FM 7-100.3

Opposing Force:

Paramilitary and Nonmilitary Organizations and Tactics

Approved Final Draft
21 January 2004

HEADQUARTERS, DEPARTMENT OF THE ARMY

FOREWORD

In today's complicated and uncertain world, it is impossible to predict the exact nature of future conflict that might involve the U.S. Army. So the Army must be ready to meet the challenges of any type of conflict, in all kinds of places, and against all kinds of threats. This is the nature of the contemporary operational environment (COE), and training for such an environment requires a different type of Opposing Force (OPFOR) than that of the past.

The Deputy Chief of Staff for Intelligence (DCSINT) of the U.S. Army Training and Doctrine Command (TRADOC) is the Executive Agent for the development, management, administration, integration, and approval functions of the OPFOR Program across the Army. Thus, the TRADOC DCSINT is responsible for documenting the doctrine, organization, and capabilities of a contemporary OPFOR that is appropriate for training the Army's leaders, soldiers, and units for the COE.

In the FM 7-100 series, the TRADOC Office of the Deputy Chief of Staff for Intelligence (ODCSINT) has created a flexible baseline for an OPFOR that can be adapted to meet a variety of different training requirements in a number of different scenarios that reflect the COE. The various types of paramilitary OPFOR and nonmilitary organizations outlined in FM 7-100.3 represent a realistic composite of potential adversaries and noncombatants the Army might encounter in the real-world situations of the foreseeable future. However, the world is continually changing, as are the threats and challenges for which the Army must be prepared. The Army must remain flexible, as must the OPFOR designed to serve as a challenging sparring partner in the training environment.

This manual is approved for use in all Army training venues. However, as the contemporary OPFOR and other aspects of the COE are integrated into Army training, the TRADOC ODCSINT and the intelligence community will continue research and analysis of real-world developments and trends. The goal of this continued effort is to keep our OPFOR and our understanding of the COE truly contemporary and relevant as the world around us changes. Thus, this manual is intended to be a living document, and the ODCSINT will modify and change it as often as necessary in order to ensure its continued relevance in light of changes and developments in the COE. In anticipation of such changes, this manual will be published primarily in electronic format with only limited distribution of hard-copy, printed manuals. The electronic version is available on the Army Knowledge Online (AKO) at http://www.us.army.mil and the General Dennis J. Reimer Training and Doctrine Digital Library (ADTDL) at http://www.adtdl.army.mil. Users also need to monitor the TRADOC ADCSINT-Threats Knowledge Center on AKO for information regarding periodic updates.

MAXIE L. MCFARLAND
Deputy Chief of Staff for Intelligence
U.S. Army Training and Doctrine Command

FM 7-100.3

Field Manual
No. 7-100.3

Headquarters
Department of the Army

Opposing Force: Paramilitary and Nonmilitary Organizations and Tactics

Contents

Preface

This manual is one of a series that describes a contemporary Opposing Force (OPFOR) for training U.S. Army commanders, staffs, and units. See the Reference section for a list of the manuals in this series. Together, these manuals outline an OPFOR than can cover the entire spectrum of military and paramilitary capabilities against which the Army must train to ensure success in any future conflict.

Applications for this series of manuals include field training, training simulations, and classroom instruction throughout the Army. All Army training venues should use an OPFOR based on these manuals, except when mission rehearsal or contingency training requires maximum fidelity to a specific country-based threat. Even in the latter case, trainers should use appropriate parts of the OPFOR manuals to fill information gaps in a manner consistent with what they do know about a specific threat.

The proponent for this publication is HQ TRADOC. Send comments and recommendations on DA Form 2028 directly to the OPFOR and Threat Integration Directorate of the TRADOC Office of Deputy Chief of Staff for Intelligence at the following address: Director, OPFOR and Threat Integration Directorate, ATTN: ATIN-L-T (Bldg 53), 700 Scott Avenue, Fort Leavenworth, KS 66027-1323.

This publication is available at Army Knowledge Online (AKO) at http://www.us.army.mil and on the General Dennis J. Reimer Training and Doctrine Digital Library (ADTDL) at http://www.adtdl.army.mil. Readers should monitor those sites and also the TRADOC ADCSINT-Threats Knowledge Center on AKO for the status of this manual and information regarding updates. Periodic updates, subject to the normal approval process, will occur as a result of the normal production cycle in accordance with TRADOC regulation 25-36, paragraphs 2-17 and 4-7. The date on the cover and title page of the electronic version will reflect the latest update.

Unless this publication states otherwise, masculine nouns or pronouns do not refer exclusively to men.

Introduction

This manual is part of the FM 7-100 series that describes a **contemporary Opposing Force (OPFOR)** that exists for the purpose of training U.S. forces for potential combat operations. Other manuals in this series focus on an OPFOR that represents the forces of an artificial country called "the State," which is a regional power in its part of the world.[1] The State develops and maintains its Armed Forces and its other instruments of national power primarily with the aim of maintaining and expanding its regional dominance. The State also maintains internal security forces designed to protect the regime from internal threats, but some of these paramilitary forces are also capable of actions against external threats from regional or extraregional opponents, if necessary. The State's military and paramilitary forces may also operate in conjunction with nonstate actors.

This manual also describes other types of paramilitary forces that—unlike the State's internal security forces—are not part of a government structure. These include insurgents, terrorists, large-scale drug and criminal organizations, and private security organizations. They may operate independently or become affiliated with the State's military or paramilitary forces.

This manual also deals with other, nonmilitary entities that are not part of a government and fall under the category of noncombatants. These nongovernment, nonmilitary elements may include transnational corporations, international humanitarian relief organizations, media, small drug and criminal elements, and other civilians on the battlefield.

When a major extraregional power, such as the United States, becomes involved in a region, it may have to deal with any or all of these types of paramilitary and nonmilitary elements. It might encounter these elements individually or, more likely, in combination with other such elements or with the military forces of a regional power (the State). Whether these elements operate in concert or independently, they are an important part of the **contemporary operational environment (COE)**.

CONTEMPORARY OPERATIONAL ENVIRONMENT

The DOD officially defines an *operational environment* (OE) as "a composite of the conditions, circumstances, and influences that affect the employment of military forces and bear on the decisions of the unit commander" (JP 1-02). The *contemporary operational environment* (COE) is the operational environment that exists today

Contemporary Operational Environment (COE)

The operational environment that exists today and for the clearly foreseeable future.

[1] In specific U.S. Army training environments, the generic name of the State may give way to other (fictitious) country names such as Atlantis, Upper Flambokia, or Westland.

and for the clearly foreseeable future**.** There are some "constants" or common threads that define the general nature of this COE:

- The United States in not likely to have a peer competitor until 2020 or beyond.
- However, nations will continue to field armed forces and use these forces as a tool to pursue national interests.
- As nations use their armed forces (or other instruments of national power) in pursuit of national interests, their actions may cause U.S. intervention, either unilaterally or as a coalition partner, with or without United Nations mandate.
- Nations that believe the United States may act to counter their national interests will develop diplomatic, informational, economic, and military plans for managing U.S. intervention.
- Nations will continue to modernize their armed forces within the constraints of their economies, but in ways that may negate U.S. overmatch.
- Advanced technology will be available on the world market for a wide variety of nation-state and non-state actors.
- Non-state actors will play an important role in any regional conflict—as combatants or noncombatants.
- All combat operations will be significantly affected by a number of variables in the environment beyond simple military forces.

Thus, one of the constants is that there are variables. Those "variables" in the COE result in a number of different OEs that can occur in specific circumstances or scenarios.

CRITICAL VARIABLES

Any OE, in the real world or in the training environment, can be defined in terms of eleven critical variables. While these variables can be useful in describing the overall (strategic) environment, they are most useful in defining the nature of specific OEs. Each of these "conditions, circumstances, and influences" and their possible combinations will vary according to the specific situation. In this sense, they are "variables." These variables are interrelated and sometimes overlap. Different variables will be more or less important in different situations. Each OE is different, because the content of the variables is different. Only by studying and understanding these variables—and incorporating them into its training—will the U.S. Army be able to keep adversaries from using them against it or to find ways to use them to its own advantage.

Critical Variables of COE

- Nature and Stability of the State.
- Regional and Global Relationships.
- Economics.
- Sociological Demographics.
- Information.
- Physical Environment.
- Technology.
- External Organizations.
- National Will.
- Time.

Nature and Stability of the State

It is important to understand the nature and stability of the state (or states) with which or in which the conflict takes place. Study of this variable measures how strong or weak a country is and determines where the real strength of the state lies; it may be in the political leadership, the military, the police, or some other element of the population. Understanding this variable will allow U.S. forces to better understand the nature of the military campaign and the true aims of an enemy campaign, operation, or action. It also helps determine what kinds of threats may be present in a particular country. The real threat to U.S. forces may come from elements other than the military.

Regional and Global Relationships

Nation-states and/or non-state actors often enter into relationships, which can be regional or global. These partnerships support common objectives, which can be political, economic, military, or cultural. An actor's membership or allegiance to such a relationship can determine its actions of support and motivation. Virtually all conflict will occur with alliances and coalitions, some involving the United States and some involving its adversaries. When actors create regional or global alliances, it can add to their collective capability and broaden the scale of operations and actions.

As the world moves away from the traditional long-term, fixed alliances of the past, regional and global relationships are much more fluid and unpredictable. The choice of a state to be nonaligned does not mean that it will not become involved in a conflict or crisis. It simply means that the state does not make a commitment to another state, alliance, or cause before a situation arises. This lack of precommitment makes it difficult to predict how actors and forces may align when a situation does arise. Alliances can form or change rapidly, even during the course of an operation or campaign.

Economics

The economic variable establishes the boundaries between the "haves" and the "have-nots." This gap of economic differences among nation-states and other actors can cause conflict. Economic superiority, rather than military superiority, may be the key to power or dominance within a region. However, economic position often represents a nation or non-state actor's ability to buy military technology or to conduct prolonged operations.

Economics help define the relationship between a nation or non-state actor and other actors at the regional or global level. These regional or global economic relationships could result in military or political assistance.

Sociological Demographics

The demographics variable includes the cultural, religious, and ethnic makeup of a given region, nation, or non-state actor. Extreme devotion to a particular cause or significant hatred of a particular group may provide an enemy with an unshakable will and a willingness to die for the cause. U.S. forces may also find that large segments of the population around them are sympathetic to the same cause as the enemy force. The needs of the local population can create heavy demands on U.S. military units, particularly their supply and medical systems.

Refugees and internally displaced persons may increase the complexity of the environment. The enemy may use civilians as shields or obstacles or as cover for hostile intelligence services.

Information

Media and other information means can make combat operations transparent to the world, visible to all who have access to data. Various actors seek to use perception management to control and manipulate how the public sees things. They will exploit U.S. mistakes and failures and use propaganda to sway the local population to support their cause. Media coverage can impact on U.S. political decision making, international opinion, or the sensitivities of coalition members.

Even without sophisticated sensors and information systems, actors native to the area or region often have greater situational awareness than U.S. forces. Various actors are able to access commercial systems (such as satellite communications and imagery) for the larger picture. For a more detailed view, they can use human networks operating over normal telephone lines or with cellular telephones to maintain situational awareness.

Physical Environment

The main elements in the physical environment are terrain and weather. Potential enemies clearly understand that less complex and open environments favor a U.S. force with its long-range, precision-guided weapons and sophisticated reconnaissance capability. So they will try to avoid the types of operations and environments for which such U.S. forces are optimized. They will try to operate in urban areas and other complex terrain and in weather conditions that may adversely affect U.S. military operations and mitigate technological advantages.

Technology

The technology that nations or non-state actors can bring to the OE includes what they can develop and produce, as well as what they could purchase and import. Access to technological advances available on the global market is slowly eating away at the technological advantage the United States has enjoyed in the past.

It is likely that some high-end forces in a particular region of the world could field a few systems that are more advanced than those of the U.S. force deployed there. Easy access to new technology allows potential adversaries to achieve equality or even overmatch U.S. systems in selected niche areas. Many countries are trying to acquire relatively low-cost, high-payoff, new technologies. In addition, upgrades and hybridization allow older systems to compete with more modern capabilities, thus neutralizing the technical advantage of many modern forces. In urban areas or other complex terrain, less advanced systems may still find effective uses. Various actors may find adaptive and innovative ways of using systems for other than their originally intended applications.

External Organizations

When the U.S. Army goes into a failed state or into areas torn by conflict, it is likely to find international humanitarian relief organizations at work there. These external organizations continue to grow in influence and power, as well as

in willingness to become involved in crisis situations that were previously purely military operations. These external organizations can have both stated and hidden interests and objectives that can either assist or hinder U.S. mission accomplishment. The presence of transnational corporations operating in a country or region can also place added pressure on U.S. forces to avoid collateral damage to civilian life and property. U.S. forces may have to divert troops and resources from their assigned missions to conduct rescues or provide security for various external organizations.

National Will

The variable of national will reflects how much each country's people and government are behind what the military or paramilitary forces are doing. This can influence the objectives of a conflict, its duration, and the conditions for ending it.

A country will try to attack its opponent's national will and still preserve its own. Clearly, most foreign countries view U.S. national will as a point of vulnerability. Thus, a potential adversary may perceive the collective will of his people as a comparative advantage against the United States.

History has proven that battlefield victory does not always go to the best-trained, best-equipped, and most technologically advanced force. Victory often goes to the side that most wants to win, needs to win, and is willing to sacrifice to do so.

Time

In most cases, potential opponents of the United States view time as being in their advantage. When U.S. forces have to deploy into the area over long time and distance, the opponent can use this time to adjust the nature of the conflict to something for which the U.S. forces are not prepared.

First, the opponent will try to control the entry of U.S. forces into the area. If access control fails, the enemy still has the opportunity to oppose lightly equipped U.S. early-entry units and try to prevent full deployment of the rest of the force. The opponent will try to speed up the tempo, to rapidly defeat its local or regional enemy or to defeat U.S. early-entry forces before the United States can deploy overwhelming military power. If that fails, the opponent will try to prolong the conflict and to outlast the U.S. will to continue.

Military Capabilities

Military capabilities of a nation-state or non-state actor may be the most critical and the most complex variable that affects military operations. However, the military variable does not exist in isolation from the other variables that help determine the overall OE. It interacts with the other variables, and all the other variables can affect military capabilities. Potential enemies can use any or all of these factors against the Army as it tries to accomplish its missions in various parts of the world or in various training environments.

REAL WORLD

In the real world, the COE is the entire set of conditions, circumstances, and influences that U.S. Armed Forces can expect to face when conducting military operations to further the national interests of the United States, its friends, and allies. The COE is "contemporary" in the sense that it does not represent conditions that

existed only in the past or that might exist only in the remote future, but rather those conditions that exist today and in the clearly foreseeable, near future. This COE consists not only of the military and/or paramilitary capabilities of potential real-world adversaries, but also of the manifestations of the ten other variables that help define any OE.

TRAINING

In training environments, the COE is the OE created to approximate the demands of the real-world COE and to set the conditions for desired training outcomes. This involves the appropriate combination of an OPFOR (with military and/or paramilitary capabilities representing a composite of a number of potential adversaries) and other OE variables in a realistic, feasible, and plausible manner. Other, non-state actors that fall in the category of nonmilitary forces or elements are not part of the OPFOR, but could be part of the COE used in the training environment. The purpose of the COE in training simulations is to produce the necessary training outcomes.[2]

Even in the COE for training, it is possible to speak of an overall COE that addresses the qualities of virtually any OE in which the units or individuals being trained might be called upon to operate. In this sense, there are the same "constants" as in the real-world COE.

INTERACTION AND LINKAGE OF VARIABLES

The variables of the COE do not exist in isolation from one another. The linkages of the variables cause the complex and often simultaneous dilemmas that a military force might face. In order to provide realistic training, training scenarios must try to simulate this synergistic effect to the maximum degree that is feasible.

The COE is not just about the OPFOR. The COE variables and their interaction provide the robust environment and context for OPFOR operations. The complexity of the specific OE in training can be adjusted to keep it appropriate for the required training objectives and the training state of various U.S. Army units.

ADAPTIVE AND CHANGING

The nature of the COE is adaptive and constantly changing. As the United States and its military forces interact with the COE in a real-world sense, the OE changes. As the Army applies the lessons learned from training in a COE setting, the OPFOR and potential real-world adversaries will also learn and adapt.

The development of the COE for training started with research to develop an understanding of the real-world COE and trends that affect military operations. Then, taking into consideration the desired training outcomes and leader development goals, the authors of the FM 7-100 series proceeded to document an OPFOR doctrine and structure that reflect the real-world COE, and the Army began integrating this OPFOR and other COE variables into training scenarios. Meanwhile, the authors of the FM 7-100 series are continuing to research the real-world COE and to mature the OPFOR and the COE in training in order to

[2] The same type of COE conditions can be created to support some combat development activities that do not require simulation of a specific real-world potential adversary. However, some combat development activities may require portrayal of an OE that extends further into the future than is typical for the COE.

provide a richer, appropriately challenging training environment and keep the OPFOR and the COE truly “contemporary.”

ENEMY, THREAT, AND OPFOR

Before going further into the COE, the contemporary OPFOR, and the intended uses of this manual, it may be useful to define some key terms and the distinctions among them. It is important to distinguish among the terms *enemy*, *threat*, and *OPFOR* and to use them correctly.

ENEMY

The U.S. Army defines *enemy* as "the individual, group of individuals (organized or not organized), paramilitary or military force, national entity, or national alliance that is in opposition to the United States, its allies, or multinational partners." In other words, the *enemy* is whoever is actually opposing the United States in a particular conflict.[3] Thus, this term is synonymous with adversary or opponent.

THREAT

A potential adversary is sometimes designated as a threat. In this sense, the Army defines *threat* as "any specific foreign nation or organization with intentions and military capabilities that suggest it could become an adversary or challenge the national security interests of the United States or its allies." To be a threat, a nation or organization must have both the *capabilities* and the *intention* to challenge the United States. Once hostilities actually begin, the threat becomes the enemy.

OPPOSING FORCE

An *Opposing Force (OPFOR)* is a training tool that should allow the U.S. Army to train against a challenging and plausible sparring partner that represents the wide range of possible opponents the Army could face in actual conflict. It enables training of all arms of the Army and prepares the Army for potential combat operations.

During the road to war leading up to events in a training scenario, the OPFOR may play the role of a "threat" (potential enemy) that is on the verge of becoming an enemy. However, the actual training event usually deals with a state of hostilities. Thus, once hostilities begin in the training event, the OPFOR acts as the "enemy" of the U.S. force in the training environment.[4]

---

[3] This definition of *enemy* is from the U.S. point of view. After this Introduction, the chapters of this manual address their topics from the OPFOR point of view. So, *friendly* refers to the OPFOR and its allies, and *enemy* refers to the enemy of the OPFOR, which may be an opponent within its own country or region or an extraregional opponent (normally the United States or a U.S.-led coalition).

[4] From the OPFOR point of view, its leadership plans and develops forces and methods to deal with one or more threats to its own interests, goals, or survival. For a nation-state OPFOR, these threats can be internal, regional, or extraregional. For a non-state paramilitary OPFOR, the threats are different. (For a drug or criminal organization, for example, the threats include law enforcement agencies.) Unless the paramilitary organization can infiltrate or co-opt the threatening element, that element becomes the "enemy" as soon as the paramilitary organization begins the actions or activities that characterize it.

During the Cold War period, the Army employed OPFORs based on specific real-world threats. However, the Army needs a different type of OPFOR to meet its training requirements for the COE.

Cold War OPFOR

When the Army established its OPFOR program in 1976 with Army Regulation 350-2, it could hardly have envisioned today's computerized constructive and virtual simulations, or even the evolving requirements of live simulations. It defined an *OPFOR* simply as "an organized force created by and from U.S. Army units to portray a unit of a potential adversary armed force." Thus, all OPFORs were originally threat-based, in the sense that they replicated the forces, capabilities, and doctrine of a particular country officially recognized as a threat or potential adversary. In the midst of the Cold War, the 1976 regulation identified only one potential adversary against which to train: the Soviet Union; in 1978, a revision of the regulation added North Korea as a second threat for replication by an OPFOR. Over time, the Army developed other OPFORs to replicate other threats emerging in places ranging from Latin America and Southwest Asia.

In its time, the threat-based OPFOR served the Army very well, particularly for units targeted against specific threats. The benefits of this training were borne out, for example, in Operation Desert Storm. Techniques and doctrine, including deep attack and the intelligence preparation of the battlefield, developed to cope with specific threats and honed against the OPFOR, enabled the Army to achieve decisive results on the battlefield. However, the operational environment (OE) is dynamic, and the pace of that dynamism has increased with the end of the Cold War and the rapid advancement of information technology.

Contemporary OPFOR

Contemporary OPFOR

A plausible, flexible military and/or paramilitary force representing a composite of varying capabilities of actual worldwide forces, used in lieu of a specific threat force, for training and developing U.S. forces.

Training U.S. forces for the COE requires a different kind of OPFOR from that of the past. The contemporary OPFOR must be less predictable and not based on the armed forces of a particular country. In today's world, the U.S. Army must be prepared to go into any OE and perform its full range of missions. It must be ready to do so in the face of a wide variety of possible threats and at the same time be prepared to deal with third-party actors that may have other interests. Not all threats are purely military in nature. Therefore, the U.S. Army now defines an *OPFOR* as "a plausible, flexible military and/or paramilitary force representing a composite of varying capabilities of actual worldwide forces, used in lieu of a specific threat force, for training and developing U.S. forces."

Thus, in some training environments, a paramilitary force alone may be the OPFOR. In other cases, paramilitary forces may act as part of a larger OPFOR, in loose affiliation with military forces, or separately from the military forces present within a particular training environment. These relationships depend on the scenario, which is driven by training requirements.

Various agencies and experts have different lists of real-world threats the United States might have to face. If the U.S. Army were to pick any one of these threats as *the* threat against which to train, that threat would almost certainly not be the one it would actually fight. What is needed is a composite that is representative of the full range and variety of possible threats and OEs. It must have a bit of everything—it could be virtually anybody, anywhere. Therefore, this manual defines this representative composite in a way that is flexible enough to fit the most demanding U.S. Army training requirements and provides a framework for training that creates the leaders, soldiers, and unit skills necessary for success on the next battlefield.

CONTEMPORARY THREATS AND OTHER ACTORS

There are many types of actors or participants in today's complex world environment. Some of the actors are countries (also called nation-states) and some are not. Nation-states are still dominant actors. However, some power is shifting to nontraditional actors and transnational concerns. There are many potential challenges to traditional concepts like balance of power, sovereignty, national interest, and roles of nation-state and non-state actors.

Of course, not all actors are threats. To be a threat, a nation or organization must have both the capabilities and the *intention* to challenge the United States. The capabilities in question are not necessarily purely military, but encompass all the elements of power available to the nation or organization.

NATION-STATE ACTORS

Nation-states fall into four basic categories according to their roles in the international community. The categories are core states, transition states, rogue states, and failed or failing states.

The category of *core states* includes more than half of the nearly 200 countries in the world today. These are basically democratic (although to varying degrees) and share common values and interests. Within this larger group, there is an "inner core" of major powers. These are the advanced countries, including the United States, that generally dominate world politics. Most conflict with global consequences will involve the core states in some fashion or another.

Transition states are other larger, industrial-based countries—mostly emerging regional powers—that are striving to become major powers. High-end transition states are moving from an industrial-based society to an information-based society. Low-end transition states are seeking to move from an agricultural-based society to an industrial base. As states try to make this transition, there are cycles of political stability and instability, and the outcome of the transition is uncertain. Some transition states may successfully join the ranks of core states and even become major powers within that context; others may become competitors.

Rogue states are those that are hostile to their neighbors or to core states' interests. These countries can sponsor international terrorism or even confront U.S. military forces operating in the region. *Failed or failing states* are fragmented in such a way that a rule of law is absent; their instability is a threat to their neighbors and the core states.

Countries can move from one category to another, as conditions change. Sometimes countries join together in multinational alliances and coalitions. Together, they have more strength and can become a power to be reckoned with.

NON-STATE ACTORS

Non-state actors are those that do not represent the forces of a particular nation-state. Such non-state elements include rogue actors and third-party actors.

Like rogue states, *rogue actors* are hostile to other actors; however, they may be present in one country or extend across several countries. Examples include insurgents, guerrillas, mercenaries, and transnational or subnational political movements. Particular sources of danger are terrorists and drug-trafficking or criminal organizations, since they may have the best technology, equipment, and weapons available, simply because they have the money to buy them. These non-state rogue actors may use terror tactics and militarily unconventional methods to achieve their goals.

Third-party actors may not be hostile to other actors. However, their presence, activities, and interests can affect the ability of military forces to accomplish their mission when operating in a foreign country. These actors can be refugees, internally displaced persons, and other civilians on the battlefield, including international humanitarian relief agencies, transnational corporations, and the news media. These individuals and groups bring multiple sources of motivation, ideology, interests, beliefs, or political affiliations into consideration. They may be sources of civil unrest. Their presence may require military forces to consider the potential impacts of traffic congestion, demonstrations, sabotage, and information manipulation.

REAL-WORLD AND TRAINING CONSIDERATIONS

When U.S. forces become involved in a particular country or region, they must take into account the presence and influence of these various types of threats and other actors. In a training environment, an OPFOR can represent a composite of those nation-state or non-state actors that constitute military and/or paramilitary forces that could present a threat to the United States or its allies. Other, non-state actors that fall in the category of nonmilitary forces or elements are not part of the OPFOR, but could be part of the COE used in the training environment.

BASELINE OPFOR AND NONMILITARY ACTORS

This manual introduces the baseline organizations and tactics for various types of paramilitary forces and nonmilitary elements related to the COE and the contemporary OPFOR. It is applicable to the entire training community, including all of the combat training centers (CTCs), the TRADOC schools, and units in the field.

The OPFOR is a training tool, although it may be used for other purposes. It must be tailored to meet training requirements, but it also must be a challenging, uncooperative sparring partner, capable of stressing any or all battlefield operating systems of the U.S. force. Nonmilitary elements are also an important part of the training environment, and the replication of the role they play in the COE is also a training tool. Trainers need to consider the total OE in order to de-

termine which paramilitary and nonmilitary elements are appropriate to be present and to what degrees in a particular training environment.

FLEXIBILITY

In the baseline presented in this manual, the FM authors often say that a particular paramilitary or nonmilitary element "may" be able to do something or "might" or "could" do something. The baseline includes examples of organizations with various sizes and capabilities. Such descriptions give scenario writers considerable flexibility in determining what capabilities a particular entity might have at a given point in time or a given place on the battlefield—in a particular scenario.

The composite examples provided in this baseline may meet the requirements for OPFORs and nonmilitary elements in many U.S. Army training environments. For cases that require an OPFOR or nonmilitary element with characteristics different from those described in this manual, this baseline provides a framework from which trainers can develop an organization with capabilities appropriate for their particular training requirements.

The OPFOR and nonmilitary elements must be flexible enough to fit various training requirements. They must be scalable and adjustable. Depending on the training requirement, the OPFOR or the nonmilitary element may be a large, medium, or small organization.

For paramilitary forces, this manual provides examples of possible organizational structures, sometimes including personnel strengths in various subordinate elements. In some cases, the examples show a relatively small organization of a particular type. For larger organizations, in most cases, trainers could increase the personnel strength numbers by a factor of up to three, if necessary. The presence or numbers of the various subordinate elements shown, and their relative personnel strengths, depend on the training requirement.

Among the nonmilitary elements discussed in the Noncombatants chapter, this manual provides an example organizational structure only in the case of a humanitarian relief organization. Again, this structure is scalable and adjustable, according to the training requirement.

ADAPTABILITY

This manual describes each type of paramilitary OPFOR as a thinking, adaptive organization. In each case, it describes how the OPFOR is motivated and thinks, whether it is facing threats and challenges within its own country or region or is forced to deal with an extraregional power such as the United States. This thinking determines basic OPFOR strategy, its organizational structure, and its specific actions and activities. It also determines how the paramilitary OPFOR would interact with other nation-state or non-state actors that may be present in the COE.

Just because the U.S. force knows something about how the OPFOR has fought in the past does not mean that the OPFOR will always continue to fight that way. A thinking OPFOR will learn from its own successes and failures, as well as those of its potential enemies. It will adapt its thinking, its makeup, and its way of fighting to accommodate these lessons learned. It will continuously look for innovative ways to deal with all possible opponents—including the United States

novative ways to deal with all possible opponents—including the United States and its armed forces, if that becomes necessary.

Generally, paramilitary forces are dealing with an enemy force of superior military strength, at least initially. (Possible exceptions could be in the case of a large and powerful drug or criminal organization or of internal security forces employed against internal threats.) This means that their normal modes of operation are to avoid direct, head-to-head confrontation with superior forces. They must use whatever capabilities they have in adaptive, "unconventional" ways and at a time and place of their own choosing. They choose conditions that are most favorable to their own success and preclude the enemy from being able use all of his capabilities or exploit them to the full extent. In other words, they must adapt their capabilities and tactics to fit the situation.

Whether or not they already had to use "adaptive" approaches against local or regional opponents, all paramilitary forces will have to adapt or continue to adapt when a U.S. force becomes involved in their country or region. If possible, they will use whatever means are available to preclude this outside intervention. During the course of conflict, they will make further adaptations, based on experience and opportunity.

INITIATIVE

For each of the types of paramilitary forces, this manual, therefore, describes the organizations and tactics of a flexible, thinking, adaptive OPFOR. Unlike a purely military OPFOR, a paramilitary OPFOR may not have a formalized doctrine, especially when it comes to dealing with the United States. Rather than having a rigid, prescriptive doctrine, paramilitary organizations typically allow subordinates considerable freedom for bold, creative initiative in any situation.

The types of paramilitary OPFOR that U.S. units may encounter in various training venues will not have a rigid doctrine that they apply blindly or unthinkingly, but will use their experience and assessments to interpolate from a general doctrinal baseline in light of specific situations. Doctrine guides OPFOR actions in support of the paramilitary organization's objectives; OPFOR leaders apply it with judgement and initiative. In general, the types of contemporary OPFOR derived from the baseline presented in this manual will be inherently unpredictable and difficult to template as they adapt and attempt to create opportunity.

SUMMARY

The COE is extremely fluid, with rapidly changing regional and global relationships. New actors—both nations and non-state actors—are constantly appearing and disappearing from the scene. Many of the key actors in the COE do not represent the regular military forces of a particular country. This manual describes the organizations and actions typical of the most common types of paramilitary and nonmilitary actors. As the real-world geopolitical situation continues to change, the FM authors will update this manual to keep pace with the evolving capabilities and methods of the various actors.

In a particular training environment, as in a real-world situation, the operational environment may not have all the different types of paramilitary forces and nonmilitary elements described in this manual. However, the manual presents a

composite of the various types of forces that may exist in real-world countries or regions, or on an international scale. U.S. forces must be prepared to encounter and deal with any or all of these types, which may operate in conjunction with regular military forces or independent of them. All these elements, or a combination of them, may be part of any contemporary operational environment.

Chapter 1

Regional and Global Framework

This chapter describes the role of paramilitary and nonmilitary organizations within the regional and global framework. While some of these organizations may have global reach, their activities are more commonly confined to the particular region of the world in which they are located. In either case, these organizations may come into conflict with an extraregional power, such as the United States. They may participate in such a conflict with or without links to a regional power (called the State) that is also at war with the extraregional power.

PARAMILITARY AND NONMILITARY ORGANIZATIONS

1-1. Figure 1-1 depicts the various categories and subcategories of paramilitary and nonmilitary organizations. Paramilitary organizations may be either regular, government forces or irregular, nongovernment forces. Most nonmilitary organizations are not associated with the government and fall under the category of noncombatants.

Paramilitary	Regular	Internal Security Forces	Government
	Irregular	Insurgents	Nongovernment
		Terrorists	
		Large-Scale Drug and Criminal Organizations	
		Private Security Organizations	
Nonmilitary	Noncombatant	Transnational Corporations	
		International Humanitarian Relief Organizations	
		Media	
		Drug and Criminal Elements	
		Other Civilians on the Battlefield (COBs)	

Figure 1-1. Categories of Paramilitary and Nonmilitary Organizations

1-2. *Paramilitary organizations* are those organizations that are distinct from the regular armed forces but resemble them in organization, equipment, training, or purpose. Basically, any organization that accomplishes its purpose, even partially, through the force of arms can be considered a paramilitary organization. These organizations can be part of the government infrastructure or operate outside of the government or any institutionalized con-

trolling authority. The primary paramilitary organizations are internal security forces, insurgents, terrorists, and large-scale drug and criminal organizations. Of these, the internal security forces are regular, government forces and the remaining types of paramilitary forces are irregular, nongovernment forces.

1-3. *Nonmilitary organizations* are those organizations that ostensibly do not rely on the force of arms for accomplishing their purposes. Therefore, they do not resemble military forces in their organization, equipment, training, or purpose. These forces can include the media, international humanitarian relief organizations, transnational corporations, some drug and criminal elements, or other civilians on the battlefield (COBs).[1] These groups generally fall under the heading of noncombatants. It should be noted that, while considered noncombatants, some of the nonmilitary elements may be armed. Also, some large transnational corporations might even have their own private security forces.

WAR AND ARMED CONFLICT

1-4. Even more so than with State forces, the organizations behind nongovernment paramilitary forces make a differentiation between *war* and *armed conflict*, with war being the more comprehensive of the two. For these organizations, armed conflict may not even be the principal form of struggle in war. In addition to a paramilitary force, such organizations typically have other instruments of power: diplomatic-political, informational, and economic.

1-5. The diplomatic-political part depends on the organization's cause or motivation. Each organization has some sort of leadership body that sets its policies and objectives, directs the use of all instruments of power (including negotiations with other entities) to those ends, and determines when those ends are achieved. Even the armed actions of a paramilitary organization often serve as means of achieving informational or psychological effects rather than military-style objectives. The economic part may be strong or weak (or external to the organization), but each organization has to have some economic power or support base. Because these instruments of power do not represent the forces of a nation, other nations may not consider their application to constitute "war," although the paramilitary organization may consider itself at war against a particular state or condition.

1-6. A paramilitary organization's struggle for a particular cause may sometimes coincide in time and space with an open and declared state of war between opposing nations. Paramilitary forces are likely to seize the opportunity to step up their activities in the country in which they are operating, if that country's forces are otherwise occupied in a conflict with the State. This is particularly true of insurgents. However, terrorists and drug and criminal organizations may also flourish in such an environment.

1-7. The State may help finance, train, and/or equip insurgent or terrorist groups operating against its regional opponent. If an extraregional force be-

[1] Media may include government-controlled media as well as independent, "free" media. International humanitarian relief organizations are sometimes referred to as nongovernmental organizations (NGOs) or private voluntary organizations (PVOs).

comes involved, the State may continue or begin to support such paramilitary forces in order to draw some of that opponent's assets away from the war with the State.

1-8. Drug and criminal organizations, with or without State support or ties, will take advantage of the turmoil of war in order to pursue their own interests, primarily for financial gain. However, they would not be averse to accepting financial aid from the State, as long as they were assured that the State would not interfere with their own operations after the war. Criminal organizations may also steal weapons or supplies from the extraregional force in order to sell them to insurgent or State forces.

1-9. Nonmilitary organizations, such as media and humanitarian relief agencies, often become involved in a region because of the affects of armed conflict. Civilians on the battlefield only occur when there is a battlefield. Indeed, the extraregional force may bring COBs to the battlefield in the form of contractors needed to support its operations.

NATURE OF THE CONFLICT

1-10. Paramilitary and nonmilitary organizations may become involved in conflict with a superior extraregional force in conjunction with major military actions going on in their region of the world. Even within such a context, they may still be pursuing their own interests and objectives and operating independently from the regular military forces of the State or any other country. If their own interests and objectives coincide with or are at least compatible with those of the State, they may choose to become affiliated with the State in order to defeat or expel a common adversary. For the same reason, they may establish links with other paramilitary or nonmilitary organizations of various types.

1-11. Paramilitary forces may engage extraregional forces, such as the U.S. Army, on their own initiative and under conditions of their own choosing. Even more so than the military forces of a State, paramilitary forces are likely to be overmatched in conventional power by such an adversary. Therefore, such forces are likely to use many of the same types of "adaptive" approaches as outlined in FMs 7-100, 7-100.1, and 7-100.2 for regular military forces of the State. They will also add some adaptive approaches of their own.

1-12. The State and its armed forces include in their planning and execution the use of paramilitary forces. It is important to stress that, with the exception of internal security forces, those paramilitary organizations that are not part of the State structure, and do not necessarily share the State's views on national security strategy. Nevertheless, the State will attempt to use these additional forces to further its strategic goals.

1-13. Nonmilitary organizations will almost inevitably be present in the area of conflict. Combatants, including military and/or paramilitary forces, will attempt to use the presence of these noncombatants to their advantage. If possible, they will use these conditions to help change the nature of the conflict to something for which the extraregional enemy is not prepared.

BASIC PRINCIPLES OF PARAMILITARY ORGANIZATIONS

1-14.Paramilitary organizations are groups of individuals united to attain a common goal by force of arms. In pursuance of that goal, they generally subscribe to certain basic principles that guide their organization and actions. Since paramilitary forces in many ways resemble military forces, some of these principles are very similar to basic military principles. In some cases, however, they are tailored to specifically address the considerations of paramilitary forces and their goals. Depending on the type of organization, and its individual goals and motivations, some or all of the following principles may be adhered to in varying degrees.

Basic Principles

- Discipline.
- Perseverance.
- Legitimacy.
- Aggressiveness.
- Mobility.
- Initiative.
- Flexibility.
- Adaptive Use of Available Technology
- Concentration.
- Effective Coordination.
- Surprise and Audacity.
- Preservation of Combat Effectiveness.

DISCIPLINE

1-15. Discipline is the ability to put the goals of the organization ahead of individual needs. Members demonstrate discipline while living and operating in hostile environments for lengthy periods, and even years, often without a dedicated support structure. Additionally, the organization's leaders rely upon the discipline of members to operate in small groups and follow mission-type orders. The principle of discipline is continually reinforced through indoctrination.

PERSEVERANCE

1-16. Perseverance is the long-term commitment to keep fighting until the organization accomplishes its goal. Organizations must develop an overall, integrated plan to achieve long-term goals or, as a minimum, to achieve short-term goals that support the attainment of long-term goals. Ultimately, the long-term goals and victory may be defined by mere survival until the enemy withdraws—a process that may entail decades or generations. Organizations will achieve their goals if they persevere longer than the enemy. The enemy may attempt to resolve issues within a timetable, while the paramilitary organization rests, refits, and prepares itself to continue the struggle until it is over.

LEGITIMACY

1-17. Legitimacy is a condition by which a group of people confers authority upon others. In the short term, an organization's members may confer authority on themselves without regard to the local population's political structure or local goals. It is not necessary that this authority be derived from formal laws but simply that the organization's actions are acceptable and justifiable under existing conditions. The members organize and recruit others to their cause. Until this leadership gains acceptance from a larger segment

of the population, however, it confers legitimacy upon itself. Over time, the organization must gain legitimacy from the domestic populace and official recognition from external states and/or organizations in order to accomplish long-term goals. Once established, organizations must sustain the legitimacy of their causes, their leadership, and their actions. However, legitimacy is also key for the enemy's success; therefore, they also attempt to degrade the legitimacy of the enemy.

AGGRESSIVENESS

1-18. Aggressiveness is the principle of the offensive spirit. Paramilitary forces want to dominate the environment, and are able to do so through offensive actions. Organizations must demonstrate aggressiveness down to the individual level. The leadership relies on its members to maintain the initiative through aggressive actions. A less capable group can defeat a highly trained and well-equipped enemy by employing the principle of aggressiveness. However, aggressiveness must be tempered with patience, waiting for the right opportunity to take aggressive action.

MOBILITY

1-19. Mobility is the ability to move virtually undetected and unconstrained within areas controlled or occupied by the enemy. One way to achieve this is by blending in with the population and maintaining anonymity. When mobility through anonymity is unattainable, forces use secrecy in an effort to evade detection and confrontation with the enemy. Seemingly impassable terrain should be used as avenues of approach to accomplish what, to the enemy, seems impossible. Sometimes, as in urban combat, a force may use masses of people or animals, and corridors through them, in the same manner as terrain and obstacles. The enemy may not expect forces to have great mobility or he may be unable to track movement of group members. In-depth knowledge of terrain facilitates mobility. A paramilitary force may initially have an advantage over the enemy regarding knowledge of terrain. It should try to exploit this advantage in order to reposition assets or conduct bold offensive actions. A high degree of mobility enables paramilitary forces to use available combat power with maximum effect at the decisive time and place on the battlefield.

INITIATIVE

1-20. Initiative forces the enemy to react to the actions of the paramilitary force. Success in battle goes to the side that conducts itself more actively and resolutely. Initiative implies that friendly forces, not the enemy, control the environment. Initiative allows the leadership to make and implement bold decisions and to establish or change the terms of the confrontation. It allows subordinate leaders to take advantage of new developments immediately. It allows paramilitary forces to overcome a position of relative operational inferiority by creating conditions of local superiority. Initiative also takes advantage of exploiting the enemy's restrictive rules of engagement (ROE).

FLEXIBILITY

1-21. Flexibility is the ability to conduct activities anywhere within the target area, regardless of weather, terrain, or other conditions in the operational environment. When operating within their own region, personnel of paramilitary forces are already acclimated and are intimately familiar with the terrain, indigenous resources, and the populace. This familiarity, coupled with initiative, allows them to adapt rapidly to operate under any conditions and to take advantage of fleeting windows of opportunity.

1-22. The lack of rigidity in paramilitary force structures—particularly in irregular forces—facilitates flexibility in their employment. Such organizations can easily be tailored to a particular task under particular conditions.

ADAPTIVE USE OF AVAILABLE TECHNOLOGY

1-23. Paramilitary forces, while similar to a regional adversary in overall power, may not be able to match such an enemy in each aspect of technology. This means that they must use all technology available to them, sometimes in adaptive or innovative ways. Forces take advantage of opportunities to upgrade equipment or ordnance primarily through captured equipment, the black market, or outside support. Additionally, low-technology solutions could be used against an enemy's high-technology systems. For example, a force may use antitank grenade launchers or even small arms fire against helicopters.

CONCENTRATION

1-24. For paramilitary forces, concentration is the ability to mass the effects of whatever assets are available to them. Concentration allows smaller forces to achieve comparatively greater gains. Concentration of effort at the decisive time and place is critical to success. As soon as it has accomplished that particular mission, the paramilitary force immediately disperses again. The need for concentrating effects from dispersed locations stems from the necessities of operating with relatively few personnel and without an extensive logistics system.

