Strategic Insight

Homeland Security: Intelligence Indications and Warning

By guest analyst Lt. Col Kenneth A. Luikart, USAF. Lieutenant Colonel Luikart is the air intelligence officer for the 165th Airlift Wing, Georgia Air National Guard. Colonel Luikart served 18 months in Vietnam; supported Operation TEAM SPIRIT in Korea; Operation BADGE TORCH in Thailand; Operations CORONET OAK and VOLANT OAK in Panama, providing intelligence support to anti-drug trafficking missions in Central and South America. He supported Operations PROVIDE PROMISE, JOINT ENDEAVOR, and JOINT FORGE, flying important airlift missions into Bosnia and Herzegovina. Colonel Luikart supported Operation SUPPORT HOPE, flying humanitarian missions into Rwanda and Zaire; and the 1996 Summer Olympic Games, where he supported the State Olympic Law Enforcement Command as the Senior Air Intelligence Liaison Officer for Task Force 165.

Strategic Insights are authored monthly by analysts with the Center for Contemporary Conflict (CCC). The CCC is the research arm of the National Security Affairs Department at the Naval Postgraduate School in Monterey, California. The views expressed here are those of the author and do not necessarily represent the views of the Naval Postgraduate School, the Department of Defense, or the U.S. Government.

December 2, 2002

September 11, 2001 demonstrated that policy makers and intelligence organizations had conducted business in traditional ways, not in response to today's threats to our nation. The attacks in September suggest that inadequate information sharing between law enforcement and national intelligence agencies led to lost opportunities to thwart the attacks launched by Al-Qaeda. Little has yet been done to fix many of these problems. The nation has failed to formulate significant changes in the way it tasks, collects, analyzes, produces and disseminates intelligence information. The architecture needed to provide intelligence for homeland defense has not yet emerged. The September 11 attacks are a "watershed event" that should change our current intelligence organization, perhaps resulting in legislation as important as the National Security Act of 1947.[1]

Intelligence is the Analytical Spin on Information

Most experts in the intelligence field agree that intelligence is the analytical spin put on information and the ability to communicate this information to policymakers who can put it to good use. David Khan, in his book *The Code Breakers*, notes, "Intelligence faces two all-encompassing, never-ending problems. Both are ultimately unsolvable. The first problem is how to foretell what is going to happen." The second problem, "as old as mankind," is "how to get statesmen and generals to accept information that they do not like."[2] In 1992, before the Senate Intelligence Committee, General Paul Gorman, U.S. Army (Ret) explained, "intelligence remains information, no matter how adroitly collected, and no matter how well analyzed, until it is lodged between the ears of a decision maker."[3] Gorman went on to say that intelligence dissemination is often at fault when our nation, or our commanders in the field, suffers a strategic surprise. Intelligence for homeland security thus poses a special challenge because it requires the collection of data from non-traditional sources (e.g., state and local law enforcement agencies) to create all source analysis to head off homeland security threats.

Redefining the Threat to the United States

Prior to the demise of the Soviet Union, most intelligence agencies focused on Moscow. Since then, policy makers and intelligence analysts have struggled with redefining the threat faced by the United

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
02 DEC 2002		**00-00-2002 to 00-00-2002**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Homeland Security: Intelligence Indications and Warning	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School,Center for Contemporary Conflict,1 University Circle,Monterey,CA,93943**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**4**	

States. Today intelligence and law enforcement agencies confront a world that has many "targets" and a vast amount of information and misinformation, some of it transmitted by new means of communication (e.g., the Internet). Today's severe threat list is long and growing.

Major Threats to the United States

1. *Foreign Armed Forces Threat*
2. *Economic Espionage*
3. *Weapons of Mass Destruction*
    - *Nuclear and Radiological*
    - *Chemical and Biological Weapons*
4. *Gray Area Phenomena Threat*
    - *Terrorist Organizations*
    - *Rogue States*
    - *Illicit Drug Trade and Narco-Terrorists*

These new threats will force intelligence organizations to rethink their traditional analytical agenda.

