Order Code IB10012

Issue Brief for Congress
Received through the CRS Web

Intelligence Issues for Congress

Updated July 19, 2002

Richard A. Best, Jr.
Foreign Affairs, Defense, and Trade Division

Contents

Intelligence Issues for Congress

SUMMARY

The U.S. Intelligence Community continues to adjust to the post-Cold War environment. Congressional and executive branch initiatives have emphasized enhancing cooperation among the different agencies that comprise the Community by giving greater managerial authority to the Director of Central Intelligence (DCI).

Priority continues to be placed on intelligence support to military operations and on involvement in efforts to combat narcotics trafficking and, especially since September 11, 2001, international terrorism. Growing concerns about transnational threats are leading to increasingly close cooperation between intelligence and law enforcement agencies. This relationship is complicated, however, by differing roles and missions as well as statutory charters.

The September 11, 2001 terrorist attacks, for which no specific warning was available, have led to increased emphasis on human intelligence, better cooperation between law enforcement and intelligence agencies, and on consideration of organizational changes to the Intelligence Community.

Intelligence Community leadership and congressional committees have expressed determination to enhance analytical capabilities. A major concern is an imbalance between resources devoted to collection and those allocated to analysis, with collected data much exceeding analytical capabilities.

In several regional crisis areas, the role of the U.S. Intelligence Community is especially important. Provisions for U.S. intelligence to monitor security arrangements between Israelis and Palestinians have been a factor in efforts to resolve Middle East tensions. Intelligence efforts have also been important in attempting to enforce U.N. sanctions on Iraq and monitoring peace agreements in Bosnia.

Cruise missile and bomb attacks on Afghan targets in the campaign against the Taliban, and on Serbian targets during the Kosovo crisis have been heavily dependent upon precise targeting data provided by intelligence sensors. The mistaken attack on the Chinese Embassy in Belgrade resulted from faulty information provided by the Intelligence Community.

A particular concern for many in Congress has been the Intelligence Community's assessment of the missile attack capabilities of foreign countries, especially North Korea. Some believe that U.S. vulnerability to missile attack may arrive sooner than has been estimated by intelligence agencies.

MOST RECENT DEVELOPMENTS

The House is scheduled to consider H.R. 4628, the FY2003 Intelligence Authorization, on July 24. The accompanying report from theHouse Permanent Select Committee on Intelligence (HPSCI), H.Rept. 107-592, indicates approval of "substantial increases for intelligence" but notes serious concerns that the Intelligence Community "did not take into account sufficiently the complexity and importance of the growing threat from terrorism associated with Islamic fundamentalism." Furthermore, HPSCI strongly criticizes the imbalance between resources devoted to collection and those devoted to analysis, the failure of the DCI and the Community Management Staff to forward required reports to Congress, an underemphasis on the acquisition of foreign language skills, and an increasing reliance on supplemental appropriations to fund core mission support. As a result of questionable management and cost growth, the Air Force's Global Hawk Unmanned Aerial Vehicle (UAV), has become, according to HPSCI, a platform "too expensive to risk losing."

On July 17, the HPSCI Subcommittee on Terrorism and Homeland Security issued a report on the background to the 9/11 attacks. The unclassified summary of the report concluded that the intelligence community should "institutionalize its sharp reorientation toward going on the offensive against terrorism." The summary noted specific challenges facing CIA, NSA, the FBI, and the Congress.

Legislation to establish a Department of Homeland Security (H.R. 5005) includes provisions for an information analysis directorate that would process and analyze information forwarded by intelligence and law enforcement agencies relating to terrorist threats to the U.S. The new department would not itself collect intelligence, but would draw upon information collected by intelligence and law enforcement agencies.

BACKGROUND AND ANALYSIS

The end of the Cold War, now a decade past, continues to reverberate throughout the United States Intelligence Community. Since the beginning of the first Bush Administration, intelligence agencies have been reduced in size (reportedly by some 30%) and priorities shifted away from the Soviet Union and its erstwhile allies. Yet the post-Cold War world has its own complexities—political, economic, and technological—that continue to require the attention of intelligence agencies. The attacks on the World Trade Center and the Pentagon on September 11, 2001, dramatically demonstrated the changed nature of threats facing the United States. The Intelligence Community is challenged by the variety of topics on which information is needed, changing technologies that may limit success in acquiring information, and, not least, by temporary and not-so-temporary needs for expertise in many different foreign languages.

Changes in the nature of the world beyond U.S. borders, the sole focus of intelligence agencies, have required a shift in the purposes and goals of the Intelligence Community. Gone is the relentless focus on Soviet submarines, missile silos, and conventional military capabilities; new threats include terrorism, transfers of Weapons of Mass Destruction (WMD), and political, ethnic, and social upheavals in a variety of regions. Gone also is the massive military infrastructure of the Soviet Union that could be observed by overhead

imagery platforms. Intelligence agents must be able to move beyond contacts with foreign government officials and tap into political sects and terrorist cells often having no perceptible infrastructure.

As a result, some observers believe that intelligence agencies may be in for a period of transition and adaptation exceeding the one that followed immediately upon the dissolution of the Soviet Union and the Warsaw Pact. In particular, it is argued that **the three major "INTs,"** the major intelligence disciplines—signals intelligence (sigint), imagery intelligence (imint), and human intelligence (humint)—will have to be fundamentally reinvented and this process will have major technical and organizational ramifications. There will have to evolve, it is further argued, a coherent community-wide managerial structure that will respect the varied and changing needs of military and civilian intelligence consumers while keeping costs within bounds and avoiding unnecessary duplication of effort. Making some of these changes may not save money, and may even require budgetary enhancements; according to this argument, a failure to confront changed realities may result in substantial waste of the $27+ billion now invested in intelligence and intelligence-related activities.

