
Intelligence and Its Role in Protecting Against Terrorism

Richard J. Hughbank

HALO Corporation and U.S. Army, rhughbank@understandterror.com

Don Githens

U.S. Air Force

Follow this and additional works at: <https://scholarcommons.usf.edu/jss>

 Part of the [Defense and Security Studies Commons](#), [National Security Law Commons](#),
and the [Portfolio and Security Analysis Commons](#)

pp. 31-38

Recommended Citation

Hughbank, Richard J. and Githens, Don. "Intelligence and Its Role in Protecting Against Terrorism." *Journal of Strategic Security* 3, no. 1 (2010) : 31-38.

DOI: <http://dx.doi.org/10.5038/1944-0472.3.1.3>

Available at: <https://scholarcommons.usf.edu/jss/vol3/iss1/4>

This Article is brought to you for free and open access by the Open Access Journals at Scholar Commons. It has been accepted for inclusion in *Journal of Strategic Security* by an authorized editor of Scholar Commons. For more information, please contact scholarcommons@usf.edu.

Intelligence and Its Role in Protecting Against Terrorism

By Richard J. Hughbank and Don Githens

Many intelligence reports in war are contradictory; even more are false, and most are uncertain.

- Karl Von Clausewitz
Prussian soldier and intellectual (1780–1831)

Introduction

Intelligence is information that is analyzed and converted into a product to support a particular customer. Intelligence is both a process and a product and has played an important role in diplomacy and warfare throughout history. In the information age, intelligence has taken on an even greater importance. But in the popular media, the role, means, and purpose of intelligence is very often misrepresented at best. Only a tiny fraction of intelligence officers perform clandestine intelligence gathering. They don't assassinate people, carry weapons or even wear trench coats. The vast majority of the intelligence community carries out its mundane tasks at a computer terminal and, while intelligence alone cannot stop the next terrorist attack, it is *the* critical first step in identifying and possibly preventing one.

The art and science of gathering critical operational intelligence has been defined in many ways and is beyond our needs for this writing. Throughout the course of history, many wars have been fought depending heavily on various forms of intelligence. During our most recent actions in the War on Terror, intelligence analysis has played a critical role in both offensive and defensive operations in Iraq and Afghanistan. With such varying fact-finding techniques available and utilized in the defense of our country, it has become an arduous task to collect, decipher, package, prioritize, disseminate, and act upon everything that comes down the pipe.

Intelligence is even more important in homeland defense and security. Our society is suspicious of intrusions on personal liberties. Mandated identity cards, restricted vehicle access and random searches of airline passengers are generally not well received. That makes it especially important to prevent terrorist attacks by interdicting the terrorists and

their resources before they can reach their targets. The primary means of accomplishing this is through a combination of intelligence and law enforcement work.

Military intelligence branches have been extremely effective while operating in various countries with the use of multiple forms of intelligence: Human Intelligence (HUMINT), Geospatial Intelligence (GEOINT), Measurement and Signature Intelligence (MASINT), Open Source Intelligence (OSINT), Strategic Intelligence (STRATINT), Signals Intelligence (SIGINT), and Technical Intelligence (TECHINT). Simply stated, and reduced to the lowest common denominator, intelligence is information of the world about us. Regardless of the form of intelligence, the world can be divided into short-term, narrow focus, Tactical Intelligence, and long-term broad focus, Strategic Intelligence.

Strategic Intelligence

Strategic intelligence is used for long-term planning and other broad topics such as operational capabilities of a potential opponent and political assessments. With painstaking analysis and the use of computers to produce clear evaluations and concise intelligence assessments, local law enforcement can have a foundational tool to effectively use in an effort to identify potential terrorist operations and targets within their community. It's this functional ability to "predict" when and where future operational terrorist acts might occur and which tactical targets might prove more advantageous for a terrorist organization—whether it is psychological, economical, or political in nature—through the use of gathered and processed data from varying sources that places homeland defense in better offensive and defensive postures to successfully preempt and thwart their next attack.

