Intelligence Aim Veers To Amassing Overt Information

By Robert K. Ackerman

Commercial data systems to monitor new threats from terrorists, privateers, organized criminals.

The U.S. intelligence community is about to employ new technologies for collecting vast amounts of information on potential threats from unconventional adversaries. This technology thrust, rather than relying on advanced research and development, will feature extensive use of commercial off-the-shelf information systems to gather and process these readily available data.

Collection resources are being retargeted to accumulate a variety of easily obtainable information published in open sources. This mass of diverse data will be melded to draw an accurate picture of emerging trends or threats.

The Soviet Union's collapse has altered the community's focus away from monitoring a known adversary and toward uncovering new threats as they emerge. Vulnerable targets for foreign espionage include U.S. companies that could be menaced by high-technology pirates or even terrorist groups seeking tools to aid mass destruction.

All these efforts will be pursued in spite of an expected $7 billion reduction in funding for the intelligence community over the next four years, according to Richard S. Haver, executive director for intelligence community affairs.

Richard S. Haver, executive director for intelligence community affairs, warns of a variety of espionage threats from new sources.

Haver states in a *SIGNAL* interview that the community probably will maintain its current balance of human and technology resources. However, he notes that "the technology push is our future," as the world becomes more sophisticated and complex. Capitol Hill has provided strong support for research and development as well as acquiring future technologies.

The bulk of technology programs likely will be geared toward processing and disseminating intelligence rather than gathering it. Haver notes that information gathering, which he credits with recent spectacular successes, has leveled off in the past few years.

The main drive will be toward fulfilling specialized intelligence needs, especially in areas such as counternarcotics efforts, nuclear non-proliferation, environmental issues and counterterrorism. Haver offers that the key lies in taking advantage of commercially available technologies that enhance processing and dissemination. This area will provide the most dramatic changes in the way the intelligence community functions over the next five to 10 years, he predicts.

These changes will be fundamental, Haver adds, because information sources and processing goals are changing. To handle large volumes of data efficiently, the community hitherto has concentrated its processing in one place under centralized management. The resulting intelligence product is distributed in a finished form to a variety of consumers, he describes.

Technology such as information highways, internetting and the ability to move bulk data will enable the community to tailor its disseminated intelligence to suit each individual customer's needs, Haver avers. This will involve placing more analytic and production power closer to the consumer where the information would be more responsive to the user's needs. New information handling technology will enable siting large volumes of raw material at analysts' fingertips, he says.

Haver relates that the intelligence community has had a "push" approach to information dissemination. This has involved presenting the community's 287 consumers with a final, published product based on anticipated needs.

While some prefer to receive processed intelligence in that manner, the new approach will permit other users to employ their own expertise to cull their own information—operating in a "pull" mode, Haver explains. A smart computer terminal would allow a customer to reach into data bases representing all levels of information ranging from raw intelligence to a finished product stored on optical disk.

Haver notes that the private sector, especially industry and academia, is leading the way in this technology. He believes that this approach will revolu-

tionize the intelligence community's way of doing business without exorbitant expenses.

"This will redefine the professional skills and work routines for as much as 60 percent of the intelligence community," Haver predicts. The goal is a 50 to 100 percent change in effectiveness. It is the only way to balance the community's "resource pinch" with the expanding demand for information on a variety of topics, he adds.

With the demise of the Soviet threat, government and industry officials have called for the U.S. intelligence community to turn its resources toward commercial intelligence of foreign companies for the benefit of U.S. concerns. Haver notes that openly available information can provide substantial insight into economic performance, science and technology, corporate and national investment strategies and technology trends. Much of this information can tell U.S. analysts a great deal about domestic policies and industrial planning, he adds.

The intelligence community will concentrate on providing this openly available information to government leadership for dissemination at the direction of federal policy makers. Haver offers that the community "will steer as clear as we can of anything that smacks of industrial espionage or of undertaking potentially illegal or nefarious operations against foreign businesses or organizations. That is a very slippery slope that causes consternation and difficulties every time it is even mentioned." There is no enthusiasm within the intelligence community for stealing foreign company secrets, he adds.