The events of September 11, 2001, persuaded many observers that there may a need for a wide-ranging review of the **organizational structure of the Intelligence Community**. Media reports in early November 2001 indicated that a review of the Intelligence Community by an Administration panel, headed by former National Security Adviser Brent Scowcroft, would recommend transferring three major intelligence agencies to the direct control of the DCI and the separation of the DCI from day-to-day management of the CIA. The conferees on the FY2002 intelligence authorization bill indicated their conclusion that "today's intelligence structure is not suitable to address current and future challenges." Defense Secretary Rumsfeld, however, has indicated in early April 2002 that there has been no decision on reported recommendations and noted disadvantages that may derive from centralization of intelligence gathering.

Sigint collection is the responsibility of the National Security Agency (NSA) at Fort Meade, Maryland. Sigint operations are classified, but there is little doubt that the need for intelligence on a growing variety of nations and groups that are increasingly using sophisticated—and rapidly changing—encryption systems requires a far different sigint effort than the one prevailing for several decades. In 1998 the House Intelligence Committee concluded that "very large changes in the National Security Agency's culture and method of operations need to take place ...." Some observers believe that an inevitable restructuring of NSA will be required at the cost of many billions. The Senate Intelligence Committee acknowledged that "NSA's core mission is an essential national capability, and must be dramatically rejuvenated" but added that some new initiatives, already underway, will require "a significant infusion of funds." Observers credit the current Director of NSA, Lt. Gen. Michael Hayden, with launching a long-overdue reorganization of the Agency, but adapting it to changed technological and geopolitical conditions will remain a significant challenge.

Several reports sponsored by the European Parliament have alleged that NSA operates an international sigint collection effort, known as **Echelon**, that intercepts communications worldwide in order to provide economic intelligence to U.S. corporations. On July 5, 2000, the European Parliament voted to undertake a further investigation of Echelon; the resultant draft report on Echelon was made public on May 18, 2001. Maintaining that NSA operates in accordance with existing statutes and executive orders, senior U.S. officials have strongly

disputed claims that intelligence agencies assist U.S. corporations competing with foreign firms. They acknowledge, however, that intelligence agencies collect information regarding the use of bribery and other illegal efforts by foreign firms in competition with U.S. corporations. Indications of such foreign efforts are provided to the State and Commerce Departments. (See CRS Report RS20444, *Project Echelon: U.S. Electronic Surveillance Efforts*, by Richard A. Best, Jr.)

A second major intelligence discipline, imagery or **imint** is also facing profound changes. Imagery is collected in essentially three ways, satellites, manned aircraft, and unmanned aerial vehicles (UAVs). (See CRS Report RL31369, *Imagery Intelligence: Issues for Congress*, by Richard A. Best, Jr.) The satellite program that covered Soviet Union and acquired highly accurate intelligence of submarines, missiles, bombers and other military targets is perhaps the greatest achievement of the U.S. Intelligence Community. The demise of the Soviet Union and experience in the Persian Gulf War have indicated that there is likely to be a greater number of collection targets than in the Cold War and that more maneuverable satellites may be required. At the same time, the advent of high-quality commercial satellite imagery has raised many questions about whether at least some coverage can be obtained less expensively from the private sector. (See the discussion of India's nuclear tests below.) Concern has been widely expressed that imagery architecture is unbalanced, that acquiring collection platforms has been emphasized at the expense of analytical and dissemination efforts.

Imagery as a collection discipline has been affected by the establishment in 1996 of the National Imagery and Mapping Agency (NIMA) to manage imagery processing and dissemination to national decision makers and combat commanders. NIMA is composed of agencies with disparate backgrounds, including the Defense Mapping Agency, which was never a member of the Intelligence Community. Inevitably, there have been start-up problems, especially in terms of financial management.

Manned aircraft—the U-2 and other aircraft used by the services for tactical intelligence collection—remain important sources of imagery. The SR-71, which flew at very high altitudes, has been retired, and no replacement is apparently envisioned. The U-2s, the earliest of which were procured in the 1950s, are being upgraded with new interception capabilities and new navigational equipment, but some observers express concern that a follow-on will not be available because of a questionable assumption that they can be completely replaced with unmanned aerial vehicles. Limited inventories of airborne platforms that are in high demand have led some industry officials to suggest business-class jets equipped with a number of sensors for use in military missions.

UAV procurement has been a continuing source of difficulties. Some UAVs were used during the Vietnam War, the advantages of these pilotless craft have been more generally appreciated in the last decade or so when they have been equipped with electro-optical devices and real-time communications. Since the Persian Gulf War, they have been widely recognized as relatively inexpensive sources of tactical imagery that do not place the lives of U.S. personnel at risk; they have been widely used to monitor peacekeeping operations in Bosnia. UAV procurement efforts, however, have been beset by problems. Several systems have been canceled after millions of dollars were spent without producing operational platforms. The UAV effort has been perceived by many in Congress as lacking in focus and unable to meet operational requirements. The Global Hawk UAV, currently undergoing

testing, is the most promising approach to obtaining a high-altitude, long-endurance unmanned platform; see CRS Report RL30727, *Airborne Intelligence, Surveillance & Reconnaissance (ISR): The U-2 Aircraft and Global Hawk UAV Programs*, by Christopher Bolkcom and Richard A. Best, Jr. The House versions of the Intelligence Authorization bill for FY2002 directed a full-scale review of requirements for airborne reconnaissance; airborne reconnaissance has been extensively employed in Afghanistan operations despite losses of several UAVs, including one Global Hawk.

A long-standing criticism of the Intelligence Community's imint effort has been an imbalance between collection and analysis: that far more imagery is collected than can ever be evaluated with large quantities remaining "on the cutting room floor." Intelligence budgets moreover reflect an emphasis on the procurement of collection systems with fewer resources allocated to processing and analysis. Some also argue that priority is given to the concerns of operational military forces rather than to matters of interest to senior political leaders, *e.g.*, it has been alleged that in 1995 imagery analysts were concentrating on Serb air defenses to an extent that delayed finding evidence of mass grave sites of acute interest to the State Department. The House intelligence committee has concluded that, "the emphasis on collection at the expense of downstream activities [i.e., processing and analysis] permeates the [Intelligence Community] at all levels and in most collection disciplines." During House consideration of FY2000 intelligence authorization legislation, concern for a better balance between collection and analysis was reiterated; Representative Lewis stated in the floor debate on November 9, 1999: "In this bill, Congress has told the administration enough is enough. We have said that, unless there is a plan implemented that will process the satellite data ..., we will not buy the satellite system as currently proposed."

