion, increased detail, and persistent surveillance, may be viewed as a radical departure from current operations, but its ability to function in the face of a wide range of threats is yet to be determined.

Air Force. The Air Force says its transformation effort builds on the successes it has already achieved in being able to reach targets with stealth aircraft and strike them very accurately with guided weapons. It emphasizes integration of current capabilities with modernization of its fighter force (the F-22 Raptor and the Joint Strike Fighter), improved airborne reconnaissance and command and control aircraft including UAVs, and networking.[45]

---

[42] Brigadier General Paul Eaton, Deputy Commanding General for Transformation, Training and Doctrine Command, press briefing, May 18 2001.

[43] Chris Strohm, "Army Intel Community Wrestles with Effects of Transformation," *Defense Information and Electronics Report*, August 17, 2001, pp. 8-9.

[44] Interview with Mr. Pete Fisher.

[45] Christopher Bolkcom, *Air Force Transformation: Background and Issues for Congress*, CRS Report RS20859, p. 4.

The Air Force is the largest military provider of surveillance and reconnaissance as it operates most surveillance and reconnaissance aircraft and is DOD's executive agent for space. It is focusing its ISR transformation effort on creating multiple platforms which together can watch a battlefield regardless of the terrain, time of day or weather conditions, and communicate the observations in a way that an identified target can be destroyed within ten minutes of the initial observations.[46] Technologically, the challenges the Air Force perceives are in integrating today's platforms to provide one coherent picture of the battlespace, reducing the need for human transfer between systems of basic technical data such as location information, and determining if or when to move ISR capabilities currently performed by airborne platforms to space. Key procurement programs are the Space-Based Radar and "Smart Tanker" (a program to equip all aerial tankers with surveillance sensors and communications equipment) to increase the military's persistent surveillance, the Multi-Platform Radar Technology Insertion Program to improve tracking moving ground targets, Predator B and Global Hawk UAVs for airborne persistent surveillance and reconnaissance, Theater Battle Management Core System, Network Centric Collaborative Targeting and the Air Operations Center Common Operating Picture for coordination with operations, and the previously mentioned Distributed Common Ground Station for analysis and dissemination.[47]

To some observers, the operational changes the Air Force is now attempting to develop in ISR are more incremental than revolutionary. As noted earlier, the Air Force claims that revolutionary changes have already occurred, such as the integration of UAVs into the Air Force's operations and the ability to get the process of identifying targets and subsequently destroying them down from days to minutes in length. The Air Force believes it is doing a good job providing ISR at the theater level, but is not yet able to provide a global perspective. Moving most of the Air Force's surveillance and reconnaissance assets to space could significantly increase world-wide coverage, and may be the next major change in ISR operations, if appropriate technology develops. Such a move, however, will surely be quite costly, and also risks a loss in flexibility, as satellites have historically been difficult to move quickly from one target area to another, and have also been more difficult than aircraft to repair or replace when necessary. Observers also question whether more emphasis should be placed on analysis, rather than on more equipment. For example, bomb damage assessment, the process by which the commander determines how much damage an attack caused on a given target, and therefore whether it needs to be struck again, has been called a weak area for Operation Enduring Freedom.[48]

Organizationally, the Air Force has made several moves to improve its ISR. Its re-organization in the early 1990s combining Strategic Air Command with Tactical Air Command to form Air Combat Command could be seen as a step toward ISR transformation, as it brought most ISR assets under one commander. Previously, the

---

[46] Amy Butler, "Jumper's ISR Vision Focuses more on Integration than Platforms," *Inside the Air Force*, August 17, 2001, pp.3-4.

[47] Interview with Lt Col Charles Bartlett, AF/XOIR, February 20, 2002.

[48] Lisa Burgess, "Critics Say Flaws in DOD Approach Keep Smart Bombs from Reaching Potential," *European Stars and Stripes*, April 10, 2002, [http://ww2.pstripes.osd.mil/01/research1.html].

Air Force's "strategic" reconnaissance aircraft like the RC-135, U-2, and SR-71, belonged to Strategic Air Command, and were reserved primarily for tasks associated with defeating the Soviet Union. With the formation of Air Combat Command, these aircraft have been made much more available to units fighting theater wars, such as Iraq, Bosnia, and Kosovo. Another organizational change the Air Force has made which may support ISR transformation is the designation of its senior intelligence officer as the functional manager for all ISR, giving that person responsibility for all ISR resourcing and management. Also, in 1997 the Air Force formed a center now known as the Aerospace Command and Control and Intelligence, Surveillance and Reconnaissance Center (AC2ISRC) which focuses on standardizing Command and Control as well as ISR systems for both the joint and coalition audience.[49] The Air Force's recent designation as DOD's executive agent for space, including director of the National Reconnaissance Office (NRO), has increased its responsibility and authority to coordinate and guide the use of space for ISR. The Air Force has also formed a new office, the deputy chief of staff for warfare integration. This office is expected to ensure that all Air Force systems fit into a common architecture, with particular emphasis on command and control and ISR systems.[50] Finally, the Air Force has formed seven functional "task forces" in its headquarters staff, each headed by a Colonel. One of these is the Air and Space/C2ISR Task Force. The task forces are meant to be able to cut across traditional program areas and staff lines focused on weapon systems such as "bombers," design new concepts of operation, and advocate for required capabilities with a stronger, more coherent voice than has previously occurred.[51]

Do the Air Force's activities in ISR support transformation? Judged by the standards of interoperability, support to changed methods of warfighting, and ability to confront a wide range of threats, the answer is unclear. Interoperability stands at the top of the Air Force's stated priorities. The various changes in Air Force organization which have occurred since the end of the Cold War appear to be the most aggressive of all the services. The availability and applicability of space assets to warfighting has increased significantly, adding greatly to the services' access to a world-wide perspective as well as in-depth intelligence. As noted earlier, Air Force efforts appear to have played a large role in establishing the lauded ISR capabilities, particularly their persistent surveillance, for Operation Enduring Freedom. However, some observers believe the Air Force is primarily achieving technical improvements to established programs and operating methods, rather than a radical change appropriate to a potentially radically different enemy. Another point made is that while the Air Force owns the vast majority of ISR aircraft, these aircraft have been operating at a very high rate for a number of years, such that the aircraft and crews are significantly more stressed than most of the Air Force. This leads to situations

---

[49] William S. Cohen, Secretary of Defense, *Annual Report to the President and the Congress*, 2000, p. 201.