Adm. William O. Studeman, USN, deputy director of the Central Intelligence Agency (CIA), concurs with this assessment. He notes that a substantial body of law exists that recognizes the concept of intellectual property. Trade secret acts, copyrights and patent laws all have been internationalized to a substantial extent.

Haver notes that an existing threat threshold might trigger intelligence-seeking efforts against some foreign companies. This threshold includes areas such as proliferation of mass destruction weapons, for instance. An intelligence effort of this nature would come about only after consultations with the attorney general and possibly Congress, he adds. The severity of the threat would determine the aggressiveness of the community's efforts to acquire and distribute information.

Haver believes that the brainpower of the intelligence community—principally that of the CIA—will be asked to provide more analysis and understanding of the international marketplace and the U.S. role in it. Again, he notes that the vast amount of material in this arena comes from open sources presented by governments and companies, and the U.S. intelligence community has increased its reporting on this topic considerably over the past two years.

The intelligence community will pay significant attention to foreign attempts at obtaining U.S. industrial secrets, Haver states, but U.S. firms also must be vigilant against penetration from a variety of unconventional foes. In addition to foreign intelligence services, potential adversaries include overseas business rivals, organized crime profiteers and terrorist groups seeking to acquire catastrophic technology.

"The United States still is considered around the world as the leader in virtually all critical technology categories," Haver declares. "As a result, businesses that are at the center of that leadership can almost be assured that they are targets for a large number of organizations seeking inside information."

Efforts to penetrate firms located in the United States will be blunted by domestic legal and law enforcement processes, Haver notes. However, overseas assets are much more vulnerable, and the community faces a more difficult task in dealing with this threat. "I would not want U.S. businesses to believe that no news is good news," he cautions. "Significant gaps exist both in knowledge and in our ability to handle this challenge," he warns.

Far thornier, he says, is the problem of forays made by smaller, non-governmental cells such as criminals or terrorists. "This is an even more difficult problem, and the processes and procedures for dealing with this are not well understood—either in the government or in the private sector," he cautions. Haver offers that the intelligence community and industry probably do not have an adequate understanding of the threat, much less know how to gather information and advise protective measures.

One problem is that, regardless of countermeasures, this form of espionage is extremely lucrative to a variety of organizations, he notes. The results of a successful espionage foray against a commercial U.S. target would be of such great use to an adversary that the United States must "turn up the heat very high" in policy or

action to maintain some form of deterrence, Haver offers.

U.S. companies first must be aware of the problem and be on guard in a range of circumstances, he says. In some foreign environments, U.S. firms must show a higher level of vigilance for materials in their possession as well as for how their materials are handled by overseas concerns. U.S. companies operating overseas need to be aware, leery and on guard, he reiterated.

The intelligence community in turn must determine which locales offer a higher level of incidents or difficulty, he states. Some problems are very subtle, especially in areas where the lines that define illegal acquisition of commercial information are not sharp. "What might be illegal in the United States is not necessarily illegal in another nation—even an advanced Western country," Haver relates.

Regional instability likely will remain the dominant issue for diplomatic and military concerns, Haver suggests. Keeping abreast of these problems will require an understanding of political, economic and social factors at work in each crisis. Incidents in Somalia, Iraq and Bosnia are indicators of future challenges, he says, adding that the intelligence community does not have the resources to concentrate on each potential problem the way it did with the Soviet Union.

Another area that will strain the intelligence community's resources is military needs. Haver states that the services will require a greater level of intelligence support for precision guided munitions and force mobility. Large volumes of precise information provided on a timely basis will be necessary for the military's new missions and advanced systems.

However, a key change in the way the intelligence community presents information will center around the availability of data. Future intelligence seekers will obtain vast amounts of vital information from open sources rather than through extensive covert operations. This is diametrically opposite from the old focus on the Soviet Union and its secretive society. Haver relates that most necessary information "is there for the asking," and the community must develop a network to process this open information for screening and dissemination.