Intelligence from human contacts—**humint**—is the oldest intelligence discipline and the one that is most often written about in the media. (Humint collection is to be distinguished from covert actions although they may on occasion involve the same agents; see CRS Report 96-844, *Covert Action: An Effective Instrument of U.S. Foreign Policy?*, by Richard A. Best, Jr.) The Central Intelligence Agency (CIA), which is responsible for most humint collection, had important successes during the Cold War; disaffected Soviets and others provided invaluable help in providing information about weapons programs and political intentions that were not obtainable from any other source. In large measure, targets of U.S. humint collection during the Cold War were government officials and military leaders. Intelligence agency officials working under cover as diplomats could approach such potential contacts at receptions or in the context of routine embassy business. Today, however, the challenge is making contacts with influential figures in heretofore obscure third world states, clandestine groups, or narcotics traffickers who speak a variety of foreign languages. Humint regarding such sources can be especially important as there may be little evidence of activities or intentions that can be gathered from imagery and their communications may be carefully limited.

Contacts with such persons usually cannot be made in the course of embassy business or in diplomatic receptions; in many cases contacts between a U.S. embassy and terrorist figures or narcotics smugglers would be unacceptable to either side. Placing U.S. intelligence officials in foreign countries under "non-official cover"—in businesses or other private capacities—is possible but it presents significant challenges to the agencies. Administrative mechanisms are vastly more complicated; special arrangements have to be made for pay, allowances, retirement, and healthcare. The responsibilities of operatives

under non-official cover to the parent intelligence agency have to be reconciled with those to private employers and there is an unavoidable potential for many conflicts of interest or even corruption. Any involvement with terrorist groups or smugglers has an inevitable potential for major embarrassment to the U.S. government and, of course, physical danger to those immediately involved.

Responding to allegations in the early-1990s that CIA agents may have been involved too closely with narcotics smugglers and human rights violators in Central America, the then-DCI, John Deutch, established **guidelines** in 1995 (which remain classified) to govern the recruitment of informants with unsavory backgrounds. Although CIA officials maintain that no proposal for contacts with persons having potentially valuable information has been disapproved, there is a widespread belief that the guidelines serve to encourage a "risk averse" atmosphere at a time when information on terrorist plans, from whatever source, is urgently sought. Section 903 of the USA Patriot Act (P.L. 107-56), enacted October 26, 2001, expressed the sense of Congress that intelligence officials "should be encouraged, and should make every effort, to establish and maintain intelligence relationships with any person, entity, or group" to acquire information on terrorist groups. The FY2002 Intelligence Authorization Act (P.L. 107-108) directed the DCI to rescind and replace the guidelines.

Another problem is the availability of personnel trained in appropriate languages. Cold War efforts required a supply of linguists in a relatively finite number of foreign languages, but in recent years the Intelligence Community has needed experts in a wider range of more obscure languages and dialects. Various approaches have been considered: use of civilian contract personnel, military reservists with language qualifications, and substantial bonuses for agency personnel who maintain their proficiency. The House Intelligence Committee has called for consideration of the establishment of a new Intelligence Community language training facility and for language proficiency requirements for intelligence analysts.

A fourth INT, measurement and signatures analysis—**masint**, has received greater emphasis in recent years. A highly technical discipline, masint involves the application of more complicated analytical refinements to information collected by sigint and imint sensors. It also includes spectral imaging by which the identities and characteristics of objects can be identified on the basis of their reflection and absorption of light. A key problem has been retaining personnel with expertise in masint systems who are offered more remunerative positions in private industry.

In the current geopolitical environment, another category of information, open source information–**osint** (newspapers, periodicals, pamphlets, books, radio, television, and Internet Web sites), is increasingly important. Whereas the Soviet Union was a tightly closed society with access difficult to come by, most (but not all) countries of interest today are far more open in their media. A much greater proportion of information can thus be obtained without the use of human agents or sophisticated collection platforms. At the same time, requirements for translation, dissemination, and systematic analysis may even have increased, given the multitude of different areas and the volume of materials. Most observers believe that intelligence agencies should be more aggressive in using osint; some believe that the availability of osint may even reduce the need for certain collection efforts. The availability of osint also raises questions regarding the need for intelligence agencies to undertake collection, analysis, and dissemination of information that could be directly obtained by user agencies.

Whether the statutory authorities of the DCI are adequate is subject to debate; proposals to transfer all intelligence agencies to the operational control of the DCI have not gained pervasive support in either the executive or legislative branches. The budgetary authorities of the DCI, enhanced in the Intelligence Authorization Act of FY1997 (P.L. 104-293), allow him to prepare a consolidated national intelligence budget that in turn permits making tradeoffs among different INTs and programs before budgets are submitted to Congress. This authority, however, can realistically be exercised only with the cooperation of the Defense Department, given the location of intelligence agencies within DOD and the enormous influence exercised by the Pentagon over intelligence spending. Although extensive readjustments have been made by Congress, some argue that they could be more efficiently undertaken within the executive branch.

The widespread use of computers and new communications systems means that although there is a greater need for coordinating the INTs at the Washington level, intelligence products are used at many different levels of government and that quite low-level users can access information from Washington-area agencies. In addition, there has been increased availability of tactical intelligence collectors—sigint systems, aircraft and UAVs—that are operated by military commanders who are also the immediate recipients of the information acquired. Some observers express concern about excessive emphasis on tactical intelligence, arguing that national priorities may be downgraded. Others note, on the other hand, that organizational structures, traditionally focused on providing information from each "INT" to the Washington agency in charge of that "INT" (a practice known as "stove piping") do not adequately serve current needs of military commanders. Observers suggest that there will be increasing needs to share national and tactical intelligence and for organizational and individual flexibility.

