

Intelligence and Sept. 11

Col. (Ret.) Dan Smith, USA, Director of Research, dsmith@cdi.org

IN THE AFTERMATH of the attacks of Sept. 11, the accusation was “intelligence failure.”

In the aftermath of the series of revelations in May and June 2002 about bureaucratic bungling in the weeks before the attacks, the accusation was “what did the president know and when did he know it?”

On June 4, a special joint intelligence committee of Congress began a series of closed door and public sessions to examine whether and to what extent there was an “intelligence failure.” From the publicly available information to date, the congressional

probe will concentrate on pinpointing organizational shortfalls, communications failures, and “cultural” impediments that may have contributed to the inability of intelligence agencies to uncover more of the plot and the plotters of Sept. 11. Concurrently, the Senate Judiciary Committee is examining what went wrong within the Federal Bureau of Investigation (FBI).

From mid-May to June 4, the battle over who fell down on the job was waged largely in the press. Overall, the weight of recrimination fell on the FBI, whose traditional anti-crime, counter-espionage, and counter-intelligence

missions (and associated intelligence collection activities) are oriented on what transpires (or can be linked to events and persons) within the United States. What is now painfully clear is that, in today’s more interconnected world in which event time-lines are collapsing and communications are virtually instantaneous, this mainly internal focus is insufficient.

FBI Director Robert S. Mueller III stated as much during a press briefing on May 29. In addressing the FBI’s approach to the international terrorist threat, he said: “What we need to

CONTINUED ON PAGE 2

National Missile Defense Program Heads in to the “Black”

Christopher Hellman, Senior Analyst, chellman@cdi.org

ON MAY 15, 2002, *Defense Daily*, a major trade publication, revealed that the Pentagon’s Missile Defense Agency (MDA) was going to classify significant portions of its testing program. According to *Defense Daily*, the agency will give a “secret” classification to details regarding the targets and countermeasures used in all future intercept tests of its Ground-Based Midcourse Defense system — the heart of the Bush administration’s proposed national missile defense network. Starting with the next test — planned for late July — MDA will

withhold specifics about the targets and decoys used.

“We simply have reached a point in our flight test program where divulging that type of information would seriously compromise our technology development and the national security aspects of dealing with potentially hostile nations,” said Air Force Lt. Col. Richard Lehner, an MDA spokesperson quoted in the *Defense Daily* article (“MDA Classifies Missile Defense Flight Test Target, Countermeasure Data”).

The new policy seems reasonable at first glance. Potential enemies might

benefit if they knew what types of targets elude the U.S. system. Likewise if they had information about what types of countermeasures were effective in defeating U.S. interceptors. Yet the structure of future near-term tests will not reveal this type of information, and advanced testing of the system will likely not occur in this decade.

According to Philip E. Coyle, III, a CDI Senior Advisor and former head of the Pentagon’s office of Operational Testing and Evaluation, roughly 20 developmental tests will be needed before

CONTINUED ON PAGE 4

INTELLIGENCE

CONTINUED FROM PAGE 1

do better is be predictive. We have to be proactive. We have to develop the capability to anticipate attacks. We have to develop the capability of looking around corners.”¹

He might have added: “and we must be willing to take risks.”

Many point to a culture of risk-aversion that permeated FBI upper management as the chief failing of the Bureau. The FBI had its own version of the military’s “zero defects” culture in which senior officers, to protect their own careers, micro-managed and second-guessed subordinates who often were more knowledgeable. Risk-aversion may be more acceptable when the emphasis is on defensive measures that raise awareness of or reduce vulnerability to attacks. But if the objective is to prevent or deter attacks, a healthy dose of original, intuitive thinking — thinking like one’s opponent — has to inform the indications and warning process.

Related but deeper “cultural” problems contributed to the abject failure of the indications and warning process with respect to Sept. 11. These are an absence of a corps of intellectual rebels (akin to the military’s “red teams”) who are authorized and able to chal-

lenge received wisdom and ways of doing business, and who are supported or at least liberally tolerated by senior officials. Absent such a nucleus and such support, the process of innovative questioning that leads to equally innovative predictive scenarios becomes almost impossible to sustain. And if the process does not demand innovation, information that could suggest new and original approaches may never be sought and therefore never considered.