EFFECTIVE COORDINATION

1-25. Effective coordination ensures success through the coordinated efforts of all the forces participating in an action. Leaders must closely coordinate the roles of many diverse elements to ensure the mutual support of all elements involved. They initially indoctrinate members of their organizations to ensure they understand the goals of the organization. They use simple, understandable language so that all subordinates comprehend their orders and the reasons for them. They conduct the majority of command and control (C^2) in person or through trusted members. Personal contact is the preferred means of conducting coordination. Other means include written messages, voice communications, and the Internet.

SURPRISE AND AUDACITY

1-26. Surprise is striking the enemy at a time and place where he is not expecting it or in a manner for which he is unprepared. It is demonstrated by being unpredictable and cunning and by conducting deception activities. Surprise delays the enemy's reactions, causes delays in his responses, and confuses his

command and control. It allows paramilitary forces to accomplish more with fewer assets. They may achieve surprise against a prepared enemy through deception activities used in conjunction with operations security (OPSEC). These measures are used to prevent indicators of friendly intentions from being identified, and to not give forewarning of a planned overt action, or a covert or clandestine action.

1-27.Surprise may be achieved by changing tactics or the intensity of actions without warning the enemy. It delivers victory as a result of timing, boldness, and concentration. For example, friendly forces may suddenly conduct a series of ambushes after conducting security operations for a long period. The adaptation of weapons for use other than their intended purpose can be used to great effect.

1-28. Modern warfare requires great emphasis on the speed and timing of operations. Paramilitary forces usually have the luxury of being able to anticipate enemy actions, which are mostly offensive in nature. Actions of the paramilitary forces are rapid, deliberate, and well-planned in advance to exploit enemy weaknesses and vulnerabilities when most advantageous to friendly forces.

1-29. Audacity is the ability of the force to take bold actions without regard to normal political and legal considerations. It is similar to surprise, because both actions are conducted in an unexpected way. A simple plan boldly executed is likely to succeed with minimum risk to the mission. Audacious, calculating commanders who are willing to take risks based on the importance of the target are likely to succeed.

PRESERVATION OF COMBAT EFFECTIVENESS

1-30. Paramilitary forces use all the above principles to enhance their combat effectiveness. However, the preservation of effectiveness equals sustainment. This is an essential part of all activities. Paramilitary forces seek to forecast materiel requirements for their activities in the earliest stage of planning, in order to provide the needed supplies prior to execution. Planners anticipate the specific types of equipment or ordnance required for future actions. Forces may pre-position equipment and supplies in the vicinity of a target so that they can infiltrate a target area by blending in with noncombatants and then arm themselves just prior to the action. Such methods can ensure rapidity and secrecy in all activities.

1-31. Since the majority of support may not come from a nation-state, support must be attained elsewhere. A paramilitary force may steal, capture, extort, purchase, or fabricate equipment and supplies, or it may solicit and accept donations of funds. It usually depends upon internal support from the local population and from sympathetic members of its enemy's populace, forces, and governing body. Some well-established organizations reach out to obtain financial support from sympathizers outside their own country who share a common ethnic or religious background or other common interests. While these contributors usually participate willingly, they may also be subject to extortion, or may be deceived as to the nature and goals of the group. An organization may also receive materiel from sympathizers with access to the materiel stores of the police or military forces of the nation in which they operate.

1-32. Because arms, ammunition, and high-technology equipment may be difficult to acquire, forces must carefully protect the available supply and sources of resupply. Similarly, because of the wide range of equipment and ordnance used, resources must be closely managed. Paramilitary leaders and decision makers must carefully weigh the benefit of a proposed action against the cost of losing or expending precious resources, such as trained personnel, materiel, and political capital. Leaders usually take advantage of truces and periods of inclement weather to rest, train, and sustain their forces.

PRINCIPLES VERSUS ADVERSARY OF GREATER POWER

1-33. Aside from government-based internal security forces, other paramilitary forces generally must attempt to accomplish their goals against an adversary that overmatches them in conventional military power. When facing an enemy of greater power and capabilities, paramilitary forces will continue to apply the basic principles described above, to the extent still possible. However, they have devised some additional principles for applying their various instruments of power against an adversary with superior power. These are similar to the "adaptive" principles that regular military forces might use when facing superior forces.

Adaptive Principles

- Cause Politically Unacceptable Casualties.
- Control Access into Region.
- Employ Operational Shielding.
- Neutralize Technological Overmatch.
- Control Tempo.
- Change Nature of the Conflict.
- Allow No Sanctuary.
- Conduct Varied Actions.

1-34. Paramilitary forces also must assume the possibility of intervention by a major extraregional power in any local or regional conflict. If this occurs, the overall strategy of the paramilitary force remains relatively unchanged, since it deals with the reason for its existence as an organization—its goals and motivation. However, its immediate concern is to get the extraregional force to leave or stop interfering in regional affairs.

1-35. In evaluating extraregional threats, paramilitary forces carefully study the strengths and weaknesses of an extraregional power (such as the United States). They generally view the United States as the sole superpower, with an overall advantage in technology and warfighting capability. Despite these strengths, they also see some weaknesses that adversaries of the United States may be able to exploit:

Vulnerability of coalitions.

Unwillingness to accept heavy losses.

Sensitivity to public opinion.

Lack of commitment over time.

Preference for standoff combat.

Lack of optimization for close, dismounted combat.

Dependence on high technology.

Dependence on information dominance.

Predictable operations.

Lack of cultural awareness.

Vulnerability of force projection.

Dependence on robust logistics.

Reliance on contractor support.

Downsizing after conflict.

Based on these perceived vulnerabilities (see FM 7-100 for more detail), paramilitary forces have devised principles for dealing with a major extraregional power. Some of these principles apply specifically to an extraregional adversary, while others are equally applicable to any adversary that overmatches the paramilitary force in conventional power.

1-36. These principles attempt to exploit weaknesses or vulnerabilities believed to exist in the enemy's activities, organization, or force structure. By following these principles, a smaller or less capable force can hope to neutralize the overmatch afforded to technologically or numerically superior forces. Actions used against superior foes will focus on perceived centers of gravity such as national will and the enemy's willingness to endure casualties, hardship, stress, and continued deployments over time. Many of these principles are interrelated and overlapping, since all contribute to the overall goal is to prevent a more powerful adversary from bringing sufficient military power to bear to defeat the paramilitary forces.

1-37. These principles are idealistic, indicating what a paramilitary force would like to do, but not, in all cases, what it might be capable of doing. If the paramilitary force is not capable of implementing these principles on its own, it may choose to become affiliated with other paramilitary forces or with the regular military forces of a regional power (the State).

CAUSE POLITICALLY UNACCEPTABLE CASUALTIES

1-38. Paramilitary forces must attempt to inflict highly visible and embarrassing losses on enemy forces to weaken the enemy's domestic resolve and national will to sustain the deployment or conflict. Modern wealthy nations have shown an apparent lack of commitment over time, and sensitivity to domestic and world opinion in relation to conflict and seemingly needless casualties. Conversely, this is the strength of a highly-motivated paramilitary force. A comparative advantage against superior forces may be the collective psyche and will of the paramilitary organization and the people who support it to endure hardship or casualties, while the enemy may not be willing to do the same.

1-39. This difference in ability to endure losses can help a paramilitary organization establish or build the perception of its own legitimacy, while degrading that of its adversaries. In the case of a regional adversary, inflicting debilitating or demoralizing losses on the enemy can cause the populace to doubt the legitimacy or viability of that regime. The paramilitary force's ability to endure losses on its own side and still persevere can add to the impression of the correctness of its cause and lead larger segments of the populace to join it.

1-40. Against an extraregional power, paramilitary forces often have the advantage of disproportionate interests. The extraregional power may have limited objectives and only temporary or casual interest in the conflict. In contrast, the paramilitary organization approaches it from the perspective of total war and a threat to its aspirations or even to its survival as an organization. Paramilitary organizations are willing to commit all means necessary, for as long as necessary, to achieve their strategic goals. Compared to an extraregional enemy, they stand more willing to absorb higher casualties in order to achieve victory. They will try to influence public opinion in the enemy's homeland to the effect that the goal of intervention is not worth the cost. Especially in the case of terrorists or terror tactics used by other paramilitary forces, the casualties do not necessarily have to be within the enemy's military forces. The enemy may be even less willing to accept civilian casualties.

1-41. Victory has always been measured in national and human will. History has proven time and time again that victory does not always go to the best-trained, best-equipped, and most technologically advanced force. National or human will encompasses a unification of values, morals, and effort between the population, the leadership or government, and their forces. Through this unification, all parties are willing to individually sacrifice for the achievement of the unified goal. The interaction of military or paramilitary actions and political judgements, conditioned by national and human will, serves to further define and limit the achievable objectives of a conflict for all parties involved, and to determine the duration of a conflict and conditions for its termination.

CONTROL ACCESS INTO REGION

1-42. Extraregional enemies capable of achieving overmatch against the paramilitary forces must first enter the region using power-projection capabilities. These forces are not located in the areas of the world where regional conflicts involving paramilitary forces will be fought. They must have the capacity to project and sustain power over long time and distances, with forces originating in their respective homeland. Therefore, the first reaction to threatened intervention is focused on *access control*—to selectively deny, delay, and disrupt entry of extraregional forces into the region and to force them to keep their operating bases beyond continuous operational reach. Thus, access-control operations come in two basic forms: limiting access and operational exclusion.

1-43. Access-control activities can begin even before the time the extraregional power declares its intent to come into the region, and are continuous throughout a conflict. They can reach beyond the country or region within which the paramilitary forces predominantly operate.

1-44. *Limiting access* seeks to affect an extraregional enemy's ability to introduce forces into the region or country. The goal is to limit the accumulation of applicable combat power to a level and to locations that do not threaten the goals of the paramilitary organization. Disrupting the enemy's force projection capabilities is the easiest manner of preventing the massing of enemy combat power. Paramilitary forces can achieve this through many methods and types of action within the region, at the enemy's home stations (even in military communities), and at all points in between. . For example, airfields, seaports,

transportation infrastructures, and lines of communication (LOCs) should be attacked featuring coordinated actions of all available forces, possibly using terror tactics and weapons of mass destruction (WMD) to present the enemy with a nonlinear, simultaneous battlefield. Paramilitary organizations might exploit and manipulate international media to paint foreign intervention in a poor light, decrease international resolve, and affect the force mix and rules of engagement (ROE) of the deploying extraregional forces.

1-45. *Operational exclusion* seeks to selectively deny an extraregional force the use of or access to forward bases of operation within or near the region. For example, through economic or political connections, information campaigns, and/or hostile actions, paramilitary organizations might seek to deny the enemy the use of bases in nearby foreign nations. They might also attack population and economic centers for the intimidation effect, using terror tactics or even WMD.

EMPLOY OPERATIONAL SHIELDING

1-46. Paramilitary forces will use any means necessary to protect key elements of their combat power or infrastructure from destruction by a more powerful force—particularly by air and missile forces. This protection may come from use of any or all of the following:

- Complex terrain.
- Noncombatants.
- Risk of unacceptable collateral damage.
- Countermeasure systems.
- Dispersion.
- Fortifications.
- IW.

1-47. Operational shielding generally cannot protect the entire force for an extended time period. Rather, the paramilitary organization will seek to protect selected elements of its forces for enough time to gain the freedom of action necessary to prosecute important actions in keeping with the other principles for dealing with a more powerful adversary.

NEUTRALIZE TECHNOLOGICAL OVERMATCH

1-48. Against a technologically superior force, paramilitary organizations will disperse their forces in areas where complex terrain limits the enemy's ability to apply his full range of technological capabilities. However, they can rapidly mass forces and fires from these dispersed locations for decisive combat at the time and place of their own choosing.

1-49. Another way to operate on the margins of enemy technology is to maneuver during periods of reduced exposure. Paramilitary organizations train their forces to operate in adverse weather, limited visibility, rugged terrain, and urban environments. Such conditions can shield them from the effects of the enemy's high-technology weapons and deny the enemy the full benefits of his advanced reconnaissance, intelligence, surveillance, and target acquisition (RISTA) systems.

1-50. To the extent that such technologies are available to them, the paramilitary forces too may employ surveillance technologies, precision munitions, and sophisticated camouflage, deception, decoy, or mock-up systems to negate or eliminate the effects of enemy high-technology weaponry. Also, they can employ low-cost GPS jammers to disrupt enemy precision munitions targeting, sensor-to-shooter links, and navigation.

1-51. Paramilitary forces will concentrate their own RISTA, maneuver, and fire support means on the destruction of high-visibility (flagship) enemy systems. This offers exponential value in terms of increasing the relative combat power of the paramilitary forces and also maximizes effects in the information and psychological arenas. High-visibility systems that may be identified for destruction would be stealth aircraft, advanced main battle tanks or attack helicopters, counterbattery artillery radars, aerial surveillance platforms, or rocket launcher systems. Other potential targets are airfields, radars defending those airfields, and aircraft taking off and landing. The suppression or degradation of these systems can be achieved through the use of infiltration, portable weapon systems, and persistent chemical agents. Losses among these premier systems may not only degrade operational capability, but also undermine enemy morale. Thus, attacks against such targets are not always linked to military-style objectives.

1-52. Paramilitary forces may have easy access to commercial products to support precision targeting and intelligence preparation of the battlefield. The proliferation of advanced technologies permits organizations to achieve a situational awareness of enemy deployments and force dispositions formerly reserved for the militaries of technologically advanced nations. Much information on sources of such technology is readily and cheaply available on the Internet and in open-source documents. Those media also can provide paramilitary forces extensive information on the enemy and his armed forces. Intelligence can also be obtained through greater use of human intelligence (HUMINT) assets that, among other sources, gain intelligence through civilians or local workers contracted by the enemy for base operation purposes. Similarly, communications technologies are becoming more reliable and inexpensive. Therefore, they could act as a primary communication system, or a redundant measure. There will be little the enemy can do to prevent the use of these assets, especially since it is becoming harder to discriminate between civilian and military-type usage.

CONTROL TEMPO

1-53. Paramilitary forces should vary the tempo of operations, as required, to suit the friendly situation. They initially employ rapid tempo in an attempt to achieve their goals in the country or region before an extraregional force can be introduced. They will also use rapid tempo to set conditions for access-control operations before the extraregional force can establish a foothold in the region. Once having done that, they need to be able to control the tempo—to ratchet it up or down, as is advantageous to their own plans.

1-54. Most superior extraregional forces rely on power-projection capabilities. This fact is an exploitable weakness and should be used against them. Prior to or during the initial phases of enemy entry into the region, paramilitary forces should employ a high operational tempo to take advantage of the

weaknesses inherent in enemy power projection. Once enemy deployment begins, while efforts are ongoing to limit further enemy access, they would use all available forces to exploit the enemy phased deployment by attacking weaker or smaller initial-entry forces. Friendly forces hold the initiative early in most conflicts, taking advantage of surprise in conflict initiation. These measures, taken together with diplomatic and informational efforts, aim to terminate the conflict quickly, before the enemy can establish a foothold and bringing his main forces to bear.

1-55. If the paramilitary forces cannot end the conflict quickly, they may take steps to slow the tempo and prolong the conflict. This is an attempt to take advantage of enemy lack of commitment over time and can apply to either regional or extraregional adversaries. In protracted conflict, the preferred tactics for paramilitary forces are the raid and ambush as a means of wearing down the enemy while avoiding decisive combat with superior forces. These activities may not be linked to maneuver or ground objectives. Rather, their purpose is to inflict mass casualties or destroy flagship systems, both of which reduce the enemy's will to continue the fight. The paramilitary forces will try to mass fires and forces from dispersed locations to destroy key enemy systems or formations or to execute decisive combat at the time and place of their own choosing.

CHANGE THE NATURE OF CONFLICT

1-56. Paramilitary forces will try to change the nature of conflict to exploit the differences between friendly and enemy capabilities and sensitivities and to present the enemy with conditions for which he is not prepared. The most advantageous way to achieve a change in the nature of conflict is often to exploit the enemy's ambiguous political-military objectives.

1-57. Against an extraregional adversary, the paramilitary forces can take advantage of the opportunity afforded by the initial period of a phased enemy deployment to change the nature of the conflict. During that period, paramilitary forces may continue to operate as usual against their regional opponents, while engaging in access-control activities directed at the extraregional force. Against extraregional early-entry forces, the paramilitary forces may still be able to use the methods they employed in previous operations against their original regional opponents, particularly if access-control activities have been successful.

1-58. By changing the nature of the conflict as enemy forces are deployed, paramilitary forces can render the enemy force package inappropriate to the threat or environment. As the extraregional force builds up power to the point where it threatens to overmatch them, the paramilitary forces will change their methods of operation to focus on preserving combat power and exploiting enemy ROE. This shift in the focus of operations will present the fewest targets possible to the rapidly growing combat power of the enemy. They are prepared to disperse their forces to a greater degree and employ them in ways that present a battlefield that is difficult for the enemy to analyze and predict.

1-59. Modern militaries and coalition forces usually operate under restrictive ROE in activities short of war. Paramilitary forces must intently study the limiting factors with respect to the application of ROE and attempt to operate

outside the limits of the ROE. This can highlight restrictive ROE in a way that can undermine the enemy's national will. It could also cause the enemy to establish less restrictive ROE that expose coalition sensitivities or weaken international support.

1-60. Paramilitary organizations must adjust their tactics to the strengths and weaknesses of an adversary. They must capitalize on interoperability issues among the enemy forces and their allies by conducting rapid actions before the enemy can respond overwhelmingly. They may use international borders with a sympathetic population to provide refuge or a base of attack for paramilitary forces. Also, they may introduce terror tactics against enemy civilians or soldiers not directly connected to the intervention, as a device to change the fundamental nature of the conflict.

1-61. Paramilitary forces may disperse their forces in areas of sanctuary. The sanctuary may be physical, often located in complex terrain that limits or degrades the capabilities of enemy systems. However, the paramilitary forces may also use moral sanctuary by placing their forces in areas shielded by civilians or close to sites that are culturally, politically, economically, or ecologically sensitive. They will defend in sanctuaries when necessary. However, they will move out of sanctuaries and attack when they can create a window of opportunity or when opportunity is presented by physical or natural conditions that limit or degrade the enemy's systems. The paramilitary forces do not avoid contact; rather, they often seek contact, but on their own terms.

1-62. A key concept in changing the nature of the struggle is that paramilitary forces may have different criteria for victory than does the enemy. For them, the definition of victory may not require convincing military performances, or merely inflicting numerous casualties upon the enemy. The perception of victory may equate to survival of the movement or cause that they champion. Thus, paramilitary forces may stand willing to sacrifice excessive numbers of soldiers or civilians to attain victory. In some cases, however, a stalemate may be good enough, as long as the paramilitary organization maintains enough power to live to fight another day.

ALLOW NO SANCTUARY

1-63. While paramilitary forces intend to use complex terrain as sanctuary from the effects of enemy forces, they seek to deny enemy forces the use of such terrain. This forces the enemy to operate in areas where the paramilitary forces can attack him effectively with forces and fires out of their own sanctuary areas. Raids, ambushes, and terror tactics are effective means for denying sanctuary to enemy forces.

1-64. Against an extraregional adversary, paramilitary forces seek to deny enemy forces safe haven during every phase of a deployment and as long as the enemy is in the region or threatening to intervene there. They are prepared to attack enemy forces anywhere on the battlefield, as well as to his strategic depth. Attacks should feature coordinated actions of all available forces. The resultant drain on enemy manpower and resources to provide adequate force protection measures can reduce his strategic, operational, and tactical means to conduct war. Through astute use of diplomacy and IW, the paramilitary organization can deny the enemy the use of bases in nearby coun-

tries. All these efforts seek to disrupt the enemy's force projection operations and his ability to sustain the conflict.

1-65. The goal is to present the enemy with nonlinear, simultaneous actions within the region and possibly beyond. Such actions will not only deny the enemy sanctuary, but also erode his national will. This is particularly true against an extraregional power, if the paramilitary forces or their allies can strike targets in the enemy's homeland.

CONDUCT VARIED ACTIONS

1-66. To best attack superior forces, paramilitary leaders must utilize initiative to conduct battles or actions at a time and place their choosing, to disperse and isolate the enemy, and to negate or mitigate the differences between forces. This may mean fighting in complex terrain, such as urban or mountainous environments, or fighting during periods of reduced visibility to offset enemy advantages and maximize sanctuary from enemy effects. Similarly, this requires forces to conduct dispersed and decentralized activities and to coordinate simultaneous actions involving various paramilitary forces. It may also involve distributed activities in which the actions of various paramilitary forces are synchronized, perhaps with those of the military forces of a regional power (the State).

1-67. Decentralized, dispersed, and distributed activities are present in most of the principles to some degree. Nevertheless, these concepts warrant emphasis separately from others due to their special relevance to the future battlefield. Each approach seeks to reduce vulnerabilities to air power, precision munitions, and larger massed forces. The major difference between the activities is in the realm of command and control.

1-68. *Decentralized* actions are employed when only erratic or degraded C^2 measures exist. These activities feature autonomous action by forces, once given the mission from the higher command authority or organizational leadership. Elements outside of delineated areas need not cooperate, reducing C^2 requirements and coordination. This also insulates elements from the effects of further C^2 disruption. Decentralization makes it virtually impossible to mass combat power; however, it also presents less vulnerability to enemy attack or precision munitions, since units will not mass to achieve effects. Pattern analysis and templating become challenging for the enemy. Decentralized actions also serve to prolong the conflict in question, making decisive combat actions unlikely. Complex terrain is ideal for this type of action, and positions are organized for security. Between positions, countermobility efforts, especially mine warfare, are key, since paramilitary forces need only limited mobility corridors for maneuver.

1-69. *Dispersed* actions require elements to work independently in their areas, guided by the purpose their higher headquarters is attempting to achieve, and this is attained through modern C^2 systems. These activities deliberately bring together geographically separate friendly elements through centrally coordinated and integrated measures to reduce their vulnerabilities, while retaining the ability to assemble and strike key enemy systems at opportune moments. Once the action is complete, these elements return rapidly to their separate locations to avoid enemy counterstrikes. Complex terrain

within mutually supporting distance is ideal for this type of activity, and it is facilitated by pre-positioned munitions and by foot infiltration. The fluidity and seemingly disjointed appearance of these actions challenge pattern analysis and templating. Ambushes (both air defense and ground) are employed to deny air and ground reconnaissance of the chosen areas of interest. Logistics support of the force is difficult, and planning, preparation, and mobility are of paramount importance to allow efficient employment and shifting of forces.

1-70. *Distributed* actions require good C^2 networks with digital mechanisms to synchronize the combat operations of geographically separate elements to take advantage of fleeting opportunities on the battlefield. These activities use the capabilities of all sizes and types of forces in a coordinated effort to capture the initiative from the enemy and achieve decisive strategic and operational results. This can involve paramilitary forces operating in concert with affiliated State forces, especially Special-Purpose Forces (SPF). It is conducted through well-prepared, simultaneous actions throughout the entire area of interest to maximize the effects of friendly combat power within complex environments. These actions employ all available forces in an adaptive manner, and also integrate the strengths of each type of force to maximize the results of the action.

THE ROLE OF PARAMILITARY FORCES IN OPERATIONS OF THE STATE'S ARMED FORCES

1-71. In consonance with its concept of using "all means necessary" to achieve its strategic goals, the State views the various paramilitary organizations as assets that can be used to its advantage in time of war. The primary paramilitary organizations are the internal security forces, insurgents, terrorists, and large-scale drug and criminal organizations. Within its own structure, the State has formally established this concept by assigning its internal security forces, part of the Ministry of the Interior in peacetime, to the Supreme High Command (SHC) during wartime. Additionally, the State cultivates relationships with and covertly supports nongovernment paramilitary organizations to achieve common goals while at peace and to have a high degree of influence on them when at war.

1-72. The degree of control the State has over these organizations varies from absolute, in the case of internal security forces, to tenuous when dealing with terrorist and drug and criminal organizations. In the case of those organizations not formally tied to the State structure, control can be enhanced through the exploitation of common interests and ensuring that these organizations see personal gain in supporting State goals.

1-73. The State views the creative use of these organizations as a means of providing depth and continuity to its operations. A single attack by a terrorist group will not in itself win the war. However, the use of paramilitary organizations to carry out a large number of planned actions, in support of strategy and operations, can play an important part in assisting the State in achieving its goals. These actions, taken in conjunction with other adaptive actions, can also supplement a capability degraded due to enemy superiority.

BASIC TYPES OF ACTION AT STRATEGIC LEVEL

1-74. In pursuit of its national security strategy, the State is prepared to conduct four basic types of strategic-level courses of action. Each course of action involves the use of all four instruments of national power (diplomatic-political, informational, economic, and military), but to different degrees and in different ways. The State gives the four types the following names:

- **Strategic operations**—strategic-level course of action that uses all instruments of power in peace and war to achieve goals of the State's national security strategy by attacking the enemy's strategic centers of gravity.
- **Regional operations**—strategic-level course of action (including conventional, force-on-force military operations) against opponents the State overmatches, including regional adversaries and internal threats.
- **Transition operations**—strategic-level course of action that bridges the gap between regional and adaptive operations and contains some elements of both, continuing to pursue the State's regional goals while dealing with the development of outside intervention with the potential for overmatching the State.
- **Adaptive operations**—strategic-level course of action to preserve the State's power and apply it in adaptive ways against opponents that overmatch the State.

Each of these types of "operations" is actually the aggregation of the effects of tactical, operational, and strategic actions that contribute to the accomplishment of strategic goals. The type(s) of operations the State employs at a given time will depend on the types of threats and opportunities present and other conditions in the operational environment.

1-75. Strategic operations are a continuous process not limited to wartime or preparation for war. Once war begins, they continue during regional, transition, and adaptive operations and complement those operations. Each of the latter three types of operations occurs only during war and only under certain conditions. Transition operations can overlap regional and adaptive operations.

INTERNAL SECURITY FORCES

1-76. The internal security forces subordinated to the SHC provide support zone security and collect information on foreign organizations and spies. They perform civil population control functions and ensure the loyalty of mobilized militia forces. Some units are capable of tactical-level defensive actions if required. These basic tasks are not all-inclusive, and within their capability these forces can perform a multitude of tasks limited only by the commander's imagination. While performing these functions, internal security forces may be operating within their own hierarchy of command, or they may be assigned a dedicated command relationship within an operational-level command or one of its tactical subordinates.

1-77. During *regional operations*, internal security forces may serve to control the population situated in newly seized territory. They are an excellent source of HUMINT and can provide security for key sites located in support zones. Internal security forces can either augment or replace regular military

organizations in all aspects of prisoner-of-war processing and control. While continuing their normal tasks in the homeland, they can assist regular military organizations in the areas of traffic control and regulation.

1-78. During *transition operations*, internal security forces evacuate important political and military prisoners to safe areas where they can continue to serve as important sources of information or means of negotiation. Traffic control and the security of key bridges and infrastructure take on a higher level of importance as the State repositions and moves forces transitioning to adaptive operations. Internal security forces can continue to gather intelligence from the local population and assist in mobilizing civilians in occupied territory for the purpose of augmenting military engineer labor requirements. Finally, the use of qualified personnel to stay behind as intelligence gatherers and liaison with insurgent, terrorist, and criminal organizations can provide the State an increased capability during the adaptive operations that follow.

1-79. Especially important in the conduct of *adaptive operations* is the ability of internal security forces to free up regular military organizations that can contribute directly to the fight. The security of support zones within the area of responsibility (AOR) of an operational- or tactical-level command is just one example of this concept. Where necessary, some internal security forces equipped with armored vehicles can augment the defense or defend less critical areas, thus freeing up regular military forces for higher-priority tasks. Stay-behind agents working with insurgent, terrorist, and criminal organizations can contribute by directing preplanned actions that effectively add depth to the battlefield. Their actions can cause material damage to key logistics and C^2 assets, inflict random but demoralizing casualties, and effectively draw enemy forces away from the main fight in response to increased force-protection requirements.

INSURGENT FORCES

1-80. The State ensures that the exploitation and use of insurgent forces operating against and within neighboring countries is an integral part of its strategic and operational planning. Insurgent forces, properly leveraged, can provide an added dimension to the State's military capabilities and provide options not otherwise available. During peacetime, a careful balance is kept between covert support for insurgent groups that may prove useful later and overt relations with the government against which the insurgents are operating.

1-81. During peacetime, support to insurgents can consist of weapons, staging and sanctuary areas within the State, and training by the State's SPF. It is during this time that the State attempts to cultivate the loyalty and trust of insurgent groups they have identified as having potential usefulness in their strategic and operational planning. In all operations of the State's strategic campaign, insurgent forces serve as an excellent source of intelligence.

1-82. For the paramilitary commander, the systems approach to combat is not an end in itself. It is a key component in his planning and sequencing of tactical battles and engagements aimed toward achieving assigned goals. The systems approach supports his concept; it is not the concept.

1-83. During the conduct of *regional operations*, the decision to influence insurgents to execute actions that support operations of the State's armed forces will depend on a number of factors. If the State views extraregional intervention as unlikely, it may choose to keep insurgent participation low. A key reason for making this decision is the potential for those forces to become an opponent once the State has accomplished its goals. On the other hand, the State may plan to have these groups take part in directly supporting its operations in anticipation of further support in the case of an extraregional intervention. Insurgent involvement during regional operations may be held to furthering State IW objectives by creating support for the State's actions among the population, harassing and sniping enemy forces, conducting raids, and assassinating politicians who are influential opponents of the State. Insurgents can also serve as scouts or guides for the State's regular armed forces moving through unfamiliar terrain and serve as an excellent source of political and military intelligence.

1-84. The usefulness of insurgent forces can be considerable in the event of extraregional intervention and the decision to transition to adaptive operations. During *transition operations*, insurgent forces can support access-control operations to deny enemy forces access to the region or at least delay their entry. Delay provides the State more time to conduct an orderly transition and to reposition its forces for the conduct of *adaptive operations*. The principal means of support include direct action in the vicinity of air and sea ports of debarkation (APODs and SPODs) and along LOCs in the enemy's rear area. Dispersed armed action for the sole purpose of creating casualties can have a demoralizing effect and cause the enemy to respond, thus drawing forces from his main effort. The State's regular armed forces can coordinate with insurgents, supported by SPF advisors, to execute a variety of actions that support the strategic campaign or a particular operation plan. Insurgents can support deception by drawing attention from an action the State is trying to cover or conceal. They can delay the introduction of enemy reserves through ambush and indirect fire, cause the commitment of valuable force-protection assets, or deny or degrade the enemy's use of rotary-wing assets through raids on forward arming and refueling points and maintenance facilities.

TERRORIST AND CRIMINAL ORGANIZATIONS

1-85. Through the use of intelligence professionals and covert means, the State maintains contact with and to varying degrees supports terrorist and criminal organizations. During peacetime, these organizations can be useful, and in time of war they can provide an added dimension to State strategy and operations.

1-86. Although the State recognizes that these groups vary in reliability, it constantly assesses both their effectiveness and usefulness. It develops relationships with those organizations that have goals, sympathies, and interests congruent with those of the State. In time of war, it can encourage and materially support criminal organizations to commit actions that contribute to the breakdown of civil control within a neighboring country. It can provide support for the distribution and sale of drugs to enemy military forces, which creates both morale and discipline problems within those organizations. The

production of counterfeit currency and attacks on financial institutions can help to weaken the enemy's economic stability. Coordination with and support of terrorists to attack political and military leaders and commit acts of sabotage against key infrastructure (such as ports, airfields, and fuel supplies) add to the variety and number of threats that the enemy must address. The State and its military leadership also have the ability to promote and support the spread of these same kinds of terrorist acts outside the region. However, they must carefully consider the political and domestic impact of these actions before making the decision to execute them.

Chapter 2

General Paramilitary Tactics

This chapter addresses the general tactics employed by paramilitary forces. Generally, these organizations use tactics that resemble those used by regular military forces, but may differ in terms of scale or sophistication. Later chapters more specifically describe how certain types of paramilitary forces would execute a particular tactic or action. Such specific tactical applications depend on the specific goal, motivation, and capabilities each different type of organization. Thus, paramilitary forces are not restricted to the tactics described here as general guidelines.

To determine how best to employ forces, tacticians study the weaknesses or vulnerabilities of the enemy force. Tactics are chosen based upon goals and objectives, and modified based on analysis of the current situation, the physical environment, and the capabilities of available weapon systems. Paramilitary forces attempt to fully understand the environment in which they and their enemies operate, and they modify their tactics to capitalize upon enemy weaknesses. They then conduct offensive or defensive actions, as well as information warfare (IW) and intelligence activities, to exploit these weaknesses.

OFFENSE

2-1. In most environments, paramilitary organizations recognize that they can achieve victory through survival, outlasting the enemy, and by inflicting unacceptable levels of casualties on the enemy. These goals may best be achieved through offensive actions. The offense gains the initiative, inflicts the most casualties on targeted segments of the enemy or population, and forces the enemy to react. An offensive action, thoroughly planned and meticulously executed, often results in success, or at least the appearance of success.

2-2. When conducting offensive actions, it is important to establish mission withdrawal or mission abort criteria as the deciding factor for when to break contact. However, the constraints of these criteria will vary depending on the mission, the superior commander's intent, available resources, and the motivation of the force to achieve its desired goal. In all cases, the senior commander must authorize the withdrawal. After attainment of the goal, it is important to disengage from the enemy in a timely and organized manner. The paramilitary force seeks to disengage without unnecessarily losing combat capability or exposing its support network.

2-3. Offensive actions common to many paramilitary organizations include assaults, raids, seizing objectives, ambushes, standoff attacks, harassment, and the selective use of terror tactics. These organizations would also use

conventional military doctrine as the basis for refining their own standing operating procedures for offensive actions.

ASSAULT

2-4. Although the assault is the least practiced of offensive techniques, paramilitary organizations do conduct assaults similar to conventional military forces. These assaults, often successful, are launched to take control of, or regain control of terrain. Yet this type of action requires a significant level of training, equipment, and coordination often lacking in paramilitary forces. Tactical assaults are described in FM 7-100.2.

RAID

2-5. A raid is an attack, usually small in scale and time, which surprises the enemy and includes a planned withdrawal. It requires a high degree of intelligence information about the target and the terrain. It is usually carefully planned because of the expected high expenditure of resources. Typically, a raid is conducted against a "soft" target, such as a communications site, storage facility, or other target with limited security. The raiding force rehearses the plan and all of its contingencies to ensure success. Forces can conduct raids to—

- Destroy enemy personnel and equipment.
- Discourage enemy activity in a particular area.
- Liberate captured personnel.
- Distract and/or divert enemy resources from other areas.
- Cause international and domestic embarrassment to the enemy leadership.
- Collect information and supplies.

2-6. Each type of paramilitary force modifies the size and disposition of the raiding force to fit its mission and capability. See FM 7-100.2 for a general discussion of raid tactics.

SEIZING OBJECTIVES

2-7. The idea of capturing and holding objectives differs from the concept of a raid in that the paramilitary force plans to retain the objective for a political or tactical reason, or at least force the enemy to contest the seizure. The plan for this type of action may include a defense of the objective. The principles used in any defense will hold true when holding the objective. The paramilitary force emplaces flank and rear security elements and observation posts, develops a detailed fire plan, and plans withdrawal routes and criteria. Active and passive security measures are employed to protect against enemy actions designed to impair friendly effectiveness. Additionally, captured weapons can be integrated into the defense.

AMBUSH

2-8. An ambush is a surprise attack conducted from a defensive posture against a moving enemy. Ambushes are frequently used because they have a great chance of success and provide the best protection to the ambush force. Ambushes are conducted to—

- Destroy or capture personnel and equipment.
- Restrict the enemy's freedom of movement.
- Collect information and supplies.

2-9. Each type of paramilitary force modifies the size and disposition of the ambush force to fit its mission and capability. See FM 7-100.2 for a general discussion of ambush tactics.

STANDOFF ATTACKS

2-10. A standoff attack is conducted to serve many purposes. The weapons of choice used in these types of attacks are mortars, rockets, or recoilless rifles. Standoff attacks are a very cost-effective method to cause chaos and demoralize the enemy or the population. By launching a few sporadic mortar rounds into a marketplace or on a symbolic target, a force can capitalize on the people's belief that they cannot protect themselves from these attacks. Standoff attacks can also cause the people to lose confidence in the government's ability to stop these attacks or protect them from these incidents.

2-11. Additionally, when targeting military forces, standoff attacks can harass the enemy, destroy equipment, attrit forces, depress morale, and cause fatigue. However, insurgent forces must consider the possibly undesirable consequences of indiscriminate standoff attacks, since they frequently kill innocent civilians. This could result in a loss of popular support for the insurgent cause.

2-12. A paramilitary force may not necessarily be bound by conventional ethics, beliefs, or the laws of warfare. Therefore, it may use the grounds of schoolyards, churches, or hospitals to emplace weapons for standoff attacks. By doing so, it forces the enemy to decide whether to fire in retaliation or not.

HARASSMENT

2-13. Harassment is any persistent act or repeated acts designed to annoy. Paramilitary forces primarily use harassment to annoy the enemy, goad him into an act prejudicial to his cause, or degrade his effectiveness. They may also use harassment against the populace in order to degrade popular cooperation with the enemy, overcome populace neutrality, or degrade the legitimacy base of the enemy among a populace that the enemy cannot protect from harassment.

2-14. Harassment is conducted in many ways, such as passive resistance, information campaigns in the media, sniping, establishing roadblocks to impede the enemy's movement, inciting crowds to riot, or not complying with established procedures. It includes attempts to force the enemy to commit acts that violate his rules of engagement or acts that friendly forces can use as propaganda. For example, a paramilitary force can request or coerce a

group of peasants to sit on a route used by the enemy. This act slows the enemy's movement and may eventually provoke him to act in a negative way. If the enemy acts adversely toward the peasants, the paramilitary force may highlight enemy brutality against them. Another example is the planting of rumors, false documents, and false media reports. These actions give enemy personnel and individual leaders the impression of deceit by higher enemy leadership, treachery by other members of enemy forces, desertion or adultery by family members and friends, and abuse or neglect of family members.

TERROR TACTICS

2-15. Terror tactics are an efficient means to accomplish goals without direct confrontation. Terror tactics are most often used as part of an IW campaign to focus domestic and/or international media and political attention on the cause of the paramilitary organization and to raise international and/or domestic public pressure against the enemy.

2-16. Terror tactics may also be used to—

- Discourage enemy activity in certain areas.
- Restrict the enemy's freedom of movement.
- Demoralize personnel of the enemy force, members of the enemy leadership, or the general populace.
- Distract and/or divert enemy resources from other areas.
- Cause international and domestic embarrassment to the enemy leadership.
- Discredit enemy leadership and degrade its legitimacy.
- Destroy enemy leadership, command and control, and/or cohesion (especially through assassination and kidnapping).
- Collect information about the enemy's reactive capability and his will to sustain activities against the paramilitary force.

2-17. Terror tactics are usually not employed with the intention of causing the enemy to escalate his activities. However, they may indeed be used to cause the enemy to escalate the intensity of actions in the hope of causing mistakes, forcing the expenditure of resources, causing the loss of popular support, or undermining enemy legitimacy. Terror acts can be surgical in nature, especially when conducted by sophisticated, high-technology forces. However, some terror actions may intend large-scale collateral damage to humans and property in order to heighten their effect. The use of terror tactics is not without risk. They may backfire when used incorrectly, incompetently, against a poorly chosen target, or in the wrong political climate.

2-18. Chapter 4 provides examples of how terrorist groups conduct terror tactics: extortion, kidnapping, hijacking, hostage-taking, assassination, maiming, and sabotage. It also describes several means, such as bombs and chemical and biological weapons, used to execute terror tactics. Each paramilitary force modifies the described tactics, techniques, and means to fit its mission, goals, and capability.

DEFENSE

2-19. Paramilitary forces believe defense is a necessary condition to hold key terrain, preserve resources, or gain an economy of force. Defense also allows for the implied advantages of rest and recuperation, refit and maintenance of equipment, and training. Defensive actions also allow forces to withdraw, hold occupied positions, or create conditions favorable for resuming offensive actions.

2-20. Paramilitary forces take active and passive security measures to protect themselves against enemy actions designed to impair their effectiveness. Security measures are employed based on the perceived enemy capability, level of resources, and the value of the items or action being protected. The leader of a group may employ bodyguards, whereas a member may take his own personal security precautions. Leaders conduct a risk assessment or cost-benefit analysis; they weigh the costs of taking security measures against the potential loss of the resource being protected.

2-21. Security is paramount for all paramilitary organizations. The most basic form of security is the denial of knowledge regarding friendly capabilities, intentions, and activities to those organizations perceived as the adversary. All attempts must be made to ensure that this knowledge is guarded to maintain secrecy. (See Protection and Security Measures under IW below.)

INFORMATION WARFARE ACTIVITIES

2-22. Information and communications technologies have grown exponentially in recent years. Cellular and satellite communications, personal computers, and the Internet are a few examples of the capabilities widely available to nations, as well as independent organizations and individuals. The concepts of time, space, force, speed, precision, and lethality have changed because of the capabilities of information-age technology and the availability of information. These changes have a tremendous effect on how forces—including paramilitary forces—conduct activities.

2-23. Paramilitary forces define *information warfare* as specifically planned and integrated actions taken to achieve an information advantage at critical points and times. The fundamental goal of IW is to influence an enemy's decision making through his collected and available information, information systems, and information-based processes, while retaining the ability to employ friendly information, information-based processes, and systems. IW includes offensive elements, as well as defensive, protective measures. One side attempts to gain an advantage by affecting enemy information and information systems while defending its own information systems.

2-24. IW is continuously conducted by all paramilitary forces—without regard to strict organizational boundaries. The leadership integrates all elements of power—diplomatic-political, economic, military, and informational—to implement an information strategy. One element of power may have primacy over the others at a given time, but all work together.

IW ELEMENTS

2-25. Across the spectrum of competition, conflict, and war, the following elements are integrated when developing and implementing IW:

- Electronic warfare (EW).
- Computer warfare.
- Deception.
- Physical destruction.
- Protection and security measures.
- Perception management.
- Information attack (IA).

The resources and capability of a particular paramilitary force, and the appropriateness of the IW medium to the target, determine the choices and the extent to which the various IW elements are employed and integrated.