Another issue is funding. Some alternatives to current platforms and procedures may produce cost savings, but observers suspect that they may be outweighed by increases found necessary in other areas. Satellites will remain high-cost programs, greater numbers of UAV systems and human collectors will have to be supported and trained. Observers generally expect that intelligence activities will probably continue to absorb some 10% of the defense budget in any given year. It is uncertain whether such percentages will be adequate to accommodate major changes in NSA's operations, the acquisition of additional imagery platforms, and a reorganized humint effort.

Although much of the restructuring that arguably is required could be accomplished by executive branch initiative, Congress remains responsible for appropriations and for oversight. Even at a time of budgetary surpluses, significant increases in intelligence spending will have to be balanced against other national priorities. In recent years Congress has emphasized the need for expanded humint capabilities and has insisted upon a major role in the acquisition of new imagery collection platforms. Other concerns—and directives—are undoubtedly expressed in the classified annexes to intelligence authorization bills. Even if Congress and the leadership of the Intelligence Community concur on the need for major changes in these and other areas, ensuring the reorienting of long-established organizations is a difficult task.

Implementation of other changes enacted in 1996 remains an ongoing process. In May 1998, Joan Dempsey, a career intelligence official, was confirmed by the Senate to fill the newly established position of Deputy DCI for Community Management. Two other positions,

designated as requiring Senate confirmation, have been filled without formal Senate action as a result of an understanding reached between the Administration and the Senate Intelligence Committee.

For budgetary purposes, intelligence spending is divided between the National Foreign Intelligence Program (NFIP), which covers Washington-based agencies and Tactical Intelligence and Related Activities (TIARA) (also known as intelligence-related activities), which covers programs supporting the operating units of the armed services, and the Joint Military Intelligence Program (JMIP), which covers programs, not-necessarily tactical, that are of primary concern to the Defense Department. Jurisdiction over these programs is somewhat different in the House and the Senate, but in both chambers members of both intelligence and armed services committees are involved in oversight efforts.

For a number of years some Members have sought to make public total amounts of intelligence and intelligence-related spending; floor amendments for that purpose were defeated in both chambers during the 105th Congress. In response, however, to a lawsuit filed under the Freedom of Information Act, DCI Tenet stated on October 15, 1997 that the aggregate amount appropriated for intelligence and intelligence-related activities for FY1997 was $26.6 billion. He added that the Administration would continue "to protect from disclosure any and all subsidiary information concerning the intelligence budget." In March 1998, DCI Tenet announced that the FY1998 figure was $26.7 billion. Figures for FY1999 have not been released and the Administration has thus far prevailed against legal efforts to force release of intelligence spending figures. On May 23, 2000, the House voted 175-225 to defeat an amendment calling for annual release of an unclassified statement on aggregate intelligence spending. Some have suggested that if intelligence spending totals were made public it would no longer be necessary to "hide" intelligence programs within the Defense Department budget; national programs at least could broken out and consolidated under the DCI and the two intelligence committees. Others contend that the current system ensures that national intelligence programs are closely related to military operations and are considered in conjunction with defense programs.

A significant concern continues to be the need to provide **intelligence support to operating military forces**. In 1997, the House intelligence committee noted that "intelligence is now incorporated into the very fiber of tactical military operational activities, whether forces are being utilized to conduct humanitarian missions or are engaged in full-scale combat." The Persian Gulf War demonstrated the importance of intelligence from both tactical and national systems, including satellites that had been previously directed almost entirely at Soviet facilities. There were, nonetheless, numerous technical difficulties, especially in transmitting data in usable formats and in a timely manner. Many of these issues have since been addressed with congressional support, but many observers believe that significant technical and organizational challenges remain. Among issues of concern are capabilities to disseminate imagery rapidly, the procurement and use of unmanned aerial vehicles (both tactical and high altitude) and manned reconnaissance aircraft, along with associated sensors and communications systems. Expressing concern about "substantial mismanagement and lack of communication," the Senate Intelligence Committee has called for a report identifying "specific actions that have been taken or are being taken to enhance cooperation between Department of Defense and the Intelligence Community by improving the provision, handling, and use of intelligence information in preparation for, during, and after battle."

Making usable intelligence available to military commanders in a timely fashion has been a principal preoccupation of the Intelligence Community since the Persian Gulf War. Further efforts will undoubtedly be necessary, given the Defense Department's increasing emphasis on "dominant battlefield awareness" as reflected in Joint Vision 2010 and the Quadrennial Defense Review (QDR). Operational concepts now under consideration in the Department of Defense (DOD) clearly will require even greater intelligence support for precision targeting, bomb damage assessment, and other purposes. The House committee noted, however, that the QDR did not project increased intelligence funding, and, in fact, called for the reduction in the procurement rate of the Joint Surveillance and Target Attack Radar System (JSTARS) aircraft. The Senate committee also noted inadequate manned reconnaissance platforms and indicated a need for a long-term airborne reconnaissance recapitalization plan.

The House intelligence committee has given special attention to **weaknesses in analysis**, expressing concern about "a largely inexperienced workforce; lack of language skills and limited in-country familiarity ...; and a predominant focus on current intelligence that is eroding the [Intelligence Community's] ability to conduct comprehensive strategic analysis." The bureaucratic tendency to emphasize current intelligence over long-term analysis has been noted for many years. It has been enhanced by the shift from enduring targets such as the Soviet Union to the disparate and fluctuating concerns of the post-Cold War period. The House committee advocates the establishment of core groups of analysts to undertake research-oriented projects aimed at assessing strategic issues. It further expressed support for a civilian intelligence reserve program that would utilize the expertise of former intelligence officials as well as civilian experts and linguists. Provisions authorizing competitive analysis of intelligence products having national importance and for quadrennial intelligence reviews to complement the Quadrennial Defense Review were included in the FY1999 Intelligence Authorization Act.