[50] James Roche, Secretary of the Air Force, "Special Briefing on Army and Air Force Headquarters Reorganization,"Department of Defense Public Affairs, December 18, 2001.

[51] John Barry, Maj Gen, USAF, "Transformation Across the Spectrum of Conflict," Briefing at 2002 HQ USAF/XP Air and Space Conference, March 6, Washington, DC.

where ISR aircraft are unavailable to fly missions for commanders who need them. Observers wonder why the Air Force has not yet fixed this problem.[52]

Navy and Marine Corps. The Navy and Marine Corps' primary effort for transformation is their concept of network centric warfare, linking today's weapon systems in local and wide-area networks such as the Cooperative Engagement Capability (CEC) for air and missile defense and the Navy and Marine Corps Intranet (NMCI) to exchange information and control actions. In addition, the Navy is studying new ship designs and operational concepts to improve naval capability in littoral waters and for sea-basing to defeat the "anti-access" threat where no near-by land bases are available.[53] The Marine Corps seeks to improve its ability to fight in the urban environment. This includes less-than-lethal weapons, tactical and man-portable UAVs, and networking.[54]

The Navy and Marine Corps' plans for ISR are toward better networking and integration, as well as organic sensors for persistent surveillance.[55] The Navy's CEC has been successfully deployed with the USS John F. Kennedy carrier battle group, earning accolades from some observers as the military's first true "network-centric" program.[56] While CEC is not specifically an ISR program, it ties many Navy sensors together to achieve a much better picture of the battlespace. For networking and analysis, DCGS forms the foundation for bringing all sources of intelligence together, while the Naval Fires Network is the primary program supporting the Navy's entire process of identifying targets and striking them. The P-3 Aircraft Improvement Program and S-3 Surveillance System Upgrade, both still in development but used with success in Afghanistan, aim at significantly improving that process.[57] Concerning sensors, most effort is on unmanned platforms with new sensors for better SIGINT and MASINT. The Navy expects to procure the Global Hawk UAV, at least for testing, and is actively developing an unmanned underwater vehicle (UUV), while the Marine Corps is speeding the fielding of its man-portable Dragon Eye UAV and continues work toward a vertical-takeoff and landing UAV to replace its Pioneer UAV.[58]

---

[52] Lisa Burgess, "Critics."

[53] Ronald O'Rourke, *Naval Transformation: Background and Issues for Congress*, CRS Report RS20851, p. 3, and Ronald O'Rourke, *Navy Network-Centric Warfare Concept: Key Programs and Issues for Congress*, CRS Report RS20557.

[54] O'Rourke, *Naval Transformation*, p. 3.

[55] Dennis McGinn, Vice Admiral, USN Director of Naval Warfare, interview in *Aviation Week and Space Technology*, December 24/31 2001, p. 39.

[56] Chip Cummins, "Already On Board," *Wall Street Journal*, March 28, 2002, p. R-6.

[57] Gail Kaufman, "U.S. Navy Considering New Mission for Old Plane," *Defense News*, November 12-18, 2001, p. 30.

[58] Interviews with CAPT Jack Dorsett, USN, Office of Chief of Naval Operations, N20, February 26 2002, and Lt Col John B. Lang, HQ USMC, Intelligence Department, IPP, February 08, 2002.

Operationally, some degree of transformation appears to have occurred as shown by the successful integration of Navy ISR assets, particularly the P-3 and space assets, with Air Force assets to produce persistent surveillance and a common operating picture of the battlefield for all services' combat assets operating in Afghanistan. In the Marine Corps, a shift in ISR operations began after Operation Desert Storm, when it was thought that the marines received poor intelligence support. In 1993 the Corps initiated a plan to produce professional intelligence officers, with their own career plans and command opportunities.[59] The Corps now has experienced intelligence officers at all levels, apparently contributing directly to the success of the Marine units in Afghanistan. The Marine Corps is also expanding its Intelligence Analysis System, which brings the various sources of intelligence together for analysis by intelligence personnel.

Organizationally, the Navy has implemented some of the same concepts as the Air Force in its bid to transform its ISR. Its senior intelligence officer is also designated the functional manager for ISR. In addition, the Navy has implemented a concept very similar to the Air Force's seven functional task forces. It has identified six "mission capability packages," each overseen by a Navy Captain, to cut through the traditional weapon systems focus, design new concepts of operation, and build the architectures needed. One of these mission capability packages is dedicated to ISR.[60] The mission capabilities packages are overseen by the Navy's Office of Warfare Integration and Assessment, which began operation in October, 2000.[61] Finally, the Navy has designated a new command, the Naval Network Warfare Command, to begin operation in May 2002.[62] While not limited to ISR, its charter to oversee the development of all networks in the Navy should have a major impact on Navy and Marine Corps ISR.

Do the Navy and Marine Corps activities in ISR support transformation? Like the Army and Air Force, interoperability appears to be stressed in the naval ISR programs. The Marine Corps' Intelligence Analysis System appears to be making progress on improving fused assessments for its units. Some observers believe the Navy deserves just as much credit as the Air Force for the establishment of a successful persistent ISR network in Operation Enduring Freedom.[63] In addition, the naval programs appear, more than the Army and Air Force, designed to deal with a wide range of threats as they consider littoral and urban warfare as well as the "anti-access" scenario of having to fight completely from the sea with no nearby land-based support. Their programs promise to provide the detail and persistence warfighters believe they need to defeat these threats.

