Intelligence Requirements and Threat Assessment

10

CHAPTER TEN

Intelligence Requirements and Threat Assessment

Information is needed to make decisions – the higher the quality and the more comprehensive the information, the more sound the decision. If an executive is going to make a decision about implementing a new program, he or she needs information on the costs, benefits, and risks of the program as well as the more difficult dimension of what benefits will be lost if a program is not implemented. Typically, the information sought is not conclusive, but based on probability, the experience of others, experimentation, logic or, sometimes, an educated guess. Not having sufficient reliable information makes the decision process more difficult (and risky).

The same phenomenon applies to the operational world of criminal intelligence. To adequately assess the threats from a terrorist group or criminal enterprise, information is needed for a comprehensive analysis. Oftentimes during the course of the analytic process, critical information is missing that prevents a complete and accurate assessment of the issue. This is a gap, an unanswered question related to a criminal or terrorist threat. An intelligence requirement is identified and information needs to aid in answering questions related to criminal or terrorist threats.[177]

In order to adequately ASSESS THE THREATS from a TERRORIST GROUP or CRIMINAL ENTERPRISE, information is needed for a COMPREHENSIVE analysis.

Filling Gaps/Fulfilling Requirements

177 FBI Office of Intelligence. *The FBI Intelligence Cycle: Answering the Questions….* A desk reference guide for law enforcement. (Pamphlet form). (July 2004).

The information collection process needs to be focused so that specific information needs are fulfilled. This increases efficiency of the process and ensures that the right information needs are being targeted. Too often in the past a "dragnet" approach was used for collecting information, and analysts and investigators would examine the information in hopes of discovering the "pearls" that may emerge. As illustrated in Figure 10-1, there are a number of differences between the traditional approach and the requirements-based approach to information collection. In essence, the requirements-based approach is more scientific; hence, more objective, more efficacious, and less problematic on matters related to civil rights.

Figure 10-1: Traditional Collection vs. Requirements-Based Collection[177]	
Tradition-Based	**Requirements-Based**
• Data-driven	• Analysis-driven
• Exploratory	• Contemplative
• Emphasizes amassing data	• Emphasizes analysis of data
• Infers crimes from suspected persons	• Infers criminal suspects from crimes
• An aggregate approach to information collection (dragnet); even mere suspicion	• Targeting/specificity on information regarding reasonable suspicion of crimes
• Explores all general inferences about potential criminality	• Selectively explores crime leads based on priorities and evidence
• Explores collected information to see if there are questions to answers	• Answers questions by collecting and analyzing information
• Develops intelligence files for contingency needs, (i.e., just in case information is needed)	• Develops intelligence files in support of active crimes and investigations
• Statistics produced for descriptive purposes	• Statistics produced for decision making

Since this is a scientific process, the intelligence function can use a qualitative protocol to collect the information that is needed to fulfill requirements. This protocol is an overlay for the complete information collection processes of the intelligence cycle. The numbered steps in the box below are action items in the protocol, the bulleted points are illustrations. This is not a template, but a process that each agency needs to develop to meet its unique characteristics.

177 Carter, David L. (2003). *Law Enforcement Intelligence Operations*. Tallahassee, FL: SM&C Sciences, Inc.

1. Understand your intelligence goal
   - Arrest terrorists and/or criminals
   - Prevent or mitigate terrorists attacks
   - Stop a criminal enterprise from operating
2. Build an analytic strategy
   - What types of information are needed?
   - How can the necessary information be collected?
3. Define the social network
   - Who is in the social circle of the target(s)?
   - Who is in the regular business circle of the target(s)?
   - Who has access to the target(s) for information and observation
   - What hobbies, likes, or characteristics of the target's social behavior are opportunities for information collection, infiltration, and observation?

4. Define logical networks
   - How does the enterprise operate?
   - Funding sources
   - Communications sources
   - Logistics and supply
5. Define physical networks
   - Homes
   - Offices
   - Storage and staging areas
4. Task the collection process
   - Determine the best methods of getting the information (surveillance, informants, wiretaps, etc.)
   - Get the information

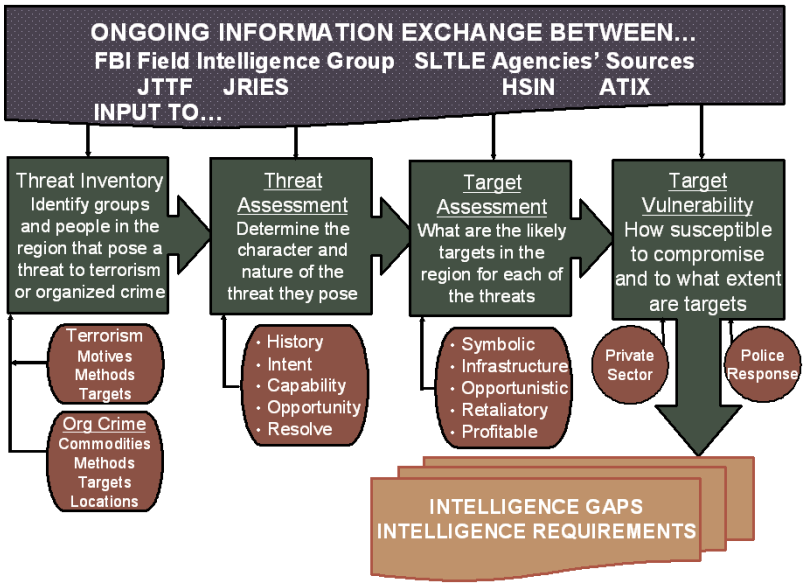
As information sharing becomes more standardized and law enforcement intelligence as a discipline becomes more professional, law enforcement agencies at all levels of government will use the requirements-driven process. In all likelihood, this approach will become a required element for information sharing, particularly with the FBI and the Department of Homeland Security (DHS).