The Intelligence Community's failure to provide advance notice of **India's nuclear tests** in May 1998 produced searching reviews of analytical efforts and capabilities both in the executive branch and Congress. The initial review, undertaken by Admiral David Jeremiah, former vice chairman of the Joint Chiefs of Staff, has not been made public, but in a press conference Admiral Jeremiah described his conclusions. Although the Indian government that took office in late March 1998 had indicated its intention to "exercise the option to induct [*sic*] nuclear weapons," most observers believed that India would conduct a lengthy assessment prior to undertaking tests. Admiral Jeremiah concluded that "both the intelligence and policy communities had an underlying mindset going into these tests that the BJP [the party heading the new Indian government] would behave as we behave." The Indians also undertook various efforts to mask their intentions and to hide their test preparations. The Intelligence Community provided more detailed information on the follow-on Pakistani tests.

Admiral Jeremiah called for more rigor in analysts' thinking and urged that outside experts be brought into the analytical process. There is, he maintained, a need for "greater collaboration and coordination of intelligence agencies and disciplines." There is also, he pointed out, an imbalance between the vast quantities of imagery collected and limits on numbers of analysts. "In everyday language, that means there is an awful lot of stuff on the cutting room floor at the end of the day that we have not seen." In essence, Jeremiah concluded that the DCI needs to ensure greater coordination among intelligence agencies in

regard both to collection and analysis. DCI Tenet accepted Jeremiah's recommendations. Appreciating that no system can prevent any future intelligence surprise or "failure," many observers believe that inadequate coordination may have contributed significantly to the inability to monitor Indian nuclear efforts more closely. (See CRS Report 98-672, *U.S. Intelligence and India's Nuclear Tests: Lessons Learned*, by Richard A. Best, Jr.)

Further concerns about the quality of intelligence analysis resulted from the **North Korean launch of a three-stage Taepo Dong 1 missile** on August 31, 1998. The Intelligence Community had long anticipated a two-stage Taepo Dong missile launch, but its capability to be used as a space launch vehicle with potential for striking some U.S. territory was unexpected.

Congress remains concerned with the potential for abuses by intelligence agency personnel and has addressed the question of **whistleblower protection** for officials working in intelligence agencies who may not be covered by other whistleblower legislation. The FY1999 Intelligence Authorization Act established procedures by which an intelligence agency official (or contractor) who seeks to provide information to Congress with respect to an urgent concern would first report such concern to the inspector general of his or her agency. The IG in turn would forward the information to the agency head within 14 days. The agency head would then forward it to the congressional intelligence committees within 7 days. If the IG does not transmit the information (or does so inaccurately) the complainant could forward it to the intelligence committees directly if the agency head is notified. The conference report noted that "an intelligence committee Member or staff employee receiving such complaints or information must abide by the rules of the intelligence committees."

Encryption remains an important legislative concern that has significant intelligence implications. Given advances in technology that may make obsolete the current controls on the export of encryption systems, bills have been introduced in both the House and the Senate to create a new regulatory framework. One proposal, H.R. 850, would loosen export controls on sophisticated encryption systems. Officials in intelligence and law enforcement agencies have expressed concerns that such liberalization would serve to provide protection to the communications of international terrorists and rogue states. The Senate Intelligence Committee expressed concern in May 1999 that loosening export restrictions "may severely damage the Intelligence Community's ability to perform its SIGINT mission." On July 15, 1999, the House Intelligence Committee unanimously adopted an amendment to H.R. 850 that would provide broader grounds for the President to control exports of encryption; see the Intelligence Committee's report, *Encryption for the National Interest Act*, H.Rept. 106-117, Part 5. In September 1999, the Administration announced changes to its encryption policy making products exportable (after a technical review) to any country except seven terrorist states. A request for comments on an interim final rule revising regulations on the export of encryption items was published on January 14, 2000 (65FR2492-2502). (For further background on the encryption question, see CRS Issue Brief IB96039, *Encryption Technology: Congressional Issues*, and CRS Report 98-905, *The Encryption Debate: Intelligence Aspects*, by Keith G. Tidball and Richard A. Best, Jr.)

With growing concerns about **terrorism**, U.S. policymakers have become increasingly concerned about transnational threats, including narcotics smuggling, terrorism, and especially the possibility that terrorist groups might obtain access to weapons of mass destruction. Since such transnational threats are often best dealt with in law enforcement

channels, **greater cooperation between intelligence and law enforcement agencies** has been encouraged in recent years. This cooperation has raised a number of difficult issues: potential duplication of effort, the use of information obtained by intelligence agencies in court trials, the danger that the methods of covert intelligence collectors might be used routinely in law enforcement cases, the undermining of legitimate foreign policy and defense initiatives. (For additional background, see CRS Report RL30252, *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S.*, by Richard A. Best, Jr.)

Concern that information from both law enforcement and intelligence agencies may not be reaching those responsible for dealing with international terrorist threats has grown since the incidents of September 11, 2001. Much information about Osama bin Laden and the al Qaeda network was accumulated for trials of individuals connected with the 1993 World Trade Center attack and an aborted January 2000 attack on the Los Angeles airport. Critics charge that much of this information was not made available to intelligence agencies, and some of that which was available may not have been thoroughly exploited. Further, some argue that information available to intelligence agencies was not shared with the law enforcement agencies that could have apprehended (because of immigration violations) some of those involved in the September 11 attacks. The USA Patriot Act (P.L. 107-56) was designed to facilitate the greater sharing of information available to law enforcement agencies (including grand jury testimony) with the Intelligence Community in accordance with guidelines to be established by the executive branch.

Proposals to establish a **Department of Homeland Security** envision an Information Analysis and Infrastructure Protection division that will be responsible for analyzing information provided by intelligence and law enforcement agencies. The new Department will, according to reports, not itself engage in collecting intelligence, but will receive analyses and, to some as yet unknown extent, unanalyzed information from other agencies. Based on its threat analysis, the Homeland Security Department would effect necessary measures to protect the U.S. public and infrastructures.

Congress also remains concerned about intelligence support provided to the government's counter-narcotics effort. The Explanatory Statement accompanying the FY1998 intelligence authorization conference report expressed concern about funding the **National Drug Intelligence Center (NDIC)** through the National Foreign Intelligence Program inasmuch as NDIC functions within the Department of Justice. Nonetheless, NDIC funding has continued to be incorporated in defense authorization and appropriation acts. FY2002 intelligence authorization legislation provides NDIC with $44 million and the accompanying report indicates satisfaction with NDIC's recent performance.