Electronic Warfare

2-26. EW spans the entire electromagnetic spectrum, and ranges from highly technical to primitive methods and means. Methods depend on available equipment and on what portion of the spectrum the paramilitary forces are trying to manipulate, employ, or deny. Methods include, but are not limited to, high-technology activities that use advanced signal employment, digital manipulation, and computers. There are also low-technology methods that include meaconing, intrusion, and communications and non-communications jamming. Paramilitary forces can apply both lethal and nonlethal methods, such as destroying a radio-relay site and jamming tactical radio nets and communications.

Computer Warfare

2-27. Computer warfare is the newest and perhaps most ominous of all the IW elements. Although it overlaps with other elements, computer warfare requires sophisticated expertise to perform. Paramilitary organizations may contract hackers, disgruntled employees, or other foreign agents to provide computer warfare assistance. By hiring these services, they reduce the possibility of tracing the act back to their own organization.

2-28. Computer warfare includes altering data and performance characteristics through the use of viruses or other database manipulation techniques. It may also include unauthorized access, such as hacking; and computerization, miniaturization, and robotization of weaponry and equipment. Paramilitary forces can exploit the availability of computer technology on the open and black markets to determine vulnerabilities in their enemy's information systems.

Deception

2-29. Paramilitary organizations can thoroughly integrate deception within all domains (physical, electronic, and virtual) across all actions. Economic organizations, such as front companies, may publish false financial figures; official spokespersons may initiate a rumor campaign; military-type units may use decoys or conduct a feint. Each deception action has a specific target, ob-

jective, story, and means allocated to make it believable and at least to some extent verifiable. Paramilitary forces must allocate sufficient resources when executing the deception operation so the enemy will believe the deception story.

Physical Destruction

2-30. Physical destruction is powerful when integrated with other elements of IW. Within a paramilitary organization, forces that conduct destruction actions may not be aware that they are involved in an integrated IW campaign. For example, a direct action cell or a fire support element may receive a mission to destroy a target at a certain time or using a particular technique. Upon completion, the force continues with other assigned missions.

2-31. The destruction element of IW highlights the importance of precision-guided weapons or "smart" weapons. A technologically advanced paramilitary force may be able to acquire and employ weapons and equipment with sophisticated information components, such as guided weapons and munitions, or global positioning systems. The goal of this is to link real-time intelligence systems and long-range precision weapons within a faster decision-making cycle than that of the enemy. Less-sophisticated forces, however, must continue to target high-value targets with available weapons systems, such as artillery and direct action units.

Protection and Security Measures

2-32. Protection and security measures are broader than the concepts of operations security and force protection. Information is a critical resource and, to protect it and maintain secrecy, paramilitary forces use appropriate protective measures, such as censoring, camouflage, counterreconnaissance, and encryption. They can employ a variety of systems to collect, process, and use information to determine friendly and enemy weaknesses and vulnerabilities, or to assess and evaluate IW campaigns.

Perception Management

2-33. Perception management includes all planned activities against foreign and domestic targets, which are intended to change, manipulate, control, or otherwise manage a target's perceptions. Paramilitary forces use truthful and false information, misinformation, and "spin" information to fit their needs. Censorship and public affairs programs aimed at a sympathetic population are an important component of perception management. When conducting IW, the skillful use of the media and other neutral players, such as nongovernmental organizations, can benefit the paramilitary organization's cause and deter enemy actions. The paramilitary forces can use psychological warfare (PSYWAR) and the media to achieve their perception management goals.

2-34. **Psychological Warfare.** Paramilitary forces conduct PSYWAR activities to achieve many of the same objectives as those of conventional military forces. They can use many of the same techniques that conventional forces use, but on a smaller scale and possibly employing less sophisticated, situationally- and culturally-appropriate delivery means. For example, in-

stead of dropping leaflets from aircraft, paramilitary organizations may distribute them hand-to-hand, or enclose them in bulletins at religious services.

2-35. When conducting PSYWAR activities aimed at the local populace, a paramilitary organization has a definite advantage over foreign forces and, in many cases, even indigenous conventional military forces. This is because the paramilitary force usually—

- Has a better feel for the pulse of the people.
- Has a much better understanding of the motivational factors influencing the populace.
- Exists within the target populace as members, not as actors imposing from the outside.

2-36. **Media.** A paramilitary organization can use and/or manipulate local news sources to convey the message to its target, either directly to a decision maker or by influencing an audience to put pressure on the target. A small printing press, hand-lettering, or a photocopy machine may be used to generate leaflets which communicate the message. Organizations may use a laptop computer with built-in fax or electronic mail to distribute press releases to local or international media. Conversely, an organization may have its own newspapers and journals, with its own accredited members of the press corps. A group spokesman may be interviewed by members of the international media or provide them press releases. An organization may ensure that the mainstream media picks up a story placed in an obscure foreign newsletter or journal. In efforts to gain local support, a paramilitary organization may use culturally appropriate media such as orators, poets, storytellers, or the theatre instead of radio or television to spread its message.

Information Attack

2-37. Paramilitary forces incorporate IAs when appropriate. This type of action (sometimes called cyber attack) focuses on the intentional disruption of a digital information system in a manner that supports a comprehensive IW campaign. Civilian attacks on the commercial Internet have demonstrated the vulnerability of information systems to innovative and flexible penetration, disruption or distortion techniques. As information systems continue to evolve, attacks by civilian hackers and crackers will likely increase. Paramilitary information attackers learn from and expand upon these methods and constantly seek ways to create opportunities to disrupt, confuse, or mislead the enemy.

2-38. IA presents a powerful tool for paramilitary forces. For example, an information attacker may target an information system for sabotage (electronically or physically) or manipulate and exploit an information system for intelligence collection purposes. This may involve altering data, stealing data, or forcing a system to perform a function for which it was not intended, such as spoofing an air traffic control grid. Likely targets for an IA are the critical infrastructures of an opponent: telecommunications links and switches, electrical grids, commercial infrastructures, transportation networks, and economic infrastructures.

IW METHODS AND MEANS

2-39. Paramilitary organizations attempt to detect, deceive, manipulate, disrupt, degrade, or destroy the enemy's information systems. For example, by using disguised personnel or electronically mimicking an authorized user, they can hide an attempt to access an enemy's information system. This information system can be a person (such as an analyst) or an object (such as a database). Similarly, groups may manipulate or deny service by destroying or degrading hardware and software used by their enemy. Methods short of destruction may provide a bigger payoff than physically destroying a target, in terms of attaining the organization's goals.

2-40. A paramilitary organization may have subordinate elements with IW-type missions. Examples of this could be an intelligence cell of an insurgent force, a direct action cell of a terrorist group, or a front company of a narcotics-trafficking organization, or a television station owned by a large criminal organization. Some of these missions require specialized equipment, such as jammers to conduct electronic jamming, or secure communications to support narcotics trafficking.

2-41. In planning an IW campaign, paramilitary forces consider various organic and commercially available equipment and organizations that have the potential to conduct IW-type missions. Lack of traditional military-type equipment, such as jammers and artillery, does not imply that an organization cannot conduct an integrated IW campaign. The limiting factor in implementing IW is not technology, but rather the imagination and resolve of leadership, and their ability to do the unexpected.

2-42. Often, an individual leader, hero, martyr, or spokesperson—through personal charisma and presence—may become lionized by the domestic populace and/or an international audience. Quite supportive for the cause of the paramilitary organization, local and international entrepreneurs and artists may decide to capitalize upon the image of the individual, and utilize it for marketing purposes, thus enhancing the impression of the cause's worldwide influence.

INTELLIGENCE ACTIVITIES

2-43. Paramilitary organizations can conduct intelligence activities using the same key techniques and procedures as those of conventional military forces, but often on a smaller scale. Sometimes, they conduct these activities with lower-level technology, but with a greater appreciation for the cultural setting of the area of responsibility (AOR). Every member of a paramilitary organization is an intelligence-gathering mechanism, and his knowledge of the AOR is likely to be greater than that of an intelligence officer in a conventional military force. The principal intelligence tasks of a paramilitary force are reconnaissance, general political and military intelligence, and counterintelligence. The classical factors of the intelligence cycle (collection, evaluation, production, and dissemination) are just as valid for a paramilitary force as for a conventional force.

RECONNAISSANCE

2-44. Reconnaissance is an action undertaken to obtain information. Paramilitary forces use the information to plan future activities and determine

the feasibility of planned actions. In the offense, efforts are concentrated on the enemy at his location and the area surrounding the target. In the defense, the reconnaissance effort is to determine when and where the enemy will conduct offensive actions against friendly forces.

2-45. Forms of reconnaissance include surveillance, use of informants, and infiltration of enemy organizations. All paramilitary organizations conduct reconnaissance, but each modifies the techniques used based on the organization, environment, and level of capability. For example, an insurgent force may conduct reconnaissance patrols or possibly utilize unmanned aerial vehicles (UAVs), whereas a narcotics-trafficking organization may buy commercially available satellite imagery.

2-46. **Surveillance.** Conduct of both active and passive surveillance is essential. Active surveillance includes patrols (on foot or using watercraft, aircraft, and other vehicles), observation posts, and planting observers in crowds or buildings. These patrols and observers can conduct operations under the guise of exercise, normal curiosity, or the conduct of legitimate business. Passive surveillance includes employment of remote sensors, communications monitoring, and satellite imagery.

2-47. **Informants.** Informants are persons who, because of their location or access, can provide information to the paramilitary organization. Such organizations use informants when they cannot collect this information themselves. There are two types of informants: those who provides information voluntarily and those who provide it involuntarily. A voluntary informant who provides information may be sympathetic to the cause of the paramilitary organization or may receive payment for services. The informant either volunteers information or the group recruits him to provide information. For example, during a farmer's normal duties, he observes the enemy conducting patrols and reports this information. Conversely, an organization may coerce potential informants with access to the enemy to provide information involuntarily. As an example of this, a criminal organization may coerce or threaten an individual working for a law enforcement agency to provide information regarding future police actions.

2-48. **Infiltration.** If a paramilitary organization is unable to recruit or coerce an individual to act as an informant, it may infiltrate the enemy organization. For example, a technician might infiltrate a company that provides information or communication services to the enemy. He is then able to collect information or place listening devices to gather information.

GENERAL POLITICAL AND MILITARY INTELLIGENCE

2-49. A paramilitary force usually produces its own general intelligence, to include order of battle. Information in raw or finished form may also be provided as a free service by sympathizers in the enemy organization or by a foreign state or organization. Raw information and finished products may also be purchased on a case-by-case or contract basis from international or domestic firms that produce intelligence on a legitimate commercial basis. A paramilitary organization's general military intelligence is often superior to the enemy's due to the first-hand knowledge of the area, penetration of gov-

ernmental structures, relationships with the population, and the ability to maintain observation across the countryside or urban area.

COUNTERINTELLIGENCE

2-50. A paramilitary organization places great emphasis on the conduct of internal counterintelligence activities because of the criticality of maintaining cohesion within the hazardous environment in which it operates, and the susceptibility to infiltration by enemy agents. Members are encouraged to report inappropriate and/or risky behavior, and dedicated agents follow up to observe members who are identified as security risks. Personnel who are suspected security risks are usually not afforded conventional due process.

Chapter 3

Insurgent Organization and Tactics

Insurgent forces are groups that conduct irregular or unconventional warfare within the borders of their country in order to undermine or overthrow a constituted government or civil authority. The distinction between terrorists and insurgents is often blurred because of the tactics employed by each. Some terrorists groups have become insurgent organizations, while insurgent organizations have used terror tactics. An insurgent organization may use more than one form of tactics and, based on its strategy, its actions could cut across the entire spectrum of warfare—employing terror, guerrilla, and conventional military tactics to achieve its goals. Typically, most insurgent groups use the first two.

While insurgent forces, by definition, operate within their own country, another country in the region (identified in OPFOR manuals as "the State") may identify and support insurgencies that it believes can help further its political goals in the region. The degree and type of support rendered are strongly influenced by the political ramifications. Support can consist of open political and even material support, or it can be purely material and clandestine. In either case, the goal is to achieve as much influence over these organizations as possible and cause them to take actions that are beneficial to the State.

TYPES AND GOALS

3-1. An insurgent organization's goals and strategies are often a reflection of its type. Some may reject a current social, economic, or political system, while others seek wealth within the status quo.

REJECTIONISTS

3-2. Overthrowing, seceding from, or gaining autonomy from the current government are all ways in which an insurgent force may establish itself. In this type of "rejectionist" philosophy, the group's ethnicity often provides its basic identity. Political agenda, as well as religious, economic, or cultural motives distinguish the rejectionists, who may be referred to as traditionalists, pluralists, secessionists, reformists, or preservationists.

3-3. The rejectionist organization's population support base may clearly indicate that it would be satisfied with autonomy within a geographic area, the right of judicial autonomy for its ethnic or religious group, relief from repression, a significant change in the current national laws or government, or even the right of self-determination. However, the leadership may not be content with anything less than eventual secession, recognition from external gov-

ernments as a legitimate political entity, and the establishment of a new government with a guarantee of leadership and choice positions for its senior membership. Often, when the chronological span of the struggle extends through several generations, conflict becomes a way of life, and those in leadership positions begin to see continuation of an interminable struggle as a goal in itself. Even if the conflict is resolved satisfactorily, some fervent members either may not accept the conclusion, or may be so consumed by the guerrilla lifestyle that they will seek other groups to which they can offer their services.

WEALTH-SEEKERS

3-4. Leaders of the "wealth-seeking" type of insurgency gain popular support by highlighting the disparate lifestyles between the government leaders and the populace. They seek to attract the support of the populace by offering them a share in the wealth. Wealth-seekers may join forces with rejectionists to overthrow the existing order, although for different reasons. Alternatively, the wealth-seekers may seek or form loose alliances with large-scale drug or criminal organizations.

SHORT- AND LONG-TERM GOALS

3-5. Regardless of their type, insurgent organizations clearly distinguish between short- and long-term goals. In the short term, the rejectionist force wants the indigenous population to recognize its legitimacy. True insurgencies are political movements and, as such, place a priority on gaining and maintaining popular support. In practical terms, the military aspects of an insurgent strategy are subject to the political, social, and economic aspects. Without legitimacy and popular support, the group cannot survive long enough to develop its capability or reach its long-term goals. The most successful insurgent groups also receive backing from populations of neighboring countries with similar ethnic, religious, or cultural heritage.

3-6. The wealth-seekers' initial goals are the rapid accumulation of wealth, followed by protection of that wealth. The long-term goals are acquisition of political legitimacy to preserve and enhance wealth and exercise power, and the acquisition of social legitimacy, power, and prestige, for its members and their families. In simpler terms, rejectionists seek power through legitimacy, while the wealth-seekers seek legitimacy through power.

3-7. Rejectionists and wealth-seekers may work together as parts of a single insurgent movement. Both need the support of the population in order to undermine or overthrow the current order. Because of the difference in their long-term goals, however, there is likely to be a falling out among these partners after victory.

INSURGENT ENVIRONMENT

3-8. The typical insurgent is capable of using the resources of his environment (either rural or urban). He is comfortable with night travel, may be trained or experienced in hunting or stalking, can maneuver in difficult rural or urban terrain, has an intimate knowledge of local terrain, and rehearses tactics and plans before every mission. Most insurgents are ideologically motivated, and many are willing to give their lives for their beliefs.

3-9. Insurgents have usually spent their entire lives in the culture and terrain in which they operate. They are comfortable in using the infrastructure, transportation, and sources of refuge and sustenance. They have personal networks of support based upon family ties or friendships. Often they have been raised from infancy in rebel or refugee camps, or enclaves of displaced persons, and know no other way of life than insurgency.

3-10. To survive, the insurgent organization must have good leadership. Most leaders are extraordinarily intelligent, courageous, and charismatic. The leadership usually has had access to higher education, specialized formal military training either locally or abroad, and/or has a talent for military leadership coupled with close study of foreign (often U.S.) military doctrine. They must be able to attract followers, organize them, and instill a disciplined zeal matched only in the most elite military organizations. A leader is an individual whose family background is either of middle-class or wealthy means. Ideals of an improved society inspire him.

3-11. Followers are typically from rural or poor urban areas. A better life, their leaders' promises, family or ethnic allegiances, or perhaps the loss of a family member to enemy forces motivate these insurgents to join the cause. Although some may receive special training in weapons, individual and small-unit tactics, booby traps, improvised explosive devices, martial arts, and field fortifications, the soldier ranks are usually filled with untrained individuals who receive their practical training through experience. After serving as an infantry soldier, an insurgent may be selected to receive advanced training in communications, demolitions, first aid, social work, publishing, internet use and website development, intelligence functions, ordnance manufacturing, smuggling, or other skills.

STRATEGY

3-12. From an insurgent view, strategy is the integration of means to achieve goals. Sometimes the strategy is formally stated in published documents, such as a manifesto or constitution. Alternatively, a developing insurgent organization may have a loosely established concept promulgated in speeches and short writings. While there are several types of strategy, the protracted popular war (commonly thought of as the Maoist strategy or mass-oriented insurgency) and military-focus strategies are the most common. The strategy may or may not focus on urban areas.

POPULAR PROTRACTED WAR

3-13. The popular protracted war strategy is the classic Communist insurgency model. Mass popular support and escalating violence are the cornerstones of this strategy, which advocates a three-phase approach. It presumes the presence of a political, social, or economic irritant that causes a considerable number of people to advocate dramatic change that they cannot obtain in a satisfactory or speedy manner within the current system. Those who are willing to commit their persons or resources to such radical change identify themselves to each other overtly or in secret. Then they coalesce into an entity capable of establishing a structure, articulating goals and recruiting adherents and resources. In any of the phases of popular protracted war, significant support may be provided by an established legitimate political, religious, or economic entity outside the country.

Phase One

3-14. Phase one, sometimes referred to as *incipient or latent insurgency*, equates to strategic defense. Gaining substance and legitimacy is the primary goal during this phase. Insurgents must obtain, preserve and consolidate resources; the enemy may not recognize the threat posed by the organization. Insurgents actively but carefully recruit, establish organizations at wide levels, gain popular support, and conduct limited intelligence collection against the government or enemy. While the insurgent organization recruits during this phase, internal security is the primary concern. Thus, recruits are carefully screened to prevent possible government infiltration. Activities conducted during phase one include demonstrations, labor strikes, recruiting, guerrilla training, propaganda activities, civic actions, and the infiltration of government and other organizations. Information warfare initiatives are also initiated, such as the establishment of Internet websites, operation of radio stations, sponsorship of cultural events and organizations, and widespread use of posters and graffiti.

Phase Two

3-15. Phase two, or *guerrilla warfare*, occurs when the insurgents, having developed sufficient organization, leadership, resources, and internal or external support, and logistics support, initiate organized warfare against the enemy. During phase two, the enemy and the insurgency are at a strategic stalemate. The government acknowledges the organization's existence and attempts to eliminate it. The organization's goal is to discredit the government. It embarks upon a long-range effort to isolate and alienate the people from the government while preventing the government from exercising its power. The basic strategy is to force the government to try to do everything everywhere, so that its means are quickly dissipated. A supporting strategy is to force the government and its allies into mistakes and abuses, which deter from its legitimacy. Destroying the government's legitimacy while continuing to build the insurgent organization's legitimacy is crucial during this phase.

3-16. Expansion into more aggressive acts requires the formation of local military-type elements to engage in warfare. The leadership element stays hidden. Full-time leaders coordinate the activities of the part- and full-time members at the district and regional command levels. Small units conduct raids and ambushes against a wide variety of political, economic, and military targets. Tactics are employed that allow the insurgents to avoid decisive engagement. The objective is to reinforce the idea that the government is incapable of protecting and providing for the population. Meanwhile, the insurgent organization expands civic-action programs to highlight its own capabilities. Logisticians expand internal and external support mechanisms, sanctuaries, and facilities for materiel support. Finance personnel begin to establish internal and external funding and funds management mechanisms. Similarly, skilled information warfare operators appeal to the international community, possibly through the media, for political and logistics support. Diplomatic representation is established.

Phase Three

3-17. In phase three, known as *war of movement* or *conventional war*, the insurgency is on the strategic offensive. Long-term goals, such as overthrowing the government or establishing a separate country, have primacy in this phase. A portion of the insurgent organization may take on a more military structure, and engage enemy forces in conventional military actions.

3-18. The size and duration of actions depend on the level of development of the insurgent organization. Large-scale insurgent units attempt to destroy the government's military forces while small forces conduct attacks against strategic targets, such as the enemy leadership. Also, riots and acts of sabotage characterize phase three. The military-type organizations sustain combat activities by employing well-developed logistics and communications systems. They also continue the tactics and strategies employed in phases one and two.

Compressed Phases

3-19. There is no clear-cut distinction between the three phases of an insurgency, and insurgent groups may not pass through all of the three phases. If the leadership of large elements of trained military forces of the government converts to the cause, and their troops are known to be personally loyal to the insurgency, the insurgents may have the necessary strength to intimidate or challenge the remaining government forces in a force-on-force battle. The insurgent organization may also co-opt existing ethnic-based militias or obtain the services of contract or volunteer forces. Similarly, an organization may train a well-equipped force in a foreign or internal sanctuary and thus move quickly into phase two or three. Furthermore, an insurgency may have elements operating within all three phases simultaneously in different parts of the country. Therefore, the enemy's perception of, and reaction to the level of insurgency will be influenced by the type of threat in a particular area (for example, political rally versus force-on-force operations). The strength and resolve of the government, the degree of support at local levels, the organizational development of the insurgent group, and the external factors all influence the capability of the insurgency.

MILITARY-FOCUS STRATEGY

3-20. The military-focus strategy differs from the strategy of protracted popular war in the importance of popular support. No attempt is made to mobilize the population. This strategy assumes that popular support either already exists or will exist. A weak government may lead the insurgency to adopt this strategy, which is not as time-dependent as the protracted strategy. Proponents of this method believe that a small, elite group can conduct raids, ambushes, and terror activities that will cause the government to collapse. With each victory, the insurgency gains additional popular support, leading to its leadership's replacing the government leadership. Because this strategy occurs over a relatively short period, the insurgent leadership develops a concept and an organizational structure for a political system that it can implement once it topples the government.

URBAN-FOCUS STRATEGY

3-21. The urban-focus strategy features a limited insurgent organization, with small cells employing terror tactics within one or more cities to exploit today's vulnerable environment. The distinctive nature of this strategy is to turn a political crisis into an armed conflict. This is achieved by performing violent acts that will force those in power to transform the political situation of the country into a military situation. The government's lack of ability to restore security, and government overreaction as its forces attempt to control the violence, will eventually turn the masses away from the government. An urban insurgency typically follows five phases.

Phase One

3-22. The first phase is characterized by an active information campaign emphasizing economic or political repression by the government. In their propaganda, the insurgents include threats of violence against targets symbolic of government repression.

Phase Two

3-23. In the second phase, the insurgent group organizes. It begins recruiting, establishes a cellular structure, and begins infiltration of the government. Then it develops control over areas of the city by demonstrating its power through selective acts of terror and sabotage.

Phase Three

3-24. In phase three, the insurgency attempts to control the streets by targeting government security forces and demoralizing the government through intimidation. The insurgent organization begins providing an alternative government.

Phase Four

3-25. The fourth phase of an urban insurgency is the mobilization of the masses. The urban insurgents attempt to provoke the government into arbitrary and indiscriminate reprisals, such as martial law, suspension of civil liberties, and mass arrests. Insurgents exploit the governmental reactions to undermine the legitimacy of the government, and further unite the people into active opposition and participation. Popular discontent shows itself in labor strikes, marches, and rioting organized by overt insurgents.

Phase Five

3-26. The fifth and final phase is characterized by the urban uprising. Terror tactics and widespread mass demonstrations and rioting combine to cause large-scale defections from security forces. This can produce political collapse and a power vacuum, creating opportunity for the insurgents to seize control and power.

ORGANIZATION

3-27. As an insurgent group develops, its organizational structure changes. Figures 3-1 through 3-5 depict examples of generic insurgent organization, progressing from low-capability to high-capability organizations.

BASIC CELLULAR STRUCTURE

3-28. A low-capability insurgent force typically has a cellular structure that is capable of limited actions and primarily conducts recruiting, intelligence, and propaganda activities. The structure at this level of capability is similar to that of terrorist organizations, except that it tends to be more hierarchical in nature. A low-capability insurgent organization may initially consist of single cells based on function. Not every organization has all the types of cells or the numbers of them shown in the example in Figure 3-1.

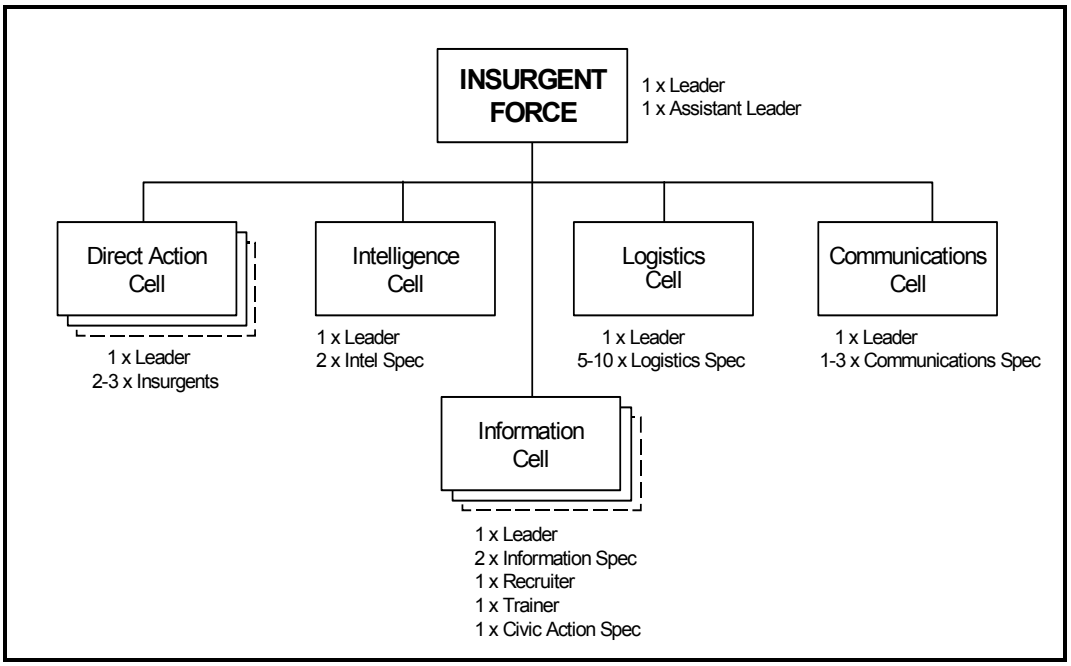

Figure 3-1. Cellular Structure of a Low-Capability Insurgent Force (Example)

3-29. Cells may be organized based on social or work relationships, on a geographic basis, or by specific functions such as direct action and intelligence. Alternatively, a low-capability insurgent force may combine some functions into multifunctional cells. Cell members remain in close contact to provide emotional support, and to prevent desertion or breach of security procedures. Each cell has a leader who communicates and coordinates with higher levels and other cells.

3-30. As low-capability forces grow, organizational development may take one of two paths. In some cases (such as an urban insurgency), there might be an expanded version of the cellular structure, with a larger number of cells and possibly some functional cells expanding into larger "sections" that,

in turn, break down the functions into more highly specialized cells. More often, however, the insurgent group would evolve into more military-type insurgent organizations, with direct action cells combining to form squads, platoons, and companies, and some of the other functional cells expanding into sections. The following paragraphs describe the functions of the various cells (or sections).

Direct Action Cells

3-31. In a low-capability insurgent force, direct action cells conduct raids, ambushes, terror tactics, and harassment. Some direct action cells may have specialized functions. Direct action cells receive baseline support from intelligence, logistics, communications, and information cells. However, they usually perform their own final target reconnaissance and close-in logistics and communications.

3-32. As an insurgent group develops into a higher-capability, military-type organization, direct action cells combine to form insurgent squads, platoons, companies, and battalions. In some cases, squads could again break down into direct action cells, if necessary. A platoon or company may retain some direct action cells for special functions. There can also be separate cellular structures that are not part of a company or battalion.

Intelligence Cells

3-33. Intelligence cells (or sections) collect, process, and disseminate intelligence and information on the enemy, terrain, and weather; conduct counterintelligence and espionage; plan for and conduct reconnaissance and surveillance missions; and conduct various intelligence and security functions, such as signals reconnaissance and personnel security. Intelligence cells form the foundation of intelligence sections in insurgent battalions and larger insurgent organizations, and are usually found within the structures of the organization's support staff.

3-34. In a low-capability insurgent group, the intelligence cell members primarily collect information from open sources, such as the media, the military, and the indigenous population. As the force develops, the intelligence cell (or section) employs more sophisticated techniques, such as signals reconnaissance, collection using electronic devices, infiltration of government organizations, espionage, document counterfeiting, and counterintelligence activities.

Logistics Cells

3-35. Logistics cells (or sections) provide all types of logistics support. They obtain, maintain, store, and issue supplies and material; arrange and conduct transportation of insurgents, supplies, and materials; transmit funds; operate safe houses and front companies; and provide medical and pharmaceutical support. In an insurgent battalion or higher military headquarters, there are separate cells in a logistics section for many of these functions, specifically financial and medical. When the insurgent organization at a particular level does not have a separate engineer element, logistics cells or sections could be responsible for limited engineer support.

Communications Cells

3-36. Communications cells (or sections) facilitate communications within the insurgent organization. Members provide courier service, maintain and service dead-drop locations, develop codes and ciphers, and operate a multiplicity of communications equipment. In a low-capability insurgent force, communications cells may also conduct electronic warfare activities, such as communications intercept, jamming, and deception in cooperation with the intelligence cells because of its members' expertise. (In a larger insurgent force, the intelligence section has primary responsibility for electronic warfare activities.)

3-37. The communications cell leader often dispatches members to support other elements during preparation for and execution of an action. In a large force, communications personnel and equipment are permanent members of a unit. Each company in an insurgent battalion, for example, has its own communications cell. When necessary, the communications section at the battalion level augments lower-level communications cells.

3-38. With the availability of modern communications systems (such as cellular telephones and computers) on the open and black markets, communications assets are limited only by financial constraints. In many cases, insurgent groups use primitive communications techniques (such as opening and closing windows, the location of a tethered animal, or the arrangement of laundry) to avoid enemy detection and increase the organization's flexibility.

Information Cells

3-39. Different from the intelligence cells, information cells (or sections) develop, produce, and disseminate propaganda, recruit and indoctrinate members, and coordinate information campaigns. These cells conduct overt activities to obtain media exposure, in order to show the ineffectiveness of the government or to show the increasing power of the insurgent organization. This cell coordinates with the communications cell to operate clandestine radio and television stations and gain access to the Internet to disseminate propaganda.

3-40. In a larger insurgent force, information sections specialize. Within the section, one cell may develop and produce products while others disseminate over certain means, such as print, audio-visual, and computer. Additionally, a cell may specialize in strategic perception management actions aimed at external sources of support.

MILITARY-TYPE STRUCTURES

3-41. As the insurgent organization grows, the cellular structure typically evolves into a more hierarchical military-type structure resembling that of a conventional military force. (See Figures 3-2 through 3-4.)

Insurgent Company

3-42. Within an insurgent company, direct action cells combine to form squads and platoons. (See Figure 3-2.) In some cases, a platoon or company may retain some direct action cells (possibly for terror tactics). Alternatively,

squads could break down into direct action cells, if necessary. Except for a communications cell, other functional cells are normally consolidated at the battalion level.

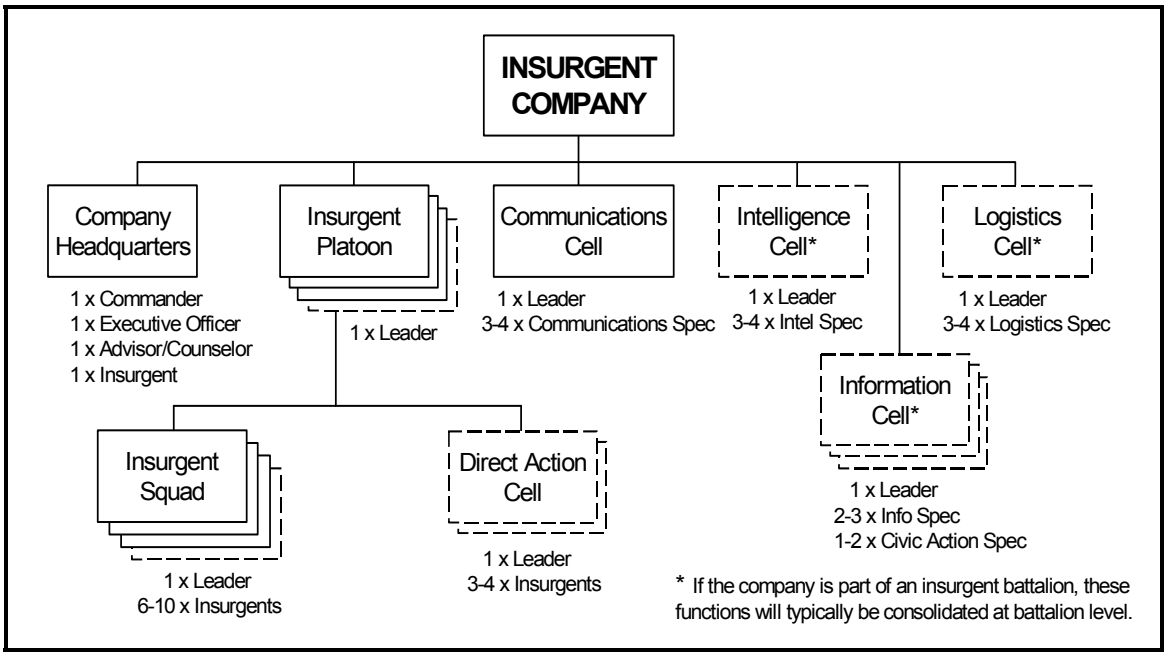

Figure 3-2. Insurgent Company (Example)

Insurgent Battalion

3-43. An insurgent battalion operates like a military organization. Each insurgent battalion differs, but all have a similar structure—a battalion headquarters, support staff, and combat and support elements. (See Figure 3-3.) The headquarters staff may include a deputy commander and/or executive officer, political advisor, administrative staff, and legal advisor.

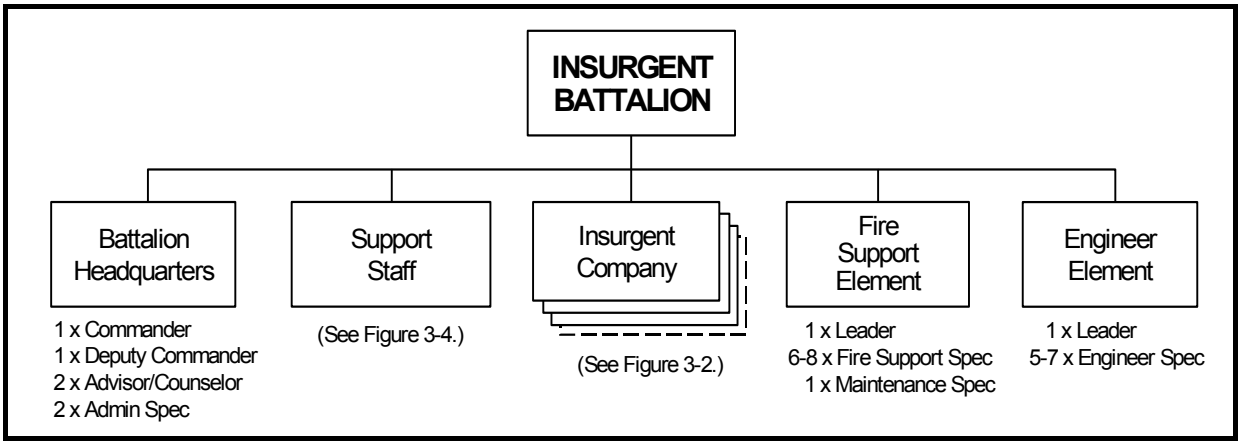

Figure 3-3. Insurgent Battalion (Example)

3-44. Within an insurgent battalion, most direct action cells combine to form insurgent squads, platoons, and companies. Some of the other functional cells expand into sections in a support staff that supports the companies and other elements of the battalion.

3-45. In the support staff, the sections (intelligence, logistics, communications, and information) often consist of more specialized cells (see Figure 3-4). An intelligence section, for example, may have counterintelligence, electronic warfare, and surveillance cells. Likewise, a logistics section may have cells dedicated to transportation, medical, finance, or other materiel support functions.

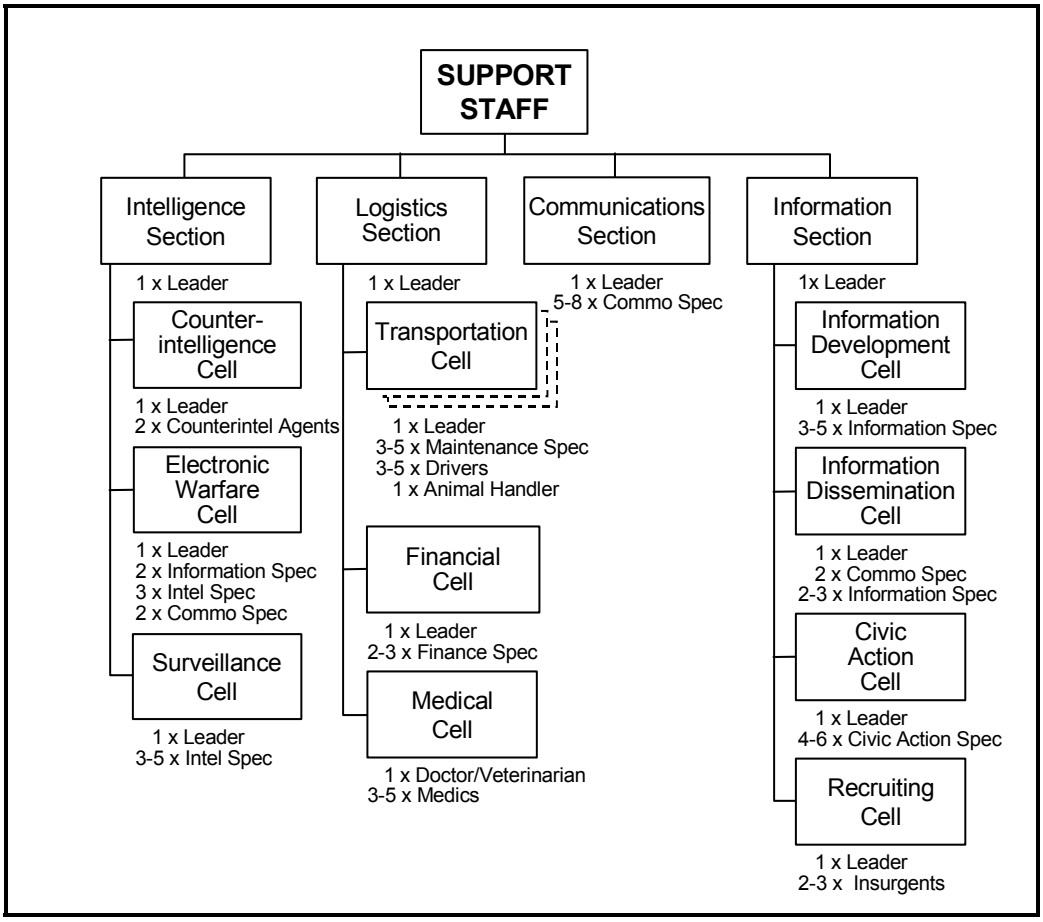

Figure 3-4. Insurgent Battalion Support Staff (Example)

3-46. Mortars and light artillery (122-mm and smaller) compose the fire support element. The fire support element is light, not necessarily out of austerity but for practical reasons: the lightness of the equipment enhances mobility.

3-47. The engineer element provides primarily countermobility and survivability support, such as obstacles and field fortifications. Insurgent engineer support to the companies, platoons, or direct action cells comes from the engineer element at battalion level.

3-48. An insurgent battalion is capable of a variety of activities. With sufficient equipment and resources, it can conduct sustained company-level combined arms actions. A fully capable insurgent battalion, for example, could conduct a raid with three or more companies supported by mortars and light artillery. When employing guerrilla tactics, an insurgent battalion may not fight as a battalion but instead direct platoon- and company-size actions within a geographic area.

POLITICAL-MILITARY STRUCTURE

3-49. As an insurgent organization develops and grows, it often forms a political headquarters to communicate with the indigenous population, external supporters, and the enemy. The leaders in this central political headquarters direct the military forces and ensure that the insurgency remains focused on reaching its long-term goals. Figure 3-5 illustrates the various political and military headquarters and the command and coordination links among them.