With respect to the FBI, these points are made by Michael Bromwich, the Department of Justice inspector general from 1994 to 1999, in a recent and telling opinion piece in the *New York Times*.² “Intelligence collection and analysis [in the FBI] have long been undervalued... Analysts assigned to cases have been the lowest people on the totem pole. Counterintelligence agents have been second-class citizens... The free and unfettered exchange of ideas and the willingness to challenge and question the way business is done are fundamental to a culture in which analysis is prized.”

Bromwich’s last point goes to the heart of analysis. Good intelligence — what professionals like to term “actionable” — most often is the result of piecing together, from a variety of sources, snippets of information that form a mosaic (or part of a mosaic). The consensus is that the FBI is good at collecting information,³ but this is only one part of the entire intelligence process.

What makes information useful is what one does with it. If not circulated within the collecting agency, let alone not shared with others (for knowledge is power within and between bureaucracies), its true value may never be apparent — or be apparent too late. But information flowing through a central hub staffed by skilled analysts can produce, even from an emerging

A healthy dose of original, intuitive thinking — thinking like one’s opponent — has to inform the indications and warning process.

mosaic, informed hypotheses and sometimes inspired conclusions indicating the capabilities and intentions of an opponent.

“An emerging mosaic” is a very important caveat in the analytical process, for more often than not the mosaic will be incomplete by the time preventive offensive (counterterrorism) action is required — and one might wait forever for the final bits of information that give the complete picture. And it is this caveat that elevates to a high plane the requirement to have skilled analysts in place — people willing to probe, to speculate, to question, unafraid to be wrong — looking from many angles at the patterns as they emerge.

The FBI is only one of 13 intelligence organizations at the federal level, all of which traditionally have seemed uninterested in sharing information. Director Mueller himself made this point during his May 29 press briefing: “We have to do a better job of collaborating with others. And as critically important, we have to do a better job managing, analyzing and sharing information.”

Perhaps predictably, as June unfolded, the same charge of failing to

CONTINUED ON PAGE 3

FRONTLINE: “MISSILE WARS”

The PBS broadcast of “Missile Wars,” the Frontline/Azimuth Media documentary about the behind-the-scenes battle on national missile defense, has been re-slated for Fall 2002.

For updated information, visit our website at: www.azimuthmedia.org.

INTELLIGENCE

CONTINUED FROM PAGE 2

share information was made against the Central Intelligence Agency (CIA) in connection with Sept. 11. Dueling stories appeared in the *New York Times* and *Washington Post*, centering on who knew what when during 2000 and early 2001 and what information was passed between the CIA and FBI. Both agree that they were alerted by the National Security Agency of a meeting of suspected al Qaeda operatives in Malaysia that was held in the first few days of 2000. What neither the CIA nor FBI seems to have done was to share this or subsequent information about two attendees at the al Qaeda meeting, Khalid al-Midhar and Nawaf Alhazmi, with the Immigration and Naturalization Service and the State Department, which could have prevented either from entering the United States. The latter two agencies did not learn of the connection until late August, well after the suspects had re-entered the United States and dropped out of sight.⁴

What Sept. 11 reminds us, as various failings come to light, is that collaboration is not a one-way street. It really is not even a two-way street. Intelligence collaboration is like a traffic circle with many roads (organizations or data points) feeding in information that mingles with other bits of information entering or already in the circle. Like a police officer directing and smoothing the flow of traffic, analysts integrate the various information streams, forming, breaking apart and reforming, and refining the mosaics de-

scribed above. The products then are made available to participating agencies to use to carry out their particular mandate (political, military, economic, social, environmental/energy, anti-terrorism). Done properly, this is a never-ending ebb and flow, one that should be occurring simultaneously at multiple horizontal and vertical levels within and among agencies.

The joint congressional Intelligence Committee and Judiciary Committee hearings, and others that may eventu-

ally occur, will undoubtedly try to identify and hold accountable those responsible for mistakes or omissions. But the main energy needs to be directed toward reforming systems and procedures so that the FBI, CIA, and other intelli-

gence agencies — including the proposed Department of Homeland Security — become more open to a spirit of closer collaboration that will enable the entire intelligence community to become adept at countering the largely unstructured, non-nation state

*Breaking down
mind-sets and
bureaucratic barriers
will not be easy.
Neither will it be
done quickly.*

threat that has been emerging for the past few decades.