In February 2000, the Clinton Administration announced the establishment of an interagency **Counter Drug Intelligence Coordinating Group** composed of representatives of major federal law enforcement and intelligence agencies. The Group's responsibility will be to ensure coordination in the narcotics intelligence efforts of federal departments and agencies. An interagency staff, the Counterdrug Intelligence Executive Secretariat, with some 30 personnel has been created to support the Group and roles and missions have been assigned to the four major national narcotics intelligence centers–the DCI's Crime and Narcotics Center (CNC), the National Drug Intelligence Center (NDIC), the El Paso Intelligence Center (EPIC), and the Financial Crimes Enforcement Network (FinCen).

Although most observers acknowledge the need for close coordination among intelligence and law enforcement agencies in regard to narcotics intelligence, some questions exist about the implications of the creation of this interagency structure for the DCI's statutory responsibilities for the national intelligence effort. Questions also remain concerning policy guidelines and procedures for the use of intelligence information for law enforcement purposes. Concern has also been expressed about the role of U.S. intelligence agencies in support of counter-narcotics efforts in South America, with some observers expressing concern about the value of the contribution and others noting the danger of involving the U.S. in local insurrections fueled by drug money. Others have pointed to the dangers involved in U.S. intelligence officials or contractors providing intelligence to foreign countries who use this data to attack suspicious civilian aircraft. Section 1012 of the FY1995 Defense Authorization Act (P.L. 103-337) provided official immunity for U.S. agents involved in authorized support to foreign counter-narcotics efforts, but some observers call for a review of the whole policy in light of the April 2001 attack by a Peruvian aircraft on a missionary plane with the loss of two lives.

For some years concerns have been expressed about issues of **secrecy and classification**. Some argue that classification and declassification authorities and procedures should be more closely based in statutory law. Others believe that far too much government information is classified and withheld from the public, especially given the end of the Cold War. A Commission on Protecting and Reducing Government Secrecy, chaired by Senator Moynihan, recommended in 1997 a series of measures to establish the basic principles of security classification and declassification. These measures were incorporated in legislation introduced in the 105th Congress (H.R. 1546/S. 712), but the bills did not receive floor consideration in either chamber. Similar legislation (S. 22) was introduced in the 106th Congress and eventually incorporated into the Intelligence Authorization Act for FY2001 (P.L. 106-567). (For additional background, see CRS Report 98-298, *Managing Secrecy: Security Classification Reform—the Government Secrecy Act Proposal*, by Harold C. Relyea.)

Other provisions of the FY2001 intelligence authorization bill would have established criminal penalties for the **unauthorized disclosure of properly classified information**. Previous legislation established penalties only for disclosure of specific types of classified material, *e.g.* codes and cryptographic devices and information related to nuclear programs. Proponents of the provision maintained that recent leaks of highly sensitive intelligence information have not only risked the loss of valuable collection capabilities but also jeopardized important security interests. Critics argued that the provisions in H.R. 4392 were overly broad and would preclude the type of leaks that in the past have ultimately benefitted the public. The bill was vetoed by President Clinton on November 4, 2000, and another version (H.R. 5630) with the unauthorized disclosure provisions deleted was enacted on December 27, 2000, as P.L. 106-567.

Consideration was given to including similar provisions in FY2002 legislation, but Attorney General Ashcroft requested that the Administration be given time for a thorough interagency study of the need for legislation to provide additional protections against unauthorized disclosures of classified information. Accordingly, FY2002 intelligence authorization legislation provides that such a review be conducted by the executive branch and a reported submitted to Congress by May 1, 2002.

CIA and the Israeli-Palestinian Situation. The accord between Palestinian and Israeli leaders (the "Wye River Memorandum") signed in Washington on October 23, 1998, provided for a Trilateral Security Committee of high-ranking Israeli, Palestinian, and U.S. officials to oversee the implementation of the agreement and coordinate efforts to combat terror and terrorist organizations. Media accounts at the time indicated that, as a result of ongoing efforts by CIA officials to assist in the establishment of security arrangements, both the Israeli and Palestine leadership supported a more formal role for the Agency.

The accord assumed that CIA officials would continue liaison efforts, which were ongoing for several years, to improve communications between the two sides on security matters and to enhance the professionalism of Palestinian security forces. According to DCI Tenet, however, CIA officials were not to interpose themselves between the two sides, conduct interrogations, or assume a direct role on the ground. Some observers expressed concern that CIA officials might become responsible for making judgments as to whether "violations" had occurred, a responsibility that, holders of this view maintain, should be reserved to policymakers. With the deterioration of Israeli-Palestinian relations in the spring of 2001, media reports indicate that the CIA role has been reduced. DCI Tenet visited the region, but CIA-sponsored meetings between Israeli and Palestinian security officials were unproductive. In the aftermath of the fighting that has occurred in 2001-2002, the future role of the CIA in working with Palestinian security officials remains highly uncertain. Although some argue that a CIA advisory role could be accepted by both sides, others believe that further involvement could complicate the CIA's primary responsibilities of gathering intelligence for U.S. policymakers and entangle it in complex peacekeeping efforts.

In the final stages of negotiations of the Wye Accord, Israeli Prime Minister Netanyahu pressed President Clinton to pardon **Jonathan Pollard**, a former Navy Intelligence analyst, who was convicted of spying on behalf of Israel in 1986. Subsequent Israeli leaders have also pressed Pollard's case. Media reports indicate that many Intelligence Community officials, including DCI Tenet, strongly oppose any presidential pardon and opposition has been expressed by Members of both intelligence committees. (See CRS Report RS20001, *Jonathan Pollard: Background and Considerations for Presidential Clemency*, by Richard A. Best, Jr. and Clyde Mark.)