---

[59] Interview with Lt Col John Lang.

[60] Interview with CAPT Jack Dorsett.

[61] "Navy Adds Homeland Defense to Mission Capability Packages," *Navy News & Undersea Technology*, January 2, 2002, pg.1.

[62] Dale Eisman, "Navy Setting Up Command for Information Network," *Norfolk Virginian-Pilot*, March 16, 2002, p. B3.

[63] Craig Covault, "Navy Space Ops Crucial to Afghan War," *Aviation Week and Space Technology*, April 8, 2002, p. 86.

Special Operations Forces (SOF). SOF are elite, specialized military units that can be inserted into enemy territory. These forces both require and collect intelligence at all levels–one of their capabilities is strategic reconnaissance.[64] While much of the equipment SOF uses is procured by the services, Special Operations Command (SOCOM) has authority unique among the unified commands to procure systems specific to SOF requirements. Its main effort for transformation appears to be successful fielding of the CV-22 tilt-rotor aircraft and the Advanced SEAL Delivery System (ASDS) mini-submarine to be launched from former ballistic missile submarines which the Navy is converting to guided missile submarines.[65]

The unique capabilities SOF are seeking in ISR concentrate on receiving the highest-quality intelligence at the lowest tactical level. They are developing the Joint Threat Warning System to provide a downlink for intelligence broadcasts and a SIGINT receiver for immediate warning. This system will be designed in several physical configurations, from body-worn to maritime-based. They are also designing an upgrade to the SOF Intelligence Vehicle, a modified "humvee" with communications links and analysis terminals which may increase the availability of intelligence and tailored analysis to personnel in the field.[66] Man-portable UAVs are also being procured.[67]

Operationally, SOF actions in Afghanistan suggest that some transformation has already occurred, as SOF personnel determined how to identify and communicate potential targets for aircraft to strike. While this type of operation has long been a SOF skill, the melding of GPS and other immediately available data such as Predator video with the human observations of the SOF personnel had not been possible in previous conflicts.[68]

Organizationally, the naval component of SOCOM, Naval Special Warfare Command, which previously did not have a dedicated intelligence analysis capability, is establishing a Mission Support Center which will include intelligence analysis. The other components, Air Force Special Operations Command and Army Special Operations Command, are increasing the size of their intelligence organizations, mostly in response to the increased requirements of the global war on terrorism. The

---

[64] Edward F. Bruner, Christopher Bolkcom and Ronald O'Rourke, *Special Operations Forces in Operation Enduring Freedom: Background and Issues for Congress*, CRS Report RS21048.

[65] Ron Laurenzo, "Osprey, SEAL Mini-Sub Top Special Ops Priorities," *Defense Week Daily Update*, March 12, 2002; OSD/PA Press Release, "Special Briefing on Special Operations Forces Capabilities," December 12, 2001.

[66] Telephone interview with LTC Jim Boardman, U.S. Special Operations Command SOIO-IN-OP, March 05, 2002.

[67] Robert Wall, "Counterterror Combat Shrinks Special Ops Inventory," *Aviation Week & Space Technology*, March 18, 2002, p. 28.

[68] Telephone interview with LTC Jim Boardman.

Special Operations Command Joint Intelligence Center's production capability may expand considerably, as well.[69]

To many observers, the special operations forces have always been transformational. At least within their own community, interoperability is stressed, and they have historically used different ways of fighting against unconventional enemies. The plans outlined above for ISR may appear to be only incremental, but this may be appropriate for a force which is believed to already have a culture of transformation. The effort in unmanned vehicles may improve SOF's ability to provide surveillance, while the increasing size of their intelligence centers promises an improved world-wide perspective, potentially at a greater level of detail than before. A caution may be that SOF, while interoperable and innovative among themselves, have in the past had difficulty communicating and coordinating with non-SOF assets. This appears to have been overcome in Operation Enduring Freedom, at least with respect to calling in air strikes, receiving other types of air support, and sharing intelligence. If after-action reports of the war in Afghanistan bear out these early observations, SOF will probably be considered by most to still be on the leading edge of transformation.

Coast Guard. The Coast Guard, probably more than any of the other services, is undergoing a mission change due to the attacks of September 11, 2001. It is moving from a force which emphasized maritime safety, protection of natural resources, and law enforcement to focus more on its maritime security and national defense missions, including port security both in the United States and at overseas ports where U.S. forces are located.[70] At the same time, the Coast Guard is undergoing a wholesale replacement of many of its ships, boats, and aircraft in an effort to replace obsolete systems while achieving full integration and interoperability. This acquisition program, named "Deepwater", has been in planning for several years and should be contracted out in 2002. It will not replace systems type for type, but instead will use an integrated mix of surface and air platforms with appropriate connectivity to achieve the required capabilities.[71]

Coast Guard acquisitions, including Deepwater, claim to strongly emphasize interoperability. Much more than the other services, however, for the Coast Guard interoperability implies the ability to communicate and operate with civilian vessels and other non-defense agencies, as well as with defense organizations. Thus, one key ISR program is its National Distress Response Modernization Program, providing VHF radio towers to improve communications with all maritime activities, particularly its ability to receive distress calls. Another program aims at expanding SIPRNET, the standard DOD-wide secure internet system for classified data, to all

---

[69] Telephone interview with LTC Jim Boardman.

[70] Interview with CAPT Richard Kelly, USCG, Sponsor's Representative for Deepwater Program, March 11, 2002.