Breaking down mind-sets and bureaucratic barriers will not be easy. Neither will it be done quickly. Mueller, in speaking of the FBI, has provided a broad outline of what the entire intelligence community must do: “From new priorities, to new resources, to a new structure applying a new approach, I do believe that we are on the way to changing the FBI. And while we believe that these changes are relatively dramatic and a dramatic departure from the past, in the end, our culture must change with them.”⁵ ■

Notes

- 1 Robert S. Mueller III, Press Briefing, May 29, 2002. At <www.fbi.gov/pressrel/speeches/speech052902.htm>.
- 2 Michael Bromwich, “The Hard Work of Transforming the F.B.I.” *New York Times*, June 2, 2002 (p.19).
- 3 For example, 23-year FBI veteran field agent Harry Brandon, in comparing the roles of FBI “crime fighters” and counter-intelligence operatives, observed: “You know, there’s not a lot of difference. They collect information. The targeting, what they do with the information may be different...this is not totally new to the FBI.” “Redesigning the Bureau,” *The NewsHour* with Jim Lehrer, May 29, 2002. At <www.pbs.org/newshour/bb/fedagencies/jan-june02/fbi_5-29.html>.
- 4 David Johnson and Elizabeth Becker, “C.I.A. Was Tracking Hijacker Months Earlier Than It Had Said,” *New York Times*, June 3, 2002 (p. 1), and Walter Pincus and Dan Eggen, “CIA Gave FBI Warning on Hijacker,” *Washington Post*, June 4, 2002 (p. 1).
- 5 Mueller, op. cit.

“In a Sept. 10 [2001] submission to the Bush administration’s budget office, [Attorney General John] Ashcroft refused to endorse an FBI request for \$58 million for 149 new counterterrorism field agents, 200 additional analysts, and 54 additional translators. He also proposed a \$65 million cut for a program that would have given state and local counterterrorism grants for equipment and training. After Sept. 11, Ashcroft proposed \$2 billion for FBI counterterrorism measures.”

— *New York Times*, June 2, 2002 (p. 24)

MISSILE DEFENSE

CONTINUED FROM PAGE 1

the Ground-Based Midcourse Defense system is ready for realistic operational testing. (“Why the Secrecy Shield,” the *Washington Post*, June 11, 2002.) Until then, the targets and countermeasures against which the system will be tested will not closely resemble actual ballistic missiles or decoys, and will therefore not provide information that might give potential enemies an operational advantage.

Why, then, the call for increased secrecy in the program at this time? Critics of the proposal feel that it is in order to remove the troubled and costly program from public scrutiny. “They’re attempting to avoid the usual oversight by Congress, the media ...and the larger sci-

entific community,” according to Sen. Jack Reed, D-R.I., chairman of the Senate Armed Services Strategic subcommittee, which has oversight over the program. “There’s an attitude of ‘we know best, don’t bother us’.”

In fact, this is only the latest in a series of Pentagon initiatives that will have the result, if not the actual intent, of making oversight of the Bush administration’s missile defense program extremely difficult.

In July 2001, when, after almost a six month delay the Bush administration finally released detailed information on its fiscal year 2002 budget request, the Pentagon announced that the Ballistic Missile Defense Office (BMDO) was being restructured. Funds were to be allocated in general categories, rather than to specific pro-

grams. The three major new categories focused on developing technologies related to the Boost Phase, Midcourse and Terminal segments of an incoming missile’s flight. Effectively, budgetary line items within BMDO were eliminated. Without such details, it is extremely difficult, if not entirely impossible, for independent assessments of how much money is being spent on programs.

The situation was made additionally fuzzy in early January 2002, when Defense Secretary Donald Rumsfeld announced that BMDO was being redesignated as the Missile Defense Agency (MDA), with a new organizational arrangement and streamlined operational processes that gave MDA officials greater authority and autonomy. One of the ways in which the Pen-

tagon planned to streamline the development process is to exempt from normal reporting requirements key parts of the MDA program, including the Ground-Based Midcourse segment.

“Spiral Development”

As part of his January 2002 announcement, Rumsfeld stated that MDA would utilize a “capability-based requirements process” for development of a national missile defense system. In effect, rather than working to develop a system intended to meet a predetermined performance threshold, and then fully testing it to ensure it could perform at that specified level, a rudimentary system would be deployed at the earliest time, regardless of its operational effectiveness. This base system would then be improved

as new technologies became available. The Pentagon refers to this process as “spiral development.”