Threat Reports Produced in the Early 1990's

35% = Defense intelligence including international arms trade and nuclear proliferation

15% = Defense intelligence surveillance of foreign conflicts and insurgency

20% = Intelligence on terrorism

10% = Intelligence on foreign states' internal politics, general foreign policies, internal economies and international economic policies

10% = Tactical support to diplomacy and other international negotiations of all kinds, including economic

10% = Counter-intelligence, counter-espionage and residual security intelligence subjects; other miscellaneous subjects like narcotics and international crime

Source: Michael Herman, *Intelligence Power In Peace and War*, Cambridge: University Press, 1996, p. 46.

Several factors, however, complicate the process of redefining the threat and reorganizing to meet it. For instance, there are differences in perception that divide policy makers and intelligence analysts. According to Glenn P. Hastedt, policy makers expect that information always will be accurate and that threat information will be "self-interpreting." By contrast, intelligence analysts use estimative processes to create intelligence analyses. Thus they artificially create the future by selecting starting assumptions and then creating interpretative and predictive scenarios.[4] Walter Laqueur explains that intelligence "does not exist in a vacuum, even if its practitioners sometimes tend to forget this." If the users of the intelligence product, the President and senior policy makers, do not trust the validity of the assessment, then "even excellent intelligence is of little consequence."[5] Policy makers and intelligence analysts will

have to search for common ground in understanding the strengths and weaknesses of the analytical process so that warnings of the most fantastic types of terrorist activity can be used to shape policy in constructive ways.

One of the most important changes needed in the current intelligence system is to create an opportunity for intelligence analysts from different organizations to confront each other and compare notes. This would be an outstanding way to compare competing hypotheses in an environment that would force analysts to defend and sharpen their judgments and analyses.[6] In the future, law enforcement agencies and officials need to be included in this information sharing process. Much critical information is often uncovered in routine traffic stops, for instance, that uncover suspicious individuals and contraband. This kind of information now has to be brought to the attention of analysts looking at international threats to U.S. security.

Indications and Warning (I&W) for Homeland Security

To facilitate this competition of analyses and sharing of ideas and information, a new intelligence Indications and Warning (I&W) cell should be created in the Executive Branch. The head of I&W should also have direct access to senior intelligence officials and the President. It should embody at least four attributes to be effective.

First, the I&W cell should have a streamlined organizational structure. Analytical cells do not need a lot of management overhead; rather, the management process should be lean and flexible. Too much bureaucratic meddling stymies free thinking and leads analysts to look for the "book" answer, or the "politically correct" answer, rather than the right answer. Whether the new I&W agency is designed within the Central Intelligence Agency or the National Military Intelligence Center, as Admiral Bobby Inman has suggested, one thing is apparent, "all warnings would be directly reported to the Director Central Intelligence (DCI) as opposed to the Chairman of the Joint Chiefs of Staff or the Secretary of Defense."[7] The cell should come under the direct control of the Director of Central Intelligence (DCI).

Second, the cell should be located, in a virtual or physical sense, near the policymakers who are supposed to respond to terrorist threats. In other words, members of the cell must be close enough to the President, the National Security Council and the policy makers to provide all source intelligence analysis, long range threats and short range warnings to decision makers in a timely manner. There are several reasons for suggesting that members of the I&W cell remain in close contact with senior leaders. Analysts get their marching orders from the leadership's Essential Elements of Information (EEIs). EEIs are what the leader needs to know about, but does not know. The odds that finished intelligence will be irrelevant are increased if the analyst is far removed from the decision maker. The better the analyst is kept aware of policymakers' concerns, the better the analyst can support the needs of officials.