Tactical Intelligence

Tactical intelligence is used for operational units and includes, among other things, human intelligence, open source intelligence, imagery intelligence, and direct observation. These particular sources require trained and dedicated street cops who can think on their feet and identify the simplest of cultural patterns and behavioral modifications of those who regularly work, play and live within their assigned patrol areas. In this age of technology, we have become so reliant upon computers that we've almost forgotten this most important point. For the remainder of this article, we will focus primarily on tactical intelligence and its critical role in identifying and defeating future terrorist acts in our communities.

Tactical intelligence is crucial in counterinsurgency and asymmetric warfare. Initiative and surprise can be achieved only if the tactical intelligence mission is effective. All possible vetted sources must be utilized to their optimal potential, including those frequently ignored. Therefore, a central clearinghouse should be established that collects and exploits all of the accumulated information then disseminates the assembled intelligence to the shift commanders so they can be passed on either at shift change or during the shift as deemed necessary. The officers in the street, in turn, need to pass on information gathered from their neighborhood sources to their designated information collector in a timely fashion. This is the only way the intelligence mission can have a chance of functioning at a level necessary to identify and possibly stop the next terrorist attack.

Intelligence Application

So, what exactly should you be searching for and passing on to the clearinghouse while patrolling and interacting with the neighborhood on an average shift? Well, you're looking for the same things you've been looking for since you left the academy; anything that's out of place or out of the ordinary; comments from the people on your beat that have a "strange" ring to them. You already know; anything that doesn't quite seem right to you through your training and experience on the street. New people in the neighborhood who avoid patrol cars, groups that break up when you slow down as you drive by, and different attitudes of people you've known over time are just some examples of things and acts to be watchful for. Those mundane reactive shifts *must* turn into proactive conversation and a critical eye for detail.

Having the ability to gain a sense of situational awareness for a certain area within a community will either deter or assist in gaining knowledge of "new" changes that directly impact the initial stages of terroristic-guerilla warfare in your assigned sectors. Remember, you're a trained observer; so observe and report accordingly.

The Army gets this right, as every soldier is a collector of information as part of their basic duties. No one particular unit or patrol is given the individual task of collecting and passing up information while on patrol on any given mission and on varying degrees of terrain and areas of operation. Everyone receives an intelligence brief prior to beginning a mission or shift, and each individual is required to remain vigilant during their patrol with an additional requirement to continue gathering intelligence while out on the streets.

All police departments have the same potential—they rely on daily, personal interaction within their assigned sector of patrol to perform their duties. While the information they "collect" is for the purpose of protecting the populace, enforcing laws and preventing crime, some information can be useful to analysts tracking the potential terrorist threats within our borders. Almost every illegal activity can be given away by indicators. It's the observation of these indicators and the proper analysis of their significance that could directly lead to the defeat of future terrorist acts. Various stages of terrorist operations can be determined by the smallest of indicators provided during that particular operational maneuver. You won't necessarily recognize these indicators for what they are, but to an analyst who has studied a particular terrorist group or individual that indicator can speak volumes. The question is, how do you know what to look for?

In the intelligence community, the process of addressing this question is known as collection management. Analysts who study an intelligence problem (e.g., what are the plans and capabilities of a particular terrorist organization) have the best idea of what intelligence gaps exist. They identify these gaps to a collection manager (CM) in the form of a requirement. A requirement consists of priority and justification, essential elements of information and reporting requirements. The CM then integrates these requirements into a collection strategy. Finally, a collection plan is developed to detail a tactical level course of action and subsequently briefed to operators (e.g., SWAT and daily patrols) to carry out. The interaction of the analysts and collectors is absolutely essential to this entire process.

The Collection Cycle

As a process, intelligence is designed to support a person or organization. It is designed to assist decision makers, planners, operators and sometimes other intelligence organizations. Intelligence is useless if it's inaccurate, or if it is presented in an unusable format when needed. It's imperative the intelligence organization has a clear understanding of the tasking being levied. Tasking is the first step in the intelligence cycle (sometimes referred to as the collection cycle or TCPED cycle).

- **Tasking:** The tasking should originate with the person or organization being supported. The more involved the *customer* gets in tasking, and the more detailed that tasking is, the better the final product becomes. This tasking is referred to as a requirement, and it drives the rest of the collection cycle.