Missile defense is not the only weapon program that the Pentagon intends to be the product of spiral development, although it is potentially the largest and most costly. The Defense Department believes that such an evolutionary approach will allow for the quicker deployment of cutting edge technologies and cost savings. They liken the concept to that of computer software development, where makers release new versions every few years, interspersed with more frequent “fixes.”

There are a couple of problems with such an approach, however. The first is that such a program will lack an operational requirement. Weapon systems are developed with the intent to fill a particular role — in the case of a national missile defense system, that role is intercepting a limited number of incoming ballistic missiles. Yet just because a system is operational doesn’t mean it can fulfill its required role.

The second hitch is that it is very difficult to measure a program that lacks clear requirements. Questions about schedule, technology development and cost become difficult, if not impossible, to answer without a yardstick against which to measure. Needless to say, oversight becomes virtually impossible.

Congressional Response

These changes in the Pentagon’s missile defense infrastructure have been coldly received on Capitol Hill, and a number of members has taken a variety of approaches in responding to what they view as an effort to either evade or erode Congress’s oversight of executive agency activities.

CONTINUED ON PAGE 5

“There’s an attitude of ‘we know best, don’t bother us’.”

— Sen. Jack Reed, D-R.I.

MISSILE DEFENSE

CONTINUED FROM PAGE 4

Sen. Carl Levin, D-Mich., chairman of the Senate Armed Services Committee, is one of the leading critics of the Pentagon's classification proposal, and has pledged to work to ensure that the public remains informed about MDA's testing program. While Levin remains confident that Congress will be adequately informed about the status of the MDA's work even with the proposed classification regime, he does not feel that simply informing Congress is sufficient.

According to Levin, "we are going to do everything we can to make sure [information] is public so that the public can judge and the critics can judge." Levin noted the role of private organizations — and specifically mentioned the Union of Concerned Scientists, who have done a number of briefings that were critical of MDA's fight testing methodology — in providing oversight and analysis of the program. Said Levin, "We want [outside organizations] to have the information that allows them to give us different points of view."

The Senate Armed Services Committee has also responded. In a report accompanying its version of the annual defense authorization legislation, the committee noted that the service chiefs — the uniformed heads of the individual branches of the military — had not been consulted by the MDA during the preparation of the fiscal year 2003 budget request for missile defense.

The committee's report also noted that the Pentagon's plan to restructure the MDA exempted the agency from standard acquisition practices and reporting requirements, and stated that such reports "are critical to congress-

sional understanding and oversight for missile defense programs, and are required for all other major defense acquisition programs." The committee has included in its version of the authorization bill language requiring MDA to submit specific reports on the Midcourse Defense program, and sets minimum reporting requirements. While it is likely that this language will be adopted by the full Senate, the House version of the legislation contains no similar provisions, so it is uncertain if the final bill will have the reporting requirements.

The Defense Department has made clear its opposition to such initiatives. In a letter to the Senate Armed Services Committee in early June, Rumsfeld stated that he would consider recommending that President George W. Bush veto the final version of the defense bill if it included the Senate language. Such provisions, he wrote, "would impose a number of burdensome statutory restrictions that would undermine our ability to manage the program effectively."

Other members of Congress are equally concerned about MDA's failure to even comply with the reporting requirements that already exist. Rep. John Tierney, D-Mass., has asked the General Accounting Office (GAO) — the auditing arm of the federal government — to investigate whether MDA officials have violated federal law by withholding information from Pentagon officials responsible for oversight of weapons testing pro-

grams. Tierney said that his action was a response, in part, to statements by Thomas Christie, the director of the Pentagon's Office of Test and Evaluation, that his office has not been receiving all of MDA's testing data.

In his March 2002, testimony before the Senate Armed Service's Committee, Christie stated that, "I can't say at this time that we have had unfettered access to what is going on [at MDA]." In a prepared statement announcing his call for a GAO investigation, Tierney said, "The Office of Test and Evaluation

[OT&E] was created to act as the eyes and ears of Congress and the public. We should be alarmed if OT&E is prevented from doing its job. Missile defense shouldn't be immune from the same level of scrutiny that other weapon systems face."