[71] Ronald O'Rourke, *Coast Guard Deepwater Program: Background and Issues for Congress*, CRS Report RS21019, p. 3. See also [www.uscg.mil/deepwater].

port operations centers and major cutters.[72] The Deepwater contract specifically requires its system integrator to periodically upgrade sensors and ISR throughout the 30 years of the Deepwater program.[73] ISR capabilities being considered for the Deepwater program include the Global Hawk UAV, a vertical take-off and landing UAV, and other sensors such as air and surface-search radars and passive electronic surveillance systems.[74]

Operationally, the Coast Guard has a goal to inspect all suspect and other high-interest vessels such as cruise ships before they enter U.S. territorial waters. ISR must point the Coast Guard to the right vessels for inspection. Some regulatory tools, such as the requirement that all ships provide inventory and crew data 96 hours before reaching U.S. waters and the anticipated 2004 implementation of an identification transponder for all ships worldwide larger than 300 gross tons are expected to help. However, these sources of information need automated analysis not yet available. Another shift in operations involves the field intelligence teams working at major ports. The Coast Guard's goal is to post a team permanently at every major port. These teams include Coast Guard intelligence personnel and Coast Guard investigative service special agents. The teams are expected to liaise with other federal, state and local law enforcement and intelligence agencies to conduct data collection, reporting and dissemination. Finally, putting SIPRNET terminals on every ship could encourage a major change in ISR operations. These terminals provide easy access to and transmission of large amounts of classified data and communications and enhance the user's ability to coordinate with other DOD activities, including the military intelligence community. Taken together, these changes in ISR operations are expected to substantially increase the Coast Guard's production of and access to intelligence.[75]

Organizationally, the Coast Guard sees a need for shore-based fusion and analysis centers to handle the increased quantity of intelligence, and is coordinating with the Navy to establish one such 24-hour operations center on each coast. The Coast Guard is also significantly increasing its airborne and shipborne intelligence collection capability, and bringing it under the guidance of the Navy's Naval Security Group.[76]

Do the Coast Guard's activities in ISR support transformation? As with the other services, interoperability is perceived as key and appears to be receiving strong emphasis from Coast Guard planners. The Deepwater program's ISR, although conceived well before transformation became the coin of the realm in the Defense Department, seems to be aimed at allowing the Coast Guard to change its methods of operation by giving it an ability to function in tandem with the Navy and other

---

[72] Interview with LCDR Dave Vaughn, USCG C4ISR planner, April 12, 2002.

[73] Interview with CAPT Kelly.

[74] U.S. Coast Guard, Integrated Deepwater System Program, Maritime Domain Awareness point paper, [www.uscg.mil/deepwater/] accessed on March 22, 2002.

[75] Interview with LT Greg Rainey, USCG, Intelligence Resource Management planner, April 12, 2002.

[76] Interview with CAPT Kelly.

agencies, significantly farther from shore than is possible today. Finally, the Coast Guard does appear to be standing up to the new perception of the threat with its desire to intercept suspect ships at sea and increase the robustness of in-port intelligence and security. These, in turn, should add significant detail to the intelligence picture. However, the Coast Guard seems to be in uncharted waters. Deepwater is a very ambitious program, and the means to fully fuse and analyze the vastly increased amount of intelligence while coordinating with law enforcement agencies has not yet been determined.

Defense Intelligence Community

As noted earlier, military intelligence uses ISR from the entire intelligence community, not just the military services. The services depend primarily on three intelligence agencies in the Defense Department itself–the Defense Intelligence Agency (DIA), National Security Agency (NSA), and the National Imagery and Mapping Agency (NIMA). The National Reconnaissance Office (NRO), while a DOD agency, designs, launches, and flies satellites for the other agencies, and is not a primary producer of intelligence products. Service expectations concerning the future activities of DIA, NSA, and NIMA are important factors in service decision-making.

DIA. Since September 11, 2001, DIA, the military's primary source of HUMINT and strategic analysis, has received a large increase in resources to increase its production of both HUMINT and strategic analysis. This has the potential to significantly improve the military's awareness of possible threats worldwide. Service officials indicate general satisfaction with DIA's direction. The Navy, for example, appears to be reducing its expenditure on HUMINT activities in the belief that DIA will be able to successfully fill any gaps.[77] In addition, DIA runs several military-wide programs that support strategic analysis. For example, DOD officials believe the Joint Intelligence Virtual Architecture, a collaborative intelligence network, has made major headway in establishing standardized access to data and analysts throughout the military intelligence community. The architecture has incorporated many analytical tools including the Army's Pathfinder mentioned earlier as well as a single integrated data base which together may improve analysts' ability to fuse all sources of intelligence.

NSA. Analysts generally believe the nation's primary producer of Signals Intelligence, or SIGINT, is struggling to maintain and improve capability while faced with the huge world-wide changes in how information flows and is processed. For example, experts say fiber-optic cables make eavesdropping difficult. The vast increase in the quantity and variety of communications, such as by cell phones, pagers, and the internet, also increase the difficulty of finding communications of interest.[78] Due to the need to re-tool, especially in the light of its essential role in protecting the United States from terrorist attack, NSA has significantly reduced its support to tactical-level military operations. The services are acutely aware of this

---

[77] Discussions with service ISR planners, January-March 2002.

[78] Richard A. Best, Jr., *The National Security Agency: Issues for Congress*, CRS Report RL30740, p. 3.

and are devoting more resources toward tactical SIGINT, an often key element for successful time-critical targeting.[79]

NIMA. The nation's primary producer of geospatial intelligence (maps and imagery) is attempting to digitize all geospatial intelligence, aiding in the processing and dissemination of the gathered intelligence, as well as fusion with other intelligence resources. It also plans to deploy a Future Imagery Architecture which consists of a large number of small imagery satellites able to provide more persistent coverage of areas of interest than today's satellite architecture. Service representatives are generally convinced that there will be sufficient imagery data for the transformed force. They are less certain that the geo-location information required for precision strike will be available for every location the services may need to know about, and they also believe that continued emphasis on processing, exploitation, and dissemination of geospatial intelligence is needed.[80]

What Transformations of ISR Will Be Needed?