The Intelligence Community and Iraq. Persisting difficulties between the United States and Iraq present major challenges to intelligence agencies. Collecting information about the secretive Iraqi regime is difficult enough, but devising a covert strategy to remove Saddam Husayn from power has proven thus far to be insurmountable. According to information available in the media, intelligence agencies have had little success in penetrating Iraqi leadership circles. Intelligence agencies supported the efforts of U.N. inspectors charged with determining Iraqi compliance with U.N. resolutions requiring Iraq to end any programs for the acquisition or deployment of weapons of mass destruction, but such efforts have been resisted by the Iraqi government. There are, in addition, allegations that U.S. intelligence officials may have improperly interfered with U.N. inspector teams. The United States openly seeks a new regime in Bagdad and funding has reportedly been included for covert assistance to opposition elements in recent legislation, but intelligence agency officials are reportedly skeptical of providing aid to any of the existing groups working against Saddam. (See CRS Report RL31339, *Iraq: U.S. Efforts to Change the Regime*, by Kenneth Katzman; also, CRS Issue Brief IB94049 *Iraq-U.S. Confrontation: 1997-1999*, by Alfred Prados and Kenneth Katzman.)

The Intelligence Community and Missile Defense. A key Cold War-era intelligence mission that endures in the post-Cold War era is collection targeted at foreign missile capabilities, especially those capable of delivering weapons of mass destruction (WMD). As noted above, the unanticipated North Korean testing of the Taepo Dong 1 missile raised questions about intelligence collection capabilities. In addition, the July 1998 report of the Commission to Assess the Ballistic Missile Threat to the United States (known as the Rumsfeld Commission) concluded: "A new strategic environment now gives emerging ballistic missile powers the capacity, through a combination of domestic development and foreign assistance, to acquire the means to strike the U.S. within about five years of a decision to acquire such a capability (10 years in the case of Iraq). During several of those years, the U.S. might not be aware that such a decision had been made. Available alternative means of delivery can shorten the warning time of deployment nearly to zero." Although more pessimistic than much-criticized Intelligence Community estimates, this assessment underscored the vital importance of intelligence efforts in this area, especially given its key role in the debate over missile defense systems.

Kosovo/Operation Allied Force. The highly successful airstrikes against Serbian military targets, the centerpiece of Operation Allied Force, taxed U.S. intelligence capabilities. Intelligence enabled NATO to use precision munitions to destroy Serbian targets with no NATO combat casualties and with relatively limited losses of civilian lives. Nonetheless, some observers suggest that difficulties in relaying targeting data, the need for communications "work arounds," and escalating requirements for additional aircraft reflect a serious failure in the years since the Persian Gulf War to address increased requirements for imagery collection platforms for use in conjunction with precision guided munitions.

In addition to uncertainties about the future government satellite programs, critics note that DOD has been unable to acquire significant numbers of unmanned aerial vehicles (UAVs) as a result of the managerial problems that have long been subjects of congressional censure. Further, they cite the absence of plans for follow-ons to U-2 aircraft, first developed in the Eisenhower Administration, as well as a limited inventory of JSTARS aircraft with ground-radar capabilities. The FY2000 Defense Appropriations Act (P.L. 106-79) provided an increase of $15 million for the Global Hawk UAV program and requested studies on UAVs and other "low density/high demand" platforms. (See CRS Report RL30727, *Airborne Intelligence, Surveillance and Reconnaissance (ISR): The U-2 Aircraft and Global Hawk UAV Programs*, by Richard A. Best, Jr. and Christopher Bolkcom, updated December 1, 2000.) Testing of the Global Hawk continues; in April 2001 the test vehicle flew from California to Australia non-stop. Global Hawk UAVs have been deployed for use in Afghanistan, although two have malfunctioned and crashed. Further decisions on UAVs and manned reconnaissance aircraft, including the Air Force's U-2s and the Navy's P-3s, are likely to be made in the context of FY2003 budget decisions.

According to official accounts, the mistaken attack on the Chinese Embassy in Belgrade on May 7, 1999, resulted from the use of outdated maps and databases. The Yugoslav Federal Directorate of Supply and Procurement, a military supply facility, was the intended target, but it was confused with a nearby and similarly-sized building that was actually China's embassy. Although embassies were on "no-strike" lists for Operation Allied Force, along with hospitals, churches, and mosques, U.S. databases did not reflect the location of the current Chinese Embassy in Belgrade. Secretary of Defense William Cohen subsequently announced several steps to prevent future targeting errors; the State Department will be

responsible for reporting to the Intelligence Community whenever embassies move or new embassies are built, new procedures for developing target information, including procedures for updating maps will be established, and the Defense Intelligence Agency (DIA) and the National Imagery and Mapping Agency (NIMA) will establish new rapid response procedures for updating critical databases for no-strike targets.

Official spokesmen, without excusing the error, have noted the daunting challenge of maintaining a current and accurate database for a city the size of Belgrade. They also note the fact that imagery and mapping efforts, largely the responsibility of NIMA, have been affected by resource cuts in the last few years. In May 1998, the House Intelligence Committee severely criticized NIMA's management and financial accounting: "The Committee is concerned that NIMA either simply does not want to tell Congress of its dealings, or it simply doesn't know how money is being spent and managed. Neither option is good. Generally, the committee is skeptical regarding whether NIMA has the ability to forecast, manage, and execute its budget." DCI Tenet subsequently acknowledged in congressional testimony that, "We have diverted resources and attention away from basic intelligence and database maintenance, to support current operations too long."

The 9/11 Investigation. In the aftermath of September 11, 2001, there was extensive public discussion of whether the attacks on the Pentagon and World Trade Center represented an "intelligence failure." The House, in passing its version of the FY2002 intelligence bill (H.R. 2883), endorsed the establishment of a commission of individuals with experience in intelligence and national security to report on the national security readiness of the United States with respect to the events of September 11. The Senate version of intelligence authorization legislation (S. 1448) did not contain a similar provision, and the House provision was deleted by the conference committee. (Legislation, including S. 1837 and S. 1867, has subsequently been introduced to establish an independent board of inquiry.) On February 14, 2002, a joint investigation of the September 11 attacks by the House and Senate intelligence committees was announced. Britt Snider, the first staff director of the joint inquiry, resigned on April 25, 2002; his successor is Eleanor Hill, a former Inspector General of the Defense Department. Closed hearings began in early June 2002 with open hearings anticipated in late summer.