The Pentagon's desire to classify portions of the system's testing could well be simply what they've stated — the result of concerns about program security and the ability of potential enemies to gather valuable operational information. But intended or not, it will continue a trend already associated with the development of a national missile defense — reducing government and public oversight of a technologically daunting and staggeringly expensive program. Repeated experiences in the development of sophisticated Pentagon weapon systems indicate clearly that more transparency, rather than less, is the proper course. ■

"We are going to do everything we can to make sure [information] is public so that the public can judge and the critics can judge."

— Sen. Carl Levin, D-Mich.

CDI Study Examines Strategic Approaches to Homeland Security

The following is based on the Executive Summary of Homeland Security: A Competitive Strategies Approach, by F. G. Hoffman. Electronic copies of the report are available on CDI's website at www.cdi.org/products/homeland.pdf or in hard copy from CDI.

THREATS TO THE HOMELAND have a new salience since Sept. 11 and will continue to be a critical U.S. national interest for the coming decade. While U.S. military analysts have been debating the pace and scale of a potential transformation of the American armed forces, a transformation in strategic strike opportunities has quickly emerged. The motivation and the capability of potential adversaries to reach America's shores are coming together. The major options available for those wishing to strike at the U.S. homeland include: missile attack, covert delivery of weapons of mass destruction or other methods of causing mass casualties, or a crippling cyber attack.

Missile Attack

Strategic forces were the *sine qua non* of superpower status in the Cold War. While there is only one superpower today, several aspirants covet ballistic missiles of one form or another. This has resulted in concerns about proliferation of both missile technology and weapons of mass destruction. The overall number of missiles pointed at the United States has been sharply diminished since 1989, but the nature of the threat has undergone a qualitative transformation with potential destabilizing developments.

Several states, including China, Iran and Iraq, seem bent on acquiring advanced systems that could pose a threat to American interests. The pace and extent of China's strategic modernization efforts will be subject to Beijing's assessment of its desired new

strategic doctrine. In the face of American efforts to build a National Missile Defense (NMD) network against intercontinental ballistic missiles (ICBMs), it is doubtful that China will stand pat with a minimal deterrent capability; it will ensure that its force exceeds the interceptors fielded by the United States. While the scale of the proliferation problem and the corresponding direct threat is far less than the thousands of missiles aimed at the United States during the Cold War, these threats still raise a serious security issue. To quote one assessment, the United States faced a changing but not necessarily growing threat from missiles.

Covert Attack/Catastrophic Terrorism

The homeland security debate for the past decade has focused myopically on ICBMs. This is not the only threat the United States faces, as recent events have demonstrably made clear. Even if the United States could develop and deploy an effective missile shield (still in doubt), it would not provide a defense against less expensive and more likely forms of attack.

Numerous analysts have noted that there are a number of means by which weapons of mass destruction (WMD) could be covertly delivered and used

within the United States. Examples of such attacks might include detonating a crude nuclear device in a major city, spraying some chemical nerve agent over a sports stadium full of spectators, or infecting travelers with some biological pathogen or virus such as smallpox. Even before Sept. 11, national security policy experts and analysts believed that the possibility of such an attack inside our own borders was very real. Some

concluded that the use of WMD by terrorists in the United States is "no longer a matter of if, just when." Such projections were considered speculative until the events of Sept. 11, 2001, and the subsequent anthrax scare.

Thanks to the Internet and the devolution of the Soviet Union, there has been a further diffusion of technical knowledge, expertise and material for WMD. The combination of such trends has lowered the technical barriers for states and non-state actors to construct various forms of weapons able to generate mass casualties. A dedicated state or team could acquire the talent and necessary components for a bomb with very modest resources, perhaps less than \$1 million. The dissolution of the Soviet Union offers a potentially rich source of nuclear material for terrorists. Biological weapons remain the most potent form of attack, but present numerous

CONTINUED ON PAGE 7

The homeland security debate for the past decade has focused myopically on ICBMs.

HOMELAND SECURITY

CONTINUED FROM PAGE 6

technical difficulties that most analysts believed to be beyond the ability of even dedicated ultraterrorists — until this past year.

Cyber Attack

Another potentially severe vulnerability is a scenario analysts call an “Electronic Waterloo,” a surprise attack on America’s vast web of computer networks and other forms of critical infrastructure that undergird the U.S. economy and government services. Dependence on this information and communications infrastructure creates new vulnerabilities. A computer virus might attack the Pentagon’s ability to mobilize or communicate with U.S. military forces, or shut down all government services in a city.