As noted earlier, many observers believe significant transformation of ISR has already occurred and has been practiced in Afghanistan. The military's ability to move data from the reconnaissance platform to the weapon system able to take action, the so-called "sensor to shooter" sequence, generally required at least a full day in Operation Desert Storm, as imagery from a satellite or reconnaissance aircraft had to be analyzed, identified as a target, turned into hard-copy, and intensively studied by the aircrew before a weapon could be dropped accurately. In Operation Enduring Freedom, Special Operations Forces personnel on the ground identified a Taliban troop concentration, called the target back to the Combined Air Operations Center in Saudi Arabia, received permission to call in an airstrike, determined the exact coordinates of the enemy using Global Positioning System (GPS), and passed those coordinates to a loitering B-52 bomber which again used GPS to guide bombs onto the target within less than 20 minutes of the original identification of the target.[81] Similarly, Predator UAVs have been able to transmit live video pictures to waiting AC-130 gunships, which were able to attack moving targets while the Predator monitored for effectiveness, again within minutes of original target identification.[82] These examples highlight recent gains in the precision and timely

---

[79] Marc Strass, *Services Need to Maintain Own SIGINT Capability, NSA Says*, Defense Daily, August 15, 2001, pg. 3. For further discussion of NSA and its current status, see Best, *The National Security Agency*.

[80] NIMA Statement of Strategic Intent, January 2002, p. 2; Discussions with service ISR planners, January-March 2002; John M. Diamond, "Re-examining Problems and Prospects in U.S. Imagery Intelligence," *International Journal of Intelligence and Counterintelligence* vol. 14 no. 1, 2001, p. 6.

[81] Lt Gen Chuck Wald, USAF, "Air & Space Power: Evolution, Application and Vision," Briefing to HQ USAF/XP 2002 Air and Space Conference, Washington, DC, March 7, 2002.

[82] David A. Fulghum, "Intel Emerging as Key Weapon in Afghanistan," *Aviation Week &* (continued...)

communication of intelligence, as well as interoperability among weapon systems and even between services. With regard to analysis, over the past ten years the growth of an intelligence-community-wide secure intranet known as INTELINK has significantly increased intelligence personnel access to intelligence data, reports of all types, and other analysts, worldwide.[83]

Most members of the military intelligence community say they are continuing to work hard at interoperability–they appear to have agreed that the ability to share intelligence throughout the community is essential. In addition, there appear to be some significant departures from old ways of doing things which could support the other goals of transformation. The most revolutionary concepts being developed today appear to be the Army's Reconnaissance, Surveillance, Targeting and Acquisition squadron, DIA's Joint Intelligence Virtual Architecture, and the large increase in the use of unmanned vehicles already underway in all of the services. Although by no means radical to the rest of the intelligence community, the Coast Guard's plan to bring classified communications via SIPRNET onto every ship creates the possibility of a sweeping change in its use of intelligence.

Some outside observers, however, believe that in addition to these changes, the military intelligence community needs to establish a whole new method for analysis. Bruce D. Berkowitz and Allan E. Goodman, for example, note that the subject matter for most military analysts is far more fluid than during the cold war, rendering standard databases and analytical models for explaining behavior obsolete.[84] Indications and Warning, the analysis which warns of impending attack on the United States or its vital interests, depends on the ability to predict enemy activity, based on enemy plans, doctrine, and observed exercises and training. Many of today's potential adversaries offer little in the way of traditionally observable activity.[85] Berkowitz and Goodman see maintaining databases as a vastly more difficult problem today than it was twelve years ago; precision-guided munitions, world-wide interests, adversary use of western and non-traditional weaponry, and the need for increased information about civilian populations have significantly expanded and complicated military intelligence database needs.[86]

In response to this problem, the primary solution offered, both inside and outside the Defense Department, is the development of better technology. This may be artificial intelligence such as neural networks which "learn" as they are used to perform data-mining and other analytical tasks, or powerful "cookies" like those that

---

[82] (...continued)
Space Technology, March 11, 2002, p. 24.

[83] Richard A. Best, Jr., *Intelligence Implications of the Military Technical Revolution*, CRS Report 95-560F, p. 15.

[84] Berkowitz and Goodman, p. 100.

[85] Berkowitz and Goodman, p. 104.

[86] Berkowitz and Goodman, pp. 113-117.

internet marketers use to track customer responses.[87] However, senior analysts who have observed these tools believe they still require significant development before they can be applied to day-to-day intelligence analysis.[88] As noted earlier, this is an area in which DARPA is conducting research and development.

While much effort is being placed on improving the technological tools available to analysts, several observers argue that, whereas in the Cold War the vast majority of key information was obtainable only through classified intelligence methods, today most information of value is available through open sources. They propose a more market-based or decentralized approach to intelligence analysis, allowing multiple groups, possibly contractors or even the general public, to make competing inputs to databases and analyses for the decision-maker.[89]

Another possible approach is to move more intelligence analysis from the arguably insulated world of the intelligence community directly into operations analysis. Two examples of this melding are the Air Force's Checkmate analysis cell which gained public attention helping plan the air operation for Desert Storm,[90] and the Joint Warfare Analysis Center, which conducts engineering-level analyses of potential target systems such as power grids to find the linkages and vulnerabilities in them.[91] Both organizations have strong reputations within the Defense Department for finding new ways to defeat the enemy when "traditional" intelligence and operations centers do not. They are not intelligence centers, although both have intelligence analysts working in them. The intelligence analysts work side by side with operations analysts to focus all data, whether from an intelligence source or another source such as a logistics report, on the operational problem at hand. This type of analysis requires getting the intelligence community to find and produce exactly what a specific customer requests, working beside the customer from start to finish.