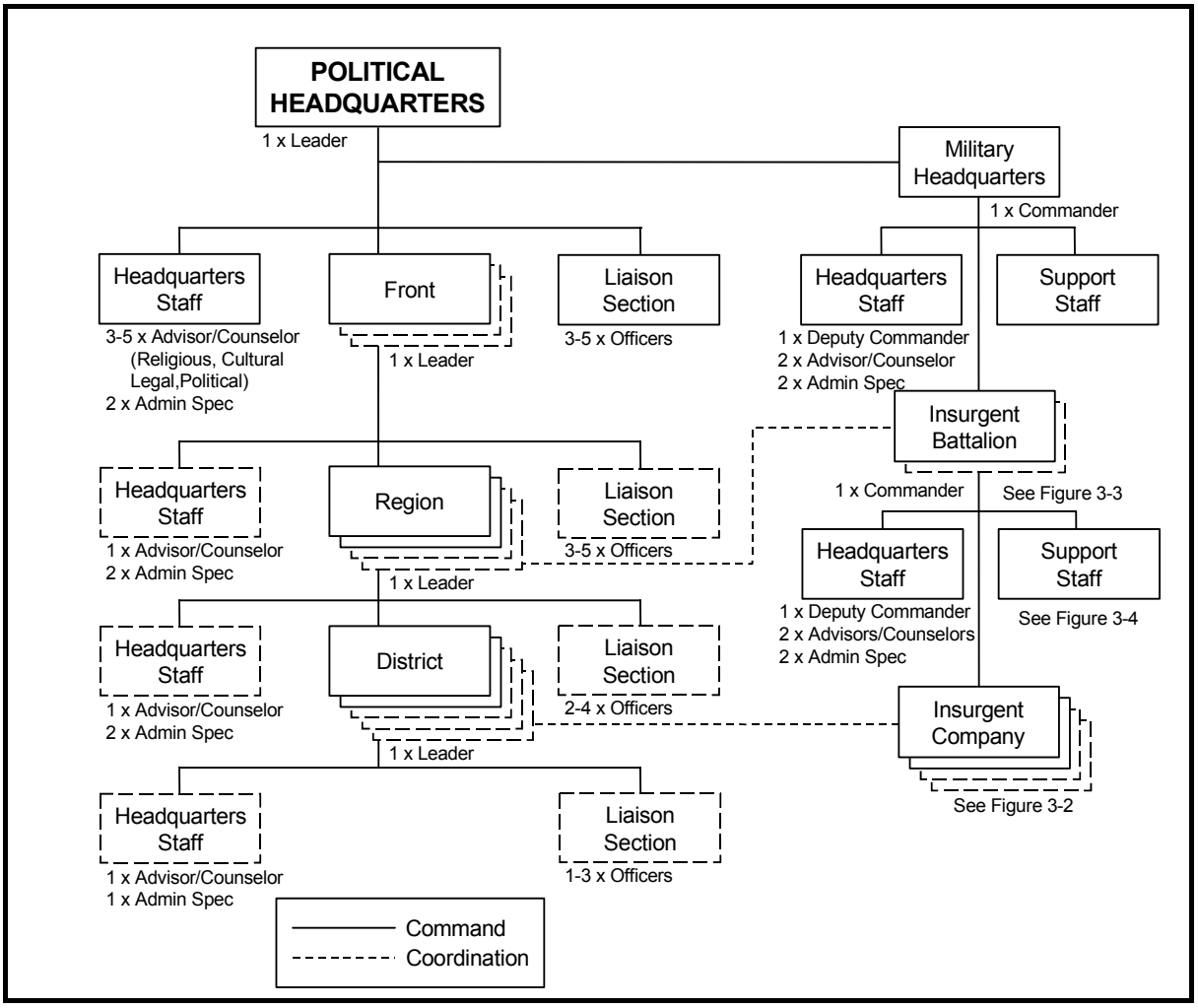

Figure 3-5. Example of an Insurgent Force

3-50. The central political headquarters guides and directs the overall insurgent organization through a series of lower-level political headquarters based on geographic location and population demographics. It also has directly subordinate to it the central military headquarters of the insurgent organization. Under this military headquarters, the insurgency's military organization, a network of insurgent units located in various parts of the targeted country, has its own command structure. Lower-level military units coordinate with the political headquarters of the geographic area in which they are operating and sometimes establish liaison sections in those political headquarters.

3-51. A front is the largest area of territorial responsibility, and includes several regions within the country. Political regions are geographical and/or demographic by design. A region coordinates the actions of its subordinate districts. Each region is comprised of a varying number of districts. Geographic relationships and/or the population distribution serve as the basis for the formation of districts. Districts typically form within a city section, encompass a large village, or several small villages occupying a large area. These regions and districts may or may not geographically align with the boundaries established by the present government.

3-52. Fronts, regions, and districts are political organizations, whereas battalions and companies are military organizations with a completely separate command structure from the political headquarters. Within the force structure, battalions and companies are subordinate to the military headquarters. The number of battalions and companies per region and district depends on the size of the region, the amount of internal support, available resources, and the overall capability of the organization. These battalions vary in composition and size.

3-53. Since the insurgency may have several political or military elements at different phases of development, some conditions may dictate skip-echelon control or subordination within both the political and military structures. The military structure may have some insurgent battalions or companies seemingly not associated with a military headquarters in that district or region. These seemingly autonomous entities are indeed within the political-military structure and have command and control (C^2) relationships similar to conventional military units referred to as "separate." For example, militarily the action may not warrant the employment or organization of a full battalion, but it may require a company. The resulting military organization, when employed or formed, then becomes subordinate to the next-higher authority. Similarly, a district may not be under the control of a region. It may be controlled directly from a front.

3-54. Coordination and communications exist between different levels of the political structures and military structures. Subordinate political entities may have a local agenda, which supports the overall political campaign. Similarly, military commanders only follow orders from their higher command. Since both political and military entities share the same geographical area and long-term goals, coordination and liaison between the two is essential. Even though the political and military structures are independent organizations they are mutually supportive, and the needs and actions of one side can influence the activities and agenda of each other to attain the mutual goal.

3-55. The organization and mission of a large, high-capability insurgent force closely approximate the characteristics of conventional military forces. Although well-developed insurgent groups are capable of conducting force-on-force actions, hit-and-run actions such as raids, ambushes, and terror tactics are preferred. These activities are low-risk and high-payoff; they minimize contact with enemy forces and are potentially very destructive. The insurgent force is unpredictable and seemingly invisible. The enemy cannot anticipate the next move and often considers this adaptive style as not fighting by the rules of conventional warfare.

TACTICS

3-56. Insurgent forces use a variety of tactics depending on unit size, level of training, firepower capability, resources available, and terrain. The tactics employed will also be tailored for actions against the targeted government. Activities become increasingly sophisticated in areas where the insurgency is at a more advanced stage, where its presence is heaviest, and where it is more difficult for the enemy to gain access, infiltrate, or respond.

3-57. Insurgent tactics include terror tactics which are described in Chapter 2 and conventional small unit tactics (described in FM 7-100.4). This section describes those tactics used by insurgents in the conduct of guerrilla or unconventional warfare. It is this form of warfare that is most commonly associated with insurgent groups.

3-58. In general terms, insurgents forces tend to fight as small units that number in the tens or hundreds at most. Their actions are target- or force-oriented and do not recognize a front or a rear. They strike where the enemy is weak, and avoid confrontation where he is strong. Insurgent tactics emphasize tactical mobility.

OFFENSE

3-59. Insurgents keep their attacks simple, thus reducing the burdens of administration and logistics support. The two basic offensive tactics used by insurgents are raids and ambushes. Depending on their level of training, insurgents may also employ many of the small unit tactics described in FM 7-100.4. Insurgent forces avoid decisive engagement until they have confidence that military victory is certain.

3-60. Offensive tactics emphasize hit-and-run techniques. Insurgents seek to mass forces sufficiently to ensure success, hit targets where least expected, and disperse immediately thereafter. Insurgent forces rely on flexibility and surprise to compensate for lack of personnel and equipment. If unexpected resistance is encountered during an attack, the mission is aborted to preclude defeat.

Raid

3-61. A raid is a surprise attack of an enemy force, installation, or site. Such attacks are characterized by secret movement to the objective area; brief, violent action; rapid disengagement from action; and swift, deceptive withdrawal. Typically, insurgents conduct raids against soft targets, such as a communications site, storage facility, or other target with limited security. To

ensure success, the raiding force rehearses the plan and all of its contingencies. Insurgents conduct raids to kill or capture enemy personnel, and destroy or capture equipment, or cause casualties among enemy supporters. Raids also serve to distract attention from other insurgent actions, to keep the enemy off balance, and to cause the enemy to expend excessive resources to protect facilities, infrastructures, and supplies.

3-62. **Intelligence.** The key to a successful raid is intelligence. Without sufficient intelligence, the insurgent force cannot adequately plan for or conduct a raid. Detailed planning is fundamental to success. The raiding force requires intelligence on the size and capability of the security force. It particularly needs information on the location and disposition of the enemy's—

- Crew-served and indirect-fire weapons.
- Leadership, C^2 facilities, and communications equipment.
- Reserve or support forces, including their response time.

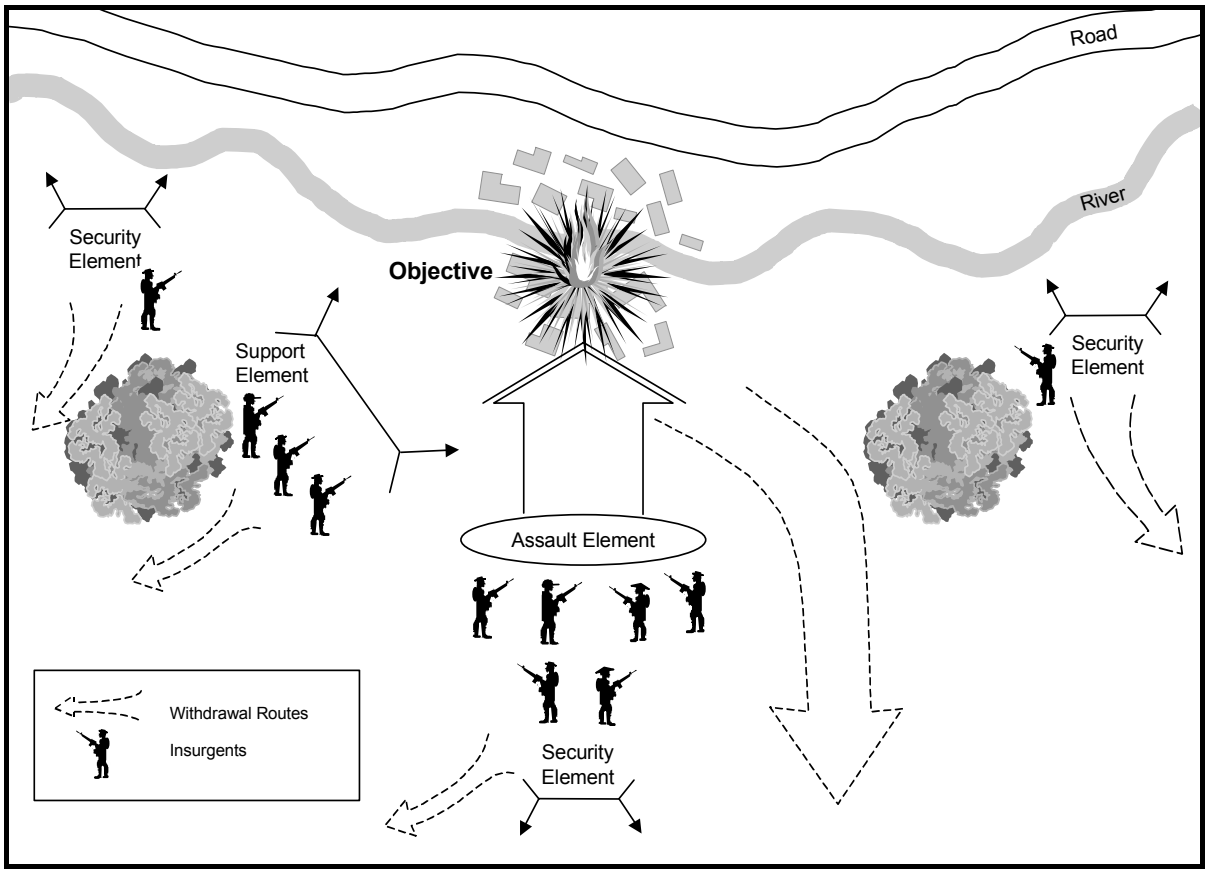

Figure 3-6. Raid Performed by Direct Action Cell (Example)

3-63. **Conduct.** The raiding force has three major subgroups: the assault element, the support element, and the security element. The assault element assaults the target, eliminates all enemy resistance by killing enemy personnel, and secures the entire objective. The support element gains control of the objective by fire and supports the movement of the assault element onto the

objective. The security element establishes security positions on all avenues of approach, provides early warning, and prevents other enemy forces from reinforcing the target. Figure 3-6 illustrates a direct action cell conducting a raid. Larger forces conduct a raid in a similar manner using more forces.

3-64. The insurgent leader's analysis of the enemy situation dictates the size and composition of the assault, support, and security elements. For example, an insurgent battalion may use a company for each element, while a low-capability insurgent force may use one direct action cell that performs all these functions or use individuals who perform some functions in sequence. Both tailor their forces to execute all the functions of the assault, support, and security elements.

3-65. **Withdrawal or Occupation.** Raids include withdrawal plans, but the raiding force may not conduct an immediate withdrawal if the enemy does not counterattack. A raiding force may elect to remain on the target until forced off by the enemy or receiving change of mission. Especially in a rural environment where government forces are not present at all or in strength, an insurgent force may take over the raided site. If a force raids a radio station, for example, it may occupy and broadcast from the station until removed.

Ambush

3-66. An ambush is an offensive attack conducted from a defensive posture against a moving enemy. Ambush forces have three basic subgroups: the assault element, the support element, and the security element. Insurgent leaders analyze the terrain and enemy to determine the ambush subgroups' size and location. The leaders dictate the purpose of ambush—annihilation, harassment, or containment—based on the desired effects and the resources available. Ambushes are frequently employed because they have a great chance of success and provide the best protection. Insurgents conduct ambushes to kill or capture personnel, destroy or capture equipment, restrict enemy freedom of movement, and collect information and supplies.

3-67. As in a raid, intelligence is critical to a successful ambush. The ambush force requires some intelligence to conduct rehearsals under conditions and in terrain resembling the actual ambush site. Whenever possible, insurgents rehearse the ambush in detail at the actual ambush site. Intelligence is required on—

- Known enemy routes.
- Types and capabilities of vehicles used by the enemy.
- Disposition, composition, and strength of enemy units.

3-68. The tactical considerations for employing an ambush may call for a linear arrangement or a variety of other spatial arrangements. Terrain, location, weapon placement, fields of fire, and placement of security elements and rendezvous positions will vary with each ambush, and must be considered prior to each ambush.

3-69. **Annihilation Ambush.** The purpose of an annihilation ambush is to destroy the enemy force. Generally, this type of ambush employs mines and other obstacles to halt the enemy in the kill zone. The goal of the obstacles is

to keep the enemy in the kill zone throughout the action. Through direct fire systems, the support element destroys or suppresses all enemy forces in the kill zone. It remains in a concealed location and may have special weapons, such as antitank weapons. The support and assault elements kill enemy personnel and destroy equipment within the kill zone by concentrated fires. The assault element remains in covered and concealed positions until enemy activity ceases within the kill zone. Once the enemy ceases his activity, the assault element secures the kill zone and eliminates any remaining enemy personnel that pose a threat. The assault element remains in the kill zone to thoroughly search for any usable information and equipment, which it takes or destroys. The security element positions itself to ensure early warning and to prevent the enemy from escaping the kill zone. Following the initiation of the ambush, the security element seals the kill zone and does not allow any enemy forces in or out. The ambush force withdraws in sequence; the assault element withdraws first, then the support element, and lastly the security element. The entire ambush force reassembles at a predetermined location and time. Figure 3-7 illustrates an insurgent battalion conducting an annihilation ambush. Other insurgent forces would conduct this type of ambush in a similar manner.

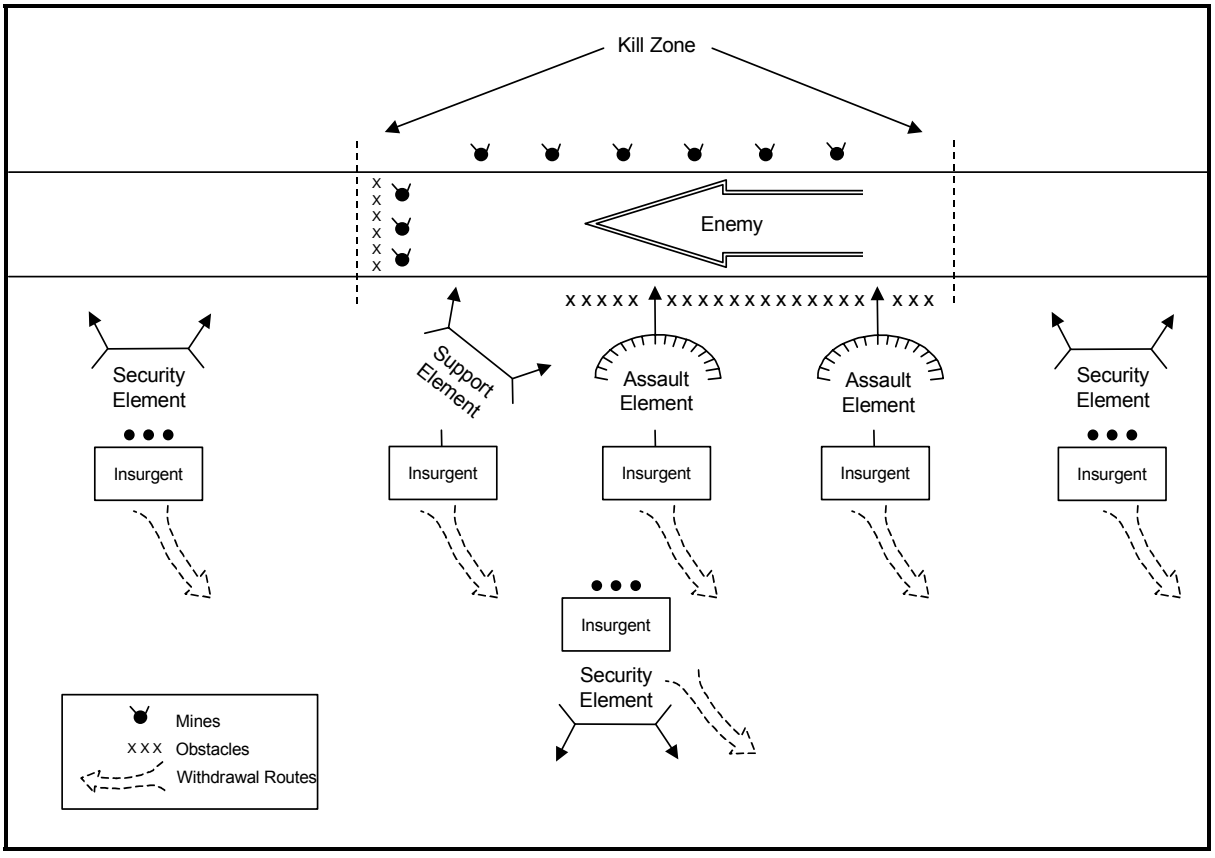

Figure 3-7. Annihilation Ambush Conducted by an Insurgent Battalion (Example)

3-70. An insurgent force that desires to conduct an annihilation ambush may recognizes that its strength at the ambush site is not on par with the enemy force. In such situations, it can hit the middle or rear of the enemy convoy to avoid the preponderance of convoy escort vehicles. The desired effect of this is that the convoy commander is not certain whether he is being ambushed or just drawing harassing fire, and the convoy may incur significant losses before he can determine which it is.

3-71. **Harassment Ambush.** A harassment ambush interferes with routine enemy activities, impedes the enemy's freedom of movement, and has a psychological impact on enemy personnel. An insurgent force may choose to conduct a harassment ambush if the enemy has superior combat power. This type of ambush does not require the use of obstacles to keep the enemy in the kill zone. The ambush force conducts the harassment ambush at a greater distance from the enemy, up to the maximum effective range of its weapons. Figure 3-8 illustrates an insurgent company conducting a harassment ambush. Other-size insurgent forces conduct this type of ambush in a similar manner.

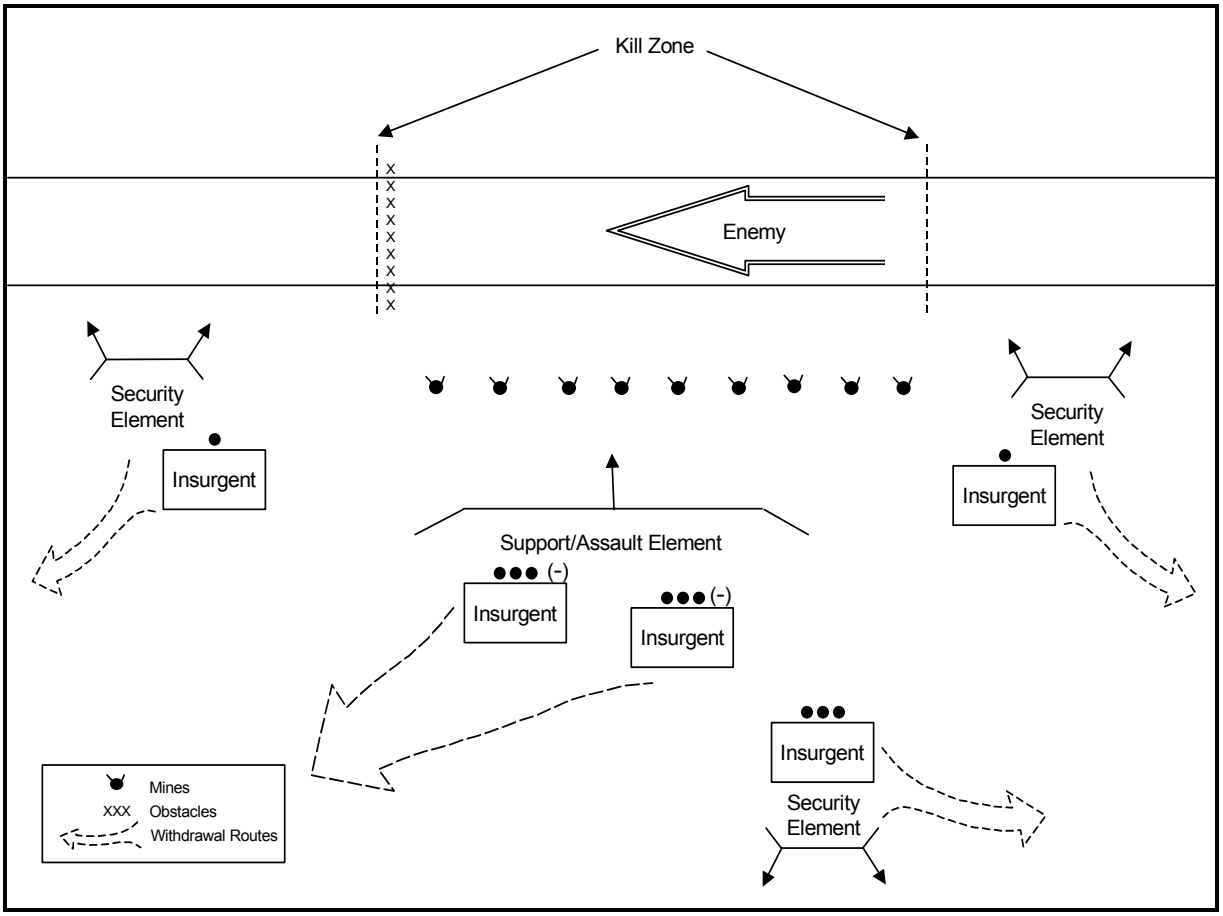

Figure 3-8. Harassment Ambush Conducted by an Insurgent Company (Example)

3-72. Many times, the assault and support elements are combined to provide better control of fires throughout the kill zone, which may be quite wide. The

assault element does not normally perform the role of assaulting the kill zone, but may if conditions permit. The assault and support elements concentrate massive direct and indirect fires in the kill zone. The security element provides early warning.

3-73. While the assault and support elements withdraw, the security element remains to provide warning and to delay enemy forces if necessary. As in all ambushes, the ambush force may emplace mines and plan for indirect fires to cover withdrawal routes. Once the entire ambush force reassembles, it quickly moves out of the area to avoid contact with enemy forces responding to the ambush.

3-74. **Containment Ambush.** A containment ambush is a security measure that is usually part of a larger action. It is used to prevent the enemy from using an avenue of approach or interdicting another action, such as a raid. The assault element may assault to secure the kill zone, as described in the annihilation ambush, although this is not required for success. The support and security elements perform the same functions as those described in the annihilation ambush. Figure 3-9 illustrates a containment ambush supporting a raid.

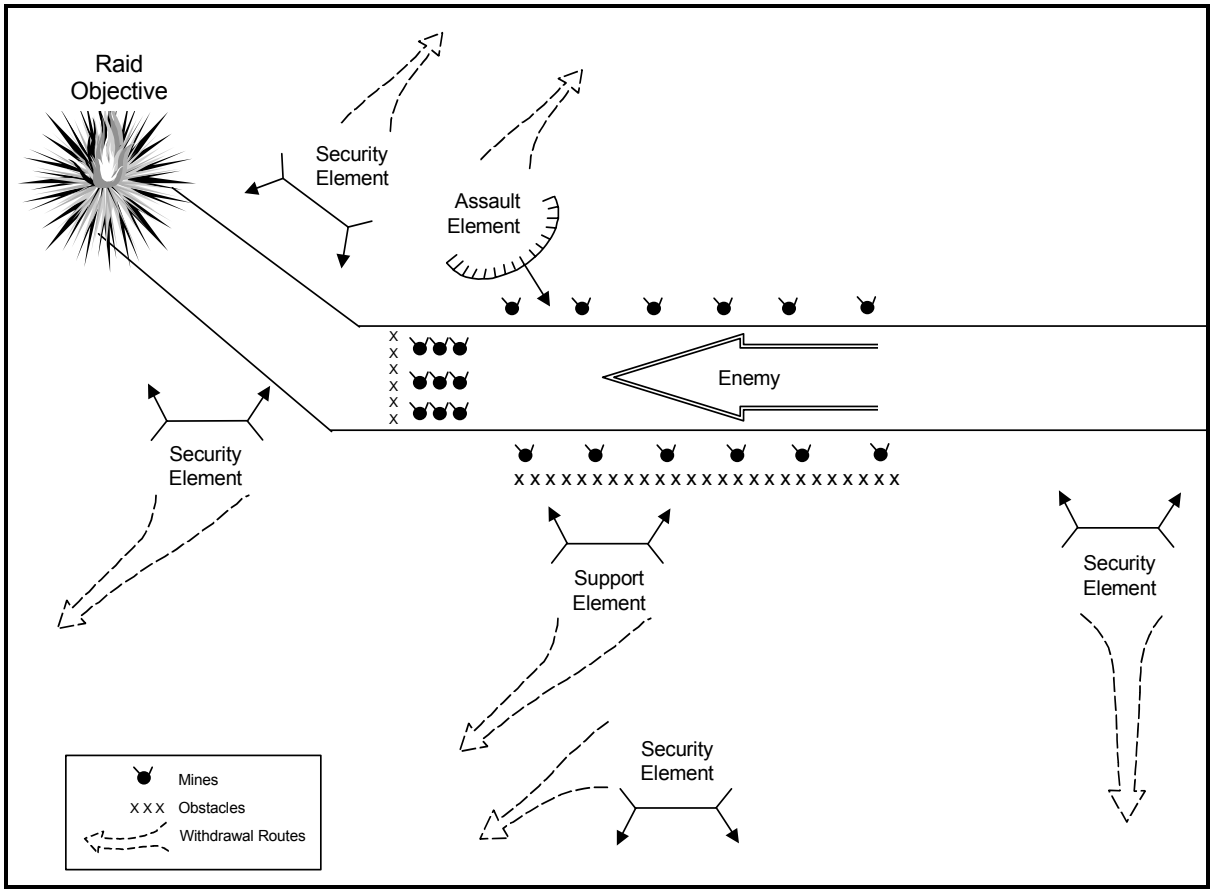

Figure 3-9. Containment Ambush Supporting a Raid (Example)

3-75. Obstacles are an integral part of a successful containment ambush. They serve two functions: to prevent the enemy from using the avenue of approach and to hold the enemy in the kill zone. Within time constraints, the ambushing force may erect multiple, mutually supporting obstacles covered by direct and indirect fires.

DEFENSE

3-76. Defense is a temporary and necessary state of combat action that provides for the holding of terrain, preservation of resources, rest and recuperation, refit and maintenance of equipment, and training. Defensive actions also allow insurgent forces to withdraw, hold occupied positions, or create conditions favorable for resuming offensive actions. Security measures are taken to protect against enemy actions, and they also are designed to impair enemy effectiveness. Defensive activities are primarily conducted through active and passive security measures, and conventional operational security methods. Based on their level of training, insurgents may also be able to employ many of the defensive techniques described for small military units in FM 7-100.4.

Active Security Measures

3-77. Active security measures are those procedures characterized by someone or something taking action or reacting. Examples of active security measures include—

- Obstacles.
- Booby traps.
- Observation or listening posts.
- Guards.
- Early warning systems.
- Checkpoints.

Insurgents often use various combinations of these measures.

3-78. **Obstacles.** Obstacles are designed or employed to disrupt, fix, turn, or block the movement of the enemy and to force additional enemy losses in personnel, time, and equipment. Most obstacles (such as wire or log obstacles and roadblocks) are covered by weapon fire and protected by early warning systems. They are concealed from enemy observation by incorporating terrain features, erected in irregular and nongeometrical patterns, and coordinated with other security measures.

3-79. **Booby Traps.** A booby trap is an explosive or nonexplosive device or other material deliberately placed to cause casualties when an apparently harmless object is disturbed or a normally safe act is performed. These low-cost, highly destructive tools range from crude or simple, to sophisticated and ingenious. Booby traps are popular because they are easy to construct and use anywhere, produce casualties and damage for a relatively low investment, and considerably slow the activities and movements of the enemy. Booby traps are used primarily to conduct sabotage, cause casualties, provide early warning, and harass. Anything can be booby trapped—buildings, weapons, corpses, and common items such as stereos, pens, and flashlights. Techniques

used to detonate these booby traps include trip wires or electronic initiation, traction, tension, pressure, magnetic, and seismic fuses. Booby traps are camouflaged and weatherized to prevent detection and unintentional detonation. Some booby traps, especially mines, feature blast resistance and antihandling devices.

3-80. Nonexplosive booby traps include spike traps, ditches, and craters. Holes of various sizes are dug, depending on the intended target, and filled with bamboo sticks, barbs, nails, coils, or other sharp items intended to inflict injury or damage. Figure 3-10 illustrates two types of nonexplosive booby traps—a spike trap and a vehicle ditch.

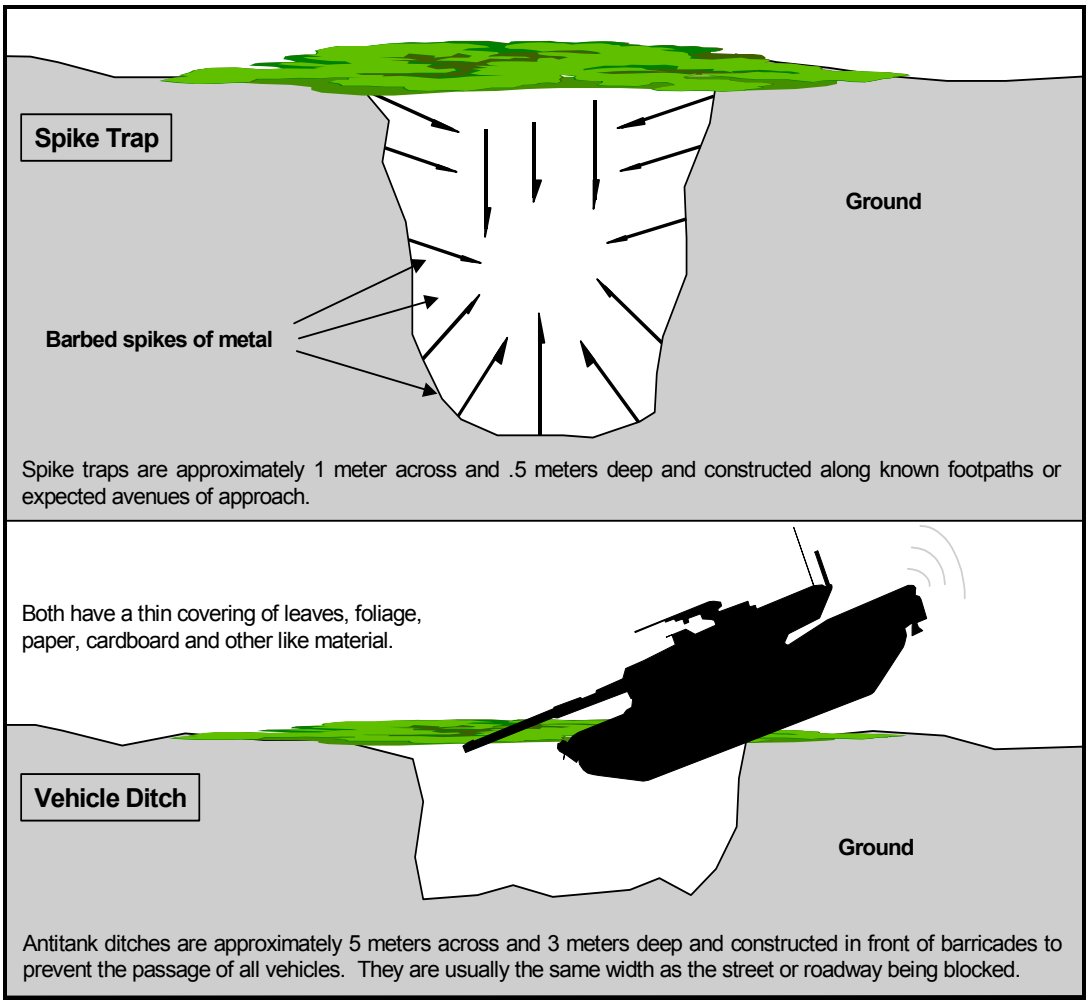

Figure 3-10. Example of a Spike Trap and a Vehicle Ditch

3-81. Mines are the most common booby trap and are available in a wide variety of shapes and sizes depending on their purpose. One of the most common devices is the claymore-type directional mine, which consists of a container filled with fused explosives and scatterable material, such as rocks, bolts, or scrap metal. Figure 3-11 illustrates a pressure mine buried under improved road surfaces.

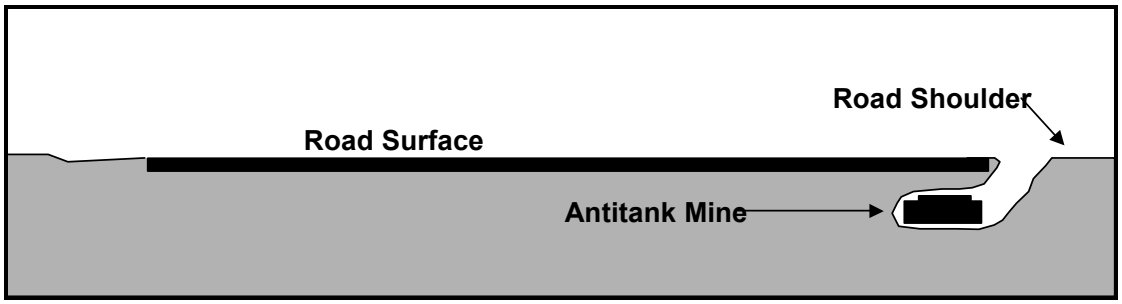

Figure 3-11. Buried Pressure Mine

3-82. The ramifications and consequences of mines must be thoroughly considered prior to their employment. The potential of collateral damage injuring or killing innocent victims could have a negative impact on the insurgents' strategic goal.

3-83. **Observation and Listening Posts.** Insurgent forces must establish observation and listening posts at all campsites and when conducting surveillance. Considering terrain and weather effects, they establish posts a prudent distance from the base camp or the enemy to ensure mission accomplishment and early warning. A force with access to night-vision and encrypted-communication devices may choose to position its posts at greater distances than a force relying on wire communications or manual methods to maximize the early warning notification time. Conversely, if security is the key concern, wire communications or runners may be employed, since these may be deemed more secure than high-technology communication methods. When establishing posts, insurgents incorporate other security measures, such as camouflage and booby traps, and employ basic tactical principles, such as good fields of vision and fire.

3-84. **Guards.** Guards may be employed to protect key facilities and personnel. They receive additional training depending on their mission. A bodyguard, for example, receives training in personal protection, hand-to-hand combat, and defensive driving techniques. Guards may act as sentries or patrols, again depending on the mission. Stationary guards may camouflage their guard posts to prevent detection or remain exposed to conduct security activities, such as verifying identity. Weapons carried by guards range from hidden handguns to crew-served weapons.

3-85. **Early Warning Systems.** Early warning systems attempt to create maximum time and space between the friendly forces and the enemy in order to avoid direct confrontation. Systems may include video cameras, motion sensors, explosive booby traps, or personnel. Insurgent forces may employ early warning systems, such as a motion sensor for an electronically-initiated booby trap, to provide security during offensive actions or at a key facility or base camp.

3-86. **Checkpoints.** Insurgents can employ checkpoints to control traffic, gather information, or harass. A typical checkpoint may be either permanent or temporary, and may include a sampling of any or all of the above- mentioned active security measures. For example, a checkpoint may employ concealed and exposed barriers (such as booby traps and mines) along the route, iron tetrahedron obstacles or barbed wire in front of the checkpoint, and weapons emplacements and guards, as depicted in Figure 3-12.

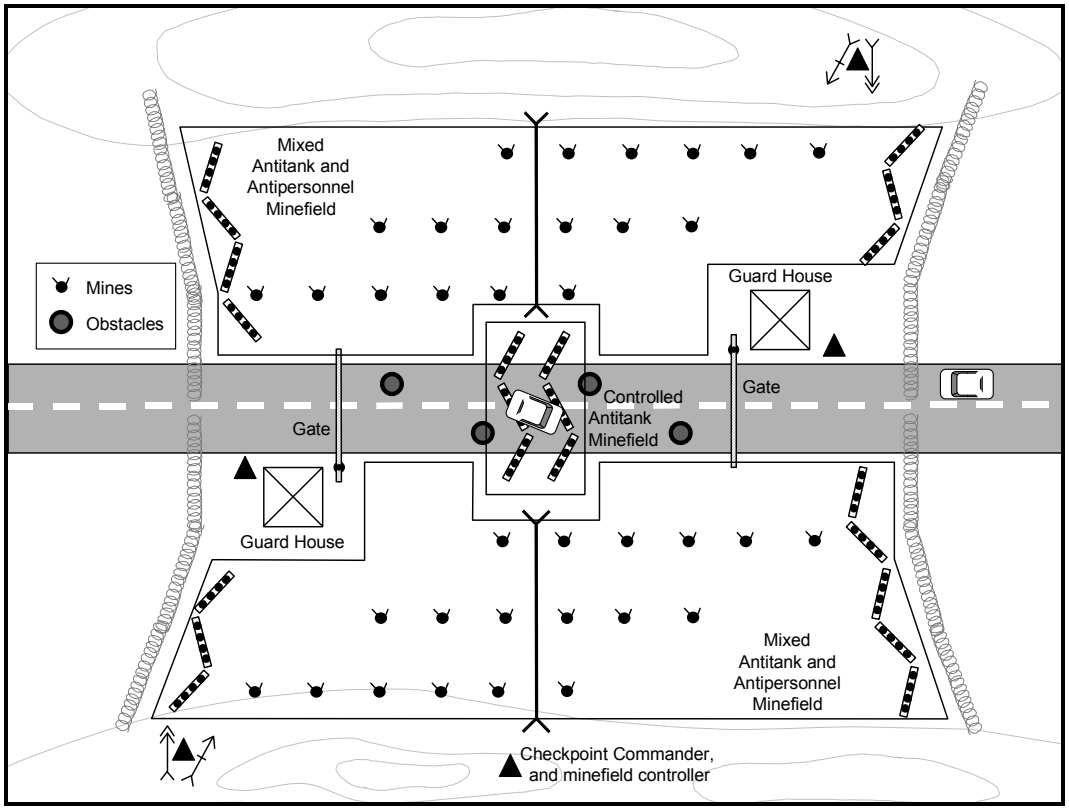

Figure 3-12. Example of a Checkpoint

Passive Security Measures

3-87. Passive security measures are those procedures taken to reduce the probability of enemy action and to minimize its effects. Such measures include—

- Field fortifications.
- Tunnels.
- Camouflage and cover.
- Countermeasures.
- Noise, light, and trash discipline.

3-88. Field fortifications are constructed as a force protection measure and to store water, food, and other essential supplies. The size of field fortifications varies according to the need. Generally, they are built inside structures or

under natural cover, and covered with lumber, layers of dirt, tires, or other protective and concealing material. Small openings permit passage in and out.

3-89. Tunnels also provide protection and help avoid detection. They range from rudimentary escape passages to sophisticated systems with multiple passages and entrances. The more sophisticated tunnel systems can be used for bases, hospitals, kitchens, and production facilities.

3-90. Camouflage and cover are of utmost importance, and all insurgent forces must be extremely disciplined when it comes to maintaining security. they employ camouflage and cover to hide, blend, or disguise their activities. They may also intentionally use poor techniques to distract the enemy to dummy sites. They can use smoke pots, natural cover, and artificial cover. Insurgents carefully observe the principle of noise and light discipline: they avoid shouting, whistling, practice shots and explosions, night lighting, and other activities that would attract undue attention.

INFORMATION WARFARE

3-91. Having an information advantage is one of the few ways in which a smaller or inferior insurgent force can change the balance of power that normally favors the enemy. Tactics executed under the umbrella of information warfare (IW) involve integrated political, legal, military, psychological, and economic considerations. After developing an information strategy to help reach its goals, an insurgent force develops an IW campaign. The campaign integrates several actions—

- Electronic warfare.
- Computer warfare.
- Deception.
- Physical destruction.
- Protection and security measures.
- Perception management.
- Information attack.

These activities are not mutually exclusive, and often overlap. (See Chapter 2 for more detail on these activities.)

3-92. Depending on its level of capability, the insurgent force may or may not be able to conduct all these activities. However, even an unsophisticated group with very little money can obtain, or even hire, a wide range of capabilities from around the world. A low-capability insurgent force primarily focuses on perception management and protection and security measures while trying to build legitimacy and recruit people. As the group becomes increasingly capable, electronic warfare and deception may take precedence.

3-93. The leader provides his information strategy and guidance to the information cell or section, which develops an IW campaign. The information cell or section coordinates and integrates various assets to implement a campaign. The IW campaign includes civic actions, radio broadcasts, indoctrination training, establishment of a web page, and selective sabotage actions, all integrated to further the short- and long-range goals.

ELECTRONIC WARFARE

3-94. Electronic warfare includes signals reconnaissance, deception, electronic jamming, and physical destruction. While destruction is the primary method used to disrupt enemy communications and radars, insurgent forces may limit destruction to acts of sabotage in order to avoid escalating the conflict. In a low-capability insurgent force, members of the communications cell conduct electronic warfare when they have the technical ability and the required equipment. In a high-capability group, members of the intelligence section conduct electronic warfare. Often, as the organization develops and grows, members with technical expertise move from the communications cell to the intelligence cell or section.

3-95. Signals reconnaissance is the sum of all intercept and direction-finding means used to identify and locate enemy electronic emissions. Members of the intelligence section perform analysis to identify high-priority targets for deception, jamming, or further exploitation. Electronic deception is always part of an overall deception plan. This ensures that what the enemy collects electronically confirms, or at least does not refute, the indicators presented by other deception means. All types of electronic equipment are vulnerable to both deception and jamming. Because of the specialized equipment required and the possibility of escalating a conflict, jamming is rare.

CYBER-INSURGENCY

3-96. Cyber-insurgency is any activity performed by insurgents or insurgent sympathizers with or to computers. For example, insurgent organizations can use the Internet to communicate within their own organization, with like-minded organizations, and with sources of internal and external support. They can use it to recruit members and raise funds. The Internet allows insurgent information campaigns to reach a large audience, both inside and outside the country, at relatively low cost. To avoid government restrictions on Internet usage, insurgents can establish foreign-based websites.

