CHAPTER 4

Information Planning and Threat Analysis

Information is the key to developing civil disturbance plans. Who are the demonstrators? When and where will they demonstrate? What are their capabilities and possible courses of action? A civil disturbance task force commander's need for current, valid information cannot be overemphasized. He must learn as much as he can about the participants, their motivations, their strategies and tactics, their targets, and their dedication. The more knowledge he has about the participants, the better equipped he is to counter their actions. He needs sound information to decide how best to use his available resources.

To be useful, collected data must be processed into "intelligence." It must be seen in relation to the social, economic, and political climate of the area, and the likelihood of active participation or support from the local populace. Obtaining and developing intelligence in a timely manner is a top priority in order to use the information to assess the threat. Threat analysis begins with a broad examination of all information bearing on the security of an installation or a community. It focuses on potential threats. It identifies likely targets and vulnerabilities. Completed, it enables a commander to assess the threat of a civil disturbance to an installation, a mission, or a community. It forms the basis for his operational plans to counteract a civil disturbance.

INFORMATION NEEDS AND SOURCES

Planners must decide what data is needed to develop a threat assessment. They must also develop a list of information sources. Planners must be able to obtain information quickly during a disturbance. And they must have ways to obtain information from many sources at once.

Useful information can come from open sources, law enforcement sources, and military sources. Having a diversity of sources is the best approach. Information from many sources prevents biased behavior.

Open sources of information are perhaps the most overlooked valuable sources of information. The installation library is usually a good source of information. It may have a wealth of open-source material on past and current political events relating to a disturbance. Newspapers and news periodicals are also good sources of information. They run articles or special sections on events that may lead to or have led to a disturbance. Often, they publish interviews with organizers. These interviews may provide insights into the thoughts, perceptions, and intentions of a crowd's leaders. Radio and television interviews are very informational. And they provide more real-time information than newspapers, which have less flexible deadlines. In some cases, radio and TV

provide live coverage of a disturbance. For this reason access to a TV and a radio is a must.

Law enforcement sources can provide useful information on criminal activists. Provost marshals, military police, and criminal investigators routinely work with criminal information. Information also can be obtained from local, state, and federal law enforcement agencies. Criminal information provided by law enforcement agencies may reveal potential agitators. It also may provide information on criminals or terrorists who may try to exploit a disturbance.

The intelligence community is the most restricted source of information. Liaison with agencies that routinely collect information or intelligence is needed to know if they can support civil disturbance control operations. The DOD intelligence organizations operate under limitations imposed by regulations and executive orders. Attempts to skirt these restrictions may violate regulations or federal statutes. But intelligence organizations often can provide important, reliable data for operational planning within these limitations. Local MI field offices must be an integral part of all plans. They know the rules for collecting and storing intelligence. And they can provide valuable advice in this area. If any doubts arise about the legality of collecting and storing intelligence, the SJA must be consulted.

INFORMATION RESTRICTIONS

Collecting information related to a civil disturbance is strictly limited to protect the civil rights of people and organizations not affiliated with DOD. Civil disturbance plans and materials must not include lists of groups or people not affiliated with DOD. But lists of local, state, and federal officials who have direct responsibility for the control of civil disturbances are exempt. Data on vital public, commercial, and private facilities that are believed to be civil disturbance targets also are exempt from this prohibition. Information on civilians and civilian organizations can be collected only with specific authorization from the Secretary or the Under Secretary of the Army. Conditions for collecting information include the existence of threats against Army personnel, functions, or property. (See AR 380-13 and AR 381-10.) Civil disturbance information available in public documents, or open source information, may be collected. But specific rules regarding its storage must be followed. Commanders must coordinate with SJA, MI, and USACIDC personnel before collecting any such information.

The Army cannot gather, process, store, or report information on civilians unless civilian activities can be linked directly to a distinct threat of a civil disturbance that may involve federal military forces. Even when information can be collected, certain restrictions apply. The key restrictions include the following

- Computerized data banks for storage of civil disturbance information are established or retained only with the approval of the Secretary of the Army.
- Civil disturbance information relating to persons or organizations is stored only when DA so orders.
- Spot reports generated by information collection efforts must be destroyed within 60 days after the disturbance ends.
- After-action reports may, for clarity's sake, contain names of people and organizations who were directly involved in the civil disturbance being reported. But the inclusion of names must be kept to an absolute minimum.

- When a civil disturbance ends, the nature and extent of all accumulated files other than spot reports and after-action reports must be reported to DA. The report also must recommend that the Department of Justice either release the files or destroy them.

Classification of information also limits storage, access, and handling. In general, classified information cannot be shared with local and state law enforcement agencies. This restriction can hinder working relationships with these agencies. The law enforcement agency may see the military only as a receiver of intelligence, providing nothing in return. If this problem arises, and time is available, planners can ask the source to release an unclassified version. Secure transmission capabilities must be used to discuss any portions of classified information being requested.

If the Department of Justice determines federal intervention in a civil disturbance is likely, information relating to the disturbance is provided to the Army Assistant Chief of Staff for Intelligence. The information is analyzed and then provided to the Director of Military Support and the task force commander for planning purposes.

Military intelligence collection efforts, except liaison, may begin only when DA so orders. During a civil disturbance, the orders must come through the CSA's personal liaison officer and the task force commander. Covert operations to gather information on nonDOD individuals and groups must be approved by the Under Secretary of the Army. Such approval is on an operation-by-operation basis, and it must come through the personal liaison officer and the task force commander.