---

[87] Markoff, "Chief Takes Over." See also [http://www.imagination-engines.com] and John Arquila and David Ronfeldt, "Fighting the Network War," *Wired*, December 2001, pp. 149-151, for further information on neural network and other technologies.

[88] Discussions with senior Defense Intelligence Agency analysts, April 10, 2002.

[89] Treverton, p. 104; Berkowitz and Goodman, p. 122; Robert David Steele, *On Intelligence: Spies and Secrecy in an Open World*, AFCEA International Press, Fairfax, VA, 2000, p. 76; Arquila and Ronfeldt, "Fighting the Network War," p. 150.

[90] Best, *Intelligence Implications*, p. 12.

[91] Joint Warfare Analysis Center information page, available on the Internet at [http://www.jfcom.mil/About/com_jwac.htm], accessed April 30, 2002.

Issues for Congress

The conference report for the Intelligence Authorization Act for Fiscal Year 2002 stated four primary concerns for the intelligence community; re-vitalization of NSA, correction of HUMINT deficiencies, correcting a perceived imbalance between collection and analysis, and ensuring adequate research and development.[92] In addition, several other issues involving the cost and quality of intelligence, as well as leadership, military intelligence's role in homeland defense and the impact of potential intelligence community reform may be considered.

Revitalization of NSA

A long-standing congressional concern has been to ensure that NSA adjust successfully to the emerging electronic environment.[93] The services note that NSA has shifted resources to help it deal with the new environment, with a resulting reduced support for tactical operations. The services have therefore identified actions needed to mitigate the loss of some NSA support. As mentioned earlier, these include upgraded airborne platforms in all services, including UAVs and aerial refueling aircraft, the PROPHET ground-based sensor, and SOF's Joint Threat Warning System. The services stress, however, that NSA must still provide them with access to technologies as they are fielded.[94] Congress may choose to monitor this aspect of NSA's performance, while funding appropriate service initiatives which fill in some of the gaps left by NSA's current focus on the strategic electronic environment.

HUMINT Deficiencies

Congress also sees a national security imperative to improve HUMINT. HUMINT is the one type of intelligence that nearly all outside experts believe needs to be increased, as it can provide access to potential enemies' plans and intentions in greater detail than other sources. This is primarily the responsibility of CIA and DIA; the services' roles at the strategic level have declined significantly since 1995 when most service HUMINT capabilities, in particular their attaches posted to embassies world-wide, were consolidated into the Defense HUMINT Service, run by DIA. Some believe this move hurt the production of HUMINT for military purposes. [95]

---

[92] U.S. Congress, 107th Congress, 1st session, Committee of Conference, Intelligence Authorization Act for Fiscal Year 2002, H. Report 107-328, December 6, 2001, p. 18. The Conference Report accompanying the FY2003 Intelligence Authorization Act adjusted this listing to emphasize information sharing and cross-community analysis. U.S. Congress, 107th Congress, 2nd session, Committee of Conference, Intelligence Authorization Act for Fiscal Year 2003, H. Report 107-789, November 14, 2002, p. 64.

[93] Richard A. Best, Jr., *The National Security Agency: Issues for Congress*, CRS Report RL30740, 7. See entire report for further discussion of NSA's re-vitalization efforts.

[94] Discussions with service ISR planners, January-March 2002.

[95] Ann Scott Tyson, "Spy Networks Being Rebuilt for Terror War," *Christian Science Monitor,* April 24, 2002, p. 2.

The services do retain some capabilities, usually for employment on or near the battlefield itself. For example, some military personnel are trained to monitor potential hostile activity in the local areas of bases and ports, for force protection. In addition, as previously discussed, the Army plans to integrate soldiers trained in collecting information into front-line squadrons. Operation Enduring Freedom has apparently used Special Operations Forces and other troops to gather tactical information to a greater extent than has occurred in other recent conflicts.

Collection is only part of the issue, however. The information gained must be analyzed and processed into usable formats. This is a difficult problem currently without a clear solution. While the other sources of intelligence data are generally objective and fit fairly easily into database formats, information derived from humans is subjective and often defies objective categorization. Entry into a database so that the information is easily available to other analysts is, at this time, very manpower intensive. Within the military community, DIA is responsible for this type of analysis and has apparently made progress on database development.[96] DIA's continued efforts in increasing the quantity and analysis of HUMINT in support of DOD, especially the global war on terrorism, may deserve examination.

Collection vs Analysis

A third area in which Congress has expressed significant concern is the apparent imbalance between collection and analysis, such that much data is collected by the intelligence community but not analyzed in a timely manner. All of the services report that analysis requires more attention. They say they are shifting manpower toward analytical positions, increasing their use of contracted regional experts, and trying to reduce redundancy in analysis. Technological solutions to the information overload problem are also being researched, as noted earlier. Institutional changes to address the analysis shortfall, such as encouraging competing analyses from outside DOD, however, are not apparent.

At the same time that there is reported to be more information than can be analyzed, continued acquisition of some specific collection capabilities may still be appropriate. Many of DOD's ISR platforms are in very high demand and are operating at a significantly higher operating tempo than most of the rest of the force.[97] These platforms collect focused intelligence of immediate value to the warfighter and cannot be replaced by the large amounts of other intelligence already being collected. In addition, acquisition of emerging capabilities designed to detect very difficult targets, such as foliage-penetrating radars and other highly-technical capabilities potentially able to detect deeply buried targets or biological and chemical laboratories

---

[96] Jonathan Weisman, "Intelligence Agencies Put their Heads Together," *USA Today*, April 12, 2002, p.11. The article states that documents found in Afghan caves and safe houses are sent to DIA, where they are scanned into a database named Harmony. Then, analysts cross-reference names, dates, addresses, and other information to establish other leads.