3-97. Easy access and relatively low cost have made information technology an attractive solution for the business of government. However, these same factors also make the government vulnerable to cyber-insurgency, which offers new forms of attack and a range of targets previously unavailable. It allows insurgents to operate without a physical presence. Insurgent groups may form or encourage “hacker collectives” to disrupt or damage government information systems.

3-98. Cyber-insurgency can use many of the same techniques as cyberterrorism (see Chapter 4). The primary difference is that cyber-insurgency seeks to disrupt government activities or cause economic damage to the government or government supporters without having harmful effects on the life and well-being of the general populace.

INTELLIGENCE

3-99. Intelligence is fundamental for success of an insurgency. All insurgent forces want and need to determine what the enemy is doing, while denying him information. Intelligence functions include information collection, counterintelligence, and reconnaissance and surveillance.

INFORMATION COLLECTION

3-100. For information collection, insurgent forces use all available assets, ranging from technical means to human intelligence (HUMINT) assets. In the absence of sophisticated technology, groups rely on HUMINT agents. However, as discussed in the section on information warfare, even unsophisticated forces can have high-technology equipment. The primary difference is in the ability to integrate collection assets in a timely manner.

3-101. Collecting information, overtly and clandestinely, is a continuous function performed by every insurgent. Overt activities include interrogation, civic actions, and open collection of information by individuals who circulate among the people. This type of activity attempts to procure copies of local maps, publications containing information about the area, and official enemy publications available to the general public. Additionally, if military or peacekeeping forces are involved, procurement of the rules of engagement (ROE) is of key interest to insurgent forces. By obtaining this information, the insurgency can exploit weaknesses or loopholes in the ROE.

3-102. The majority of information gathered comes from open sources, such as printed publications, publications available on the Internet, enemy press releases, and the media. Another important source is civilians who work or live in areas where they can observe enemy activities. Clandestine activities involve secret collection of information. Insurgent groups clandestinely collect information using electronic devices, patrols, observation posts, or HUMINT agents who may join or infiltrate popular organizations, enemy organizations, and nongovernmental organizations. When insurgents are planning any action, an intelligence section analyzes information from both overt and clandestine sources.

COUNTERINTELLIGENCE

3-103. Counterintelligence includes those activities designed to protect the insurgent force against enemy intelligence-collection actions. Counterintelligence activities are conducted against the enemy and possibly members of the insurgent organization. Insurgents acknowledge that their own organization is vulnerable to infiltration and exploitation. The cellular structure and periodic indoctrination training are two counterintelligence methods designed to enhance security.

3-104. Insurgent forces may also isolate their key leaders (especially in the early stages) and refer to them by code name only (such as *El Commandante*). This ensures their anonymity and safety should there be a breach of internal security. The true identity of these leaders may never be revealed, or at least not until the insurgency is relatively certain of success, or their visible presence is needed to gather additional support and unity.

RECONNAISSANCE AND SURVEILLANCE

3-105. Insurgent forces conduct reconnaissance to obtain information about the terrain or the activities and resources of the enemy. Observation is the most common method used to conduct reconnaissance. However, with the availability of specific equipment, reconnaissance using electronic devices is becoming increasingly popular.

3-106. Reconnaissance is crucial prior to the execution of raids and ambushes. Detailed information regarding the terrain at the raid or ambush site and the capability of the enemy is vital. Typically, a reconnaissance patrol reconnoiters the routes to and from the site and the site layout. Whenever possible, the leader uses personnel who are local residents of the area to conduct the reconnaissance mission. If possible, he personally checks the area near the raid or ambush site.

3-107. Surveillance using visual, aural, electronic, photographic, or other means is always conducted. Civilians living, traveling, or working near either a target area or the enemy can conduct surveillance on behalf of the insurgent forces. Some civilians volunteer, while others are coerced into providing this support. The leader and/or his intelligence section evaluates the information passed by civilians based on their trustworthiness and past performance. Intelligence section members also conduct surveillance.

INTELLIGENCE REPORTING

3-108. After collecting information through reconnaissance and surveillance, by coming in contact with the enemy, or by interviewing civilians, insurgent personnel prepare an intelligence report. Report information includes—

- Date and time of observation.
- Type of activity or mission of the friendly force.
- Location and disposition of the element making the observation.
- Estimated enemy strength.
- Location and disposition of the enemy.
- Type of contact made with the enemy.
- Results caused by the contact.
- Enemy activity prior to and during contact.
- Enemy attitude or peculiarities.
- Identification of enemy forces.
- Number of friendly and enemy losses.
- Attached sketch with annotations.

A low-capability insurgent force may not always use this formal reporting format, but it would include this type of information.

LOGISTICS SUPPORT

3-109. As an insurgency develops, its requirements for supplies and equipment grow. However, it often has a much less sophisticated logistics system than conventional military forces. Logistics support is divided into three principal functions—materiel support, maintenance, and medical support.

MATERIEL SUPPORT FUNCTIONS

3-110. Materiel support includes the transportation, storage, and supply of all materiel required to sustain activities. Supply bases, caches and safe houses are techniques used to store and supply materiel. All three techniques use cover, camouflage, concealment, deception, and other security measures to protect against or evade enemy detection.

Transportation

3-111. The logistics cell or section employs a variety of organic, stolen, or captured conveyances, such as animals, vehicles, ships, and aircraft. Resources and the terrain determine the type of conveyance used. Animals are a popular means since they can carry relatively large quantities of supplies and materiel over rough or difficult terrain. Land vehicles require little operator training and less logistics support and are more readily available than littoral or river vessels, and aircraft. In most cases, vehicles can be stolen, captured, or purchased from internal sources. On the other hand, ships and aircraft are typically provided by external sources.

Supply Bases

3-112. Supply bases in semi-fixed locations are the largest facilities used for the storage and distribution of equipment, materiel, and supplies. Generally, these facilities characterize the upper echelons of the supply system and are high-value targets for the enemy. For this reason, these facilities are very well protected and concealed, or often located underground. Supplies located in these bases are constantly cross-leveled or redundant in nature, so that if one base is compromised or destroyed, the capability (though diminished) will not be significantly impaired. To ensure security, the resupply actions conducted from these bases usually occur at night and are characterized by little visible traffic.

Caches

3-113. Caches are hiding places for supplies and equipment. Caches are used because supplies and equipment are critical to actions and are difficult to replace. These storage areas are found underground or in dense vegetation, caves, remote areas, basements, or false walls. Security measures employed to protect caches include obstacles, patrols, guards, and early warning systems. In case of compromise, insurgents boobytrap caches to prevent the enemy from using the equipment or supplies.

Camps and Sanctuaries

3-114. Insurgent forces cannot fight all the time. They need safe areas where they can retire, voluntarily or involuntarily. They can use these areas to rest and recuperate; to maintain, repair, and prepare equipment and weapons; or to receive training. Traditionally, these areas, called "camps," are located in remote, rugged terrain. Camps located in other countries are referred to as "sanctuaries." These camps or sanctuaries are a vital component of any insurgent strategy. When establishing a camp, insurgents consider the following factors—

- Availability of water, food, and other necessities.
- Natural terrain masking features.
- Sufficient vegetation for concealment and camouflage.
- Nearby elevations to maintain communications and observation.
- Infiltration and exfiltration routes.
- Sufficient space to conduct activities, such as large areas for a training camp.

3-115. Camps have no set pattern and can be permanent or temporary. A low-capability insurgent force is more likely to have temporary camps than a higher-capability force because of the latter's control of certain geographical areas. The purpose of the camp, size of the force using the camp, and terrain determine the size of the camp. There are four basic types of camps—base, reserve, mobile, and false.

3-116. A *base camp* is a permanent camp used for C^2 or training. The insurgent organization constructs buildings and training facilities in areas under its control or in other countries. These camps have an integral security system based on concentric rings of extensive security measures, such as observation posts, guards, patrols, obstacles, and early warning systems.

3-117. A *reserve camp* is a preselected location that forces occupy if the base camp is permanently evacuated. Once occupied, the reserve camp becomes the base camp. The location of a reserve camp is closely guarded and known only to select members.

3-118. During the conduct of actions, insurgents may establish temporary *mobile camps*. Poorly camouflaged *false camps* can deceive enemy forces regarding the actual location of camps.

Safe Houses

3-119. A safe house is a building where insurgents engage in secret activities or take refuge. A safe house is similar to a base camp in the purpose of providing sanctuary. However, a safe house is primarily (but not necessarily) a building found in an urban area, whereas a base camp is a complex found in a rural area. From the outside, a safe house is indistinguishable from any other building in the locale. However, extensive security measures (such as code words and locks) are employed to prevent compromise or at a minimum to delay enemy forces.

MAINTENANCE SUPPORT FUNCTIONS

3-120. Maintenance includes all functions conducted to maintain, repair, and prepare equipment and weapons for employment. The logistics cell or section is responsible for maintenance. It may establish a facility in which to perform maintenance or use a civilian business, such as an auto repair shop. The facility may be located underground or at a camp. Some insurgents receive maintenance training for high-value or specialized equipment, such as computers or electronic warfare equipment.

MEDICAL SUPPORT FUNCTIONS

3-121. Medical support includes the medical measures required for evacuation and treatment of casualties and for the prevention of disease. Civic actions often incorporate medical support to help build and maintain internal support. In a large organization, a specialized cell within a logistics section provides medical support.

SOURCES OF SUPPORT

3-122. Support for an insurgent group is divided into two sources—internal and external. Primarily, insurgent organizations must rely on themselves, and the various cells or sections internal to the organization for assistance. By charging itself with support internally, it ensures a measure of security in the conduct of its actions. Yet, to attain long-term goals, additional support is critical, first coming from other sources internal to the country—popular support. For some actions, or when the insurgent organization grows, external support may be needed to ensure continued activity. This external support received from other countries, organizations, or individuals sympathizing with the insurgents may help the insurgency develop or hasten its victory.

INTERNAL SUPPORT

3-123. Internal support is critical to the survival of any insurgency. Without internal support of the local populace, it cannot reach its long-term goals. Depending on its strategy, the insurgent force either needs internal support immediately (in the case of a protracted popular war or urban strategy) or it assumes internal support already exists or will exist (for the military-focus strategy). Insurgents try to force the enemy into responses that alienate the populace from the government and create popular support for the insurgency. Regardless, the insurgency cannot succeed without internal support at some point.

3-124. The indigenous population may provide active or passive support. Active supporters assist either by joining the insurgency, or by providing goods and services. They may provide information, offer refuge, maintain or repair equipment, or participate in rallies. Passive support includes those who sympathize but do not provide assistance. Techniques used to gain and maintain popular support include persuasion, coercion, or appealing to people's needs and wants.

EXTERNAL SUPPORT

3-125. External support is not always necessary for an insurgency to succeed but, in the majority of cases, it is extremely important. Outside sources provide external support primarily for ideological reasons; however, other motivations, such as political, material, or financial gain, are possible. Sources furnish moral, political, legal, or logistics support either tacitly or explicitly. An outside country, for example, may condemn the enemy for taking action against the insurgency, or it may outwardly provide arms, ammunition, sanctuary, training bases, or financing.

3-126. External support between transnational insurgent organizations can include an exchange of personnel and equipment, as well as doctrinal development, intelligence, and financing. In addition to individual and contracted mercenaries, there is a significant body of independent or loosely collaborative individuals. These personnel have served in guerrilla units in other conflicts or parts of the world where they gained actual combat experience. While their participation in their initial cause may have been supported by the governments of the nations of which they are citizens, they are now perceived as having acquired the training and experience which makes them too dangerous to be readmitted to their home countries. These “men without a country” now provide their services to ideologically sympathetic causes.

3-127. Transnational economic entities such as international business corporations, may provide support in order to further their business interests, or as the result of co-option or extortion. Individual financiers may provide support in order to advance personal agendas or cultural, ethnic, political or religious causes.

Chapter 4

Terrorist Organization and Tactics

Terrorism is the calculated use of unlawful violence or threat of unlawful violence to inculcate fear, intended to coerce or intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological. Terrorism's principal target is the psychological balance of the enemy society, its population, and its leadership. It typically accomplishes this through violence directed at civilians, and that is what distinguishes it from other forms of calculated violence used to achieve one these goals.

Many nations devote millions of dollars and man-hours to identifying, apprehending, or destroying terrorist organizations, some of which have been in existence for decades. The reason for their continued survival is an underlying empathy among certain groups and even nations for their cause, if not always their means. Their increasingly sophisticated methods of operation and the inherent security found in the way they are organized also contribute to their survivability.

Terrorist groups vary widely in size, organizational structure, motivation, sophistication, and level of activity. This chapter describes the motivations, organizations, tactics, methods, and means characteristic of such groups.

TYPES OF TERRORIST GROUPS

4-1. There are many types of terrorist groups. Some of them are autonomous, others are loosely affiliated with other terrorist groups, and still others may be state-sponsored.

AUTONOMOUS

4-2. *Formal* terrorist groups are autonomous. They have their own infrastructure, financial arrangements, and training facilities. In addition to conducting terrorist activities within their own country, they are able to plan and conduct terrorist activities in other countries, possibly at great distances from their own. Some groups are organized and operate as *transnational* or *international* terrorist organizations.

4-3. *Single-issue* terrorist groups engage in violence or other criminal activity in order to bring about specific, narrowly focused social or political changes. Their willingness to commit criminal acts in lieu of legal means to obtain policy change is what separates them from law-abiding citizens.

LOOSELY AFFILIATED

4-4. Sometimes individual terrorist groups choose to operate in concert and *loosely affiliated* with other terrorist groups and/or extremist groups that

have mutual interests. Their lack of formal structure provides them the flexibility to travel freely, obtain a variety of false identities, and recruit others from a variety of countries. Their lack of structure also complicates the ability to monitor their activities. Most significant is the fact that their cooperation can greatly multiply their collective capabilities and synergistically increase their effectiveness.

STATE-SPONSORED

4-5. Terrorists who are directly supported by the ruling government of a formally recognized state are referred to as *state-sponsored* terrorist groups. These terrorists receive intelligence, logistics, and operational support from the sponsoring government. Supporting a terrorist group is usually safer for a state than engaging in warfare. Because a close relationship with a terrorist group poses a significant risk to the sponsoring government, that government normally attempts to maintain plausible denial that it supports the terrorist group.

4-6. The State (as defined in FM 7-100) actively sponsors terrorism throughout its region and globally. During time of war, it will use terrorist organizations in support of achieving both military and political objectives. It will attempt to influence those organizations that it does not directly sponsor by providing incentives to cause them to conduct actions that support the goals of both the organization and the State. Although terrorists normally attack civilian targets, this does not prevent them from striking key military or related targets deep in the enemy rear.

4-7. In some circumstances, terrorists may organize and arm themselves to act in an irregular combatant role on the battlefield. As such, they may cooperate with the forces of ideologically or religiously compatible nations or nations with whom they share a common enemy. When terrorists act in this role, the state may provide support in exchange for the service provided.

TERRORIST MOTIVATION

4-8. *Motivation* is the need or desire that compels individuals to organize as a group, retain cohesion, and to undertake the actions necessary to achieve group goals. All terrorist organizations have specific motivations, or ideologies that reflect the social needs and aspirations of the group. Any institution, group, or individual that does not share the terrorist group's motivation and goals can be considered its "enemy."

4-9. *Ideology* is the perspective from which a group analyzes social, political, legal, and military situations of an area in which it operates. This information shapes the type and level of intensity of its external contacts, and determines attitudes toward other political or social actors locally, nationally, and internationally. The sources and levels of education, economic status, political affiliation, and religious devotion of the leaders and members are main contributors to ideological orientation. Within the group, however, individual motivations may well differ. For example, poor peasant members might desire more farmland to increase standards of living, but affluent members might desire positions in a new government.

4-10. There are many types of ideology that a group may follow. In the Cold War era, political or economic reasons were the predominant motivators for groups to rebel against the established government or economic system. Trends today show that ethnic- and religion-based movements are prevalent. Groups today may advocate the racial, religious, or cultural withdrawal or separation based on a common belief. The intrinsic goal of their separation is often independence, political autonomy, or religious freedom or domination rather than purely for economic reasons. The ideologies subscribed to include (but are not limited to) social justice or equity, anti-imperialism, or ethnic self-determination. These are based on the beliefs of—

- **Ethnocentrism.** Race as the defining characteristic of a group, with the attitude that a particular group is superior because of those characteristics, and therefore a basis of cohesion.
- **Religion.** The commitment or devotion to a certain religious faith or sectarian belief.
- **Nationalism.** The loyalty and devotion to a nation, and the national consciousness derived from placing one nation's culture and interests above those of other nations or groups.
- **Populism.** The belief in the rights and virtues of the common people.
- **Politics.** The competition between groups or factions for governmental power and leadership.
- **Economics.** The belief that commercial structure and/or economic well being are the foundation for social structure (for example, capitalism and Marxist communism). The disparity between countries, groups, and organizations with respect to the production, distribution, and consumption of goods and services may be a source of conflict. Additionally, control and access to resources can be a source of motivation when there is a large disparity between conflicting parties.

4-11. The manner of social identification forms another basis for group cohesion. A social identity tie, such as ethnicity or kinship, is a major motivator for many groups. To motivate popular support for achievement of its goals, a group may exploit ethnic identification with its leaders and/or members, and diversity among its enemies.

4-12. Motivation, through ideology or social identity, also forms the basis for maintaining organizational cohesion. When the motivation of an individual or small faction of the group conflicts with overall group motivation, rifts may occur. This may happen when an initial goal has been reached, and some group members cannot adapt themselves to the new governing arrangement, or when the appeal of a new, peaceful lifestyle pales in comparison to the excitement of their past struggle. Conversely, it may occur before the principal goal is attained. This creates friction between group members, which challenges the leadership and distracts from group efficiency.

4-13. Terrorist groups commit violence to influence selected target audiences in pursuit of political, religious, or ideological objectives. However, motivations change over time, sometimes resulting in the splitting or splintering of the group into factions.

4-14. If the terrorist group joins forces with organized crime or drug-trafficking organizations, its motivation may change to profit in the long run. The marriage of convenience among terrorist groups, organized crime, and drug-trafficking organizations meets some of each group's needs. For example, the terrorist group may obtain money from the drug organization by persuading or forcing farmers to grow drugs; the organized crime organization may provide weapons or materiel to the terrorist group. Each group joins an alliance for its own benefit, usually for finances or security—-not because of ideological similarities. Often, a terrorist group will reduce competition by either taking over the other organization or eliminating it. True terrorist groups, however, remain motivated by politics, religion, and ideology. Their leaders develop a long-term strategy to maintain the group's ideological motivation.

TERRORIST ENVIRONMENT

4-15. Terrorist group members who are native to the country or region in which they operate may blend in with their social and cultural environment. They live as and among ordinary citizens and do not appear out of place. Many, perhaps most, hold jobs in the community and, from outward appearance, live a relatively routine existence. Members may also hold important offices within their government's infrastructure.

4-16. Terrorists operating outside their country of origin may or may not blend in with the environment, although they seek anonymity among émigré populations of the same ethnicity, religion, or culture. If they can blend in with a portion of the general population, they can move freely within that segment of society with minimal support from outside their own organization. Others may not have characteristics similar to any portion of the society and thus require increased security measures and substantial local support from an organization indigenous to the foreign country in which they are operating. For example, they may pay an affiliated terrorist group with the same or similar ideology to conduct actions on their behalf. If the group cannot blend in with the local society, the indigenous organization's support requirements increase.

4-17. Terrorists are aware of the legal status and protections available to them when operating in various societies. For example, two terrorists could meet in a public or private place to plan activities, or freely collect information about targets without fear of discovery. Similarly, if the enemy apprehends a member, he may be granted the same protection and rights as other members of that society. As a protection measure, the terrorist group seeks to separate the member conducting an action from the evidence linking him to the action. For example, after a sniper conducts an assassination from a rooftop, another member secures and disposes of the weapon while another person provides a change of clothes and transports the assassin out of the area. Separating the member from his weapon and clothes is an important security precaution exercised by the group.

ORGANIZATION

4-18. Terrorist organizations begin with a few individuals who desire change in accord with a particular ideology or other motivation. As the organization develops its ideology and strategy, it increases in size. The original members recruit others, and leaders establish specialized cells. As the group grows, it establishes wings for different functions. Military nomenclature, such as "brigade" or "battalion," connotes relative size not absolute strength. A terrorist group may call an element a "brigade" but consist of 20 or 30 people.

STRATEGIC ORGANIZATION

4-19. Larger terrorist groups—or groups with capabilities to conduct operations of an international scope—may have a "strategic" level of organization. This consists of the principal organizations that develop, plan, direct and execute the strategy of the overall terrorist organization. A fully developed terrorist group typically has three wings: the social wing, the political wing, and the armed wing. All terrorist groups have an armed wing but not necessarily a political and/or social wing. The social wing concerns itself primarily with humanitarian or social issues, and may never reveal its true ties to the other wings. The political wing conducts much of its business overtly, whereas the armed wing operates covertly. The leaders of the wings form a collective leadership to direct the terrorist group. While the political leader may speak on behalf of the entire group, the collective leadership makes decisions together. Intellectuals often form the collective leadership of the terrorist group.

Social Wing

4-20. The social wing concerns itself primarily with humanitarian or social issues. It is a major component of most large and many small terrorist organizations, but may never reveal its ties to the other wings. It could also be described as the "civil affairs" or "altruistic" wing. This wing often owns, leases, or otherwise controls important facilities and infrastructure. Examples of this are educational institutions, day care facilities (geriatric and pediatric), medical facilities, self-help offices, cultural affairs organizations, family support, and literacy programs. Outside groups or individuals may contribute funding and other support to this wing with or without the knowledge of the connection to illicit activities in other wings or the possibility of diversion of their financial support.

Political Wing

4-21. The political wing conducts much of its business overtly, whereas the armed wing operates covertly. Lawyers, public affairs personnel, businessmen, and prominent intellectual sympathizers compose the political wing. It conducts business on the diplomatic level. Other governments or organizations may acknowledge the terrorist group's political wing as its legitimate voice. Representatives of the group's political wing may negotiate with the opposition. These representatives attend high-level meetings and make agreements on behalf of the terrorist group. The political wing coordinates support received from outside sources. (See the section on External Support at the end of this chapter.)

Armed Wing

4-22. The armed wing, sometimes referred to as the "military wing," forms the nucleus of the entire terrorist group. For security reasons, the armed wing usually organizes around small cells that have limited contact with each other. By minimizing contact between cells, the armed wing seeks to avoid detection and infiltration. Typically, the leader of this wing is one of very few members with detailed knowledge of the entire organization. Therefore, removing this key leader of the group often results in substantial damage to the terrorist organization.

Additional Organizational Support

4-23. In addition to these three major wings, some larger organizations include an economic wing responsible for the generation, management, and the security of financial assets. It can deal with international fund transfers, materiel acquisitions, the control of agricultural and manufacturing output, materiel export and transportation, and money laundering. The functions of this component occur on a large scale, and are distinct from the smaller-scale actions described under Logistics and Support Cells later in this chapter.

4-24. Some organizations may include a media wing, which may be composed of "print" media production agencies, such as poster and graffiti artists, newspaper printers, and Internet website developers. Additionally, the media wing may control small radio and TV stations, news bureaus, or even channels on satellites.

4-25. Finally, larger organizations may include liaison elements composed of advisors, facilitators, observers, and/or exchange personnel from other organizations, companies, or governments. These liaison elements facilitate the flow of information and services between their respective groups and the terrorist group.

TACTICAL ORGANIZATION

4-26. Below the strategic level, the terrorist group consists primarily of a cellular structure within the armed wing.[1] Thus, *cells* serve as building blocks of a terrorist group. These may be the smallest organizational elements, or individual cells may be broken down into specialized *teams*. One of the primary reasons for a cellular or compartmentalized structure is security. The compromise or loss of one cell will not compromise the identity, location, or actions of any other cell. For this reason, a cellular structure provides a measure of operations security (OPSEC) by making it difficult for an adversary to penetrate the entire organization.

4-27. Cells may be organized based on family or employment relationships, on a geographic basis, or by specific functions such as direct action and intelligence. Alternatively, the terrorist group may combine some functions into multifunctional cells. Besides these functional roles, groups use cells as a personnel control measure. Cell members remain in close contact to provide emotional support, and to prevent desertion or breach of security procedures. Each cell has a leader who communicates and coordinates with higher levels and other cells.

[1] In the remainder of this chapter, therefore, the term *terrorist group* will in most cases be synonymous with *armed wing* when discussing terrorist tactics, methods, and means.

4-28. A terrorist group may have only one cell or many cells operating locally, transnationally, or internationally. The number of cells and their composition depend on the size of the terrorist group, its need for specialized functions, and its ability to resource them. A terrorist group operating within one country often has fewer cells and specialized teams than a transnational or international terrorist group.

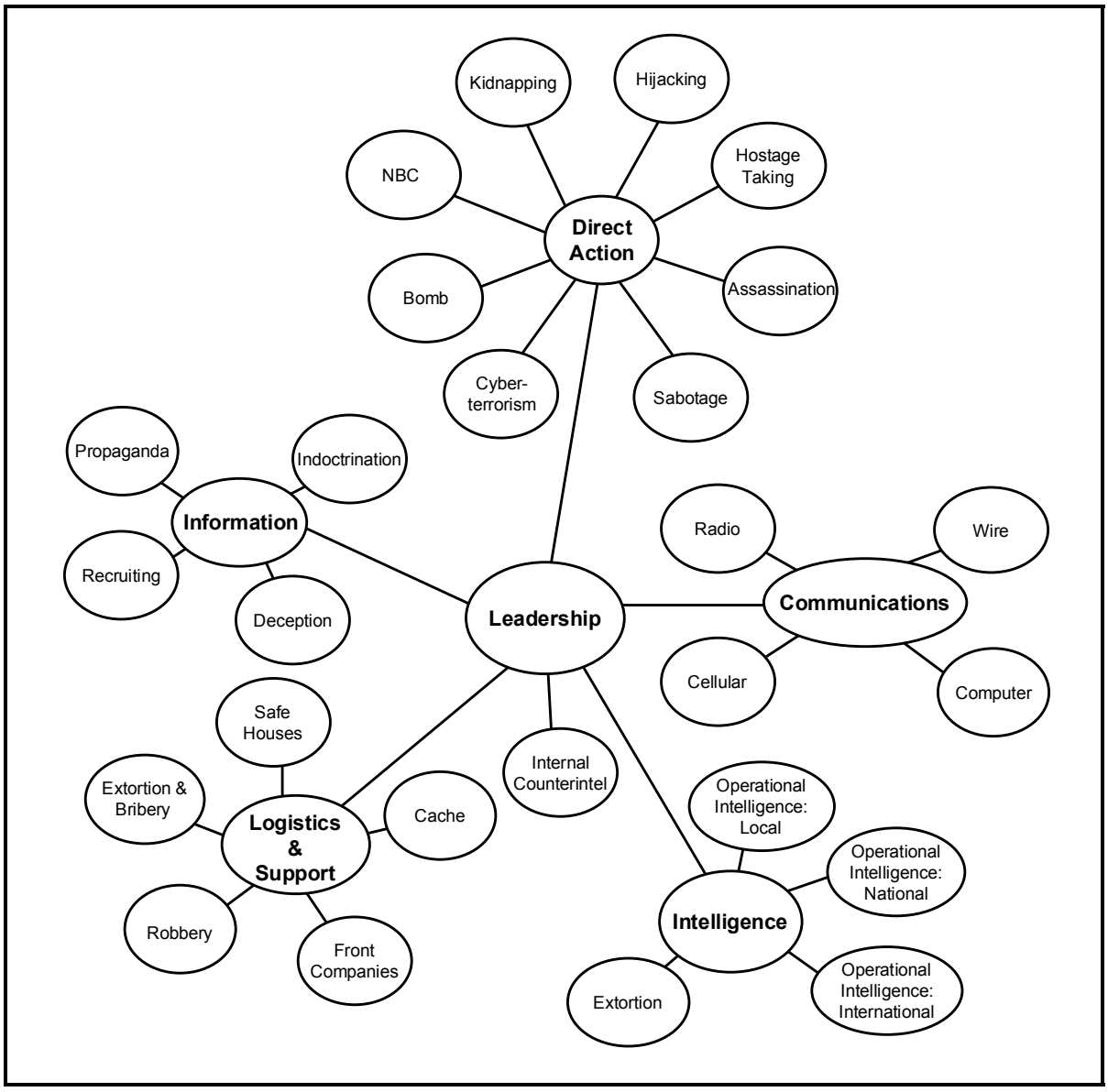

Figure 4-1. Cellular Organization of Armed Wing

4-29. An armed wing typically has a flat, circular command structure rather than a hierarchical chain of command. The armed wing leader is the center of the wing organization, encircled by compartmented cells. (See Figure 4-1.)

Not every armed wing has all the cells discussed below. The wing may combine some of these functions into multifunctional cells or have the political wing provide some services.

4-30. Cells organize based on specific functions, such as communications, intelligence, information, logistics, or direct action. Some cells may be multifunctional because of the armed wing's size or resource constraints; however, this is the exception. Just as each cell has specific functions, so too does each team. A direct action cell of a large terrorist group, for example, may have specialized teams for assassination and kidnapping activities, whereas a smaller terrorist group may have one cell to conduct both actions.

4-31. At the direction of the armed wing leader, various cells come together to conduct activities. The leader of the armed wing is solely responsible for coordinating the activities of various cells involved in an action. Each cell has a leader who communicates with the armed wing leader. During planning, only the leaders pass information among cells to ensure secrecy. The leader of the logistics and support cell, for example, advises the armed wing leader of safe house and cache locations. The armed wing leader disseminates that information to the leader of the direct action cell who, in turn, passes it to the appropriate team. During the conduct of an action, individuals from support teams, such as those in the communications cell, often report to the direct action cell leader.

Leadership Cell

4-32. The leadership cell is the nucleus of the terrorist group. This cell, with the smallest number of members, is vital to the group's survival. It consists of the armed wing leader, experienced advisors, and an internal counterintelligence team. The leader focuses on the big picture and thoroughly understands the ideology that drives the group. A leader rises from the ranks and has demonstrated his dedication through acts of terror. He determines the group's strategy and oversees its execution. The leader of the armed wing joins the leader of the political wing (and perhaps the social wing) to form a collective leadership for the entire terrorist group. The leader is knowledgeable of world politics and the complex sociopolitical environment in which his organization must survive. He is shrewd and calculating and weighs every decision, recognizing that the life of the organization and its successes depend on his decision. He exhibits leadership skills likely supplemented by personal charisma.

4-33. Skilled and experienced advisors consult with the leader on the terrorist tactics and weapons to be used, often making use of information-age technology. Such individuals also may coordinate the activities among the various types of supporting cells while the leader coordinates activities of the direct action cells.

4-34. The internal counterintelligence team (which may be a separate cell in some organizations) conducts internal security functions. This team or cell is directly subordinate to the leadership because of the sensitive nature of its activities, and the fear it wants to generate within the entire organization concerning the following of orders. It is within this team or cell that all OPSEC measures for the organization's activities, as well as security measures are developed, disseminated, and enforced. In many organizations, violation of these security rules can result in immediate death to the violator

and/or his family members. Members of the counterintelligence team or cell infiltrate other cells to identify security weaknesses or breaches. This team or cell is responsible for maiming or assassinating current or former terrorist group members who commit breaches. Paranoia among the group's members actually increases security, since all members desire to remain free of suspicion. Individuals assigned to the counterintelligence team or cell are usually mature, experienced, or senior in the organization.

Direct Action Cells

4-35. Direct action cells conduct various types of terror tactics (see below). Special direct action cells may have single-use functions, such as the recruitment and employment of suicide bombers. Direct action cells may make use of baseline material or resources from intelligence, communications, or logistics and support cells. However, they usually perform their own final target reconnaissance, communications, and close-in logistics functions. A small group might have two- to three-person direct action cells, whereas a large group might have direct action cells with 20 to 30 members. The leader of the direct action cell is responsible for coordinating with higher leadership of the armed wing or other cells for support.

4-36. The direct action cell conducts actions on behalf of the group. A terrorist group may have one or many direct action cells. Some cells may have teams proficient in one specific tactic, such as kidnapping or bombing; other multifunctional cells are proficient in many terror tactics. A specialized team includes individuals who are adept at a specific tactic. A hijacking team, for example, has specialists skilled in various techniques of hijacking and operators of a variety of conveyances. A multifunctional cell may include individuals skilled in assassination, kidnapping, and bombing techniques. Again, the group's size and its ability to resource activities determine the number and types of direct action cells and teams.

4-37. The leader of the direct action cell might need to receive authority from the armed wing leader prior to an activity, or he might have the autonomy to operate independently. Then the direct action cell leader is responsible for—

- Training direct action members to perform direct action missions.
- Coordinating with the armed wing leader regarding support.
- Coordinating the activities of various teams and support personnel to conduct an action.

During preparation for and execution of a mission, he coordinates the activities of specific direct action teams (such as the hijacking team) and support personnel (such as a communications technician) assisting from other cells. The individuals executing and supporting the action may meet with the direct action cell leader at a remote site to finalize plans and conduct rehearsals. Upon completion of the mission, the direct action cell leader relinquishes authority over the attached support personnel.

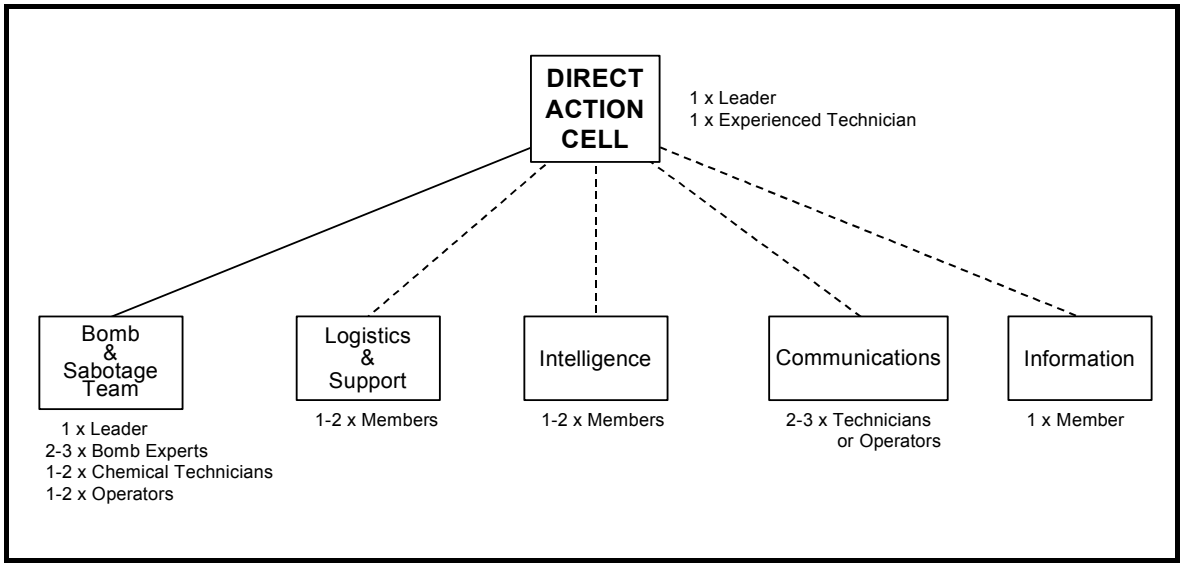

Figure 4-2. Example of a Direct Action Cell Specializing in Bombing and Sabotage

4-38. Figure 4-2 provides an example of a direct action cell specializing in bomb and sabotage missions. As previously described, the leader of the armed wing provides overall guidance and direction to the direct action cell leader, who has overall responsibility and authority for the activity. The direct action cell leader selects the appropriate team to conduct a specific action and receives support personnel and equipment from other cells. All support personnel are lightly armed with pistols or rifles for self-protection. The bomb and sabotage team includes technicians and operators who are skilled in various bomb-making and sabotage techniques. They typically carry multiple weapons for personal protection and assault purposes. The bomb and sabotage team reflects the activity conducted by this particular direct action cell. If the direct action cell is designated to conduct another type of action, such as assassination, hijacking, hostage taking, or kidnapping, then the makeup of its team(s) would reflect that mission.

Intelligence Cells

4-39. The intelligence cell gathers intelligence on the enemy and the environment. The cell may consist of local, national, and international intelligence-collection teams and extortion teams. Intelligence cell members employ both sophisticated and rudimentary collection means to gather information. The techniques used may range from conducting surveillance to purchasing satellite imagery or operating unmanned aerial vehicles. Members of the intelligence cell often use false paperwork, such as passports or other official documents. The documents may facilitate access to a restricted area or provide immunity in case of compromise. Members of the extortion team may solicit or extort information from government officials, businesspeople, or the general population.

4-40. All members of the terrorist group receive training in basic intelligence-collection and surveillance techniques. Besides the intelligence cell, other cells collect information relating to their functionality. The information cell,

for example, collects information on the enemy's psychological operations campaigns and enemy vulnerabilities. To maintain secrecy, each cell member provides information to his cell leader who, in turn, passes it to the intelligence cell leader.

Logistics and Support Cells

4-41. The logistics and support cell provides all support functions required to conduct direct action missions and sustain the armed wing. The members of this cell perform the following functions:

- Establish and maintain caches.
- Coordinate for medical support.
- Conduct activities (including bribery, extortion, and robbery, and operating front companies) to finance and resource activities.[2]
- Allocate and distribute arms and munitions.
- Establish and maintain safe houses.

All of these functions probably are not undertaken by members of the same teams. For example, a member with a cover as an entrepreneur in a front company probably would not risk compromising that cover by conducting other, illegal activities.

4-42. Armored cars, banks, or other lucrative enemy businesses are favorite targets of robbery. Robberies are completed quickly and are low-risk actions because they offer relative anonymity. The members, if apprehended, portray themselves as common criminals and not members of the terrorist group.

4-43. The logistics and support cell often owns front companies or other organizations that support the group's overall objectives. A front organization may be a legitimate business owned and operated for the purposes of generating money or an organization that hides or sustains the group's illegal activity. For example, the logistics and support cell may operate an international shipping company that facilitates movement of materiel and serves as a cover for money laundering.

4-44. The logistics and support cell is also responsible for employing simple sensors and alarm systems in safe houses or at logistics sites. Remote sensors around a cache may alert the group to a compromise. Video surveillance devices can alert of the enemy's presence or confirm the identity of a contact. The cell uses unobtrusive or passive measures instead of barriers. For example, a sensor warns of an intruder whereas a minefield would draw attention. The objectives of the group's security plan are to prevent compromise and achieve early warning.

4-45. Often, the logistics and support cell pre-positions materiel just prior to an activity in order to reduce logistics and security requirements. The cell uses primary markers to alert other group members to the path to the stored materiel. A primary marker, such as a red shirt on a clothesline, must blend into the environment to avoid alerting the enemy to possible storage sites.

[2] However, economic and financial activities occur throughout a terrorist organization. Even direct action cells may have moneymaking covers and activities; they have personnel to coordinate, pass and receive funding and support. This is an integrated function.

Communications Cells

4-46. The communications cell facilitates communication among different cells and with the political (or social) wing. Members provide courier service and maintain dead-drop locations. They are technically capable of operating a variety of communications equipment ranging from landlines to computers on the Internet to satellite communications. At the direction of the armed wing leader, the leader of the communications cell may dispatch operators, technicians, and equipment to various cells as they prepare for and execute an action. While dispatched to a direct action cell, these communications personnel receive orders from the direct action cell leader. Members of the communications cell often act as trusted middlemen, called cutouts, between various cells and the political wing.

4-47. If a terrorist group has a sufficient quantity of high-technology communications equipment, such as cellular phones and encryption devices, other cells assimilate the members of the communications cell. Since all group members receive security training, it is easy to train members to provide their own communications support. The use of the Internet for communication through electronic-mail has become particularly useful.

Information Cells

4-48. The information cell is multifaceted and has functions similar to those of the political wing at the strategic level. Information cell members recruit, indoctrinate, disseminate propaganda, and conduct deception activities. They develop, coordinate, and have primary responsibility for the group's information campaign. The successful terrorist group coordinates all of its information programs to ensure consistency. This cell strives to create, improve, and maintain the terrorist group's legitimacy and influence at local, national, and international levels.

4-49. The information cell develops, produces, and disseminates propaganda, recruits and indoctrinates members, and coordinates information campaigns. This cell conducts overt activities to obtain media exposure in order to show the ineffectiveness of a government or to show the increasing power of the terrorist group. This cell coordinates with the communications cell to operate clandestine radio and television stations and gain access to the Internet to disseminate propaganda.

4-50. In some cases, the armed wing may employ more than one information cell, with different cells responsible for different functions. One cell may develop and produce products while others disseminate over certain means, such as print, audio-visual, and computer. Additionally, a cell may specialize in strategic perception management actions aimed at external sources of support.

SPLINTER GROUPS

4-51. Although the leader of the armed wing oversees the entire group, each cell and wing has its own internal command structure. This organization often leads to splits within a terrorist group. Members displeased with negotiations conducted by the political wing may break away. Splinter groups are extremely volatile and run the risk of compromising the entire group. To maintain secrecy, the terrorist group often maims or assassinates members who

leave the group. Because of their fanaticism, splinter groups often conduct random and audacious attacks on the enemy and die in the name of the group's ideology. For example, suicide bombers kill themselves while conducting a bombing action. They become martyrs, which often inspires other young members to follow suit. Splinter groups form because they feel the parent terrorist group abandoned its ideology or sold out to the enemy, which leaves them no choice but to take action. (See Motivation above.)

TERROR TACTICS, METHODS, AND MEANS

4-52. Terrorist groups can use a wide variety of tactics, methods, and means to achieve their goals and cause widespread fear among the enemy and/or the populace in the target area. Typical terrorist actions include extortion, kidnapping, hijacking, hostage taking, assassination, maiming, sabotage, and cyberterrorism. Groups also can use overt, indiscriminate techniques such as mass casualty activities, bombings or standoff attacks, the use of mines, or use of nuclear, biological, or chemical (NBC) weapons, to accomplish their goals. More advanced terrorist organizations have the ability to use traditional weapons in conjunction with modern technological systems, such as computers, to increase their effectiveness.

4-53. The targets of these actions are primarily civilian targets, although military and other government entities may also become targets, intentionally or unintentionally. When the likelihood of civilian casualties is high, a terrorist group must consider the possible unfavorable ramifications of actions against civilian targets. However, most groups intend from the outset to cause significant civilian casualties.