Counterintelligence. Allegations that U.S. classified information regarding missile warhead design may have been provided to Chinese officials by a scientist at the Los Alamos National Laboratory (part of the Energy Department) led to charges of lax security especially in regard to visits by foreign nationals. An Intelligence Community damage assessment, released in April 1999, concluded that China obtained by espionage classified U.S. nuclear weapons information that "probably accelerated" its program to develop future nuclear weapons. According to the assessment, China obtained at least basic design information on several modern U.S. nuclear reentry vehicles, including the Trident II (W88). A report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China concluded that U.S. information accelerated Chinese nuclear weapon modernization and "helped the PRC in its efforts to fabricate and successfully test its next generation of nuclear weapons designs. These warheads give the PRC small, modern thermonuclear warheads roughly equivalent to current U.S. warhead yields."

(For additional information, see CRS Report RL30143, *China: Suspected Acquisition of U.S. Nuclear Weapon Data*, by Shirley A. Kan and CRS Report RL30220, *China's*

Technology Acquisitions: Cox Committee's Report—Findings, Issues and Recommendations. For more recent developments, see CRS Report RL30569, *Department of Energy: Status of Legislated Security and Counterintelligence Measures*, by Jonathan Medalia.)

Reflecting concern about shortcomings in the investigation of potential espionage against Energy Department laboratories, amendments to the Foreign Intelligence Surveillance Act (FISA) were included in the Senate version of the FY2001 Intelligence Authorization bill (H.R. 4392) to establish specific provisions for the review by the Attorney General of requests for surveillance and searches under FISA. The legislation would also encourage closer cooperation between the FBI and national security agencies. Title VI of the resulting Intelligence Authorization Act for FY2001 (P.L. 106-567) included provisions designed to enhance the FBI's capabilities to undertake counterintelligence investigations and authorized $7 million in additional funding for FY2001.

In light of the arrest in February 2001of FBI Special Agent Robert Hanssen for suspicion of espionage on behalf of the former Soviet Union and Russia, Congress is expected to monitor the results of the judicial processes and undertake its own review of counterintelligence efforts. Some observers advocate more extensive use of polygraph testing of U.S. intelligence officials while others criticize the reliability of such tests. An independent commission, chaired by former FBI Director and former DCI William Webster, concluded in March 2002 that the FBI had focused so intently on traditional criminal cases that it neglected the need for security and counterintelligence. The Commission made a number of detailed practical recommendations for enhancing FBI security programs.

Selected 107th Congress Legislation

P.L. 107-108, H.R. 2883. Intelligence Authorization Act for FY2002. Introduced September 13, 2001; referred to Permanent Select Committee on Intelligence; reported, September 26, 2001; passed House (amended), October 5, 2001. Passed Senate (amended) November 8, 2001. Conference report (H.Rept. 107-328) passed House on December 12; passed Senate on December 13. Signed into law December 28, 2001.

H.R. 4628 (Goss). Intelligence Authorization Act for FY2002. Introduced May 1, 2002; referred to House Permanent Select Committee on Intelligence. Reported July 18.

S. 1448 (Graham). Enhances intelligence and intelligence-related activities in the prevention of terrorism. Introduced and referred to the Intelligence Committee, September 21, 2001.

S. 2506 (Graham). Intelligence Authorization Act for FY2003. Reported as an original bill, May 13, 2002.

Congressional Hearings, Reports, and Documents

U.S. Commission on the Role and Capabilities of the United States Intelligence Community, *Preparing for the 21st Century: An Appraisal of U.S. Intelligence*, March 1, 1996.

U.S. Congress. House of Representatives. Permanent Select Committee on Intelligence. *Intelligence Authorization Act for Fiscal Year 2002*. December 6, 2001. 107th Congress, 1st session (H.Rept. 107-328).

— *Intelligence Authorization Act for Fiscal Year 2003*. July 18, 2002. July 18, 2002. 107th Congress, 2d session (H.Rept. 107-592).

— *IC21: Intelligence Community in the 21st Century*. Staff Study. April 9, 1996. 104th Congress.

— *Intelligence Authorization Act for Fiscal Year 2001*. September 26, 2001. 107th Congress, 1st session (H.Rept. 107-219).

— Subcommittee on Terrorism and Homeland Security. *Counterterrorism Intelligence Capabilities and Performance Prior to 9-11*. July 2002.

U.S. Congress. Senate. Committee on Armed Services. *Intelligence Authorization Act for FY2001*. June 29, 2000. 106th Congress, 2d session (S.Rept. 106-325).

— *Intelligence Authorization Act for FY2002*. November 1, 2001. 107th Congress, 1st session (S.Rept. 107-92).

U.S. Congress. Senate. Select Committee on Intelligence. *Authorizing Appropriations for Fiscal Year 2001 for the Intelligence Activities of the United States Government and the Central Intelligence Agency Retirement and Disability System*. May 4, 2000. 106th Congress, 2d session (S.Rept. 106-279).

— *Authorizing Appropriations for Fiscal Year 2002 for Intelligence and Intelligence-Related Activities of the United States Government, the Community Management Account of the Director of Central Intelligence, and the Central Intelligence Agency Retirement and Disability System.* September 14, 2001. 107th Congress, 1st session (S.Rept. 107-63).

— *To Authorize Appropriations for Fiscal Year 2003 for Intelligence and Intelligence-Related Activities of the United States Government, the Community Management Account, and the Central Intelligence Agency Retirement and Disability System.* May 13, 2002. 107th Congress, 2d session. (S.Rept. 107-149).

U.S. Department of Justice, Commission for Review of FBI Security Programs, *A Review of FBI Security Programs*, March 2002.

U.S. President's Foreign Intelligence Advisory Board, Special Investigative Panel, *Science at Its Best, Security at Its Worst: A Report on Security Problems at the U.S. Department of Energy*, June 1999.