[97] "DOD Refining Allocation Method for Heavily Stressed ISR Assets," *Defense Information and Electronics Report*, April 19, 2002, p. 1.

may provide previously inaccessible information of direct relevance to prosecution of the global war on terrorism and other potential threats of the 21st century.[98]

Research and Development

Another major area of congressional concern is in research and development–will the intelligence community be able to stay ahead of potential adversaries as they develop new ways to conduct and hide their activities? As noted above, both DARPA and OSD's Advanced Concept Technology Demonstrations have projects which cover many aspects of Defense ISR, particularly in unmanned reconnaissance, sensing technologies, and integrated analysis. Congress may choose to watch these projects, as well as OSD's selection of future projects, to ensure the appropriate technologies are being developed. Congress may also scrutinize the performance of the National Reconnaissance Office in this area. Widely recognized as highly innovative in its early years, the NRO has over the past several years been criticized for a reduced level of innovation as it became more a standard member of the defense bureaucracy.[99]

Some of DOD's ISR research and development programs have encountered Congressional opposition. For example, the 106th Congress killed "Discoverer-2", a space-based radar concept consisting of two experimental satellites, due to the high cost and possible overlap with NIMA's Future Imagery Architecture satellite program. In addition, some in DOD believe that the structure of the program with just two experimental satellites and no follow-on funding requirements inaccurately communicated a low DOD priority for the program.[100] In the FY2002 budget, the Air Force's Space Based Radar and Space Based Infrared System both had funding requests reduced. The cuts were due primarily to seriously escalating costs and program management issues.[101] The DOD intelligence community still believes development of these capabilities is vital, and the Air Force is re-focusing the programs in response.[102] Congress will then have the opportunity to determine whether the programs still make sense.

---

[98] Transformation Study Group Report, p. 30. For further discussion of this issue, focused on imagery and signals intelligence, see Richard A. Best, Jr., *Imagery Intelligence: Issues for Congress*, CRS Report RL31369, and Best, *National Security Agency.*

[99] Best, *Imagery Intelligence*, p. 18.

[100] James R. Asker, "Wanted Still," *Aviation Week & Space Technology*, vol. 153 no. 17, (October 23, 2000), p. 33.

[101] U.S. Congress, Department of Defense Appropriations Bill, 2002, and Supplemental Appropriations, 2002, S.Rept. 107-109 to accompany HR 3338, December 5, 2001.

[102] Robert Wall, "New Space-based Radar Shaped by SBIRS Snags," *Aviation Week & Space Technology*, February 18, 2002, p. 30.

Networks vs Quality Intelligence

A consistent theme throughout DOD is an emphasis on getting networks in place so that information can flow.[103] While even the best intelligence is only useful if it is communicated, poor data on the network can also have devastating consequences. One potential danger is that the flow of information, regardless of the quality of that information, may become a measure of success.[104] Particularly if the number of contributors to the intelligence networks grows, possibly exponentially, the data must still be analyzed and validated. While DIA appears to be making progress on this problem at the strategic analysis level, some observers believe the Marine Corps has the clearest vision on meeting this requirement at the tactical level with its design of its Intelligence Analysis System bringing all data collected by the front-line troops into one location for comparison, analysis, and dissemination. The Army's Pathfinder text analysis tool appears to be an example of the type of automated analytical tool which will be needed both in the field and in supporting intelligence centers, although it is currently primarily used by strategic analysts, not those directly supporting combat troops. Analysis tools and the doctrine and people to use them will need to develop while the networks evolve. Congress may choose to examine service networking programs to ensure that quality of data, as well as data flow, is being improved.

Cost

Will ISR for the transformed force cost significantly more than today's ISR? Due to the mix of "black" (classified) with "white" (unclassified) funding, it is impossible to quantify in an unclassified report the expected changes in the military ISR budget over the next several years. However, some feel for the impact on the budget can be measured in general terms. In the administration's budget request for FY 2003, for example, the Defense Emergency Response Fund request of $20.1 billion included $2.6 billion for increased situational awareness supporting the global war on terrorism.[105] With a significant portion of this request going toward ISR and related activities, service ISR planners note general satisfaction with the budgetary support they are receiving. One area which traditionally is quite expensive is satellite reconnaissance. While upgrades to our imagery satellite constellation are already presumably budgeted (the funding for reconnaissance satellites has always been classified), other changes to the satellite constellation, particularly in support of DOD's quest for world-wide "persistent" surveillance and reconnaissance, may significantly increase the cost of future ISR. These programs are apparently exactly

---

[103] David A. Fulghum, "Pentagon Priorities Shift to Data and Networks," *Aviation Week & Space Technology*, April 22, 2002, p. 22.

[104] Mark Lowenthal, previously cited, believes that the Joint Chiefs of Staff's *Joint Vision 2010* and *Joint Vision 2020*, the guiding documents for service transformation efforts, exhibit an "'intellectual sloppiness' that tends to use 'information systems' interchangeably with 'intelligence.'"(p. 9) He perceives an assumption in the *Joint Visions* that the information (i.e., intelligence) on the networks will be accurate, but they contain no explanation as to how that accuracy will be achieved.

[105] *The Budget for Fiscal Year 2003*, Washington DC, 2002, p. 277.

the types of programs Secretary of Defense Rumsfeld is proposing should receive funds re-directed from reduced or cancelled major weapons programs such as the F-22 fighter and Comanche helicopter.[106] On the other hand, increased ISR expenditure may hold out the promise of decreased expenditures in other areas, as potentially the services will require fewer and/or cheaper weapon systems as they experience lower attrition and more efficient employment in combat situations. These savings, however, are unlikely to compensate for the potential large increases in ISR funding requirements.