EXTORTION

4-54. Extortion is the act of obtaining money, materiel, information, or support by force or intimidation. Extortion is often used during the formative period of a group. The opportunity to engage in better money-making activities, such as drug trafficking, may eventually replace the need to extort. Extortion takes the form of "war taxes" or protection money. The logistics and support cell extorts money from local businesses in exchange for protection, which means not harming or bothering the business or its members. Members of the intelligence cell may extort to collect information.

4-55. Another form of extortion is intimidation. The intelligence cell or a specialized team intimidates people to obtain information on the group's enemy or to provide resources. Death threats against an individual or his family cause him to provide information or resources to a group with which he has no interest. The group also intimidates other people not to take action. For example, enemy security personnel may not implement required security measures because of intimidation. The information cell helps create and maintain the fear caused by extortion through its propaganda and deception actions.

KIDNAPPING

4-56. Kidnapping is usually an action taken against a prominent enemy individual for a specific reason. The most common reasons for kidnapping are ransom or release of a fellow terrorist, or the desire to publicize a demand or

an issue. The terrorist group conducts detailed planning, especially regarding movement of the kidnapped individual. The risk in kidnapping is relatively lower than in hostage taking primarily because the terrorist group takes the kidnapped victim to a location controlled by the group. The group makes demands and is willing to hold a victim for a long time, if necessary.

Leadership Cell

4-57. The leadership cell selects the kidnap target, site of kidnapping, and method of kidnapping after considering the input from other cells. Kidnappings require detailed planning and coordination of support by many cells. Various cells provide the information required for a direct action cell to carry out the kidnapping.

Communications Cell

4-58. The communications cell advises on the feasibility of the kidnapping site from a communications perspective. It determines the internal communications equipment necessary for the kidnapping. For example, members of the direct action cell may need to communicate among themselves to prevent fratricide at a constricted site. Communication between the intelligence and direct action cells updates the kidnappers on the target's location or changes. The communications equipment used must blend into the kidnapping site. For example, miniature radios with headsets may be more appropriate than cellular telephones at some kidnapping sites.

4-59. The topography of the kidnapping site also affects the selection of communications equipment. The communications cell is also responsible for emplacing communications equipment. Members may lay wire at the site days or weeks prior to the kidnapping. They may use disguises or infiltrate a legitimate company operating in the vicinity of the site to emplace equipment.

Intelligence Cell

4-60. The intelligence cell provides information on the target's vulnerabilities, weaknesses, and routine behavior. The cell must thoroughly analyze the target so that it can advise the leadership cell on selection of the target site and method of kidnapping. Human intelligence is vital when planning and conducting a kidnapping, and the intelligence cell continuously conducts surveillance on the target to identify potential security flaws. It then determines the flaws that the direct action cell can exploit.

4-61. The intelligence cell can conduct detailed reconnaissance and surveillance of potential kidnap sites to determine the best one, considering cover, concealment, and escape routes in its evaluation. It also advises on the method of disabling the victim, such as drugging, stunning, or binding him.

4-62. Once the leader selects the target and site, the intelligence cell conducts detailed analysis to provide the direct action cell with the requisite data on the target. The information required depends on the location of the target and site but includes—

- The exact route the target uses.
- The method of conveyance.

- Specifics of conveyance, such as its size, shape, speed, and construction.
- The number of security personnel, their location, disposition, and type of weapons used.
- The target's likes, dislikes, allergies, habits, and routines.

Logistics and Support Cell

4-63. In addition to its normal duties, the logistics and support cell supports the kidnapping action by—

- Establishing and maintaining rehearsal sites.
- Stealing vehicles for use in the kidnapping.
- Establishing roadblocks to prevent interference by others.
- Coordinating support for escape, such as passports and transportation.
- Establishing and maintaining the site of captivity.
- Coordinating transfer of ransoms or release of prisoner.

Direct Action Cell

4-64. The direct action cell conducts the actual kidnapping. Its leader designates a specific team or members to conduct the kidnapping. The team usually goes into isolation to conduct rehearsals and finalize planning. After receiving intelligence, the team rehearses specific kidnapping techniques, such as an ambush or abduction. The cell plans the escape route in great detail because of the complexities of transporting the victim. It usually disables the victim to make the escape easier.

Information Cell

4-65. The information cell develops an information campaign to highlight the kidnapping. It often uses simple communiqués to claim responsibility and issue demands. If the terrorist group operates an underground communications network using newspapers, pamphlets, or radio, the information cell can use them to publicize the successful kidnapping. Its members may organize demonstrations that support the group's demands and denounce any enemy actions.

HIJACKING

4-66. Hijacking is stealing or commandeering a conveyance. There are many purposes of hijacking; this section discusses hijacking for hostage taking activities, as a means of escape, or as a means of destruction.

Leadership Cell

4-67. The leadership cell determines the conveyance to be hijacked by the direct action cell and the objective of the hijacking. As with all tactics, the leadership cell is the decision-making authority. The leader may decide to conduct a hijacking to produce a spectacular hostage situation that attracts media attention. A terrorist group may also hijack vehicles, trains, buses, ships, and aircraft to escape. Aircraft offer the group the fastest method of covering great distances.

4-68. Terrorists can also exploit the potential for using these conveyances as weapons. Commercial aircraft carrying large amounts of fuel can be used to destroy symbolic targets and possibly to create mass casualties simultaneously. The use of more than one aircraft to conduct near simultaneous strikes is a proven technique. Terrorists could also apply the same principle to use other forms of conveyance as weapons.

Communications Cell

4-69. The communications cell plays a minor role during the hijacking action, because the direct action cell will use the conveyance's communications systems or the media to communicate to outside elements. The communications cell develops code words or phrases that the direct action cell uses to communicate with the rest of the terrorist group during a hijacking.

Intelligence Cell

4-70. The intelligence cell conducts route reconnaissance and infiltrates organizations associated with the targeted conveyance to gather information and to facilitate access by the direct action cell. Information collected by the intelligence cell for hijacking includes—

- The size, shape, and construction of the hijacked conveyance.
- The capabilities of the hijacked conveyance.
- Security procedures of the enemy.

Logistics and Support Cell

4-71. The level of planning for the logistics and support cell increases for hijackings, primarily because of weapons requirements. The weapons must be sufficiently effective to prevent the hostages from subduing the terrorists. Additionally, the weapons must be inconspicuous or easy to smuggle, in order to avoid detection at security checkpoints. The logistics and support cell also coordinates training required by its own members and the direct action cell. Ideally, the terrorists are capable of operating, maintaining, and sustaining the means of conveyance hijacked.

Direct Action Cell

4-72. While in isolation, the direct action cell conducts detailed rehearsals of the hijacking, especially when the objective is to hold hostages. Once the members secure the conveyance, they execute actions per the cell leader's direction. The members may read a message prepared by the information cell or coordinate for transfer of hostages for prisoners. Alternatively, if the hijacking is for escape, the members eliminate any unneeded people and material, such as hostages or baggage.

Information Cell

4-73. The information cell develops an information campaign to highlight the hijacking. The cell also prepares prepackaged scripts for the direct action cell to read after commandeering the conveyance, and ensures the proclamations and demands are the same espoused by all members of the group.

HOSTAGE TAKING

4-74. Hostage taking is typically an overt seizure of people to gain publicity, concessions, or ransom. Unlike kidnapping, where a prominent individual is taken, the hostages are usually not well known figures in the enemy's society. While dramatic, hostage situations are risky for the terrorist group, especially in enemy territory. Therefore, they attempt to hold hostages in a neutral or friendly area, rather than in enemy territory. Since hostage taking is so risky, the benefits must warrant it. For example, if the enemy captures the leader or principal members of the terrorist group, the group may take hostages to exchange for its leader. The planning and execution phases of a hostage taking and a kidnapping or hijacking are similar. The individual cells conduct actions as discussed above.

ASSASSINATION

4-75. An assassination is a deliberate action to kill political leaders or VIPs, versus the killing of common people, which is considered murder. The terrorist group assassinates or murders people it cannot intimidate, who have left the group, or who have some symbolic significance for the enemy or world community. Terrorist groups refer to these killings as "punishment." Many targets of assassination are symbolic and often have a great psychological impact on the enemy. For example, assassinating an enemy negotiator or successful businessperson can demonstrate the enemy's inability to protect its own people.

4-76. Assassination methods include remotely-detonated bombing, the use of firearms, and poisoning. The target's vulnerabilities determine the method of assassination. For example, a target who drives to work along the same route each day may be vulnerable to a sniper attack. Each action requires detailed planning by many cells. The leadership cell selects the assassination target after considering the input from the other cells. The other cells take actions similar to those taken for a kidnapping. The main difference is that a kidnapping seeks to keep the target alive, while an assassination or murder does not.

MAIMING

4-77. Maiming is a deliberate act to mutilate, disfigure, or severely wound an individual. A terrorist group uses maiming to keep fellow members in line, or as an extortion technique. The person maimed is an outward sign of the group's power and control. For example, a person with a missing body part is a constant reminder of the group's power. The effect of maiming a member of the enemy force or a fellow group member outlasts that of a killing. Therefore, the group is able to use it as a sign of power or subjugation, and as a means of control.

4-78. Maiming does not require as much detailed planning as other actions. However, the need for secrecy heightens when the target is a fellow terrorist group member. After the leaders designate a target, the activity proceeds. Typically, a member of the counterintelligence team conducts the maiming against current or former group members as a control method. The intelligence cell uses maiming as an extortion technique.

SABOTAGE

4-79. Sabotage is the planned destruction of the enemy's infrastructure. The purpose of sabotage is to inflict both psychological and physical damage. Sabotage demonstrates how vulnerable the enemy is to the terrorist group's actions.

4-80. A terrorist group normally aims its sabotage actions at elements of the civilian infrastructure, in order to reinforce the perception among the civilian population that nothing is safe. The action can have significant economic impact and the additional effects of creating mass casualties. Water purification plants, sewage treatment facilities, air traffic control hubs, and medical treatment or research facilities are just a few examples of potential targets. An example of the synergistic effects achieved through the near simultaneous attack of multiple targets is the destruction of water and sewage treatment plants, car bombs in the central city to create mass casualties, and hoax bomb threats directed at medical facilities assessed to most likely respond to these incidents.

4-81. Planning conducted for sabotage actions is similar to those steps taken for a bombing, discussed below. For example, the planning required for a communications cell member to insert a computer virus is similar to the planning conducted by the direct action cell to destroy a power grid. Terrorist groups use many techniques, such as bombing, arson, or use of contaminates, to conduct sabotage.

MASS CASUALTY ACTIVITIES

4-82. Activities designed to produce mass casualties are distinct from those previously described in two respects: intent and nature of the target. The intent of the action is to create a relatively large number of civilian casualties. A secondary effect is the destruction of historic, cultural, or religious structures that are symbolic to the enemy. The most common purposes of mass casualty activities are to—

- Demonstrate the enemy's ineffectiveness in preventing the attack.
- Gain concessions from the enemy.
- Cause an inappropriate response by the enemy, thus creating or gaining sympathy and support for the terrorist group.

A secondary purpose could be to render the enemy ineffective, particularly if key enemy personnel are among the victims.

4-83. Typical mass casualty activities include detonating a bomb in a popular market area, at a busy traffic intersection during rush hour, or in a theater. The "hoax effect" is a common deception method used with mass casualties. The mere threat of an event can have even more dramatic effects over time. The population may become complacent about warnings or hostile toward the government for its inability to counter the terrorist group.

STANDOFF ATTACKS

4-84. Standoff attacks employed by terrorist groups differ from those used by other paramilitary organizations (see Chapter 2) primarily in terms of target selection. Terrorist groups will employ standoff attacks with a more indiscriminate nature against perceived high-payoff targets of civilian or government institutions and infrastructures, in order to cause widespread panic or fear.

4-85. The weapons of choice used in these types of attacks are mortars, rockets, or recoilless rifles. By using these weapons, forces achieve a very cost-effective method to cause significant chaos, and demoralize the population. When compared to similar-caliber artillery pieces, mortars, rockets, and recoilless rifles are relatively light and maneuverable. They are difficult to detect because they are man-portable, easily hidden, and quickly emplaced. Crews require comparatively less training. They provide reduced acoustic firing signatures, and fire rounds at high trajectories. For these reasons, they are the weapons of choice for limited indirect fires, especially within urban settings.

4-86. Firing points can be established in phases utilizing secretive methods. Initially, a firing survey party will move into the area to determine weapon positions and map locations, headings, aiming stake positions, and firing data. Later, the firing party will arrive, meet the survey party, set up the weapons, conduct a quick firing raid, and depart using a getaway vehicle if available. Firing parties have the ability to launch three to five mortar rounds and depart before the first-round hits the target. On occasion, the weapon tubes are emplaced underground, covered, and concealed well in advance of a planned fire mission. Similarly, the rounds may be rigged with timing devices, so they launch themselves when no members of the terrorist group are in the area and subject to being compromised.

4-87. The terrorist group may also employ weapons in ways other than their originally intended use. For example, it might use an antitank grenade launcher against a civilian vehicle, aircraft, or building. A terrorist group often employs its limited fire support assets in conjunction with deception activities and in nontraditional ways. For example, it might place a mortar in a truck and fire it through a hole in the roof. It might infiltrate a direct action team into enemy-controlled territory to fire on populated areas and then use an information campaign to highlight the enemy's inability to protect civilians.

CYBERTERRORISM

4-88. Cyberterrorism is any terrorist activity performed by terrorists with or to computers. Such cyberterrorist attacks are increasing in volume, sophistication, coordination, and scale. Cyberterrorism is not only about physically damaging systems, inserting worms or virus but also about facilitating communication and intelligence gathering. Evidence confirms that terrorists are using information technology and the Internet to communicate, formulate plans, recruit members, and raise funds. Potential perpetuators of cyberterrorist attacks could include not only terrorist groups, but also terrorist sympathizers and thrill-seeking hackers.

4-89. Examples of cyberterrorist attacks could include use of information technology to—

- Perform acts of violence. For example, placing a number of computerized bombs around a city, all simultaneously transmitting unique numeric patterns, each bomb receiving each other's pattern. If bomb one stops transmitting, all the bombs are synchronized to detonate simultaneously.
- Disrupt banks, international financial firms, or stock exchanges.
- Attack the air traffic control systems and cause large civilian aircraft to collide.
- Attack electrical infrastructures. Most such infrastructures have sensors that assist engineers in shutting down components of the national grid in times of natural disaster, which could become vulnerable to cyber manipulation and control.
- Attack voice communication systems that are vulnerable to software attacks. This could include 911 and emergency services telephone exchanges.
- Attack utilities infrastructures. For example, remotely changing the pressure in gas lines can lead to a valve failure, causing a block of homes to detonate and burn.

4-90. The primary advantage is that all of these acts can be accomplished undetected (from the terrorist's home or another remote location) and prove to be extremely hard to trace. For the price of a computer and a modem, an extremist or would-be terrorist can become a player in national and world events.

BOMBS

4-91. Bombs are the weapon of choice for the terrorist group. They are inexpensive, relatively easy to build, and extremely destructive. With the exception of suicide bombings, the terrorist generally is not at the scene at the time of detonation. Bombs may be very sophisticated or simple. Terrorist groups use bombs in support of any of the actions previously discussed, such as—

- Assassination.
- Maiming.
- Sabotage.
- Mass casualty activities.

The leadership, communications, and logistics and support cells execute their normal responsibilities, as previously discussed.

Information Cell

4-92. The information cell designs and executes an information campaign to exploit the effects of the bombing. For example, the terrorist group can set off a bomb either in a crowded civilian area, such as an office building, or perhaps against the enemy's military or government targets, such as a headquarters building. The information cell, on behalf of the group, claims responsibility or blames the event on others, depending on the objective. Some-

times the information cell warns of an impending bomb to heighten the psychological impact of the event. Not all bomb threats become events; some are deception activities to cause anxiety and fear and to gage the reactions of the enemy.

Intelligence Cell

4-93. The intelligence cell modifies its collection based on the specific needs of the direct action cell. Depending on the location of the bomb, type of bomb used, time of day of detonation, and purpose of the bomb, the direct action cell requires specific information. For example, if the group intends to detonate a bomb during rush hour or the busiest working hours to damage property and maximize casualties, the direct action cell requires information regarding—

- Security procedures of the facility.
- Construction and design of the facility.
- Time of day when the largest number of people occupy the facility.
- Personnel with wide access to facilities, such as cleaning or maintenance personnel, in order to avoid them or perhaps impersonate them when planting the bomb.

Direct Action Cell

4-94. The direct action cell plants the bomb. The members rehearse, but not necessarily to the detail required by kidnappings, hostage taking, or assassinations. The direct action cell uses rehearsals primarily as a safety measure. Often, a member skilled at bomb making prepares the bomb and another member emplaces it. The latter member may lack experience on the finer points of bomb making and require instruction on safe handling and arming procedures. The member who plants the bomb must blend in with the environment. He uses disguises or infiltrates an organization that has access to the target location. His objective is to emplace the bomb without drawing undue attention to himself or the bomb before it is activated.

NUCLEAR, BIOLOGICAL, AND CHEMICAL WEAPONS

4-95. Terrorist groups that acquire NBC weapons pose significant dangers to local and/or foreign interests they oppose. Terrorists armed with these weapons can gain leverage for their demands because of the weapons' nature. They are the ultimate terror weapons.

4-96. Terrorists may obtain NBC weapons for a variety of motives. Such groups might threaten the use of these weapons as "saber rattlers" to raise the ante in response to foreign political or military actions or to achieve a specific objective. NBC weapons are the potential weapon of choice for organizations employing terror tactics, since the actual or threat of use of NBC weapons is real and very feasible.

Nuclear

4-97. For the present, the use of a fully developed nuclear weapon is the least likely terrorist scenario. Most terrorist groups do not have the financial and technical resources to acquire nuclear weapons, but could gather materials to make radiological dispersion devices. Some groups may have state sponsors

that possess or can obtain nuclear weapons. When and if a terrorist group does obtain a nuclear weapon, there should be no doubt that they will use it if they deem necessary.

Biological

4-98. Biological weapons consist of pathogenic microbes, toxins, and bioregulator compounds. Depending on the specific type, these weapons can incapacitate or kill people and animals, or destroy plants, food supplies, or materiel. The type of targets being attacked determines the choice of agents and dissemination systems. Biological warfare agents are virtually undetectable while they are in transit, and evidence of a biological attack may not show up for days after the actual release has occurred.

4-99. Biological warfare agents include three basic categories: pathogens, toxins, and bioregulators. Figure 4-3 lists some examples of each.

Pathogens	Toxins	Bioregulators
Anthrax	Mycotoxins	Neurotransmitters
Cholera	Venoms	Hormones
Plague	Shell fish	Enzymes
Smallpox	Botulinum	
Tularemia	Ricin	
Influenza		
Fevers		

Figure 4-3. Examples of Biological Warfare Agents

4-100. *Pathogens* cause diseases such as anthrax, cholera, plague, smallpox, tularemia, or various types of fever. These weapons would be used against targets such as food supplies, port facilities, and population centers.

4-101. *Toxins* are produced by pathogens and also by snakes, spiders, sea creatures, and plants. Toxins are faster acting and more stable than live pathogens. Most toxins are easily produced through genetic engineering.

4-102. *Bioregulators* are chemical compounds that are essential for the normal psychological and physiological functions. A wide variety of bioregulators are normally present in the human body in extremely minute concentrations. These compounds can produce a wide range of harmful effects if introduced into the body at higher than normal concentrations or if they have been altered. Psychological effects could include exaggerated fear and pain. In addition, bioregulators can cause severe physiological effects such as rapid unconsciousness, and, depending on such factors as dose and route of administration, they could also be lethal. Unlike pathogens that take hours or days to act, bioregulators could act in only minutes.

4-103. Another way to categorize biological warfare agents is by their effects. The four categories and effects of biological agents are shown in Figure 4-4.

Agent Type	Agent Effects
Antipersonnel	Disease or death causing micro-organisms and toxins.
Antiplant	Living micro-organisms that cause disease or death
Antianimal	Agents that can be used to incapacitate or destroy domestic animals through disease. Used to limit wool, hide, or fur production.
Antimateriel	Agents used to deteriorate critical materiel needed for the war effort such as leather, canvas, fuels, or electronics.

Figure 4-4. Effects of Biological Agents

Chemical

4-104. Terrorist groups have the capability to use chemical weapons. Agents like nerve gas require infinitesimal amounts to kill a human being. Properly placed and employed, chemical agents have the capability to create mass casualties.

4-105. **Agent Persistency.** One way to categorize chemical agents is according to their persistency. Persistency is the length of time an agent remains effective on the battlefield or other target area after dissemination. The two basic classifications are as persistent or nonpersistent.

4-106. *Persistent* nerve agents, such as V-agents, thickened G-agents, and the blister agent mustard, can retain their disabling or lethal characteristics for days to weeks (depending on environmental conditions). Persistent agents produce either immediate or delayed casualties. Immediate casualties occur when an individual inhales a chemical vapor. Delayed casualties occur when the chemical agent is absorbed through the skin, thus demonstrating the need for protective equipment.

4-107. *Nonpersistent* agents generally last a shorter period of time, depending on the weather conditions. For example, the nerve agent sarin (GB) forms clouds that dissipate within minutes after dissemination. However, some liquid GB could remain for periods of time varying from hours to days, depending on the weather conditions and method of delivery.

4-108. **Agent Effects.** The effects that chemical agents have on the target organism categorize the agents. *Lethal* agents include nerve, blood, blister, and choking agents. *Nonlethal* agents include incapacitants and irritants. Figure 4-5 lists examples of possible chemical agents and their characteristic effects.

Agent	Symbol/Name	Symptoms in Man	Effects on Man	Rate of Action
Nerve	G Series GB/Sarin GD/Soman (VR 55)	Difficult breathing, sweating, drooling, nausea, vomiting convulsions, and dim or blurred vision.	At low concentrations, incapacitates; kills if inhaled or absorbed through the skin.	Very rapid by inhalation; slower through skin (5-10 minutes).
	V Agent	Same as above.	Incapacitates; kills if skin is not rapidly decontaminated.	Delayed through skin; more rapid through eyes.
Blood	AC/Hydrogen cyanide	Rapid breathing, convulsions, coma, and death.	Incapacitates; kills if high concentration is inhaled.	Rapid
Blister	HD/Mustard HN/Nitrogen Mustard L/Lewisite HL/Mustard and Lewisite CX/Phosgene Oxime	Mustard, nitrogen mustard: no early symptoms. Lewisite and mustard: searing eyes and stinging skin. Phosgene oxime: powerful irritation of eyes, nose, and skin.	Blisters skin and respiratory tract; can cause temporary blindness. Some agents sting and form wheals on skin.	Blister delayed hours to days; eye effects more rapid.
Choking	CG/Phosgene DP/Diphosgene	Eye and throat irritation, fatigue, tears, coughing, chest tightness, nausea, vomiting.	Damages the lungs.	Delayed, variable.
Incapacitant	BZ	Slowing of mental and physical activity, disorientation and sleep.	Temporarily incapacitates.	30-60 minutes.
Irritant	DA/Diphenylchloroarsine DM/Adamsite CN/Chloroacetophenone CS/O-Chlorobenzylidene-malononitrile PS/Chloropicrin	Causes tears, irritates skin and respiratory tract.	Incapacitates, nonlethal.	Very rapid.

Figure 4-5. Effects of Example Chemical Agents

4-109. *Nerve agents* are fast-acting chemical agents. Practically odorless and colorless, they attack the body's nervous system, causing convulsions and eventually death. Nerve agents are further classified as either G- or V-agents. At low concentrations, the GB series incapacitates; it kills if inhaled or absorbed through the skin. The rate of action is very rapid if inhaled, but slower if absorbed through the skin. The V-agents are quicker acting and more persistent than the G-agents.

4-110. *Blood agents* block the oxygen transferal mechanisms in the body, leading to death by suffocation. A common blood agent is hydrogen cyanide. It kills quickly and dissipates rapidly.

4-111. *Blister agents*, such as mustard (H) or lewisite (L), and combinations of the two compounds, can disable or kill after—

- Contact with the skin.
- Being inhaled into the lungs.
- Being ingested.

Contact with the skin can cause painful blisters or blindness after eye contact. These agents are especially lethal when inhaled.

4-112. *Choking agents*, such as phosgene and diphosgene, block respiration by damaging the breathing mechanism, which can be fatal. As with blood agents, poisoning from choking agents comes through inhalation, since both types of agents are nonpersistent. Signs and symptoms of toxicity may be delayed up to 24 hours.

4-113. *Incapacitants* include psycochemical agents and paralyzants. These agents can disrupt a victim's mental and physical capabilities. The victim may not lose consciousness, and the effects usually wear off without leaving permanent physical injuries.

4-114. *Irritants*, also known as riot-control agents, cause a strong burning sensation in the eyes, mouth, skin, and respiratory tract. The effects of these agents, the best known being tear gas (CS), are also temporary. Victims recover completely without having any serious aftereffects.

Delivery

4-115. It is possible to disseminate NBC weapons and agents in a number of ways. Terrorist groups execute any or all of these delivery means as required to achieve the desired effects on the target.

4-116. **Nuclear.** Trucks, vehicles, and boats can be used for larger weapons, while backpacks and "suitcases" can be covertly used to deliver small nuclear weapons or dangerous radiological dispersion devices. Of the two, the latter is the most likely to be seen in the near term.

4-117. **Biological.** The objective of biological weapon delivery is to expose humans to an agent in the form of a suspended cloud of very fine agent particles. Airborne particles are the most effective because, once inhaled, particles of this size tend to lodge deep in the lungs close to vulnerable body tissues and the bloodstream. Dissemination through aerosols, either as droplets from liquid or by particles from powders, is by far the most efficient method.

4-118. Terrorist groups or civilian sympathizers can deliver biological weapons by unconventional dissemination means. These include commercially available or specially designed sprayers or other forms of aerosol generators mounted in automobiles, trucks, or boats. Backpack and "suitcase" devices also can be used to effectively disseminate biological agent aerosols. Devices resembling insecticide spray cans can be used to introduce an agent into heating, ventilating, and air conditioning systems. Drinking water can be contaminated by means of high-pressure agent injectors attached to

plumbing system components. Another way to disseminate infectious agents is by the use of insects, rodents, or other arthropod vectors. Methods of dissemination are varied and limited only by the perpetrators' imagination.

4-119. **Chemical.** Numerous means, to include mortars and bombs, can be used to deliver chemical warfare agents. Chemical munitions are fitted with different burst capabilities, according to the agent properties and the intended effect. For example, a chemical munition fitted with a long burst fuze releases the agent as a vapor or fine aerosol. This creates and immediate inhalation hazard with some of the fragmentation effect of a conventional munition. Theoretically, terrorists could obtain these munitions, modify them and emplace them by hand. Other delivery means could be by vehicle, backpack, canisters, or sprayers.

Accessibility

4-120. Radioactive materials or waste can be easily purchased legally, or on the black market. They can be obtained from governmental or civilian research and medical facilities such as power plants, construction sites, laboratories, or hospitals, or from military facilities concerned with the storage, production, and weaponization of these materials. In addition to the above sources, biological agents occur in nature and relatively easy to obtain as compared to nuclear material; they can be easily obtained from universities or medical schools. Chemical agents and their precursors can be obtained from civilian agriculture sites, textile, plastic, or civilian chemical production facilities, or the above-mentioned military research and military facilities.

4-121. Terrorist groups can gain access to NBC weapons through a state sponsor or sympathizers in countries with these capabilities. Given the increasing sophistication of terrorist groups, some can easily manufacture biological and chemical weapons in laboratories they have established and financed.

Ease of Production

4-122. Biological weapons are extremely potent, and the most rudimentary program will likely have lethal agents that have been a threat for some time. Botulism and anthrax are high-probability candidates that are difficult to reckon with. In addition, the revolution in biotechnology may produce other agents that are even more toxic and resilient.

4-123. Chemical and biological agents can be produced in small laboratories with little or no signature to identify the facility or their production. Normal biological warfare research facilities resemble completely legitimate biotechnical and medical research facilities. The same production facilities that can produce biological warfare agents may also produce wine and beer, dried milk, food, and agricultural products. It is therefore difficult to distinguish legitimate production plants from illicit ones.

4-124. The basic knowledge needed to produce an effective NBC terrorist weapon can be found in college and medical school textbooks, advanced engineering books, magazines and periodicals, and on the Internet. With minimal training, individuals can produce NBC weapons in a relatively short period of time in any home, school, or university laboratory, medical production or research facility, or commercial production facility. Minimal special equipment

is needed to produce biological or chemical weapons, and it can be easily purchased on the open market. These weapons can be produced at a relatively low cost, as compared to other types of weaponry. Some precursor agents for biological and chemical production are dual use; therefore, they are not illegal to acquire or possess and are not expensive to purchase. Some can be easily stolen from production facilities. Widespread effects of these weapons can be obtained from small-scale production lots, reducing the total production costs to achieve the desired effects.

Toxic Industrial Chemicals

4-125. There is a near-universal availability of large quantities of highly toxic stored materials. Exposure to some industrial chemicals can have a lethal or debilitating effect on humans. In combination with their ready availability, their proximity to urban areas, their low cost, and the low security associated with storage facilities, makes industrial chemicals an attractive option for terrorist use as weapons of opportunity or of mass destruction.

4-126. The most important factors to consider when assessing the potential for adverse human health impacts from a chemical release are acute toxicity, physical properties (volatility, reactivity, and flammability), and likelihood that large quantities will be available for exploitation. Foremost among these factors is acute toxicity; thus, the highest concern for human health is associated with a subgroup of industrial chemicals known as toxic industrial chemicals (TICs). TICs are commercial chemical substances with acute toxicity that are produced in large quantities for industrial purposes.

High Risk	Moderate Risk	
Ammonia	Acetone cyanohydrin	Methyl chloroformate
Arsine	Acrolein	Methyl chlorosilane
Boron trichloride	Acrylonitarile	Methyl hydrazine
Boron trifluoride	Allyl alcohol	Methyl isocyanate
Carbon disulfide	Allyl amine	Methyl mercaptan
Chlorine	Allyl chlorocarbonate	n-Butyl isocyanate
Diborane	Boron tribromide	Nitrogen dioxide
Ethylene oxide	Carbon monoxide	Phosphine
Fluorine	Carbonyl sulfide	Phosphorus oxychloride
Formaldehyde	Chloroacetone	Phosphorus pentafluoride
Hydrogen bromide	Chloroacetonitrile	Selenium hexafluoride
Hydrogen chloride	Chlorosulfonic acid	Silicon tetrafluoride
Hydrogen cyanide	Crotonaldehyde	Stibine
Hydrogen fluoride	Diketene	Sulfur trioxide
Hydrogen sulfide	1,2-Dimethyl hydrazine	Sulfuryl chloride
Nitric acid, fuming	Dimethyl sulfate	Tellurium hexafluoride
Phosgene	Ethylene dibromide	Tert-Octyl mercaptan
Phosphorus trichloride	Hydrogen selenide	Titanium tetrachloride
Sulfur dioxide	Iron pentacarbonyl	Trichloroacetyl chloride
Sulfuric acid	Methanesulfonyl chloride	Trifluoroacetyl chloride
Tungsten hexafluoride	Methyl bromide	

Figure 4-6. High- and Moderate-Risk Toxic Industrial Chemicals

4-127. Figure 4-6 lists high- and moderate-risk TICs based on acute toxicity by inhalation, worldwide availability (number of producers and number of continents on which the substance is available), and physical state (gas, liquid, or solid) at standard temperature and pressure. Within each risk category, TICs are listed alphabetically.

4-128. In addition, the current definition of TICs does not include all chemicals with high toxicity and availability. Specifically, chemicals with low volatility are not included. These low-vapor-pressure chemicals include some of the most highly toxic chemicals widely available, including most pesticides.

INFORMATION WARFARE

4-129. Having an information advantage is one of the few ways in which a terrorist group can change the balance of power that normally favors the enemy. Tactics executed under the umbrella of information warfare (IW) involve integrated political, legal, military, psychological, and economic considerations. The tools of IW include radio broadcasts, use of press releases, indoctrination training, establishment of a web page, and selective sabotage actions, all integrated to further the group's short- and long-range goals. Depending on its level of capability, a terrorist group may or may not be able to conduct all these activities. However, even an unsophisticated group with very little money can obtain, or even hire, a wide range of capabilities from around the world.

4-130. The leader provides his information strategy and guidance to the information cell. The information cell develops an information campaign and coordinates and integrates various assets necessary to implement it. It can design its campaign to support the terrorist organization's actions in general, or it can tailor the campaign to exploit the aftermath of a particular incident. For a given incident, the direct action cell makes the news, and the information cell spreads the news—with a spin conducive to the terrorist cause.

INTELLIGENCE

4-131. Intelligence is fundamental for success. All terrorist groups want and need to determine what the enemy is doing, while denying the enemy information. Intelligence functions include information collection, reconnaissance, and surveillance. All available assets are employed for collection ranging from technical to human assets. In the absence of sophisticated technology, groups rely on human intelligence-gathering agents. However, even unsophisticated groups can have some high-technology equipment.

INFORMATION COLLECTION

4-132. Collecting information, overtly and clandestinely, is a continuous function performed by every terrorist group. Overt activities include the open collection of information by individuals who circulate among the people. This type of activity attempts to procure copies of local maps, publications containing information about the area, and official publications available to the general public.

4-133. The majority of information gathered comes from open sources, such as civilians who work or live in the area in which the enemy operates, printed publications or publications available on the Internet, enemy press releases, and the media. Clandestine activities involve secret collection of information. This can include information collected through the use of extortion, bribery, or coercion. Groups clandestinely collect information using electronic devices, human-intelligence agents who may join or infiltrate popular organizations, government organizations, and nongovernment organizations. When planning any action, an intelligence cell analyzes information from both overt and clandestine sources. "Sleeper agents," members of the terrorist group who may reside within the target area for years, often have the specific mission of gathering information. The information they gather may later serve to support direct action missions conducted by these same agents or by direct action cells.

RECONNAISSANCE AND SURVEILLANCE

4-134. Terrorists conduct reconnaissance to obtain information about the activities and resources of the enemy. Observation is the most common method used to conduct reconnaissance. However, with the availability of specific equipment, reconnaissance using electronic devices is becoming increasingly popular. Civilians living, traveling, or working near either a target area or the enemy conduct surveillance on behalf of the terrorist group. The leader considers the information passed by civilians based on their trustworthiness and past performance. Intelligence cell members also conduct surveillance.

COUNTERINTELLIGENCE

4-135. Terrorist groups conduct counterintelligence activities to protect against the possibility of infiltration by enemy agents or of informants among members of the terrorist organization. The cellular structure helps ensure against the compromise of the identity, location, or activities of leaders and members of other cells should there be a breach of internal security.

SUPPORT

4-136. Support for a terrorist group is divided into two sources—internal and external. Logistics support includes the transportation, storage, and supply of all materiel required to sustain activities. Caches and safe houses are two techniques used to store and supply materiel. Both caches and safe houses use camouflage, concealment, cover, and deception (C^3D), and other security measures to protect against or evade enemy detection. The logistics and support cell employs a variety of organic, stolen, or captured conveyances.

CACHES

4-137. Caches are hiding places for supplies and equipment. Caches are used because supplies and equipment are critical to actions and are difficult to replace. These storage areas are found underground or in dense vegetation, caves, remote areas, basements, or false walls. Security measures employed to protect caches include obstacles, patrols, guards, and early warning systems. In case of compromise, terrorists boobytrap caches to prevent the enemy from using the equipment or supplies.

SAFE HOUSES

4-138. A safe house is a building where terrorists engage in secret activities or take refuge. A safe house is similar to a base camp in the purpose of providing sanctuary. From the outside, a safe house is indistinguishable from any other building in the locale. However, extensive security measures, such as code words and locks, are employed to prevent compromise or at a minimum to delay enemy forces.

EXTERNAL SUPPORT

4-139. Outside sources provide external support, primarily for ideological reasons; however, other motivations, such as moral, political, material, sanctuary, or financial gain, are possible. Such sources may include sponsoring countries, other groups with the same ideology, or other groups hostile to the terrorist group's enemy.

4-140. Outside sources can provide a range of assets or services to the terrorist group. Monetary and material support are the most common forms of support received. Sources furnish political, legal, or logistics support either tacitly or explicitly. An outside country, for example, may condemn the enemy for taking action against the terrorists, or it may outwardly provide arms, ammunition, training bases, or financing. A sponsoring country may allow the terrorist group to maintain training camps on its soil or may provide intelligence support. Training camps located outside enemy-controlled areas allow the terrorist group to arm, equip, rehearse, and otherwise prepare for activities. Intelligence support from outside sources may include satellite imagery, or information on targets or weaknesses in the enemy's organization. Other examples of support include safe houses, diplomatic cover, and access to communications systems.

4-141. External support between transnational terrorist organizations includes an exchange of personnel and equipment, intelligence, and financing. In addition to individual and contracted mercenaries, there is a significant body of independent or loosely collaborative individuals. These personnel have served in guerrilla units in other conflicts or parts of the world where they gained actual combat experience. Their participation in their initial cause may have been supported by the governments of the nations of which they are citizens. However, those governments could now perceive them as too dangerous to be readmitted to their home countries, considering the training and experience they have acquired. These "men without a country" now provide their services to ideologically sympathetic causes.

Chapter 5

Internal Security Forces

The State, like most nondemocratic nations, maintains large internal security forces to deal with various internal threats to the regime. These forces are well organized, trained, and equipped to perform a host of diverse missions. These organizations have specified missions throughout the spectrum from peacetime to total war. This chapter discusses the organizations and methods of operation, tactics, and techniques employed by all of these forces. These organizations conduct activities against a variety of enemies, such as criminals, political dissidents, and insurgents, as well as against an enemy's military during war. Accordingly, the operations and tactics employed will vary depending on the particular mission, target, and enemy origin (internal, regional, or extraregional).

MINISTRY OF THE INTERIOR

5-1. In peacetime, the Chief of Internal Security heads the internal security forces within the Ministry of the Interior. (See Figure 5-1.) These forces are responsible for internal security and all related functions to ensure the continued existence of the regime. Members of these forces are selected from segments of the population most loyal to the State government. Most of the internal security forces are uniformed, using military ranks and insignia similar to those of the other services of the State's Armed Forces.

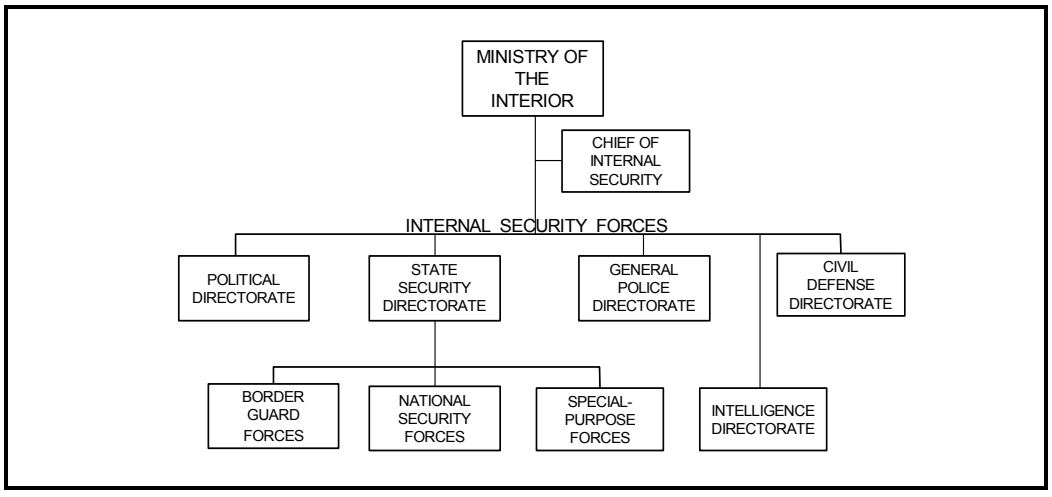

Figure 5-1. Ministry of the Interior

5-2. During wartime, some or all of these forces may come under the control of the Supreme High Command (SHC) as a sixth service of the Armed Forces. (See Figure 5-2.) At that time, the formal name Internal Security Forces applies to all forces resubordinated from the Ministry of the Interior to the SHC. Because of this relationship, volunteers or conscripts may meet their mandatory military obligation by serving in the internal security forces in peacetime or in war.

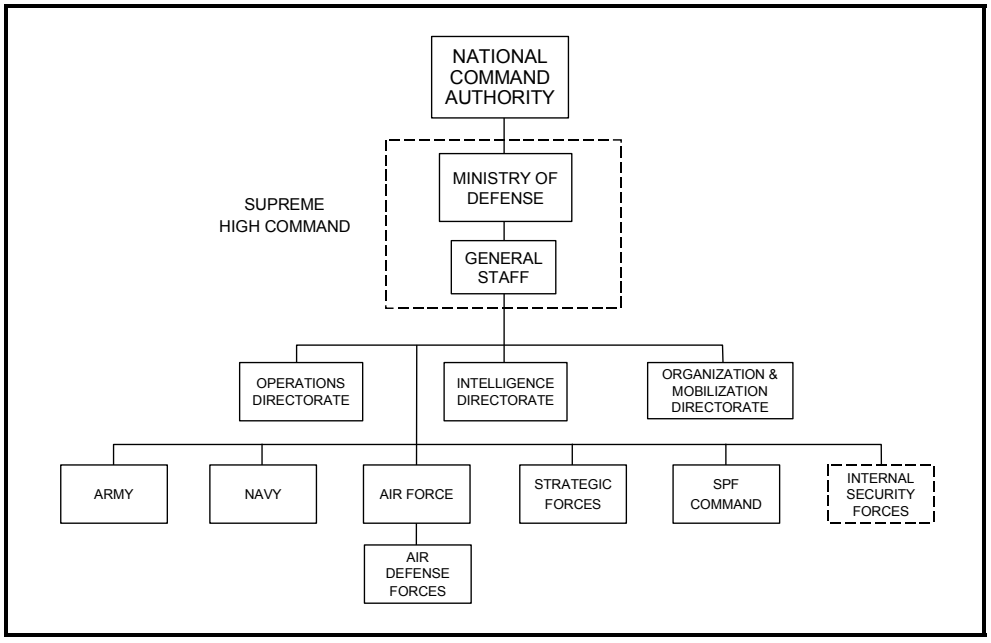

Figure 5-2. Supreme High Command and Service Components

5-3. The primary imperative for the State is preservation of the regime and all four instruments of national power (diplomatic-political, informational, economic, and military). The State will use all means available to—

- Protect political centers and the political leadership.
- Protect and control information.
- Protect key economic centers.
- Protect military forces.