The community can use its traditional intelligence systems to pinpoint areas that present access difficulties or that require higher levels of detail and precision. The community, however, will begin by researching easily available information, which is a 180-degree reversal from past methods. "I believe that we already have shifted very significantly the basic intelligence process paradigm," Haver notes.

Haver believes that the former Soviet Union would not rise again even if Russian President Boris Yeltsin were to depart his leadership role. The grassroots movement that Yeltsin represents would endure even with the departure of the head stem, Haver offers. The political situation there is highly volatile, but the reform process is being too institutionalized to be reversed easily.

Yeltsin has shown remarkable political acumen over the past few years, Haver opines, and barring an unforeseen health problem, he should endure. Nonetheless, Haver believes that the reform movement is bigger than its leader, and the Russian people are not likely to tolerate any return to totalitarianism.

The United States must be prepared for ups and downs as Russia evolves, however. It would be absurd, Haver declares, to expect a smooth, peaceful transition process through this so fundamental a political upheaval.

Haver believes that no major intelligence reorganization looms. Change instead is occurring in attitudes among various members of the intelligence community. The basic trend is away from "first person singular" individuality and toward a corporate approach among the disparate members of the community.

Intelligence agencies now are thinking in terms of shared responsibility, he states. This includes discussing shared problems rather than focusing on individual territories. Haver offers, for example, that the relationship between the Defense Department and the director of central intelligence never has been closer or more cooperative.

Many U.S. security policies and procedures were built for a different era, and several different commissions and task forces are pursuing change along these lines. Haver cites the groups founded by former CIA Director Robert Gates as the basis for this review, and he notes that Gates' successor is emphasizing this effort.

"I never saw a transition in the national security realm from one party to the other that was as rapid and cooperative as the one between Gates and [current CIA Director R. James] Woolsey," Haver states. Woolsey took over on the heels of his own major 1992 study on the community's technical collection architecture and was familiar with vital resource issues.

These task forces will be producing results through spring 1994, Haver says, with substantial changes beginning to accumulate by fall 1993. The result will be a new policy foundation that addresses current issues of change, he states.

U.S. intelligence is earmarked for a $7 billion funding reduction over the next four years. The community "took some rather heavy blows in 1993," Haver notes, and so much of that reduction already has been accomplished. The goal is to stabilize and begin initiatives necessary for modernizing the intelligence system in the changing world, Haver states.

Some congressional staffers and office holders have stated that they expected even lower budget figures, Haver says. The intelligence community has strong support on both sides of the aisle in both houses, he adds, but its budget will be in for a tough fight over the next several months. The goal is to substantiate the Fiscal Year 1994 request through the authorization and appropriation process.

Haver is equally concerned about how this year's debate will bode for future budgetary support. The intelligence community prefers long-term planning, especially in procuring long lead items or complex technical systems, he notes, and it needs a sense of commitment from Capitol Hill on programmatic directions. These programs cannot be built, contracted or even sustained on a year-to-year basis, he adds.

Congress has been steadfast in its commitment to maintaining intelligence community personnel, Haver offers. The steady reduction mandated for the next four years relies mostly on attrition and early retirement inducements to reach target figures agreed upon in a joint effort between Congress and the intelligence community.

The legislative body also has provided statutory flexibility for both the director of central intelligence and the secretary of defense in these force reductions. However, Haver claims, the intelligence community is "on the edge" where dramatic new reductions would strain the community's ability to carry out its mission.

Haver offers that it is easier to deal with members of congressional intelligence oversight committees, because they are more familiar with the community's needs. These elected officials' appreciation and sympathy for the community's mission, he notes, are not always shared by other senators and representatives who see sizable sums to be cut.

• • • — • —

SECOND INTERNATIONAL SYMPOSIUM: NATIONAL SECURITY & NATIONAL COMPETITIVENESS: OPEN SOURCE SOLUTIONS Proceedings, 1993 Volume I - Link Page

Previous	A New, Twenty-First Century Role for the Intelligence Community
Next	A Genetic View of National Intelligence

Return to Electronic Index Page