Military Leadership

The military services seem to place their greatest trust in people who are trained to directly attack the enemy with deadly force. Officers who spent much of their career in the intelligence field are rarely selected to be senior leaders of their services. Most three-star officers who spent significant time as intelligence officers, as well as Admiral Bobby Inman, U.S. Navy (ret), perhaps the only career intelligence officer to achieve four-star rank, have served at that rank only as their service's senior intelligence officer or as the head of an intelligence agency such as the National Security Agency. An exception was Lieutenant General (three star) Ervin Rokke, U.S. Air Force (ret), who served as the president of National Defense University. Invariably, the officers retire after completion of their tours as the head of an intelligence agency, rather than move back into the leadership of their parent service or the Joint Chiefs of Staff. (Admiral Inman led the National Security Agency as a three-star, then became the Deputy Director of Central Intelligence as a four-star officer.)

Consequently, the most senior uniformed members of the military continue to be people who are most familiar with the procurement, planning and employment of lethal force, rather than with the procurement, planning and employment of information and intelligence.[107] While the effect is not measurable, this fact could reduce the strength with which ISR issues are fought in the DOD bureaucracy, as well as reducing the options senior officers are willing to consider as they confront new enemies and situations. While it is probably appropriate that any officer in position to order others into combat also be a combat officer, there are positions at the three and four star level which do not command combat forces. If intelligence is becoming more important to national security and the application of force than the weapons themselves, the Senate may find it desirable to express a desire to the Secretary of Defense that more officers with an intelligence background be nominated for senior officer positions.

---

[106] Thom Shanker, "Rumsfeld Delays Decisions on Trimming Arms Programs," New York Times, May 1, 2002, p. A19.

[107] Vernon Loeb and Thomas E. Ricks, "1's and 0's Replacing Bullets in U.S. Arsenal," *Washington Post*, Feb 2, 2002, p. 1.

Military Intelligence Role in Homeland Defense

All of the services believe that they must play a greater role in homeland defense than they had before the September 11 attacks. The role of the services' intelligence capabilities, however, does not appear to be as clear. By law, the military is restricted in its authority to collect or analyze intelligence on U.S. persons or the United States. In addition, the military is in a war, the global war on terrorism, which is stretching intelligence assets. Intelligence collected and analyzed for the military should be made available to other agencies involved in homeland defense. This is already occurring between the Navy, Coast Guard, and other domestic agencies with responsibilities for port security, as well as between DIA, CIA, FBI and NSA.[108] However, a significant shift of effort by the service intelligence agencies from overseas to homeland defense may be inappropriate.

The establishment of the Department of Homeland Security (DHS) in January 2003 will affect the responsibilities of all intelligence agencies, including those in DOD. DHS will not itself collect foreign intelligence, but will depend upon intelligence forwarded from other agencies. The nature and extent of support that DOD agencies will be expected to provide DHS remains as yet uncertain.[109] Congress may wish to maintain oversight of the overall effort to coordinate and consolidate intelligence for homeland security.

Intelligence Community Reform

Reform of the Intelligence Community is a perennial subject for high-level commissions. The most recent presidential commission, headed by Lt Gen Brent Scowcroft (U.S. Air Force, ret), made a recommendation to place the defense intelligence agencies directly under the Director of Central Intelligence (DCI),[110] but no action was taken on the proposal in the 107th Congress. If such a move does occur in the future, the concern for the military services would probably be to prevent any significant reduction in current and near-term production of IMINT by NIMA and SIGINT by NSA. The services use these capabilities heavily, and subordinating the defense agencies under the DCI could lower the priority placed on military requirements. If, on the other hand, the centralization creates conditions for a transformation in analysis without significantly reducing current production, the military services may be better off in the long run.

---

[108] Interview with CAPT Rich Kelly, USCG; Weisman, "Intelligence Agencies," p. 11.

[109] See Richard A. Best, Jr., *Homeland Security: Intelligence Support*, CRS Report RS21283.

[110] "Senior CIA Official Says Rumsfeld 'Absolutely Wrong' on Intel Reform," *Defense Information and Electronics Report*, April 26, 2002, p. 1.

Appendix: Acronyms

AC2ISRC	Aerospace Command and Control and Intelligence, Surveillance and Reconnaissance Center
ACTD	Advanced Concept Technology Demonstration
ASD/C3I	Assistant Secretary of Defense for Command, Control, Communications and Intelligence
ASDS	Advanced SEAL Delivery System
BDA	Bomb Damage Assessment
C2ISR	Command, Control, Intelligence, Surveillance and Reconnaissance
CEC	Cooperative Engagement Capability
CIA	Central Intelligence Agency
DARPA	Defense Advanced Research Project Agency
DCGS	Distributed Common Ground System
DCI	Director of Central Intelligence
DIA	Defense Intelligence Agency
DOD	Department of Defense
GPS	Global Positioning System
HUMINT	Human Intelligence
IMINT	Imagery Intelligence
ISR	Intelligence, Surveillance, and Reconnaissance
JCS	Joint Chiefs of Staff
JFCOM	Joint Forces Command
JROC	Joint Requirements Oversight Council
MASINT	Measurement and Signatures Intelligence
NIMA	National Imagery and Mapping Agency
NMCI	Navy and Marine Corps Intranet
NRO	National Reconnaissance Office
NSA	National Security Agency
OFT	Office of Force Transformation
OSD	Office of the Secretary of Defense
QDR	Quadrennial Defense Review
RSTA	Reconnaissance, Surveillance, Targeting and Acquisition
SEAL	Sea-Air-Land forces
SIGINT	Signals Intelligence
SIPRNET	Secure Internet Protocol Network
SOCOM	Special Operations Command
UAV	Unmanned Aerial Vehicle
UUV	Unmanned Underwater Vehicle