5-4. Internal security forces aggressively suppress or crush organized groups of dissidents, using force when necessary, regardless of whether the dissident actions are violent or peaceful. The government may even use Armed Forces against such groups. Government-controlled media either do not report the incidents or manage public perception to put the blame on the anti-government group.

5-5. Internal threats do not exist only in peacetime, but also continue and often intensify during war. For instance, a regional enemy sharing a common ethnic, religious, or cultural heritage with segments of the State's population may incite or support anti-State activities by those groups. During wartime,

therefore, Internal Security Forces from the Ministry of the Interior become subordinate to the SHC, and the General Staff controls and supervises their activities. In war, the Internal Security Forces pick up additional missions that support the State in dealing with external elements.

POLITICAL DIRECTORATE

5-6. Under the Chief of Internal Security, the Political Directorate monitors the political activities of the State population. This directorate has a predominant role in defining, in general, which segments of the population are enemies of the State or have the potential to become enemies. It often focuses on segments of the population that are habitually defined by race, religion, or some other easily delineated category.

5-7. The Political Directorate is quite knowledgeable about internal opponents of the State's policies, as well as individuals or groups who have the potential to oppose the policies of the State. It sends agents to infiltrate possible subversive groups. These agents can add to the directorate's knowledge of various groups and their activities. They can help the directorate to undermine groups' cohesiveness or redirect their efforts in directions the regime can control. Also, the Political Directorate can be preemptive in establishing policies that suppress potential opponents before they have an opportunity to revolt or take other subversive action.

INTELLIGENCE DIRECTORATE

5-8. The Intelligence Directorate is responsible for identifying and neutralizing subversive elements, as well as unsanctioned drug and criminal organizations. It investigates and monitors subversive groups and infiltrates their ranks. It routinely eavesdrops on communications of such groups and their known leaders. It employs an extensive human intelligence (HUMINT) network. It also monitors and collects information on foreign organizations operating within the State. These include not only foreign spies, but also foreign-based corporations doing business in the State, as well as nongovernmental and private volunteer organizations that government agents may infiltrate. The State must examine such external organizations to determine how to deal with negative influences or how it can manipulate these organizations to support its own national security objectives.

5-9. To some extent, the functions of the Intelligence Directorate may overlap those of the Political Directorate. The primary difference is that the Intelligence Directorate does not make policy. It conducts its operations with a focus that is more short-term, more narrowly targeted, and more concentrated on gathering information. However, it must coordinate with the Political Directorate to ensure that the two directorates do not have agents working at cross purposes.

5-10. In wartime, the assets of the Intelligence Directorate support the Internal Security Forces and the overall national security strategy. The Internal Security Forces continue to operate an extensive HUMINT network

within the State as the cornerstone of its reconnaissance, intelligence, surveillance, and target acquisition (RISTA) capability. During regional conflict, the State expands the HUMINT network into enemy territory. This HUMINT network will also help provide the State a RISTA capability that may offset the technological advantages of an extraregional force.

STATE SECURITY DIRECTORATE

5-11. The State Security Directorate is responsible for preventing anti-government activities, investigating these activities, and prosecuting the perpetrators. During times of crisis and war, the directorate is also responsible for finding and neutralizing dissidents, spies, and others who commit crimes against the government. Thus, some of its functions may overlap those of the Political Directorate and Intelligence Directorate. Consequently, coordination among the three directorates may be necessary to ensure that their activities to not conflict with one another.

5-12. Elements of the State Security Directorate deploy throughout the State. Many of these elements are paramilitary units equipped for combat. They include Border Guard Forces, National Security Forces, and Special-Purpose Forces. Together with the regular Armed Forces, these paramilitary forces help maintain the State's control over its population in peace and war.

Border Guard Forces

5-13. The primary mission of the Border Guard Forces is to patrol the State's borders, both land and sea. They maintain security against unauthorized crossings into or out of the State. They are charged with detecting, identifying, and intercepting illegal infiltrations and with arresting anyone attempting to exit the country unlawfully. During war, they may be assigned to a military unit to guard a newly gained territory or to conduct actions against the enemy.

5-14. Border Guard units consist of a professional cadre of officers and noncommissioned officers (NCOs) supplemented by conscripts and civilian auxiliaries. The regular Border Guard personnel have military ranks, while civilian auxiliaries and most of those serving their compulsory service do not. Although not well armed, the auxiliaries serve primarily as the eyes and ears of the units they support.

5-15. When the SHC assumes control of Border Guard Forces in wartime, the General Staff provides overarching administrative and logistics support in the same manner as with a regular military force. Figure 5-3 shows the overall organization of Border Guard Forces. The intelligence unit collates information, conducts analysis, and coordinates information collection for the entire force. The training unit is responsible for all training from the individual to force level. Aviation and naval support units provide equipment and personnel to the border brigades as required.

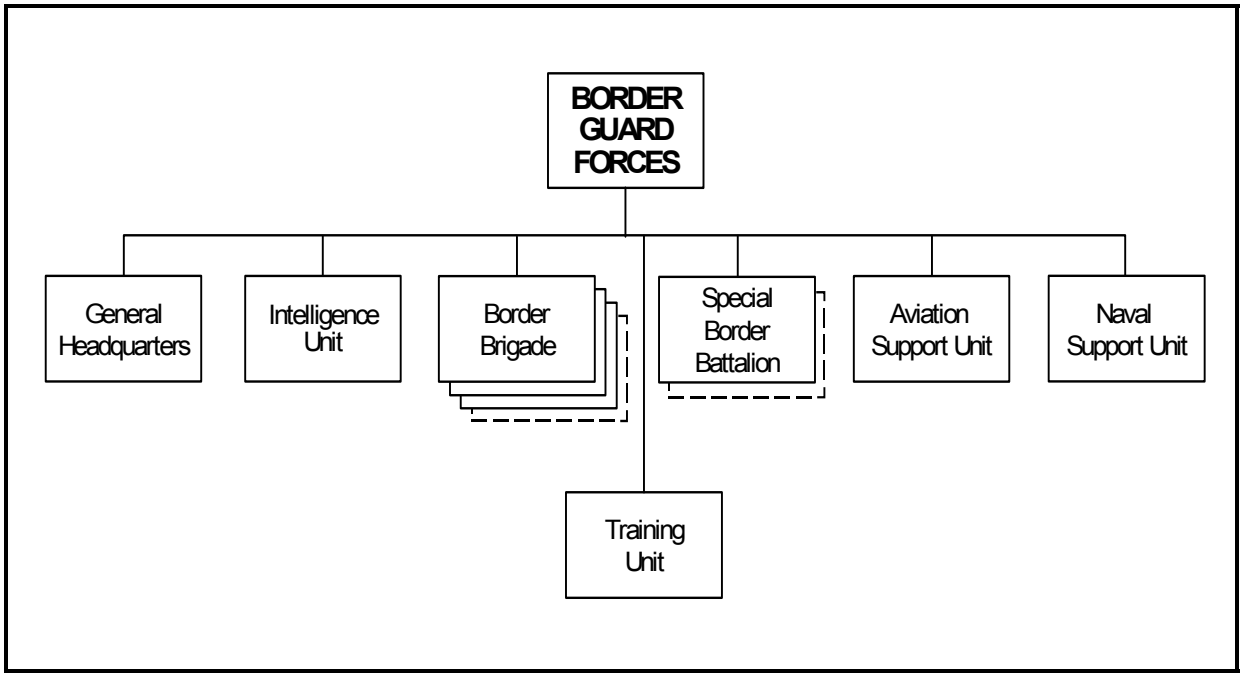

Figure 5-3. Border Guard Forces (Example)

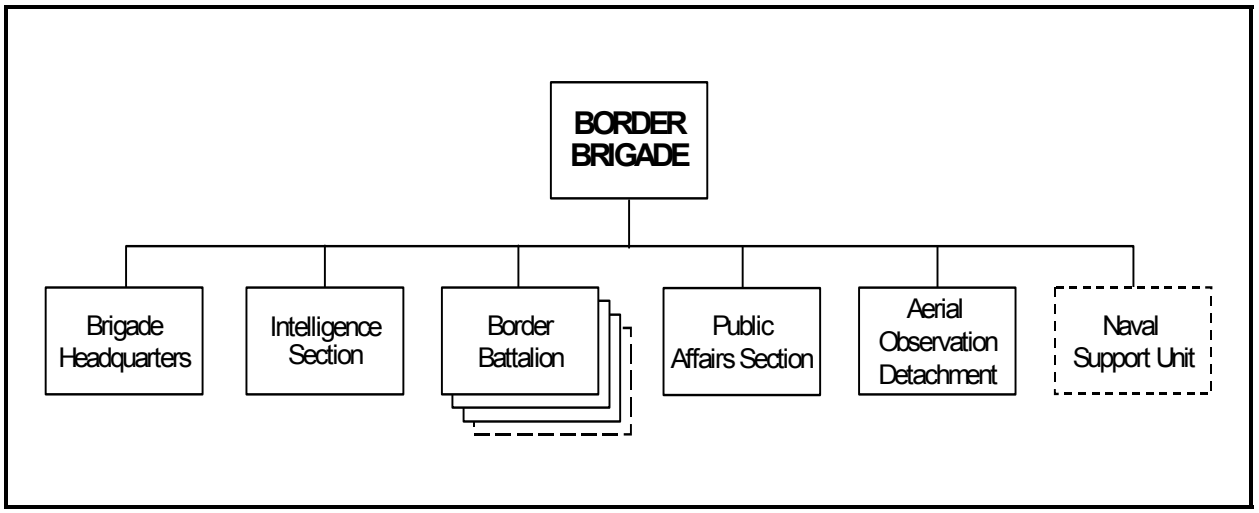

Figure 5-4. Border Brigade (Example)

5-16. The primary organizational component of the Border Guard Forces is the border brigade (see Figures 5-4). Each brigade is assigned a portion of the State's border as its area of responsibility (AOR). It is organized and equipped according to the size and requirements of its sector of the border. One or more of the brigade's border battalions might be heavy weapons battalions. The companies of a heavy weapons battalion could have a variety

of weapon systems, including armored and riot control vehicles, light artillery (122-mm and lower), and crew-served weapons. A brigade securing a portion of the coastal border would include a naval element with patrol boats and coastal surveillance radars. Figure 5-6 shows possible equipment that might be found in a border brigade or its subordinate units.

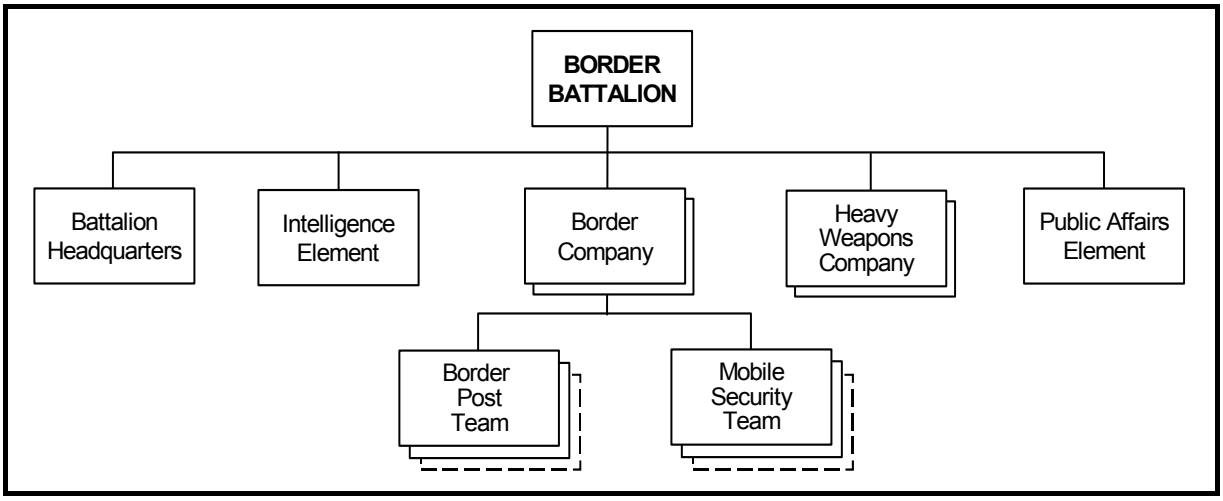

Figure 5-5. Border Battalion (Example)

5-17. The border battalion (Figure 5-5) is the basic unit of the brigade. Intelligence specialists receive additional training in HUMINT activities. The heavy weapons companies resemble those in heavy weapons battalions at the brigade level, but are less likely to include artillery. Weapons specialists, medics, and engineers receive training in their particular area of expertise.

5-18. The border companies consist of border post teams and mobile security teams. Members of both types of teams receive basic weapons and intelligence-collection training. They are equipped with small arms, dogs, and mines. Border post teams usually establish stationary checkpoints or border control posts. They typically have metal detectors, as well as devices to detect explosives or contraband. Conversely, mobile security teams conduct patrols on foot, on motorcycle, or in vehicles. They may have armed helicopters or light observation aircraft. The mobile security team includes intelligence and weapons specialists, medics, and engineers. These mobile teams are capable of conducting small-scale raids and ambushes.

Principal Items of Equipment: Border Guard Forces	Headquarters Elements	Intelligence Units	Heavy Weapons Companies	Border Companies	Training Units	Public Affairs Units	Aviation Units	Naval Units
WEAPONS								
Handgun	X	X	X	X	X	X	X	X
Assault rifle/submachinegun			X	X	X			X
Sniper rifle				X	X			
Special weapons sight				X	X			
Heavy machinegun			X					
Automatic grenade launcher			X					
Antitank guided missile (manpack)			X					
Antiaircraft gun/shoulder-fired SAM			X					
Light artillery (122-mm or smaller)			X					
COMMUNICATIONS								
Radio	X	X	X	X	X	X	X	X
Cellular telephone		X			X	X		
Facsimile	X	X			X			
Computer	X	X			X			
Encryption capability	X	X			X			
Concealed capability	X	X			X			
Wire	X			X				
VEHICLES								
Truck/all-terrain vehicle	X	X	X	X	X	X		
Armored vehicle			X	X	X			
Riot control vehicle			X	X	X			
Motorcycle				X	X	X		
Helicopter							X	
Aircraft							X	
Watercraft								X
SURVEILLANCE EQUIPMENT								
Radar		X			X			X
Camera		X		X	X	X		
Binoculars		X		X	X			X
Scope		X		X	X			X
Night-vision device		X	X	X	X			X
Listening device		X		X	X			
Monitoring equipment		X			X			
SEARCH EQUIPMENT								
Explosive detector		X		X	X			
Contraband detector		X		X	X			
Metal Detector				X	X			
PROTECTIVE GEAR								
Protective clothing		X	X	X		X		
Protective mask		X	X	X		X		

Figure 5-6. Border Guard Forces Equipment List

5-19. The Border Guard Forces may also have one or more independent special border battalions. These constitute an elite paramilitary force of airborne-qualified personnel trained in counterterrorism and commando tactics. These forces are held in reserve at the national level for rapid deployment into crisis areas on or near the State's borders. While organized administratively into battalions and companies, the special border forces normally deploy and operate in small teams or detachments combining multiple teams.

National Security Forces

5-20. The mission of the National Security Forces is to maintain the security of the State from subversive elements within its borders and from crimes against the government. They are responsible for preventing and investigating anti-government activities, locating and neutralizing dissidents and spies, and collecting information on foreign organizations operating within the State's sphere of influence, while maintaining public order. Elements of the National Security Forces have considerable authority to arrest, search, question, and jail suspicious personnel. This organization conducts liaison with other internal security forces and with other services of the State's Armed Forces and may combine with them to conduct certain actions. Figure 5-7 shows the overall organization of the National Security Forces.

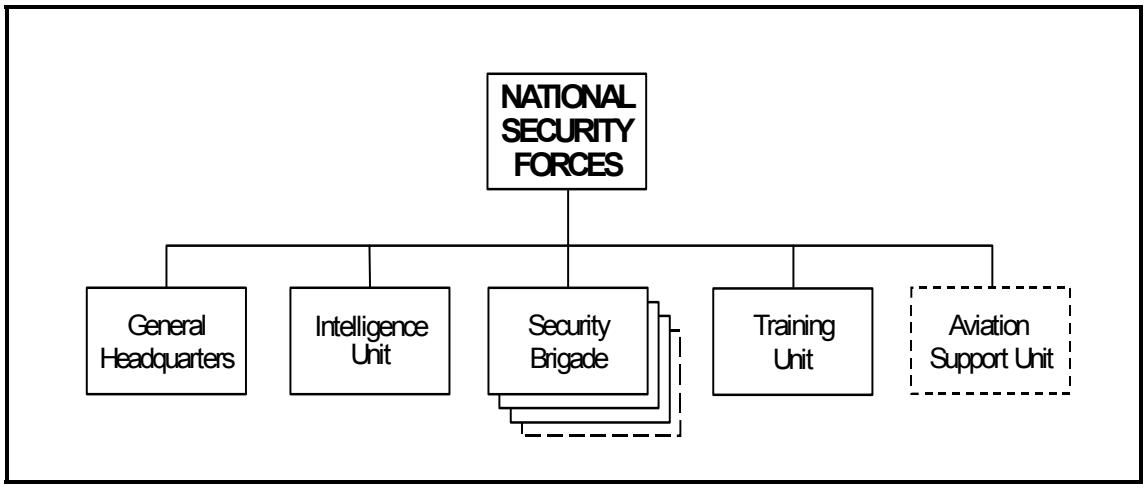

Figure 5-7. National Security Forces (Example)

5-21. During war, the mission of the National Security Forces intensifies as possible insurgent forces may increase their efforts to overthrow the government. During such crises, the regime has little tolerance for any real or perceived threats against its government. The National Security Forces will deal severely with any nonconformists, while the government-controlled media will conduct perception management to blame the anti-government group. The State will also use these forces against regional or extraregional enemies that invade the State. In turn, it can use its Armed Forces to assist National Security Forces against internal adversaries, when necessary.

5-22. The intelligence unit of the National Security Forces controls a network of covert agents to monitor and infiltrate anti-government groups. It conducts this HUMINT effort as the executive agent of the Intelligence Directorate under the national-level Chief of Internal Security. Agents are assigned to conduct surveillance in collaboration with national, district, or local police units. The training unit is responsible for training both agents and paramilitary forces.

5-23. The remainder of the National Security Forces are organized along military lines and equipped with light weapons and sometimes heavy weapons and armored vehicles. Their primary organizational component is the security brigade. (See Figure 5-8.) These brigades are equipped with light and heavy weapons capable of suppressing or crushing any expected internal threat. (See Figure 5-11 for a list of possible equipment.)

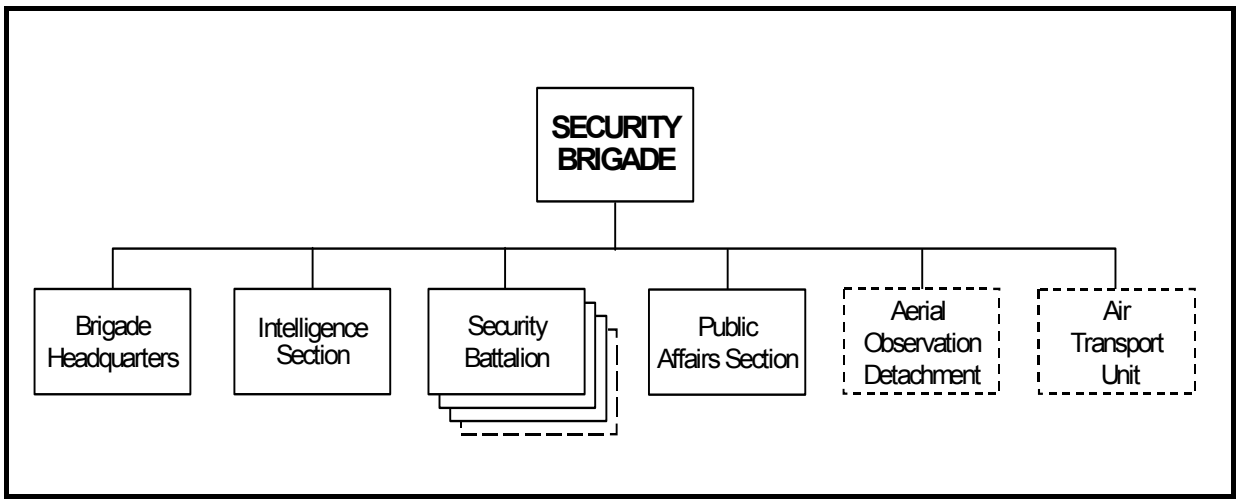

Figure 5-8. Security Brigade (Example)

5-24. A security brigade may also be assigned to a military unit during war. An operational-level command of the State's Armed Forces may include one or more security brigades to augment its military capability. This type of brigade not only increases the military combat power, but also offers a very effective and experienced force for controlling the civilian population.

5-25. Within the security brigade organization, the intelligence section (Figure 5-9) plays an important role. The deputy section chief is responsible for all day-to-day administrative functions. The administrative services subsection provides administrative, financial, logistics, and legal support. The intelligence operations and collection subsection deploys agents and employs informants to collect information. The agents attempt to remain inconspicuous to avoid detection and compromise. The intelligence operations and collection subsection may also receive information from agents dispatched from the national level National Security Forces organization and from other elements of the internal security forces. This subsection is also responsible for information collection using open sources. The intelligence production subsection conducts analysis and produces intelligence products. These products may be used in its information campaign (propaganda) or

deception activities. The communications subsection provides personnel and technical support to the organization. This subsection employs a variety of communications means, ranging from landlines to cellular telephones, and techniques such as messengers and dead-drops.

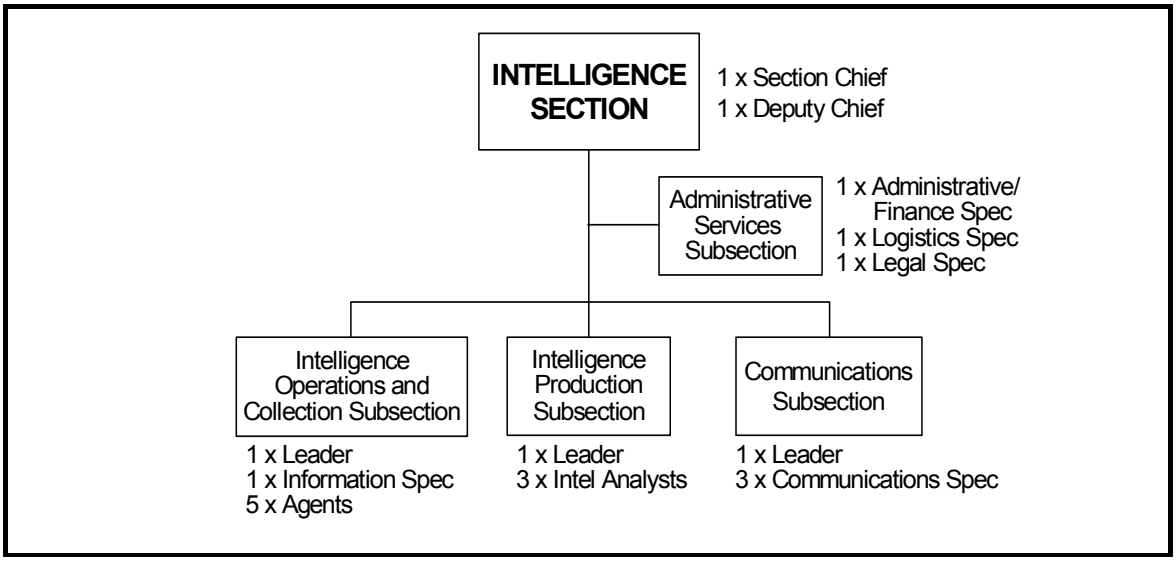

Figure 5-9. Intelligence Section of Security Brigade (Example)

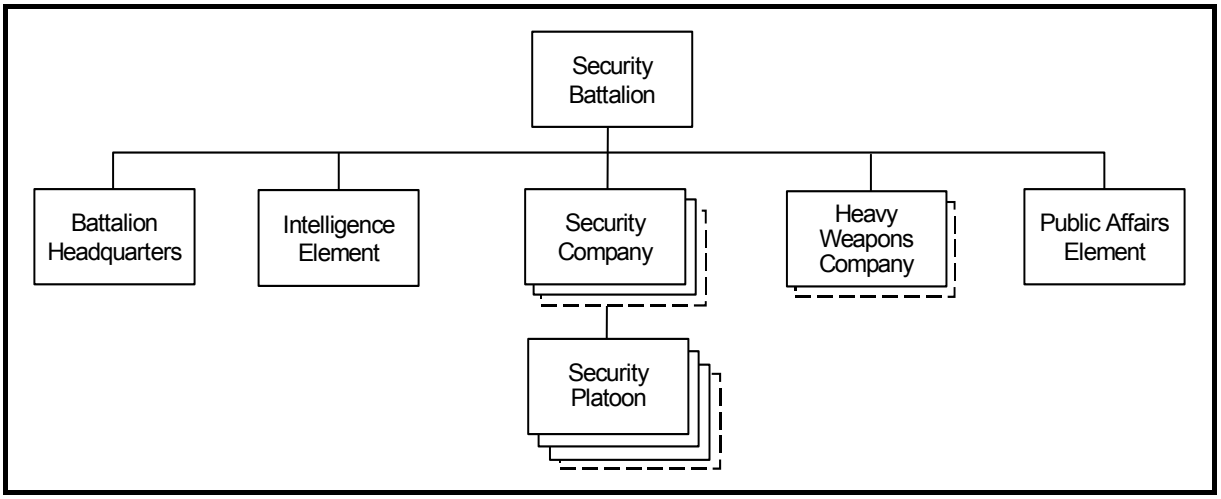

Figure 5-10. Security Battalion (Example)

5-26. A security battalion (Figure 5-10) has intelligence and public affairs elements similar to those at brigade level, but normally smaller. Its security companies and their subordinate platoons are similar to equivalent infantry units in the regular Armed Forces and can thus be used to augment such forces. In their primary internal security roles, however, units below the security battalion level often operate as small teams, sometimes grouped into detachments. Most personnel in a security battalion have small arms. A heavy

weapons company in a security battalion is similar to those found in the Border Guard Forces or in infantry battalions of the regular Army. Figure 5-11 shows the various types of equipment that may be found in National Security Forces organizations.

Principal Items of Equipment: National Security Forces	Headquarters Elements	Intelligence Units	Security Companies	Heavy Weapons Companies	Training Units	Public Affairs Units	Aviation Units
WEAPONS							
Handgun	X	X	X	X	X	X	X
Assault rifle/submachinegun			X	X	X		
Sniper rifle			X		X		
Special weapons sight			X		X		
Heavy machinegun				X			
Automatic grenade launcher			X	X			
Antitank grenade launcher			X	X			
Antitank guided missile (manpack)				X			
Mortar (82-mm or smaller)			X	X			
COMMUNICATIONS							
Radio	X	X	X	X	X	X	X
Cellular telephone		X			X	X	
Facsimile	X	X			X		
Computer	X	X			X		
Encryption capability	X	X			X		
Concealed capability	X	X			X		
Wire	X		X				
VEHICLES							
Truck/all-terrain vehicle	X	X	X	X	X	X	
Armored vehicle			X	X	X		
Riot control vehicle			X	X	X		
Motorcycle			X		X	X	
Helicopter							X
Aircraft							X
Watercraft							
SURVEILLANCE EQUIPMENT							
Camera		X			X	X	
Binoculars		X	X		X		
Scope		X	X		X		
Night-vision device		X	X	X	X		
Listening device		X	X		X		
Monitoring equipment		X	X		X		
SEARCH EQUIPMENT							
Explosive detector		X	X		X		
Contraband detector		X	X		X		
Metal Detector			X		X		
PROTECTIVE GEAR							
Protective clothing		X	X	X		X	
Protective mask		X	X	X		X	

Figure 5-11. National Security Forces Equipment List

5-27. National Security Forces are stationed throughout the State in numbers determined by the importance of governmental and industrial installations in the area and the political temper of the populace. They also possess the transport capabilities to quickly redeploy and assemble forces anywhere within the State in a crisis situation.

5-28. In wartime, the National Security Forces would continue to be responsible for finding and neutralizing dissidents and spies. However, they probably also would be charged with guarding, transporting, and interrogating prisoners or war (POWs). They may also be used to evacuate areas threatened by enemy occupation.

5-29. Troops from the National Security Forces may be used as guards for important industrial and transport installations and government buildings. They may be responsible for guarding bridges, tunnels, railway stations, and strategic sections of track or roadway against enemy attack and sabotage. They may provide external security for prisons or POW camps, and for shipments of strategic materials or military convoys. They may also provide protection for VIPs.

5-30. The National Security Forces are composed of very dedicated, highly indoctrinated, and loyal personnel. Except for covert agents, most personnel have military ranks. Most, if not all, personnel have had military training. Personnel are trained to use electronic surveillance equipment and interrogate prisoners. Some units or members could be used to augment the Armed Forces in an emergency, particularly in intelligence-related duties.

Special-Purpose Forces

5-31. Also under the State Security Directorate, the Ministry of the Interior has its own Special-Purpose Forces (SPF). These commando-type forces typically operate in small SPF teams and are the most highly-trained and best-equipped of the internal security forces. They are multifaceted, but are primarily used for VIP security, hostage rescue, counterdrug, counterinsurgency, and counterterrorist activities. In wartime, the State can use the their direct action capability to conduct sabotage in the enemy's rear area. They can infiltrate and disrupt enemy organizations (political, social, religious, and military). They can also engage in intimidation, extortion, atrocities, kidnapping, and assassination. The quality and character of individual members and their high level of training and state-of-the-art equipment enable them to perform these types of actions. They modify their tactics based on their available weapons and level of specialized training.

5-32. Although they fall under an SPF battalion for administrative purposes, these elite forces are intended for employment in small teams. SPF teams may operate separately, or they may be task organized into detachments. (See Figure 5-12.) A typical SPF detachment headquarters consists of a commander, deputy commander, and administrative, financial, intelligence, logistics, and communications specialists, who have all received training as combat troops. The SPF team includes a team leader, commando elements, and at least one sniper element. All members receive training in a variety of skills, such as parachuting, scuba diving, demolitions, weaponry, urban

activities, and hand-to-hand and close-quarters combat. (Figure 5-13 shows an equipment list for the SPF.)

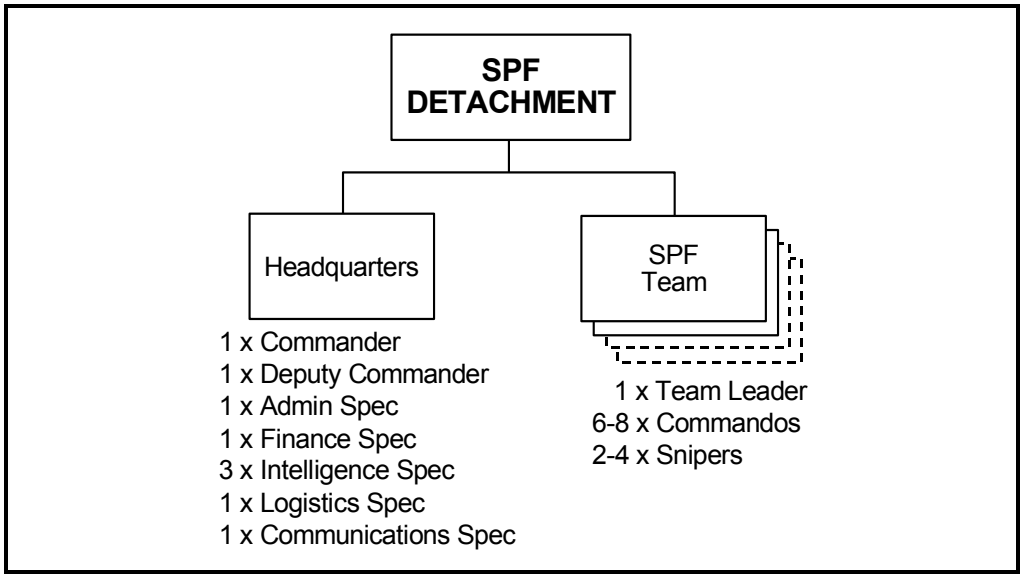

Figure 5-12. Special-Purpose Forces Detachment (Example)

Principal Items of Equipment: Special-Purpose Forces	Headquarters	SPF Teams
WEAPONS		
Handgun	X	X
Assault rifle/submachinegun	X	X
Sniper rifle		X
Special w eapons sight	X	X
COMMUNICATIONS		
Radio	X	X
Cellular telephone	X	X
Facsimile	X	X
Computer	X	X
Encryption capability	X	X
Concealed capability	X	X
VEHICLES		
All-terrain vehicle	X	X
Armored vehicle	X	X
Motorcycle	X	X
Helicopter	X	X
Aircraft	X	X
Watercraft	X	X

Principal Items of Equipment: Special-Purpose Forces (Cont)	Headquarters	SPF Teams
SURVEILLANCE EQUIPMENT		
Radar		X
Camera		X
Binoculars		X
Scope		X
Night-vision device		X
Listening device		X
Monitoring equipment		X
SEARCH EQUIPMENT		
X-ray machine		X
Metal detector		X
Explosive detector		X
Contraband detector		X
PROTECTIVE GEAR		
Protective clothing	X	X
Protective mask	X	X

Figure 5-13. Example Special-Purpose Forces Equipment List

5-33. The State Security Directorate maintains its SPF units as a strategic reserve for emergency use in any part of the State or even outside State borders. The commando-type SPF forces can conduct covert missions in support of other internal security forces. These troops, selected for their unswerving loyalty to the regime, often provide personal protection to senior State officials.

5-34. Because the SPF perform most of their activities covertly, they make no differentiation between peacetime and wartime missions. In fact, the State will utilize their efforts in preparation for war to degrade the enemy's capabilities. For a regional opponent, that may include the formation and training of an insurgent force (see Chapter 3). In wartime, the SHC may use them to secure occupied territory or to operate as combat troops in conjunction with other services of the Armed Forces.

5-35. In the event of intervention by an extraregional power, the State might focus its SPF teams to conduct missions in the new enemy's staging areas or even on his home territory. Initial targets would be aimed at preventing or disrupting the enemy's ability to deploy, while later targets might include his military support infrastructure and his civilian populace.

GENERAL POLICE DIRECTORATE

5-36. The General Police Directorate has responsibility for national, district, and local police, fire protection, and the penal system. The different levels of police organizations are all loosely organized under the General Police Directorate. Below the national level, however, these police organizations are influenced more by their local authorities than by the policies of the General Police Directorate. National Police establishments have nationwide jurisdiction, while district and local police are primarily responsible for the maintenance of law and order in a given geographical area. Their responsibilities, rather than their organizational structures or names, distinguish them from each other. The level of organization is commensurate with the level of influence. Thus, a National Police force is larger and more capable than a district or local police force. Its forces include paramilitary tactical units and special police units that are equipped for combat. Figure 5-17 shows equipment that may be found in various police forces.

5-37. Police forces primarily serve two functions: maintenance of law and order and enforcement of regulations. Maintenance of law and order includes protection of life and property, prevention and detection of crimes, apprehension and prosecution of criminal offenders, and traffic and crowd control. Regulatory functions are administrative duties, such as issuance of licenses and permits, currency protection, immigration control, trade supervision, prison management, enforcement of ordinances, monitoring of elections, inspection of facilities, and enforcement of religious law and/or custom. Many of these duties involve bureaucratic processes that lend themselves to inefficiency, graft, and corruption.

National Police

5-38. The National Police (Figure 5-14) focus almost entirely on maintaining internal security; they are charged with protecting government facilities and with suppressing dissidents. They support the highest level of government and usually focus on crimes against the government, organized crime, and black market activities. National Police may have jurisdiction over matters such as—

- Importation and/or exportation.
- VIP security.
- Religious affairs.
- Foreign persons in the country.
- Domestic political activity.

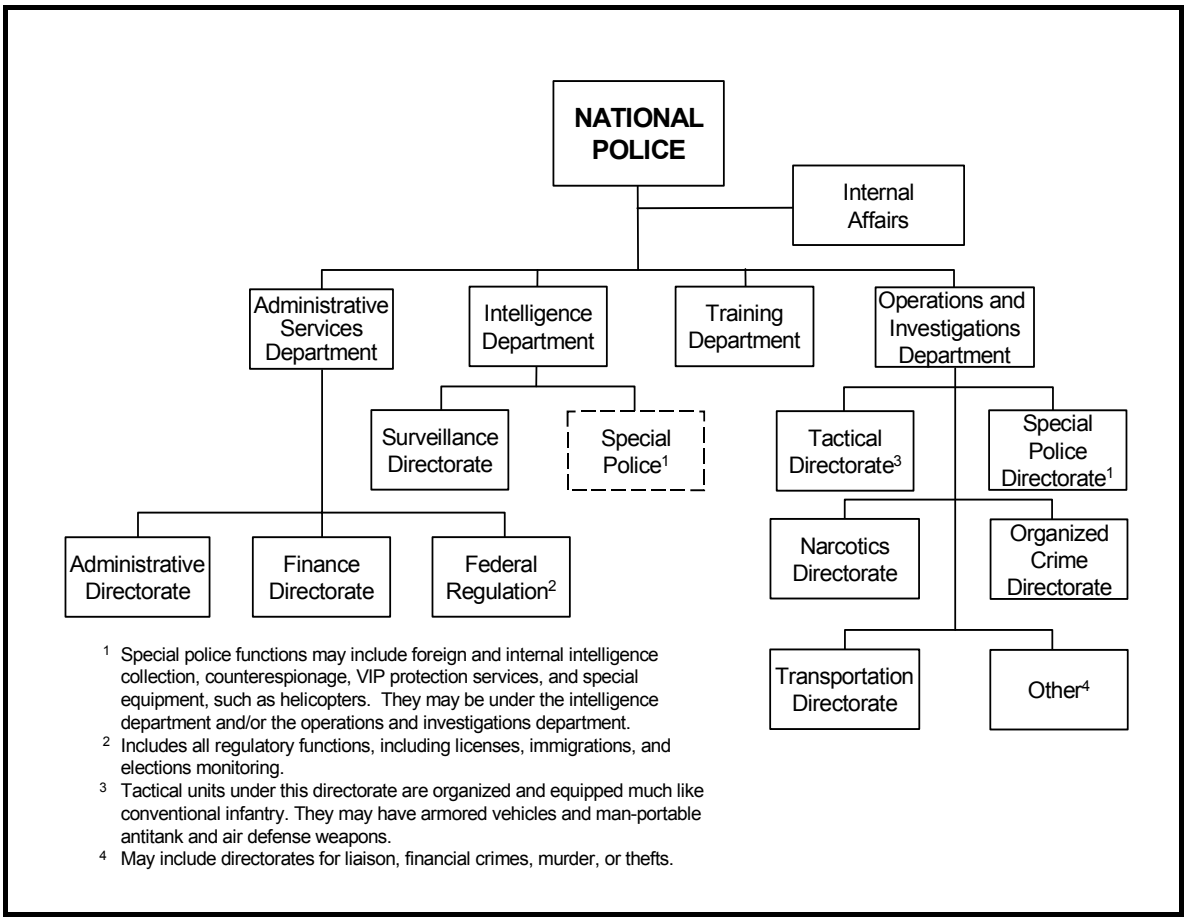

Figure 5-14. National Police Organization (Example)

5-39. National Police often have more capability than district or local police forces for two reasons. First, National Police receive funding from the highest level of government. Second, they interact closely with other government

agencies or national intelligence organizations, to include participating in counterintelligence or counterterrorist activities.

5-40. They may also assume a paramilitary mission or role in times of conflict or when mobilized as a part of a factional army or government-sponsored force. Such roles may include—

- Protection of roadways, railways, waterways, and other national transportation elements.
- Protection of key national infrastructure facilities, such as power plants, dams, roads, communications networks or sites, and telecommunications facilities (radio and television stations).
- Intelligence collection and dissemination.

5-41. The National Police forces include tactical units that may be equipped with armored scout cars, APCs, man-portable antitank and air defense weapons, and light helicopters. These uniformed forces may represent the equivalent of an infantry organization in the regular Armed Forces. The National Police may also include special police units (see discussion below).

District and Local Police

5-42. Politically, the State is divided into districts. District police typically answer to the district governor or governing body. The size and composition of a district police force depends on the geographical area, population size, and economic conditions. Large districts may be subdivided into sub-districts with their own police forces.

5-43. The district, sub-district, and local police (Figures 5-15 and 5-16) conduct activities within a defined geographical area. Each level of administrative jurisdiction will have its own police force. They coordinate often because of overlapping jurisdiction and authority. Lack of coordination, or ill-defined areas of responsibility may lead to confusion, corruption, professional jealousy, and conflict. This could manifest itself as weakness or incompetence, or as inefficiency while working with friendly military forces.

5-44. Local police answer to local government leaders and provide a full range of police services to cities and towns. District police (sometimes referred to as provincial or regional police) typically answer to a political individual or entity, such as a governor or governing body. The size of a police force varies greatly depending on the geographical area, population size, and economic conditions. A remote village may employ one police officer, with austere equipment, who performs all law enforcement activities on a part-time, paid, or volunteer basis. It may rely heavily upon “neighborhood watch”-type activities of private citizens. Conversely, a major city may have a large, well-equipped police establishment, with substantial transportation, weapons, communications, and investigative capabilities.