Proliferation of WMD has long been considered a problem, but little thought has been given to the nature of information systems and the extensive diffusion of potentially malicious ‘weapons’ and information-based technologies. Many computer attack tools are posted on the Internet, free to anyone with a mouse and modem. This easy availability of cyber tools and ‘weapons’ and their low cost have produced millions of potential cyber warriors. Unlike traditional weapons of mass destruction, cyber warfare tools are tools of mass disruption, which can be used to abet state, criminal or terrorist objectives.

America has built an economy and a way of life around an architecture that is increasingly interconnected and increasingly vulnerable. The impact of this vulnerability is already evident in the accelerating number of intrusions into civilian and Pentagon computers. This computer infrastructure has been and

will continue to be vulnerable for some time. The reliance of Western economies and governments on modern and interdependent information systems, in both the military and in civilian business sectors, is a potential major asymmetry that can be easily exploited.

Conclusions

Missile Attack

Deterrence remains the most viable strategic option against major states, while nonproliferation programs continue to offer the most effective means of raising costs for new aspirants and for negating non-state players. If the United States does not want to be checkmated at home in the pursuit of its vital interests overseas, it will have to take into account this fact and refashion its strategy. Deterrence will be more difficult than in the past, but remains a viable competitive strategy to prevent missile attacks by state actors. Nonproliferation will not be an enduring strategy against any state determined to acquire advanced systems, but it keeps costs and barriers to entry to this club high enough to retard the development of highly advanced capabilities.

Counterproliferation strategies based on active and passive defense offer a high-cost, less effective strategy that might be offset by greater offensive arsenals, countermeasures and asymmetric delivery means. If U.S. efforts to build a robust and effective NMD system are successful, the end result will likely devalue the investments that certain countries are making in ballistic missile technology. However, any NMD system may then incentivize states to invest in other delivery mechanisms that may prove cheaper and more effective, such as cruise missiles or covert action. This would push the strategic competition away from missile systems to forms

of attack for which an enduring competitive advantage for the United States will be difficult to achieve. Hence, a counterproliferation strategy based primarily on missile defense should be carefully examined to ensure that it does not make the United States more vulnerable to strategic strike than before.

Covert Attack

The relative ease of covert catastrophic attacks requires a comprehensive approach employing both nonproliferation and counterproliferation techniques. Weak states may find this to be their most effective deterrent against overwhelming U.S. military superiority. Non-state actors, motivated by rage or resentment, may find that taking on the global superpower can only be achieved through indirect means. In addition to nonproliferation and threat reduction efforts to control access to dangerous materials, defending against this threat necessitates development of a fully integrated national strategy to mitigate the consequences if an attack occurs. Well-organized response plans will ensure that the consequences of such attacks are rapidly handled, negating the panic and disruption that adversaries are seeking.

Cyber Attack

Deterrence is a suspect approach in a world where attribution and response are exceedingly difficult. A counterproliferation strategy based on defensive mechanisms appears to offer an enduring competitive advantage, although it will be imperfect. Nonproliferation is not feasible due to the ubiquitous nature of information technology. This should not exclude possible export controls over certain forms of cyber technology or tools. However, it is difficult to extend nonproliferation regimes to non-state actors. ■



Center for Defense Information
1779 Massachusetts Avenue, NW
Washington, DC 20036
(202)332-0600 • Fax: (202)462-4559
www.cdi.org

NONPROFIT ORG.
US POSTAGE
PAID
Washington D.C.
Permit No. 4627

ADDRESS SERVICE REQUESTED



THE STAFF

President and CEO:

Dr. Bruce Blair

Vice President:

Theresa Hitchens

Chief of Research:

Colonel Daniel Smith
U.S.A. (Ret.)

Senior Advisors:

Phillip E. Coyle
Rear Adm. Stephen H. Baker
U.S.N. (Ret.)
Dr. G. Wayne Glass

Senior Fellows:

David T. Johnson
John Newhouse

Distinguished Military Fellows:

General Charles Wilhelm
U.S.M.C. (Ret.)
General Anthony Zinni
U.S.M.C. (Ret.)

Executive Secretary:

Eleanor Harrison-Little

Research Staff:

Marcus Corbin
Christopher Hellman
Jeffrey Mason
Rachel Stohl
Tomas Valasek

Washington ProFile:

Nikolai Zlobin, Senior Fellow
& Editor-in-Chief
Aleksandr Grigoryev, Editor
Margarita Gorelik, Database
Mngr.

