From AFIO's THE INTELLIGENCER
JOURNAL OF U.S. INTELLIGENCE STUDIES
VOLUME 19 • NUMBER 1 • $15 SINGLE COPY PRICE Winter/Spring 2012

ASSOCIATION OF FORMER INTELLIGENCE OFFICERS
6723 WHITTIER AVENUE, SUITE 200
MCLEAN, VIRGINIA 22101
Web: **www.afio.com**, E-mail: **afio@afio.com**

Guide to Intelligence Support for Military Operations

by Karl Haigler

The importance of timely and accurate intelligence to support frontline troops can hardly be exaggerated. For the wars in Afghanistan, Iraq, and the ongoing worldwide campaign against terrorists, military commanders and civilian policy makers rely on intelligence professionals to piece together information from a variety of sources on an adversary's capabilities and intent.

One should understand the different contexts of defense intelligence: strategic, operational, and tactical. Intelligence support of military policy making and strategy development is "strategic intelligence;" support to planning operations at the national or regional level is referred to as "operational intelligence;" and intelligence that is required to execute local operations or react to an adversary's actions is "tactical intelligence."[1]

Strategic intelligence is defined as "the product of gathering information about foreign military capabilities, intentions, plans, dispositions, and equipment; analyzing the contents of that information; and disseminating the findings to decision makers, combat troops, and other recipients."[2] The Department of Defense's *2010 Quadrennial Defense Review* (QDR) identifies a variety of threats and issues of global security of strategic intelligence concern. Specific focus is given, for instance, to Weapons of Mass Destruction (WMD): "The instability or collapse of a WMD-armed state is among our most troubling concerns. Such an occurrence could lead to rapid proliferation of WMD material, weapons, and technology, and could quickly become a global crisis posing a direct physical threat to the United States and all other nations." A National Intelligence Estimate (NIE) is the Intelligence Community's product related to such a high-priority strategic issue. Underscoring the defense intelligence interest in such a threat, the Undersecretary of Defense for Intelligence (USD(I)) wrote in 2008: "The Defense Intelligence Enterprise must combat this threat through focused intelligence that identifies potential threat sources, methodologies, and threat-based protective measures. It must also develop accurate and timely risk assessments for military and civilian planning, decision making, and potential operational use."[3]

According to the Department of Defense (DoD), operational intelligence is required "for planning and conducting campaigns and major operations to accomplish strategic objectives within theaters or areas of operations." Over the past decade counterinsurgency (COIN) operations have presented challenges to traditional approaches to operational intelligence. In Iraq and Afghanistan adaptations to traditional operational intelligence doctrine, such as developing close relationships with indigenous populations, have been critical to success. Urban combat in Iraq required new ways of organizing the collection and exploitation of intelligence. One example comes from the 2d Brigade Combat Team of the 1st Armored Division. The brigade commander's account of how his unit developed indigenous human sources (HUMINT), exploited captured insurgent technology, and aligned the information gained from these sources with the brigade's special intelligence requirements (SIR) provides valuable lessons learned in COIN operations.[4]

"Tactical intelligence is ... required for planning and conducting ... military operations at the local level. It concerns information about the enemy that is designed to help locate the enemy and decide which tactics, units, and weapons will most likely contribute to victory in an assigned area, and when properly applied, it can be a significant force multiplier."[5] The tactical analyst in ground warfare evaluates information gathered from a variety of sources to support his Commander's Critical Information Requirements (CCIR). Fundamental to this task is the analyst's ability to help the commander visualize the threats that

1. John Keegan's *Intelligence in War* (2003) provides many historical cases that illustrate the differences between tactical and strategic intelligence, such as in Operation Desert Storm (p. 314).
2. *www.dia.mil/history*
3. Office of the Under Secretary of Defense for Intelligence, "The Defense Intelligence Enterprise," p. 16.
4. Baker, Ralph O., "HUMINT-Centric Operations: Developing Actionable Intelligence in the Urban Counterinsurgency Environment," *Military Review*, 87 (March-April 2007), pp. 12-21. (*http://findarticles.com/p/articles/mi_m0PBZ/is_2_87/ai_n27175922/*)
5. *www.dia.mil/history*

his forces could face in his Area of Operations (AO) as part of the Intelligence Preparation of the Battlefield (IPB).[6] One of the most prominent tactical threats faced today is the Improvised Explosive Device (IED). The evolution of this tactic of asymmetric warfare over the past two years in Afghanistan now includes the use of crude bombs that have no metal parts. The analyst needs to identify the sources and nature of these devices, including the many forms they may take—from roadside bombs to vehicle-borne and body-borne explosives. Tactical intelligence supports attacks on the human networks that make and deploy IEDs as well as defeating the devices themselves. For example, airborne electronic warfare (EW) assets have been used to remotely detonate IEDs before they pose a threat to friendly forces. Imagery from unmanned aerial systems is used to detect the planting of IEDs. Video is used to track individuals to their hiding places and bomb factories.