- **Collection:** This is the actual gathering of raw information. It can take the form of imagery (IMINT), a communications signal intercept (SIGINT), or a report from a person (HUMINT).
- **Processing:** This is the stage where raw data is converted to a useable format. SIGINT intercepts are translated, HUMINT reports are formatted and source information added, and IMINT is converted to customer specifications.
- **Exploitation:** Intelligence analysts analyze the information to determine its significance. The final product is created according to the customer's requirement at this stage.
- **Dissemination:** The finished intelligence product is delivered according to the customer's requirement.

The collection cycle for each intelligence discipline differs in timeliness and responsiveness. IMINT is probably the most timely and responsive, since technology allows for rapid processing and dissemination. IMINT is also active—an asset has to go out and take the pictures. SIGINT is not as timely, since signals usually need to be transcribed and/or translated. SIGINT technology is usually more sensitive, and thus access to the collected data is usually more restricted (classified). SIGINT also relies on the target being active in communication. HUMINT is usually the least timely, since collecting usually involves considerable risk to the person doing the collection. Security measures to ensure the safety of the collector definitely slow down the processing stage.

Fortunately, you don't need to be an expert on the capabilities of each intelligence discipline. The intelligence process is overseen by a collection manager (CM), an intelligence professional, usually experienced in a single intelligence discipline that helps the customer craft their requirement. The CM then determines the most effective intelligence discipline to satisfy the requirement, prioritizes it against other requirements, and tasks an intelligence resource to achieve the collection. A CM follows the requirement through the collection cycle, acting as an advocate for the customer.

Intelligence support can be a valuable tool to assist law enforcement agencies in the performance of their daily duties. It's especially relevant in counterterrorism investigations and operations. Terrorist organizations rely heavily on secrecy and anonymity to carry out their religious and politically driven agendas, and intelligence gathering and exploitation is best suited to stripping away this critical layer of protection and making

Journal of Strategic Security

them more vulnerable to infiltration, investigation and arrest. Intelligence work is a discipline in and of itself, just like police work, and carries its own language, rules, and culture. At times, it can be in direct conflict with law enforcement, but the goal of both remains the same; the protection of every American citizen and our way of life; our very culture, if you will.

As terrorism continues to plague the world through the global Salafi jihad movement, the United States will forever serve as a critical target for various organizations who seek to spread "pure" Islam. Through patience and vigilance, our enemies continue to further their cause through the understanding of our society. Thus, it becomes imperative we do the same. It is imperative we continue to learn about those who choose to attack our freedoms and way of life, and our law enforcement agencies will have to take the lead in this ongoing war. Indeed, the law enforcement community must develop transparent communication and intelligence links. While the days of fighting conventional crime are still at the forefront, our modern foes have defiantly presented us with a challenge that must be met with extreme prejudice if we are to successfully protect our nation and its citizens. The collection of intelligence will prove invaluable in this success, but we must learn to properly use this important tool at the strategic, operational, and tactical levels and it starts with training and utilizing every facet of our law enforcement agencies as they continue to patrol and protect our neighborhoods.

The views expressed herein are those of the authors and do not purport to reflect the position of the U.S. Air Force Academy, the Department of the Army, or the Department of Defense.

About the Authors

Richard Hughbank is a senior trainer with HALO Corporation and a Military Police officer in the U.S. Army with over twenty-one years experience. He is an adjunct for the Center for Homeland Security at the University of Colorado at Colorado Springs as a graduate course instructor in terrorism studies and homeland defense. Richard also chairs the Terrorism Studies and Standards committee for the Anti Terrorism Accreditation Board, is a Diplomate of the American Academy of Experts in Traumatic Stress, and a member of the National Center for Crisis Management. His graduate studies are in security management, counseling,

and terrorism studies, and is a doctoral candidate in Strategic Security. Richard can be contacted through his website: <http://www.understandterror.com> or at rhughbank@understandterror.com.

Don Githens is a Captain in the U.S. Air Force with nine years experience as an Intelligence Officer and Analyst. He is earning a graduate certificate in Homeland Security studies at the University of Colorado at Colorado Springs.

Journal of Strategic Security