When DA approves collection efforts, MI elements establish and maintain liaison with the appropriate local, state, and federal authorities. Using these liaisons, the MI elements collect information on incidents and the general situation. They estimate the civil authorities' ability to control the situation. Based on current plans, they report the results of their collection efforts to DA. They keep the appropriate commander informed. They provide intelligence support to the personal liaison officer and the task force commander. They also recommend other overt collection methods to DA for DA approval.

THREAT ANALYSIS

Threat analysis is a fluid and continuous process. As data for the analysis change, so do the results. Planners must adjust their plans to incorporate changes that occur during the threat analysis.

Three kinds of information are analyzed to produce a valid threat analysis: intelligence and criminal information, threat information, and installation/community vulnerabilities. Intelligence and criminal information provide information on the goals, methods of operation, techniques, strategies, tactics, and targets of individuals and groups. Threat information identifies individuals and groups. Vulnerability information identifies security weaknesses and high-risk targets.

Both subjective and objective information are analyzed. Public perceptions are compared with more objective, measurable information. This can show how much public opinion differs from the objective measurement. Key factors to be analyzed include:

- State of the economy.
- Standard of living.
- Effectiveness of law enforcement.
- Stability of the government and of the population's social and economic situation.
- Morale of the population, their support of the government, and the government's support of them.

Some factors change slowly or infrequently. These factors include the terrain of the area being analyzed and the political and ethnic traits of the population. Dynamic factors like weather, economic conditions, and security and law enforcement resources change often. Some dynamic factors can be controlled. Movements of money and weapons, security of local sites, and allocations of military personnel can all be controlled. But many dynamic factors cannot be controlled. These include the weather and the actions of local law enforcement agencies.

Planners can use the Installation Vulnerability Determining System as an analytic tool. It will help them identify vulnerabilities, set up training priorities, and allocate resources. IVDS was developed to help counter terrorist threats. But by exchanging terms, like demonstrators for terrorists and community for installation, IVDS can be tailored for civil disturbances. IVDS is a guide only. A low score does not necessarily mean that there is not a problem. For detailed information on the IVDS, see TC 19-16.

IVDS assesses:

- The installation's or community's characteristics and its attractiveness as a target for terrorist acts or civil disturbances.
- Status of training.
- Availability of communications.
- Nonmilitary law enforcement resources.
- Time and distance from US military installations that can lend assistance.
- Time and distance from urban areas.
- Geographic region.
- Proximity to foreign borders.
- Access to the installation or the community.
- Population density of the installation or the community.
- Terrain.

There are other techniques for making a threat analysis. Planners can apply a think-like-the-opposition technique and develop plans that the opposition might use. This technique can help identify vulnerabilities and how they could be exploited. Games can be used to develop scenarios to identify the threat and to plan countermeasures. Scenarios can be developed for situations involving passive resistance, blockades, violent confrontations, bombings, arson, hostages, and occupations of buildings. Although scenarios are unlikely to occur exactly as conceived, they are beneficial. They help identify potential problems that can be corrected before a disturbance becomes a reality. Command post exercises and field training exercises are useful methods for training personnel to respond to civil disturbances. CPXs can help identify high-risk targets. They also are useful in training the people who will operate the EOC. An FTX allows planners to assess response capabilities. FTXs also provide opportunities for evaluating vulnerabilities from the demonstrators' viewpoint. If an FTX cannot be held in the community where a disturbance may be expected, a community or an area with similar characteristics can be used. And committees or councils are another means of evaluating threats and vulnerabilities. Such groups should include people who would play a major role in a civil disturbance operation, particularly logistics personnel and key community officials. Groups such as these ease the exchange of information and make for more effective civil disturbance planning.

When available information has been collected and the vulnerability study is complete, an assessment of the threat can be made. Although some weaknesses cannot be corrected, others may only require the careful use of resources. Plans must be made to obtain resources that are not readily available. Using the identified vulnerabilities, planners categorize these

weaknesses based on the specific countermeasures needed to offset them. An overview of the countermeasures can reveal additional weaknesses.

To be of value, threat analysis must be a continuous function. As vulnerabilities are reduced in some areas, other areas man become more vulnerable. Changes in mission, tasks, and personnel also may have an impact on the status of the current threat analysis. Failure to update a threat analysis on a regular basis or to correct or compensate for vulnerabilities can adversely affect response capabilities for civil disturbances.

INFORMATION NEEDS FOR PLANNING CIVIL DISTURBANCE OPERATIONS

- **Goals of the groups that are likely to cause or are causing civil disturbances.**
- **Times and locations of disturbances.**
- **Causes of disturbances.**
- **Identity of persons, groups, or organizations that have distinctly threatened to cause or are causing disturbances.**
- **Estimated number of people who will be or are involved in the disturbance.**
- **Likely places where crowds could assemble.**
- **Presence and location of leaders and individuals who have threatened to cause a civil disturbance.**
- **Group structure and types of activities group can carry out.**
- **Sources, types, and locations of arms, equipment, and supplies available to the group.**
- **Possible use of sewers, storm drains, and other underground systems by participants.**
- **Attitude of general populace toward groups causing civil disturbances, toward civil law enforcement authorities, and toward federal intervention.**
- **Presence of threats to utilities that serve the public.**
- **Kinds of communications and control methods used by participants and organizers.**