Third, I&W should focus on moving information quickly to the officials who can put it to good use. The dissemination process is usually where hot intelligence is lost. Experts agree that in almost every intelligence failure, the information was there, but the distribution process failed to communicate convincing evidence to action officers who could put it to good use. To fix this problem, a "clearing house" for intelligence threat analysis, a forum for analysts from all agencies should be developed. Analysts could present their hypotheses before analysts from other agencies. Analysts from all agencies could be encouraged to staff and use this clearinghouse to test their models and theories of analysis. Results of this process then could be disseminated quickly to policymakers.

Fourth, the new I&W organization should have ties to the new Homeland Security Department. It could serve as a way to disseminate analytical techniques and products to non-traditional intelligence consumers. Law enforcement agencies, for example, might benefit from Order of Battle analysis of terrorist organizations. The new Homeland Security Department is struggling to integrate some forty departments and the new I&W cell could help integrate the intelligence effort across these different agencies. The Homeland Security Department will establish an intelligence distribution capability, but it is not clear how information will be disseminated to the Governors, state law enforcement agencies, or

National Guard Headquarters. New information distribution technology would probably facilitate the transmission of intelligence information, but valid I&W will be lost if procedures are not established to transmit information quickly to officials who can put it to good use.[8] Real problems arise when one considers the situational awareness at the federal level as opposed to situational awareness at the level of state government. There is a disconnect between federal programs and the fifty states. Many states have an Emergency Operations Center (EOC) and their own unique statewide intelligence collection and analysis capability. But it is still not clear how these state systems will merge with the Federal effort. This might be a job for a new Executive level I&W cell.

Conclusion

Intelligence failures are easily identified in retrospect. Most intelligence failures are caused by a breakdown in the dissemination of information. Thus I&W for homeland security must be able to reach not only the highest levels of government, but also local law enforcement agencies.

While policy makers and intelligence analysts will not always be on the same sheet of music, a good analyst can make the policy maker's job easier by providing him or her with the best guess at what hostile forces threaten our national objectives. It is important for the policy maker to understand that the analyst is guessing. It is even more important for officials to understand that poor analysis results from bureaucratic meddling, numerous distractions, and personnel shortages. Budget constraints cannot be used as an excuse for not staffing vacant intelligence analyst positions. The information explosion requires that all intelligence analytical agencies be fully staffed to handle the sheer volume of data to be analyzed.

There needs to be a forum at the top of the foreign and domestic intelligence structure where analysts can compare notes and intelligence theories can be tested and defended. The creation of this I&W cell will not be easy and the road to intelligence reform will be long and tedious. But, this is the path our nation must be prepared to follow if we are to protect ourselves from future threats to national security.

For more topical analysis from the CCC, see our Strategic Insights section.

For related links, see our Homeland Security & Terrorism Resources.

References

1. *Hearings Before The Select Committee on Intelligence of the United States Senate*, S.2198 and S.421, One Hundred Second Congress, (Washington: 1992), 1-46; and James Martin, "Intelligence in the Interstices." *Military Information Technology*, (Volume 6, Issue 1), 17.
2. David Khan, "An Historical Theory of Intelligence." *Intelligence and National Security*, (Volume 16, Autumn 2001, Number 3), 87-88.
3. Paul Gorman, USA (Ret), *Hearings Before Select Committee On Intelligence Of The United States Senate*, S. 2198 and S. 421, (Washington: 1992), 262.
4. Glenn P. Hastedt, *Controlling Intelligence*, (London: Frank Cass, 1991), 10-11.
5. Walter Laqueur, *A World Of Secrets: The Uses And Limits of Intelligence*, (New York: Basic Books, 1985), 71.
6. Robert H. Johnson. "Discussion by the Intelligence Advisory Board and invited Experts," April 22, 1996.
7. Bobby Inman, "Hearings on of the Commission on the Roles and Capabilities of the United States Intelligence Community."
8. Colonel Jeff Mathis, "Homeland Defense" Speech Given to the Georgia Department of Defense Joint Commanders Conference, Macon Georgia, 12 April 2002.