The military intelligence analyst receives information from a variety of technical means, each of which makes a unique contribution, as well as human sources. Signals intelligence (SIGINT), exploiting an adversary's use of the electromagnetic spectrum, has been used to provide early warning of pending enemy attacks or the disposition his forces. One historical example, when SIGINT was a crucial source, is the Battle of the North Atlantic when the U-boat threat during World War II threatened England's survival. In modern times SIGINT on enemy air defense radars provides targeting intelligence for an air campaign to establish air superiority. Used in combination with other forms of intelligence, SIGINT can reveal telltale signatures of specific military units or equipment operating in an area of interest for the purposes of identification, tracking, and targeting.

Imagery intelligence (IMINT) is used in many ways to assist both military forces and civilian decision makers. Imagery forms the basis for Geospatial Intelligence (GeoINT), which is the "exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth."[7] IMINT is collected via satellites, unmanned aerial vehicles (e.g., the Predator), reconnaissance aircraft (e.g., the U-2), and ground systems. IMINT is "the only intelligence system that allows [ground force] commanders to visualize their area of operations in near real time as the operation progresses."[8] IMINT is also critical in planning and intelligence preparation of the battlefield (IPB). Perhaps the most famous public example of IMINT was the publication of aerial photos of Russian missiles during the Cuban Missile Crisis. Given the gravity of the situation, President Kennedy's release of IMINT to make the diplomatic case at the United Nations and convince the American people of need for military action provided a precedent for the public use of imagery intelligence.[9]

Human intelligence (HUMINT) collection operations focus on "determining the capabilities, threat characteristics, vulnerabilities, and intentions of threat and potential threat forces" and involve screening, interrogation, debriefing (e.g., of friendly forces), and liaison operations with friendly foreign militaries and intelligence services.[10] HUMINT includes acquiring documents and media sources, such as computers and hard drives. The account of the 2d Brigade Combat Team in Iraq, details the identification and training of informants and the exploitation of their information for both force protection and developing actionable intelligence. HUMINT also contributes to a greater understanding of the culture and "the nuances of local demographics" such as different ethnic, sectarian, political, and tribal groups.[11] HUMINT can be crucial for military purposes. For instance, during the Cuban Missile Crisis, the CIA's asset, Oleg Penkovskiy, a colonel in the Soviet General Staff's military intelligence, provided critical intelligence on the readiness and capabilities of Soviet strategic rocket forces. Anti-Castro sources in Cuba also helped pinpoint the location of missile sites in western Cuba.[12]

"Measurement and Signature Intelligence [MASINT] is ... derived from specific technical sensors for the purpose of identifying ... distinctive features associated with [a target.][13] Among intelligence scholars there is some controversy, as noted by Lowenthal, as to whether MASINT constitutes a separate technical discipline or whether it represents a hybrid of other disciplines.[14] Nevertheless, the contributions of MASINT in detecting WMD, monitoring

6. US *Army Field Manual* 2-0, "All-Source Intelligence," Chapter 5, Paragraph 5.5.
7. *www.nga.mil*
8. US *Army Field Manual* 2-0, "Imagery Intelligence," Chapter 9, paragraph 4.
9. *www.fas.org/irp/imint/cubakent.htm*
10. US *Army Field Manual* 2-0, "Human Intelligence," Chapter 7, paragraph 5.
11. Baker, p. 17.
12. Lowenthal, Mark, *Intelligence: From Secrets to Policy*: 4th Edition, CQ Press, Washington, D.C., 2009, p. 72.
13. US *Army Field Manual* 2-0, "Measurement and Signature Intelligence," Chapter 10, Paragraph 1.
14. Lowenthal, p. 96.

potential weapons development sites, and countering an adversary's tactics of denial and deception can be significant. In addition, by identifying the electronic, physical, thermal, acoustic, and other signatures of an adversary's weapons system MASINT contributes to the library of threat models used for subsequent threat assessments and tactical scenarios.

Open-source intelligence [OSINT] produces intelligence derived from the analysis of publicly available information. It supplements and supports other intelligence gathering activities by providing background cultural or biographical information, for instance, relevant to a commander's requirements. Analysis of information from unclassified sources can be used effectively to reduce the need for more complex classified data gathering. In addition to its supporting and potential cost-saving role, OSINT provides valuable insights of its own. In a March 26, 2001 interview on National Public Radio, Lt. Col. Reid Sawyer, an Army intelligence officer and head of West Point's Combating Terrorism Center, said: "I think that open source provides a critical lens into understanding the world around us in a much more dynamic way than traditional intelligence sources can provide."