Threat Assessments

Threat assessments are often discussed, but the process remains elusive to many state, local, and tribal law enforcement (SLTLE) agencies (Figure 10-2). There are four key variables in the process:

1. Threat Inventory.
2. Threat Assessment.
3. Target Assessment.
4. Target Vulnerability.

Figure 10-2: Threat Assessment Model for SLTLE[178]



Threat inventory: The threat inventory requires the law enforcement agency to identify groups and individuals within the agency's region[179] that would pose possible threats. These may be international terrorists, domestic extremists, individuals who have an extreme special interest ideology, or a criminal enterprise. The type of information sought centers on identifying answers to certain questions: Who are the people involved? What is their group affiliation, if any, and what do they believe? To understand extremists it also is useful to identify their motives, methods, and targets. With criminal enterprises, the variables are methods, commodities, and locations. In either case, understanding how the criminal entity operates and what it seeks to accomplish can provide significant insight into their ability to act. Care must be taken to collect and retain the information in a manner that is consistent with 28 CFR Part 23 guidelines.

Threat assessment: Each threat identified in the inventory must be assessed with respect to the level of the threat posed. Some individuals make threats, but do not pose a threat. Conversely, some individuals and groups pose threats without ever making a threat. To fully assess their

178 This model was prepared by David L. Carter, Michigan State University, as part of a training program on Intelligence Requirements and Threat Assessment for the Bureau of Justice Assistance (BJA)-funded State and Local Anti-Terrorism Training (SLATT) program.

179 Realistically, the threat assessment must be done on a regional, rather than jurisdictional, basis because a specific threat and/or target will likely have an impact on the jurisdiction.

threat capacity, several factors need to be examined: What is the history of the groups? Have they committed attacks or crimes in the past? If so, what was the modus operandi (MO) and character of the act? Does the group have the capability to actually commit terrorist acts or crimes? If so, how robust is that capability? Are unique opportunities present for the group to commit an act? What appears to be the resolve or the commitment of the group? Factors such as these can develop an image to aid in determining the character of the threat posed by individuals and groups in the inventory.

Target assessment: In light of the nature of the groups in the threat inventory, probable targets can be identified in the region. It is rare that a specific target can be identified, but based on history, statements, threats, and the nature of an extremist group's ideology, the array of targets can be narrowed. Similarly, criminal enterprises tend to have targeted commodities that they traffic or types of frauds they perpetrate.

Target vulnerability: The last variable is to assess each of these targets to determine how vulnerable they are to attack. This often involves working with the private sector and often crime-prevention specialists within the law enforcement agency. Given the difficulty of identifying specific targets, the goal is to ensure that each potential target in the region is hardened against an attack.

When information is not available about the factors in this assessment model, there is an intelligence gap that must be filled by a requirement.

FBI Intelligence Requirements Templates

When going through this threat assessment process, the SLTLE agency will need information from the FBI to aid in fully identifying and assessing threats. As noted by the FBI:

> State and local agencies or entities are served by the FBI and have specific needs for tailored intelligence. … To appropriately address the information needs of state and local agencies, certain procedures can enhance this process. These include:

- Identifying, prioritizing, and addressing state and local information needs.
- Sharing intelligence, analytical techniques, and tools.
- Timely distribution of appropriate intelligence.
- Seek feedback from state and local [law enforcement concerning the] effectiveness of the support.[180]

To facilitate this information exchange, the FBI Office of Intelligence developed a template (Figure 10-3) expressly for SLTLE agencies to use for logging Intelligence Information Needs (IINs) or intelligence gaps they identify. IINs are questions expressed by customers of the FBI and other intelligence producers, the answers to which support law enforcement functions. IINs are not operational leads or questions on the status of investigations or operations. Intelligence gaps are unanswered questions about a criminal, cyber, or national security issue or threat. To illustrate this further, the FBI developed a sample of "baseline" IINs (Figure 10-4). The SLTLE agency should coordinate its use of IINs and information exchange with the Field Intelligence Group (FIG) of the FBI Field Office servicing it.

180 FBI Office of Intelligence. (2003). *FBI Intelligence Production and Use*. Concept of Operations Report. (unpublished report). Washington, DC: FBI Headquarters Divisions and the Office of Intelligence, p. 18.

IN ORDER TO FACILITATE THIS INFORMATION EXCHANGE, the FBI Office of Intelligence has developed a template expressly for SLTLE agencies to be used to log Intelligence Information Needs or intelligence gaps they identify.