CDI Moscow, Russia:

Dr. Ivan Safranчук

Research Analyst:

Michael Donovan

Research Assistants:

Victoria Garcia
Jillian Hayes
Hugo Saenz
Victoria Sampson

Research Associate:

Victoria Sampson

Office Manager/Accountant:

Judy Edwards

Web Design:

Samy Moutanabbih
Steve Welsh

Graphic Design:

Rachel Freedman

TV Production Staff

America's Defense Monitor:

Glenn Baker
Colin McCullough
Stephen Sapienza
Mark Sugg

Development:

Lynn Schuster

For a single copy of this issue, send \$1.00. CDI's publication, *The Defense Monitor*, is sent without charge to all donors of \$45 or more. CDI receives no funds from the Pentagon or from military contractors. The Center is financed by voluntary tax-deductible contributions from individuals and grants from foundations. Contributions may be mailed to the Center for Defense Information, 1779 Massachusetts Ave. NW, Washington DC 20036.

BOARD OF ADVISORS

Doris Z. Bato—Santa Fe, NM

Arthur D. Berliss, Jr.—Captain, USNR (Ret.); former Vice-President, Allen-Hollander Co., New York, NY

Edward H.R. Blitzer—Former Chairman, Lightolier Inc., New York, NY

Dick Brukenfeld—Dobbs Ferry, NY

Ben Cohen—Chairman, Ben & Jerry's Homemade, Inc., South Burlington, VT

James R. Compton—President, J.R. Compton Developments; Chair, Fund for Peace Board, Los Gatos, CA

Joseph N. Deblinger—President, Deblinger Sales & Marketing Corp., Manhasset, NY

Gay Dillingham—CNS Communications, Santa Fe, NM

James A. Donovan—Colonel, USMC (Ret.), Author, former publisher *Journal of the Armed Forces*, Atlanta, GA

Robert L. Frome—Senior Partner, Olshan, Grundman and Frome, Attorneys, New York, NY

Seth M. Glickenhau—Investment Banker, New York, NY

Yoel Haller, M.D.—Santa Barbara, CA

Mrs. Eva Haller—Santa Barbara, CA

James D. Head, Ph.D.—President, Strategy Development Company, Freeland, MI
Chairman on the Board

David H. Horowitz—New York, NY

Robert G. James—Rear Admiral, USNR (Ret.), President, Enterprise Development Associates, New York, NY

Alan F. Kay, Ph.D.—Businessman, St. Augustine, FL

Gene R. La Rocque—Rear Admiral, U.S.N. (Ret.), President Emeritus, CDI

Eugene M. Lang—Founder/ Chairman Emeritus, REFAC Technology Development Corp. and "I Have A Dream" Foundation, New York, NY

Mrs. Ellie Meyers—Deerfield, IL

Robert M. Meyers, M.D.—Deerfield, IL

David E. Moore—Rye, NY

Paul Newman—Motion Pictures, Los Angeles, CA

Mr. and Mrs. Joseph Pulitzer IV—St. Louis, MO

Rudolph S. Rasin—President, The Rasin Corporation, Chicago, IL

John M. Rockwood—Publisher, Chicago, IL

Martha S. Schauss—River Forest, IL

Julie Schecter, Ph.D.—Director, Peaked Hill Trust, Wayland, MA

Richard Schuckman—Business Executive, Fair Lawn, NJ

John J. Shanahan—Vice Admiral, USN (Ret.), Ormond Beach, FL

Adele E. Starr—Mamaroneck, NY

Phillip A. Straus—Partner, Neuberger and Berman, Members, New York Stock Exchange, New York, NY

Philip A. Straus, Jr.—Photographer, Philadelphia, PA

Andrew Ungerleider—Earthstone International Ltd., Santa Fe, NM

Albert B. Wells—President, The Abelard Foundation, Inc.; Kingsley, Schreck, Wells & Reichling, Private Investments, San Francisco, CA

Harold Willens—Former Chairman, Factory Equipment Corporation, Los Angeles, CA

Barbara Slaner Winslow, Ph.D.—School of Education and Women's Studies Program, Brooklyn College/City University of New York

Joanne Woodward—Actress-Director, Westport, CT