Reliance on any single source of intelligence information can bias an analyst's judgments or blind him to a threat. The intent of "all-source analysis" is for the analyst to draw upon a variety of sources and means. The analyst needs to be alert to an adversary's potential use of deception, especially in exploiting the US's well-known reliance on technology-based data collection. Technological advancements in intelligence, as has been noted in assessments of Operation Desert Storm, should not be viewed as making a nation "deception-proof."[15] Deception detection, then, can be one of the valuable insights that intelligence can make regarding an adversary's intent, operational vulnerabilities, or tactical predilections.[16]

"Intelligence, Surveillance, and Reconnaissance (ISR)" is the term used by the military to describe the systems, processes, and products associated with all of the information gathering capabilities of the military. ISR plays a critical role supporting the planning of operations. An interesting recent example is the raid on Osama Bin Laden's compound in Pakistan. The National Geospatial-Intelligence Agency (NGA), the Intelligence Community's experts on IMINT and GeoINT, employed both IMINT and MASINT capabilities, to do the following:

> *Create a three-dimensional rendering of Bin Laden's Abbottabad compound using imagery and laser-based sensing devices—laser radar, or ladar;*
>
> *Analyze data from a sophisticated next-generation unmanned aerial vehicle that kept watch on the compound before, during, and after the raid;*
>
> *Help the Joint Special Operations Command create precise mission simulators for the pilots who flew the helicopters to practice before the raid; and*
>
> *Provide the CIA and others assessments of the number of people who lived inside the compound, their heights and genders.*[17]

The role of the NGA in the Bin Laden raid is a classic example of the value of ISR for time-sensitive decision-making where "ISR visualization helps the commander…identify fleeting opportunities for intelligence collection or strike operations against adversary time-sensitive targets that may warrant dynamic re-tasking of collection platforms or re-targeting of strike assets."[18]

The shorter the time frame that the intelligence is needed and the closer the analyst works to the tactical level, the greater the reliance is on those assets providing the most timely, accurate information and those assets that are within the analyst's ability to "task" or access easily. This is particularly true where the location of a high-value target (HVT) of immediate interest may emerge from information that is time-sensitive. In such a case, the analyst must coordinate with assets that can provide target acquisition. This form of "combat information," data gained from ISR assets, may be shared with commanders prior to analysis depending on the urgency of the data for current operations.[19]

In cyber warfare, operations and intelligence functions blur. This is illustrated by the commander of the U.S. Cyber Command being the same person as the Director of the National Security Agency (NSA), the Intelligence Community's SIGINT organization. A recent article noted that the use of cyber viruses by the military can include "studying the cyber-capabilities of adversaries or examining power plants or [how] other

15. *www.au.af.mil/info-ops/index.htm.*
16. Sheldon, John B., "Deciphering Cyberpower: Strategic Purpose in Peace and War, *Strategic Studies Quarterly*, Summer 2011, p. 104.
17. Ambinder, Marc, "In Raid on Bin Laden, Little-Known Geospatial Agency Played Vital Role," *National Journal*, May 5, 2011 (*http://www.nationaljournal.com/whitehouse/in-raid-on-bin-laden-little-known-geospatial-agency-played-vital-role-20110505?page=1*)
18. Joint and National Intelligence Support to Military Operations, Joint Publication 2-01, Chapter III, p. 28
19. Joint Publication 2-01, Chapter III, pp. 2-3.

networks operate."[20] In combating the proliferation of WMD, the use of cyber-weapons against vital computer operating systems can disrupt and delay a target nation's ability to produce weapons-grade material, for instance, as has been speculated with introduction of the Stuxnet virus in Iranian nuclear facilities.[21]

The strategic importance of intelligence to cyber warfare is a high-priority topic, as cyber warfare can contribute to one's "ability in peace and war to manipulate the strategic environment to one's advantage while at the same time degrading the ability of an adversary to comprehend that same environment."[22] At the tactical level cyber warfare can: "disrupt and sabotage adversary cyber-dependent activities and communications; steal information that is valuable to the adversary; monitor and spy on adversary activities through cyberspace; and deceive cyber-dependent adversaries into making decisions (or not making decisions) that are favorable to the perpetrator through the manipulation of adversary information..."[23] Given the microsecond speed of cyber warfare, intelligence preparation of the cyber battlefield is essential.