CONCLUSION

The intent of intelligence requirements and threat assessments is to provide a comprehensive, consistent model for managing the threats to a community. These processes are not necessarily easy; however, the outcomes they provide can be priceless.

Figure 10-3: Intelligence Information Needs (IINs)

Purpose: This form should be used to log IINs or intelligence gaps identified by state, local, or tribal law enforcement agencies in your area of responsibility. IINs are questions expressed by customers of the FBI and other intelligence producers, the answers to which support law enforcement functions. IINs are not operational leads or questions on the status of investigations or operations. Intelligence gaps are unanswered questions about a criminal, cyber, or national security issue or threat.

IIN	Requesting Organization (Agency, department, organization)	Dissemination Instructions (Customer name, position title, mailing address, contact number, LEO or other official e-mail address)

Figure 10-4: "Baseline" Intelligence Information Needs (IINs)

Purpose: This template provides a list of sample IINs that can be presented to state, local, and tribal law enforcement partners as a baseline from which to review intelligence gaps, select issues relevant to their investigative needs, and identify additional intelligence and collection requirements.

IIN	Requesting Organization (Agency, department, organization)	Dissemination Instructions (Customer name, position title, mailing address, contact number, LEO or other official e-mail address)
National and local threat assessment reports. - Reliability of the information received - Group planning attack(s) - Target(s) - Why is the target a target? - Suspected method of attack - Weapons of attack - Time frame of attack - Response of federal entities Global, national and local trend reports regarding organizations and structures of active terrorist, criminal, drug, and hate groups in the US. - Identity of suspects and their roles in the local area - Territorial reach - Decision-making processes; degree of subordinate autonomy - Command-control-communications techniques, equipment, network Global, national and local trend reports regarding capabilities, intentions, MO of suspect groups in the US - Types of weapons, explosives, or WMD - Methods of moving, storing and concealing weapons, contraband and human traffic - Special/technical expertise possessed by groups		

IIN	Requesting Organization	Dissemination Instructions
Illegal activities of suspect groups in local jurisdictions - illegal production/acquisition of CBRNE materials/precursors, illegal drugs or substances, prohibited items or persons - illegal arms trade, theft, diversion, sales; smuggling of aliens, terrorists, or prohibited items; human trafficking - HAZMAT dumping; environmental crimes; trafficking in endangered species - links between criminal groups and terrorist or foreign intelligence organizations; bribery/extortion/corruption of public officials Identity, roles of US and foreign players sponsoring/supporting criminal, terrorist, espionage activities in local jurisdictions - criminal function of each operative or entity; extraterritorial reach - associated commercial/charitable entities; front/cover organizations - chain of custody in transport of critical technology, illegal items/persons - overseas connections (official, unofficial, private sources); group sympathizers - financial dependencies; extent of group's reliance on external support, funds Intelligence/security activities of suspect groups - surveillance, reconnaissance, concealment, "cover" activities; safe houses - counterintelligence and physical security techniques and tactics - COMSEC operations; ability to monitor LEC communications - informant/mole network available to suspect groups - production of, access to false/counterfeit documents and identification - deception, disinformation operations and techniques		

IIN	Requesting Organization	Dissemination Instructions
Modes of transportation and conveyance (air, maritime, and ground) - use of commercial transport/courier/shipping services and carriers - use of private/non-commercial carriers, couriers - types/identification of cargo containers; modifications - itineraries; favored routes; point of departure/source; nations transited - transshipment nodes; border-crossing techniques - multiple couriers chain-of-custody techniques; arrival/pick-up techniques Finances of suspect groups - support networks; state and private sponsors; shell companies - money-laundering techniques; unconventional financial transfers (e.g., hawalas) - shell companies; charity/humanitarian sponsors and covers - financial crime used to generate income; extortion of vulnerable targets - cooperative, facilitating financial institutions or service providers - financial links between public officials and criminal organizations or enterprises, hate groups, or FIS - criminal control of public, tribal financial assets or property Impact of LE or USG efforts to combat suspect groups' activities - infiltration; compromise; destruction; disruption - which tactics most/least effective; evidence of shift in suspect groups' tactics, techniques, or targets - effectiveness of LE efforts overseas		

IIN	Requesting Organization	Dissemination Instructions
- response of suspect groups to LE efforts (countermeasures) - suspect group efforts at corruption of public/LE officials or employees - evidence of foreign/external LE entities' capabilities to cooperate and collaborate in joint efforts or operations - evidence of change in policies/attitudes overseas that affect tolerance for or freedom of action of suspect groups to operate in foreign environments Recruitment; training; collaboration by suspect groups - recruitment techniques and priority targets - training received: type, location, provider, curriculum, facilities Tactics of intimidation, interference with free exercise of civil rights - targets of hate groups, ethnic supremacist organizations - incidents of violence or incitement against individuals, groups, places of worship, schools, commercial entities identified with ethnic or political minorities Capabilities, plans, intentions, MO of suspect groups to conduct computer intrusion or criminal assault on computer systems and data bases. Locally active hackers.		