CONCLUSION

The critical nature of intelligence's role in supporting military operations will not decrease over time. In fact, given the likely role of counterinsurgency warfare and the threats from non-state actors in asymmetric warfare, the foreseeable future underscores the importance of intelligence for success on the battlefield—to include "non-kinetic" warfare in cyberspace. The variety of technical means, for collection and analysis, can present challenges in and of itself for "all-source" analysts. The role of human judgment, in not being overwhelmed by the deluge of data and maintaining a sensitivity to deception, makes the education and training of analysts a high priority for the Intelligence Community. The role of the analyst supporting future military operations highlights the need to exploit "lessons learned" in current operations: an analyst's prioritizing the need for greater cultural understanding against the insatiable demands for "real time" displays of the battle area is likely to get more attention in the allocation of resources for non-traditional warfare. A well-balanced approach to the preparation of emerging analytical talent and development of the current intelligence workforce should reflect the evolving nature of the threats to the nation's security and should anticipate the implications of these threats to the needs of military commander and civilian policy maker alike.

20. Nakashima, Ellen, "List of Cyber-Weapons Developed by Pentagon to Streamline Computer Warfare," *Washington Post*, May 31, 2011. (*http://www.washingtonpost.com/national/list-of-cyber-weapons-developed-by-pentagon-to-streamline-computer-warfare/2011/05/31/AGSublFH_story.html*)
21. Sheldon, p. 104.
22. Sheldon, p. 103.
23. Sheldon, p. 104.

READINGS FOR INSTRUCTORS

The following books, articles, and documents are suggested for a greater understanding of military intelligence.

R.V. Jones, *Reflections on Intelligence*, Mandarin Paperbacks, London, 1990. See especially Chapters 5, 6 and 10.

David Kahn, *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*, Scribner, New York, 1996.

John Keegan, *Intelligence in War: Knowledge of the Enemy from Napolean to Al-Qaeda*, Alfred A. Knopf, New York, 2003. See especially Chapters 1, 3, 6, 8 and Conclusion.

Mark Lowenthal, *Intelligence: From Secrets to Policy: 4th Edition*, CQ Press, Washington, D.C., 2009. See especially Chapters 5 and 6.

Michael Warner, *The Office of Strategic Services: America's First Intelligence Agency*, Center for the Study of Intelligence, Washington, D.C., 2000.

Ralph Baker, "HUMINT-Centric Operations: Developing Actionable Intelligence in the Urban Counterinsurgency Environment," *Military Review*, 87 (March-April 2007), pp. 12-21.

John B. Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," *Strategic Studies Quarterly*, Summer 2011.

Original Sources in Intelligence:

Office of the Secretary of Defense, Department of Defense, "Quadrennial Defense Review," February, 2010. *http://defense.gov/qdr*

Office of Undersecretary of Defense (Intelligence), Department of Defense, "The Defense Intelligence Enterprise," 2008. Source document can be found at the Naval Postgraduate School's Homeland Security Digital Library, *www.hsdl.org*

Headquarters, Department of the Army, *US Army Field Manual 2-0 Intelligence*, 2010

Joint Chiefs of Staff, Department of Defense, *Joint and National Intelligence Support to Military Operations*, Joint Publication 2-01, 2004. *www.fas.org/irp/dod/jp2_01.pdf*

THE WEB SITES LISTED BELOW ARE VALUABLE SOURCES FOR UNDERSTANDING INTELLIGENCE IN SUPPORT OF MILITARY OPERATIONS.

www.fas.org: This is the website for the Federation of American Scientists. Its intelligence project has archived many historically relevant documents related to intelligence.

www.cia.gov: This is CIA's website. The link to the Center for the Study of Intelligence admits the researcher to a wealth of published and declassified studies related to intelligence.

www.dia.mil/history: This site provides a succinct account of definitions, concepts, and the intelligence analysis process.

www.hsdl.org: A searchable database that provides access to strategic, executive-level documents related to issues of intelligence located on site of Naval Postgraduate School.

www.nga.mil: This is the website of the National Geospatial-Intelligence Agency.

www.au.af.mil/info-ops/index.htm: An extremely comprehensive database that contains web sites and other resources of strategic, operational, and tactical intelligence interest. See the Intelligence Gateway to get started.

www.acronymfinder.com: Along with *www.answers.com* this is a good resource for getting information on acronyms and other esoteric intelligence terminology for beginners.

www.carlisle.army.mil: This is the site for the Army's War College.

Karl Haigler is a retired Military Intelligence officer. He served in the U.S. Army Reserve, the intelligence division of the Joint Staff, and as an analyst in the Defense Intelligence Agency's Soviet Ground Forces Division. He was the Director of Adult Education in the U.S. Department of Education and a member of the Senior Executive Service. He also served as special advisor to the Governor of Mississippi on literacy and workforce development issues. He has been a secondary school teacher and an instructor in post-secondary education.

The author wishes to thank Jeff Holcomb, David Campbell, Terry Clark, Mike Gillies, and Tom Brister for their insights and contributions on the theory and practice of intelligence. He also wants to recognize students at Wake Forest University and Forsyth Country Day School (Lewisville, N.C.) for their keen participation in intelligence analysis simulations.