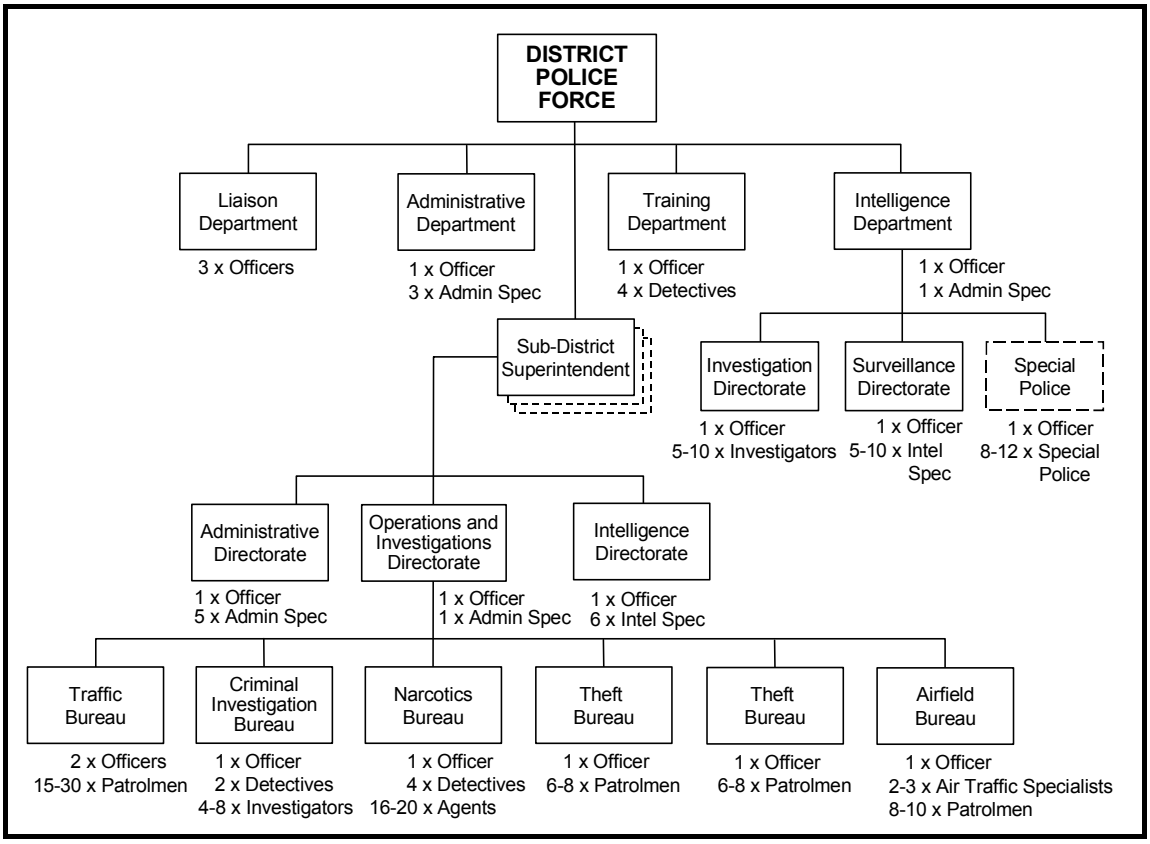

Figure 5-15. District Police Force Organization (Example)

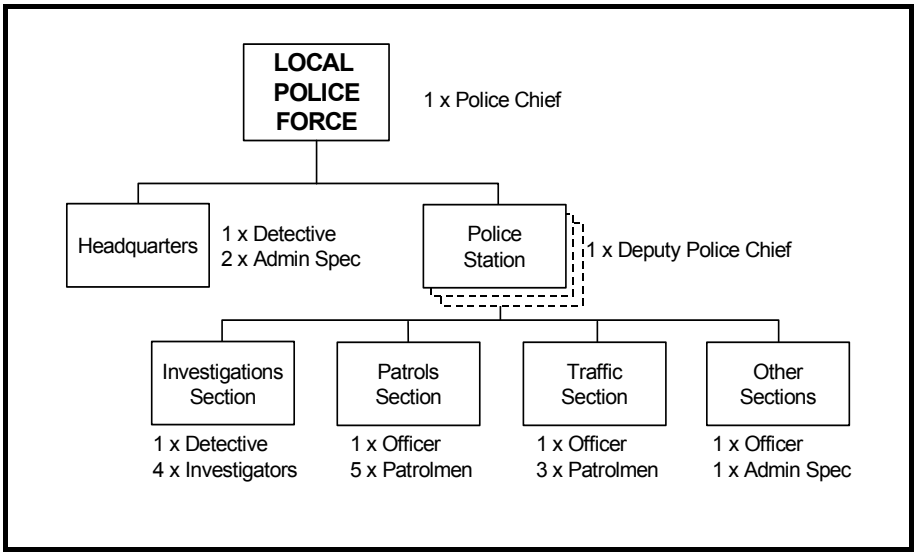

Figure 5-16. Local Police Force Organization (Example)

Special Police

5-45. Each national and district police force may have "special police" elements within its organization. These elite police units would assist in the maintenance of internal order, but may be charged with unique responsibilities or roles.

5-46. The National Police includes special police units whose members have received military training and could be expected to supplement the Armed Forces in a crisis situation. They are trained in the operation of a variety of armaments used by the Armed Forces, such as rifles, machineguns, hand grenades, and smoke bombs. Although originally intended for intervention in cases of large-scale civil disturbances and for antiterrorist tasks, these units are actually equipped and trained for SPF-type roles. Thus, they can conduct direct action attacks or collect foreign and internal intelligence. They typically operate in small teams, similar to those of the SPF under the State Security Directorate. In the National Police, the preponderance of these units may be organized into a special police battalion which, because of its elite status, may report directly to the Ministry of the Interior in peacetime or to the SHC in wartime. Its missions may include protection of high-level government officials.

5-47. Within the various national- and district-level police organizations, the special police are the forces that most resemble regular armed forces in their organization, equipment, training, and missions. They may assume responsibility for crushing organized groups of dissidents and for domestic counterintelligence. Special police may act as special weapons and tactics (SWAT) teams. They may be used to capture escaped convicts, seize weapons in public places, and crack down on public disturbances. Because some special police units are equipped with heavy weapons and armored vehicles, they can provide combat potential to conduct defensive operations if required.

Paramilitary Role

5-48. In some circumstances, police forces at all three levels of organization (national, district, and local) operate as paramilitary forces. They use military-type tactics, weapons, and equipment to further the goals of local, district, and national political organizations. The "para-police" potentially have ties to other paramilitary organizations and to government and political organizations, as well as close ties to organized crime, black market gangs, and other criminals.

Principal Items of Equipment: Police Organizations	Administrative Elements	Intelligence Elements	Training Elements	Internal Affairs Elements	Liaison Elements	Investigation Elements	Surveillance Elements	Narcotics Elements	Transportation Elements	Patrol Elements	Traffic Elements	License Elements	Tactical Elements	Special Police Elements
WEAPONS														
Handgun	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Assault rifle/submachinegun			X					X					X	X
Sniper rifle			X				X	X		X			X	X
Shotgun			X				X	X		X			X	X
Special weapons sight			X				X	X	X	X			X	X
Antitank guided missile (manpack)													X	
Shoulder-fired SAM													X	
COMMUNICATIONS														
Radio	X	X	X		X	X	X	X	X	X	X		X	X
Cellular telephone	X	X	X	X	X	X	X	X					X	X
Facsimile machine	X	X	X					X				X	X	X
Computer	X	X	X					X				X	X	X
Encryption capability	X	X	X	X		X	X	X					X	X
Concealed capability		X	X	X		X	X	X					X	X
VEHICLES														
Patrol car			X	X	X	X		X	X	X	X			
Unmarked vehicle	X	X			X	X	X	X	X	X	X		X	X
All-terrain vehicle		X	X	X	X	X	X	X	X	X	X		X	X
Armored vehicle			X										X	X
Riot control vehicle			X					X	X	X	X		X	X
Motorcycle							X		X				X	X
Helicopter									X				X	X
Aircraft									X					
Watercraft									X					
SURVEILLANCE EQUIPMENT														
Radar			X						X	X	X	X	X	X
Camera		X	X	X		X	X	X		X	X	X	X	X
Binoculars		X	X	X			X	X					X	X
Scope			X	X			X	X					X	X
Night-vision device		X	X	X			X	X	X				X	X
Listening device		X	X	X		X	X	X					X	X
Communications intercept		X	X	X		X	X	X					X	X
SEARCH EQUIPMENT														
X-ray machine			X					X	X				X	X
Metal detector			X					X	X				X	X
Explosive detector			X					X	X				X	X
Contraband detector			X					X	X				X	X
PROTECTIVE GEAR														
Protective clothing			X					X	X				X	X
Protective mask			X					X	X				X	X

Figure 5-17. Example Police Force Equipment List

CIVIL DEFENSE DIRECTORATE

5-49. Forces under the control of the Civil Defense Directorate include a variety of units, both paramilitary and nonmilitary. The Directorate divides geographic areas of responsibility of Civil Defense units along lines that generally correspond to political boundaries of districts and sub-districts within the State. These units have the collective mission of protecting the population and economic centers against the effects of all types of natural disaster and warfare. The Civil Defense Directorate also determines the

assets and the services required to perform peacetime and wartime civil engineering and construction efforts.

5-50. While the majority of Civil Defense personnel are civilians, members of paramilitary units and some staff elements at the national and district levels hold military ranks. Civil Defense units are established in many types of installations, such as factories and schools, as well as local, district and national government organizations. Civil Defense paramilitary units are responsible for the protection and defense of the area or installation where they are located. There are several types of nonmilitary units which are grouped according to their functions, including salvaging and repairing damaged installations, rendering first aid, fighting fires, and maintaining production of key industries. Both the paramilitary and nonmilitary units cooperate closely with the National Police and other internal security forces.

5-51. In peacetime, normal missions include emergency engineering, rescue, and similar disaster relief functions. Civil defense and engineering programs provide for the construction, operation, and maintenance of roads and facilities. For example, construction programs may include the building of shelters, warehouses, aboveground and underground structures, road networks, terminals, and hospitals. Engineers and support personnel may operate electric power, sewage treatment, and water and fuel storage and distribution facilities. These personnel may also conduct environmental support operations, provide fire protection, and provide water purification and disposal.

5-52. During wartime, civil defense units focus on identifying and repairing battle-damaged facilities and structures (including roads, bridges, airfields, and depots) and on minimizing or reducing the impact of enemy strikes on the overall infrastructure. They sometimes protect important military, political, or economic centers against sabotage by internal or external threats and could also perform other support area security missions. As a supplement to the combat engineers of the Armed Forces, civil engineering units also can conduct engineer reconnaissance, conduct explosive ordnance disposal, and provide force-protection construction support and logistics enhancements required to sustain military operations.

COMMAND AND CONTROL

5-53. Internal security forces may have either centralized or decentralized command and control. Centralized control exists when a few individuals have a high concentration of power or decision-making authority. Decentralized control exists when individuals at different levels have decision-making authority. For routine actions, such as operating a stationary guard post, internal security forces follow established or standard operating procedures. Other actions, such as a small-scale ambush, may require additional procedures, such as reconnaissance, additional recommendations, and final instructions and guidance. The individual organizations may agree to form a temporary control organization, such as an interagency headquarters, if more than one force is involved in an operation.

5-54. In wartime, units of the Internal Security Forces might be allocated to the task organization of an operational- or tactical-level military command that is capable of controlling joint and/or interagency operations. In such command relationships, or when they share a common AOR with a military organization, units of the Internal Security Forces send liaison teams to represent them in the military organization's staff, under the operations officer. Within such a staff, the liaison teams primarily coordinate with and advise the chief of force protection and the chief of population management. If the Internal Security Forces involved include SPF or special border or special police units with an SPF-type mission, liaison teams would also coordinate with the chief of special-purpose operations. National Security Forces or civil Defense paramilitary units that guard or protect key governmental and industrial installations may send a liaison team to the chief of infrastructure management; so may civil engineering units that build and repair roads and other infrastructure facilities. Border guard units assigned to patrol coastal border areas could coordinate with the chief of littoral warfare.

OPERATIONS AND TACTICS

5-55. All types of internal security forces conduct the following activities to differing levels: border security, counterinsurgency, counterespionage, reconnaissance, security operations, population control, and civic action. Some are trained to conduct counterterrorist activities, hostage-rescue actions, and personnel protection functions. The skills required to conduct these activities can be adapted to conduct direct actions, such as raids, ambushes, and terror tactics. Many of the tactics and techniques described below are applicable to more than one activity. An ambush, for example, may be used in border security or counterinsurgency activities.

5-56. The purpose of a raid or ambush is most often to kill or capture enemy personnel, to deny the enemy access to an area, or to collect information. These actions can also be used to harass the enemy or divert his attention and resources from other areas. Terror tactics can also accomplish these goals, but are coupled with the explicit intent to intimidate the targeted group or have psychological impact.

AMBUSHES

5-57. Internal security forces conduct two types of ambushes: annihilation ambushes and harassment ambushes. The type of ambush conducted largely depends on the enemy's capability, the objective of the ambush, and the resources available. Any internal security force may conduct a hasty annihilation ambush to thwart an opposing element. The objective may be to kill or capture a dissident. The assault element may consist of a two- to four-person team armed with high-powered rifles. The support element may consist of a one- to three-person team armed with rifles, submachineguns, or shotguns. For a hasty ambush, there are typically no security elements or obstacles. For more detailed information on the actions occurring during an ambush, see Chapters 2 and 4 in this manual, as well as FM 7-100.4, Small Unit Tactics.

PATROLS

5-58. Internal security forces conduct patrols for a number of reasons, including providing security, collecting information, and influencing the population in a positive way. The composition of the patrol and the armament carried depend on the objective of the patrol. A routine border patrol conducted by Border Guard Forces has fewer and lighter-armed personnel than a patrol conducted to capture infiltrators. Medics often accompany patrols to conduct civic action projects. Members conducting the civic action gather information and solicit support. Internal security forces use patrols to conduct reconnaissance and surveillance of areas not observable from an observation post.

OBSERVATION POSTS

5-59. Observation posts (OPs) are positions from which surveillance of the enemy or terrain is conducted. The use of OPs by internal security forces is common. They may comprise a simple wooden building or tower or a concrete, enclosed structure. A guard or guard force occupies the OP and should be capable of responding with appropriate force. The number and type of OPs and the number and composition of a guard force vary with the enemy situation, terrain, weather, and resources available.

CHECKPOINTS

5-60. Checkpoints established by these organizations are manned locations used to control movement. Checkpoints often employ roadblocks and obstacles to channel vehicles and personnel through a certain area. The purpose of checkpoints is to—

- Maintain a continuous check on road movement, apprehend suspects, and prevent smuggling.
- Prevent infiltration of unauthorized personnel.
- Check vehicles and personnel for proper documentation and contraband.
- Conduct other activities, such as tax or information collection.
- Control the population (see below).

5-61. Police or Border Guard Forces are more likely than other internal security forces to establish checkpoints. The composition and construction of the checkpoint and the armament carried depend on its objective and the level of threat. A permanent checkpoint used to check passports may have fewer and lighter-armed personnel than a checkpoint established to apprehend the enemy. Some checkpoints have extensive barrier systems while others may only consist of a vehicle with armed policemen.

POPULATION CONTROL MEASURES

5-62. Population control measures limit travel within a controlled area and provide a means to monitor the movement of individuals. Border Guard and police forces often use an internal passport system to control movement. Some areas (such as the capital, an important industrial region, or a sensitive security region) may require a special passport. Curfews are another popular control measure employed by internal security forces. Other

methods used periodically include the use of checkpoints, surveillance of suspected individuals, telephone or computer monitoring, mail opening, and searches of homes and businesses.

SMALL UNIT TACTICS

5-63. Internal security forces with organization and equipment similar to infantry units can execute small unit tactics, as described in FM 7-100.4. They can also use the general tactics for paramilitary forces outlined in Chapter 2 of this manual.

SPECIAL-PURPOSE FORCE TACTICS

5-64. The SPF under the State Security Directorate can perform reconnaissance and direct action missions similar to those described for units of the SPF Command in FM 7-100.1. Special border units and special police may also undertake such missions, especially in areas where SPF units are not available.

RECRUITMENT AND TRAINING

5-65. Internal security forces at the national and district levels recruit from personnel leaving military service—particularly officers and NCOs. However, most personnel enter directly into an internal security forces organization. For these volunteers or conscripts, a two-year tour qualifies as military service. Other members serve for a specified time and renew their contract, if offered. Another method of personnel acquisition to an internal security force is through political appointment by patronage with the appointing governmental agency. This method, which may occur at any level, would negate the requirement for military experience. These appointments can be used as a reward for past actions or allegiance to the organization. They can also be used to solidify a future working relationship between the internal security agencies and the government to achieve the planned goals.

5-66. At the national (and sometimes district) level, each internal security forces organization has a training academy that provides basic and special instruction. It is unrealistic for many local police forces to have such organized training facilities; therefore they may lack the requisite level of training possessed by their district or national counterparts.

5-67. Basic instruction covers the organization, duties, and responsibilities of the particular internal security forces organization; basic marksmanship; riot control methods; basic interrogation and intelligence-collection methods; legal training; and basic tactical instruction, such as patrolling. Special instruction includes advanced tactical instruction, such as ambushes and sniper activities; advanced intelligence-collection methods; hostage-rescue and VIP-protection techniques; and advanced skill training. Larger organizations offer professional development training throughout a member's career.

UNIFORMS AND EQUIPMENT

5-68. Most internal security forces personnel wear uniforms that may closely resemble the uniforms worn within the military services of the State's Armed Forces. Police, Civil Defense, and Border Guard forces may or may not have a distinctive uniform; members may wear clothing that is appropriate for their work. Depending on their particular function within the organization, they may wear clothing that will allow them to blend in with the surrounding environment. For example, an agent or bodyguard may wear casual or business attire, while a communications specialist may wear the uniform of the local telephone or TV company. Special-Purpose Forces usually have army-style uniforms and specialized equipment, such as night-vision goggles, stun guns, and load-bearing vests.

5-69. Internal security forces employ a wide variety of equipment. The example equipment lists shown in this chapter for various types of internal security forces depict the range of equipment that may be present but do not imply that every unit will always have all the equipment types shown. The amount and level of sophistication of the armaments used by each different internal security forces unit will vary based on the level of organization or jurisdiction, and the amount of funding provided. For example, it is doubtful that the local constabulary would have the same sophisticated weapons that the special police at the national level would have. Police forces may only use pistols, shotguns, and riot-control vehicles. On the other hand, an SPF, special border, or special police unit may use modified rifles, sniper rifles with silencers and image intensifiers, and secure, concealed communications systems. Some units may have armored vehicles or helicopters, while others rely on civilian-type transportation or are limited to movement on foot.

Chapter 6

Drug and Criminal Organizations

Drug and criminal organizations pervade the contemporary operational environment. These organizations exist in time of war and peace. They operate totally in their own self-interest, and their principal goal is to flourish and expand.

This chapter will focus on the organization and activities of large-scale drug and criminal organizations. They are normally independent of nation-state control and often extend beyond national boundaries to operate regionally or worldwide. Individual drug dealers and criminals or small-scale organizations do not have the capability to adversely affect legitimate political, military, and judicial organizations—but the large-scale organizations do.[1]

SIMILARITIES

6-1. Drug organizations and criminal organizations have many similarities in terms of capabilities and structures. After all, any drug organization that deals in illegal drugs is a criminal organization. Thus, this chapter is really about "drug and other criminal organizations."

6-2. First among the similarities is the profit motive, which drives both types of organization. Both organize like businesses, have compartmented cells, and can operate legally (through front companies) as well as illegally. Both transport items, distribute products and services, and launder money. Both may employ terror tactics and militarily unconventional methods to achieve their goals. Both organizations may also have enormous influence within a country or an area. This influence is a direct result of a desire to accumulate wealth. In some cases, the power exerted may be greater than that of recognized political, legal, judicial, and military institutions. For example, a drug organization may invest enormous amounts of money in a country's infrastructure. It may also infiltrate or bribe members of the country's political, military, legal, and judicial institutions, and wield great influence over their policies and procedures.

MOTIVATION

6-3. The primary motive of these organizations is financial. For most of them, the money is an end in itself. However, there are other groups that conduct drug-trafficking or other illegal actions as a means to finance political, terrorist, or other paramilitary activities.

[1] For brevity, the remainder of this chapter refers to these simply as *drug organizations* and *criminal organizations*, but with the understanding that discussion here applies only to *large-scale* organizations and their capabilities. Small-scale drug or criminal elements are discussed in Chapter 7.

6-4. Members of the drug or criminal organization may share common political, religious, or ethnic ties. While these ties may increase loyalty and security, they do not motivate the organization. These bonds are a result of the environment in which the people operate rather than being a reason for the existence of organization itself. For example, an organization with strong familial ties may share the same religion. However, religion is not the motivating factor or tenet of the organization.

THREATS

6-5. The enemies of drug and criminal organizations are political, military, legal, or judicial institutions that impede their actions and interfere with their ability to maximize profits. To a lesser degree, they may be concerned about drug and criminal competitors.

ORGANIZATION

6-6. The structure of drug and criminal organizations is similar to that of a vertically-integrated business rather than a hierarchical organization, such as a military unit. Normally, there is a leader or team of leaders who direct the group's actions. As in any business, the leaders are managers who attempt to cut costs and maximize profits. Many of these organizations organize under a cellular structure with each level or cell operating independently. However, this is not a mandatory requirement.

6-7. In a cellular structure, the cells or departments are organized based on a specific function, such as production, transportation, or money laundering. Although the grouping of functional experts is the organizing principle, the cellular structure inherently offers increased security. Since most cells are not familiar with the organization's entire operation, one cell can be compromised without compromising the others. The members of all cells and workers at each echelon, except the leaders in the headquarters cell, receive payments for services rendered. However, these payments are minimal with the majority of the profits shared by the leaders.

6-8. To avoid duplication, this chapter focuses on the organization of a large-scale drug organization. This basic organization can also serve as a model for criminal organizations. Occasionally, the text will refer to a criminal organization in order to highlight the peculiarities of this type of organization.

CRIMINAL ORGANIZATIONS

6-9. Criminal organizations are non-ideological groups of people organized for the purpose of acquiring money. However, it is important to understand what makes a large-scale criminal organization different from individual criminals or small criminal gangs. While money motivates both entities, the differences are in three major areas:

- A criminal organization has a distinct hierarchy; individual criminals and gangs operate outside a formal organizational structure.
- Criminal organizations develop a strategy and long-term plan, while criminals are opportunists.

- They are capable of adversely affecting legitimate political, legal, and military organizations. A criminal organization can adversely affect legitimate government institutions (political, legal, judicial, and military) through its financial transactions or criminal activities. For example, it may bribe politicians or police to take actions favorable to the organization. In contrast, a criminal does not have the power to influence entire legitimate institutions. He may be a nuisance to local law enforcement personnel, but he is not capable of bribing on a grand scale. Similarly, he cannot cause a financial crisis within a country like a criminal organization can.

PARALLEL "INDUSTRIES"

6-10. Drug or criminal or terrorist organizations can be parallel "industries" that interact synergistically. All three rely on transnational infrastructures that extend largely underground and can be shared to achieve mutual benefits. For the criminal or terrorist, drug trafficking can provide cash with which to purchase weapons and finance other actions. The drug trafficker can use sophisticated methods (including criminal action or terror tactics) to ensure the sources of his supply, and the discipline and integrity of his organization.

6-11. Drug, criminal, and terrorist organizations function outside the norms of international diplomacy and war. Whether their motivation is profit or ideology, or a combination of both, the end product is social disruption through violence that knows no national borders. Thus, the modes of operation of these organizations may converge with each other and possibly with those of the State. In such cases, the various actors may compete with one another, or they may form a "marriage of convenience."

NARCO-TERRORISTS

6-12. One possible combination of these elements is narco-terrorism. It may include some of the same techniques used by terrorist or criminal groups, but conducted to further the aims of drug traffickers. Actions conducted by narco-terrorists may include assassinations, extortion, hijackings, bombings, and kidnappings. Most of these actions are directed against judges, prosecutors, elected officials, or law enforcement agents who interfere with the drug business. However, some actions aim at general disruption of a legitimate government in order to divert attention from drug activities. Narco-terrorists may also prey upon individuals within the drug culture, to discourage competitors or to keep their own subordinates in line.

DRUG ORGANIZATIONS

6-13. Drug organizations are groups of people organized to produce, transport, and distribute illegal drugs to acquire money. Figure 6-1 depicts the functions of a vertically-integrated drug organization. Each level or cell is a separate entity, operating independently, but the actions of one cell depend on the success of others. For example, money laundering depends on the money obtained through the distribution function. Similarly, the laboratory cell depends on the cultivation function for crops and on the transportation function for delivery of crops and necessary chemicals. This organizational

structure is typical, and the sizes for the functions in the figure are relative to the actual size of the groups within the organization.

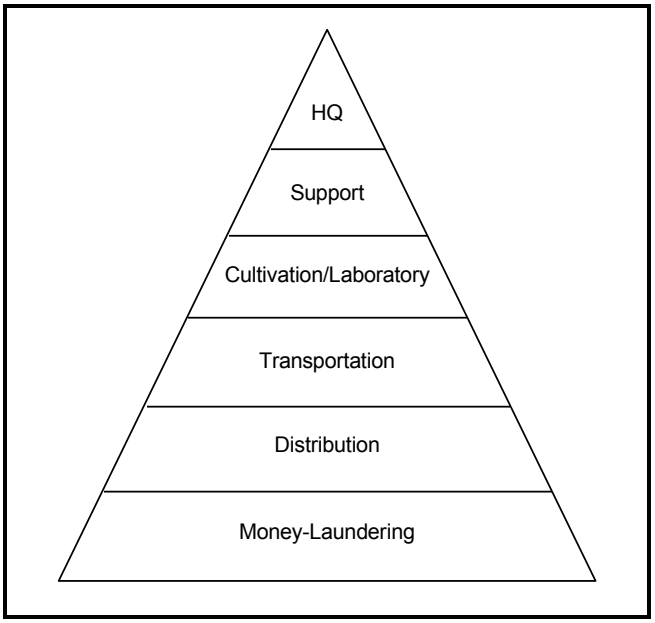

Figure 6-1. Elements of Drug Organization

6-14. While not all drug organizations have a cellular structure, or employ all of these cells, the organization or others operating on its behalf execute the same functions. The size of the drug organization determines the existence of different types of cells and the number of each. A large organization may employ many cells with more than one of each type. There may be several dedicated to one function, such as cultivation. If the organization is small, there will be fewer cells, and some cells may be multifunctional. For example, the functions of cultivation and laboratory processing may be conducted by separate organizations or by a combined "production cell."

6-15. A drug organization may outsource some functions, just as businesses contract services with other organizations. For example, the drug organization may contract with a criminal organization or local gang to conduct distribution.

6-16. If cellular structure is employed, it differs from that found in a terrorist organization. There is not necessarily any formal chain of command or hierarchy. There is little, if any, loyalty to the organization as a whole. The cells and most of their members act as "subcontractors" with the sole motive of making money.

6-17. Members of a drug organization may dress in casual attire to blend in with the local population. For example, headquarters cell members may wear suits and casual attire similar to that worn by managers and supervisors in a corporation. Similarly, members of the transportation cell may wear a uniform similar to that worn in the transportation industry, such as flight suits for pilots and mechanic's overalls for maintenance personnel. Cultivation cells dress like any other farmers.

Headquarters

6-18. Leaders, security, direct action, and communications personnel compose the headquarters cell. This cell is responsible for overseeing the activities of the entire organization, establishing and implementing high-level security plans, and conducting offensive actions, such as extortion or assassination. The leaders have detailed knowledge of the entire operation, and a leader or small group of individuals acts as the "president" or "chief executive officer" of the organization. The headquarters cell often includes "counselors." These are former leaders who have retired from active participation and now advise the current leaders on past practices and historically relevant information. The leaders of the individual cells at lower levels control and manage the activities at their respective level.

6-19. The leaders of the organization use different modes of operation depending on the power of the organization and the individual leader. Those with great power over the political, military, legal, and judicial institutions of a country may conduct their business openly with minimal fear of reprisal. Alternatively, those leaders with limited power may have to conduct business covertly to avoid arrest or detention.

6-20. Regardless of the method of leadership, security personnel protect the leaders from the enemy. Security details include personal bodyguards to protect the leaders and their families. They also include intelligence personnel who conduct reconnaissance and surveillance leaders' homes, places they visit, business establishments, and enemy personnel.

6-21. Direct action personnel conduct offensive actions on behalf of the organization. These actions may include terror tactics (such as extortion, kidnapping, hijacking, assassination, maiming, or sabotage) as well as criminal actions (such as theft and murder).

6-22. Communications specialists coordinate systems for communication within the headquarters cell, and from this unit to other the functional elements. The organization primarily uses commercial communications systems—telephones, cellular phones, faxes, and the Internet—to conduct business. The members use codes when discussing sensitive information about activities and personnel. They may also attach encryption devices to communications systems to prevent disclosure of information.

6-23. The organizations at the cellular or functional level, such as the cultivation and laboratory cells, do not require sophisticated communications and security equipment. Compromise of information at their level does not have grave consequences for the entire organization. On the other hand, compromise of some cells' members and activities could have devastating effects on the survival of the group. For example, if front companies operating on behalf of the organization compromised information that led to the halting of activities or the compromising of money laundering, the entire organization would suffer.

Support

6-24. The support cell includes a variety of individuals such as lawyers, bankers, politicians, doctors, realtors, and travel agents. They perform functions similar to things they might do if they were acting on behalf of a legitimate corporation, although some of these activities may be conducted in an illegal manner. For example, the lawyers advise commanders on the legal implications of various actions; realtors buy and sell property; travel agents book reservations. Some of these support personnel are willing participants while others are not. The organization bribes those people it can; those who refuse bribes are often targets of extortion or death threats. The organization frequently coerces and intimidates personnel to take actions in support of its operation. (This would be the job of direct action elements from the headquarters cell.)

Cultivation

6-25. The cultivation cell, comprised of farmers, is responsible for cultivating crops that others process into drugs. They are the most removed from the drug organization and are not familiar with the organization's entire operation. Typically, farmers grow these crops because the profit is greater than producing other crops, such as corn or coffee. Small profits, relative to the profits of members higher in the organization, motivate these farmers. Some drug-producing crops, such as coca, are legal, while others, such as marijuana, are illegal. The country of origin determines if the crop is legal or illegal.

6-26. The farmers often affiliate with insurgents because of the government's involvement in drug eradication. The insurgents recruit these farmers and inflame their anger against their common enemy. Some farmer's affiliation with drug production may also be due to insurgent intimidation and/or lack of government presence in the areas where they cultivate. The insurgents' interactions with the farmers do not concern the drug organization as long as the farmers keep growing drug-producing crops.

6-27. The farmers typically do not have security programs or personnel like those found in other cells, but they may have personal firearms. If the enemy or local law enforcement personnel attempt to destroy the crops, the farmers are virtually helpless. A security or armed detail from the drug organization will not intervene to prevent destruction. The farmers are expendable because there are many farmers growing crops in support of the drug organization. The farmers conduct business with a middleman who coordinates pickup and delivery of the crops. There is no communication between the farmers and other functions within the organization.

Laboratory

6-28. Chemists, cooks, lab workers, and security personnel compose the laboratory function. This cell is responsible for processing the drug-producing crop or component chemicals into a drug fit for consumption. It maintains various lab sites in less-populated areas to avoid detection or suspicion. Security is a very high priority, and security elements are established in the vicinity of its laboratories to warn of intruders. Sometimes this

security element conducts diversionary tactics to mislead the enemy. The diversion permits the laboratory members to escape and, time permitting, the members attempt to carry processed drugs or equipment with them. The security element performs warning functions, not direct action functions.

6-29. Members of the laboratory cell may have small arms for personal protection, but they would rather compromise current activities than become involved in a head-on confrontation with law enforcement personnel or the enemy. Sometimes, the drug organization leadership may intentionally compromise a smaller lab to protect a larger one. A periodic compromise of a drug lab may avoid large-scale enemy activities in a given area.

6-30. The laboratory cell attempts to disguise or camouflage its lab to prevent detection. The amount of equipment and the size of the lab depend on the drug being processed. Figure 6-2 illustrates a typical lab setup. Cocaine labs, for example, require large, ventilated areas to process leaves into paste and are labor-intensive. Business is conducted with a middleman who coordinates pickup of the drugs. As with the cultivation cell, there is no communication between the laboratory and the other functions.

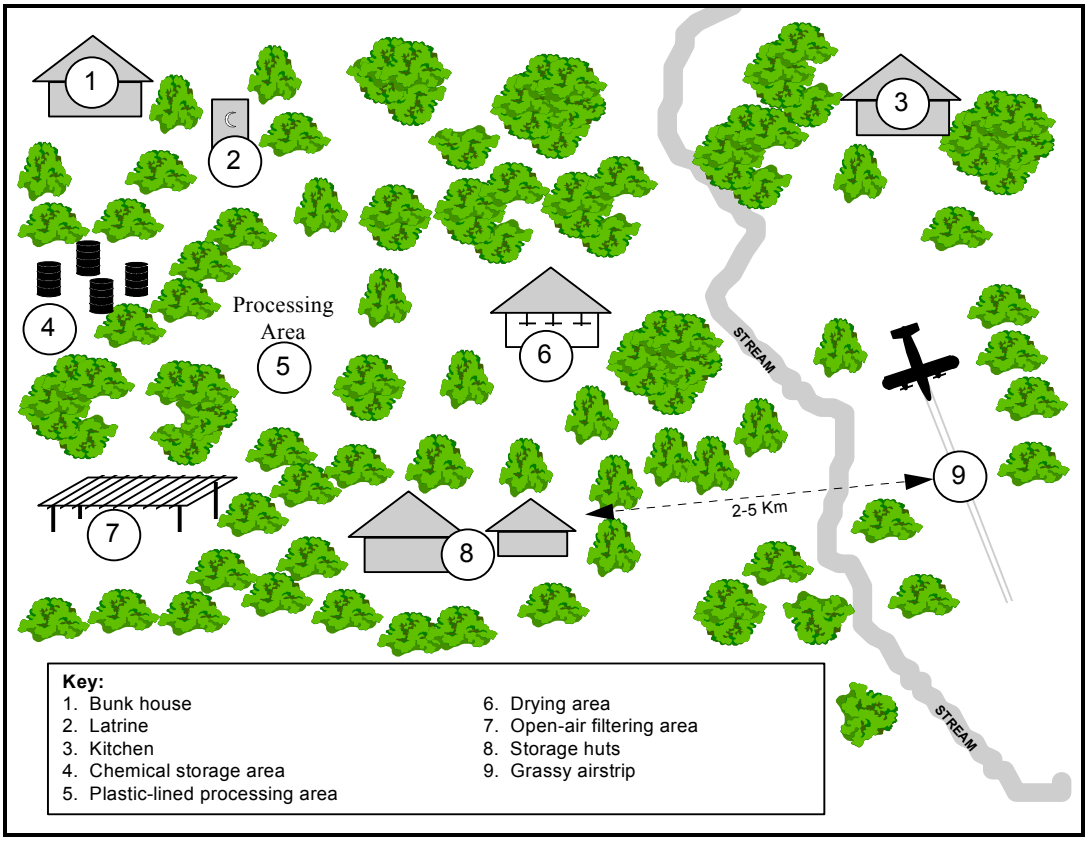

Figure 6-2. Example of a Drug Laboratory Setup

Transportation

6-31. There is at least one transportation cell per function described below:

- Transporting supplies, such as chemicals and expendables, to cultivation, laboratory, and transportation cells.
- Transporting crops from farms to laboratories.
- Transporting drugs from laboratories to distribution points.

They transport drugs along various routes using multiple means, such as animals, vehicles, boats, and aircraft.

6-32. There is usually no relationship between different transportation cells. However, one transportation cell may transfer goods to another during transit. A specific transportation cell includes personnel required for moving goods, such as vehicle drivers, pilots, boat captains, and associated support personnel. They have their own maintenance and support personnel to operate, maintain, and sustain all means of conveyance.

6-33. Sometimes, couriers are hired to transport drugs. Some couriers are willing participants in the transportation of drugs, and others are the victims of extortion and intimidation forced to support the drug business. They attempt to conceal the drugs using various techniques, such as wearing bulky clothes, swallowing condoms full of drugs, or taping drugs to their bodies. A transportation cell may use families as couriers to avoid suspicion at enemy checkpoints. Other couriers are unsuspecting individuals who think they are transporting a legal product. For example, the driver of a vehicle may not know that a group member has concealed drugs within a shipment of produce. The drug organization uses these expendable couriers during intentional compromises, which may divert the enemy's attention away from a larger shipment or prevent increased enemy observation and surveillance.

6-34. The transportation cells employ a variety of transportation conveyances. The conveyance must blend in with the environment and be feasible. Frequently animals are used in rough or impassable terrain. The animals can carry, internally if necessary, a large quantity of drugs or materiel. Animals carry many of the supplies used by the cultivation, laboratory, and transportation cells. The transportation cells also use humans as couriers in ways discussed above.

6-35. Vehicles, both commercial and private, are the conveyance of choice for the organization. With any mode of transportation however, the most significant indicator to the presence of hidden transported narcotics is the use of a masking odor (particularly for marijuana loads). Items such as laundry detergent, dryer sheets, cologne, perfume, etc., are often used to disguise the scent of illicit drugs, and to throw the authorities or a canine off of the scent.

6-36. Using vehicles requires little operator training and less logistics support from the organization. Figure 6-3 illustrates some of the areas within and on a vehicle used to conceal drugs and materiel. But smugglers will use any hollow space in all modes of transport to conceal narcotics. If sufficient space is not available, the smugglers will construct it.

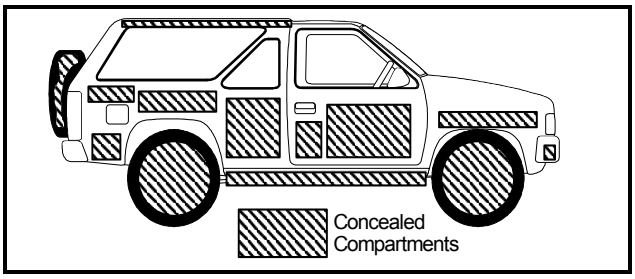

Figure 6-3. Example of Concealed Compartments in a Vehicle

6-37. By using vehicles, the risk of compromise is inherently lower than using other modes of travel for the following reasons:

- The probability of search is lower because of the sheer number of vehicles on the roads.
- Vehicles can travel over many road networks without filing plans similar to those required for waterborne craft and aircraft.
- Vehicles can divert their route without drawing attention.
- Commercial vehicles can conceal large amounts of drugs.

HISTORICAL PERSPECTIVE: NARCOTICS TRAFFICKING OVER U.S. BORDERS

The U.S. Border Patrol can attest to the fact that transporting narcotics in passenger or commercial vehicles along the borders of the U.S. is the preferred method of narcotics smugglers. The advantage is obvious, considering the vastness of the borders, the thousands of potential crossing sites into the U.S., and the difficulty of manning them. If a loaded vehicle successfully crosses, the smuggler avoids the risk of compromising a narcotics load, and the load proceeds safely to a storage or distribution center within the borders of the U.S. Additionally, by breaking up large loads into smaller vehicle-sized loads, the smuggler is actually securing his profit. For example, if a smuggler attempts to cross 600 pounds of cocaine in a tractor-trailer, and the tractor is seized at a port of entry, the smuggler loses his entire profit. Conversely, if a smuggler crosses 600 pounds of cocaine in ten vehicles with 60 pounds each, or 20 vehicles with 30 pounds each, he limits the risk of losing his entire profit. In his cost/benefit analysis he may deem it acceptable to lose one or two smaller loads. The resulting increase in logistical and command and control concerns in minimal when given the nature of the action and the enormous profits involved.

6-38. Waterborne craft offer excellent opportunities to transporters. They use crafts ranging from large commercial ships and fishing boats to pleasure and private boats to high-speed, low-profile vessels fabricated of wood or

fiberglass. The latter vessels offer outstanding protection against radar and visual detection. Concealed compartments in waterborne craft are useful to transport large quantities of drugs. (See Figure 6-4.)

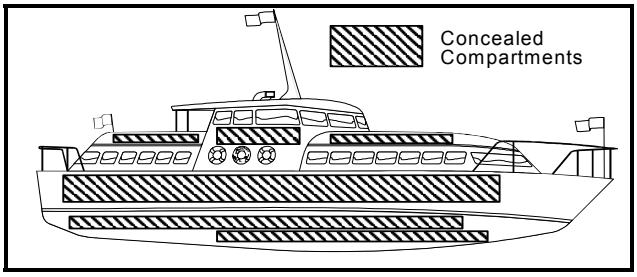

Figure 6-4. Example of Concealed Compartments in a Waterborne Craft

6-39. A transportation cell may use aircraft for delivering and air-dropping drugs and materiel. This conveyance offers the greatest potential results but is the one with the most risk. Often, contracts for air transport are made with outside companies. They pick up and deliver the drugs and receive payment upon return. Aircraft range in size from large cargo aircraft to small propeller-driven aircraft. Each aircraft has strengths and weaknesses. Large jets have great cargo capacities, are capable of long flight range, and of outrunning some enemy aircraft, but they are vulnerable to detection by radar and visual means. Small aircraft can avoid detection by flying in radar shadows, are capable of landing on unimproved landing strips, and can change routes quickly to avoid detection by enemy surveillance. Yet the capacities of these aircraft are small, and the aircraft offer few compartments for concealment.

6-40. The aircraft and waterborne craft used by the organization have sophisticated electronics and communications systems onboard. The organization spares no expense to equip these craft with the latest technology, and they are obtained through legal and illegal methods. Members may purchase, rent, steal, or otherwise commandeer a mode of conveyance. They may hire thieves to steal those vehicles used especially for international transportation.

6-41. The transportation cells employ security elements, called "screeners," to provide early warning. On transportation routes, they travel ahead of drivers and warn them of roadblocks or other obstructions so that they can reroute. Screeners may use visual signals to warn other drivers, such as a raised hood, or they may create a diversion to distract enemy personnel. A sophisticated organization may use cellular or radio communications to warn drivers. Security elements also provide early warning around loading and unloading points, to prevent compromise at these sites. Drugs must be loaded and unloaded in areas free from enemy observation and in a manner that does not draw attention. Typically, security elements are more heavily armed than the other members of the transportation cell. They use their weapons to create diversions and assist in escapes, rather than to confront enemy personnel.

6-42. Although the transportation personnel attempt to avoid contact with the enemy, they are capable of conducting actions to defend themselves. For example, if the enemy attempts to force an aircraft to land, the crew may attempt to outrun the enemy aircraft. If these attempts fail, the crew may air-drop the drugs in the ocean. Similarly, if the enemy detains a vehicle to conduct a search, the driver may attempt to escape and can use force if necessary.

6-43. When transportation chain of drugs involves multiple modes of conveyance, there are locations along the way where the drugs must be transshipped and/or broken down into different types or sizes of loads. The transport and security personnel and "management" at these locations are often paid (at least in part) with an amount of drugs. This can result in local drug-trafficking networks.

Distribution

6-44. The distribution cell is responsible for bringing drugs to the marketplace for sale and distribution. Typically, members of this group operate in enemy-held territory and include many people, such as brokers, wholesalers, and dealers. The distribution cell has a triangular structure. (See Figure 6-5.)

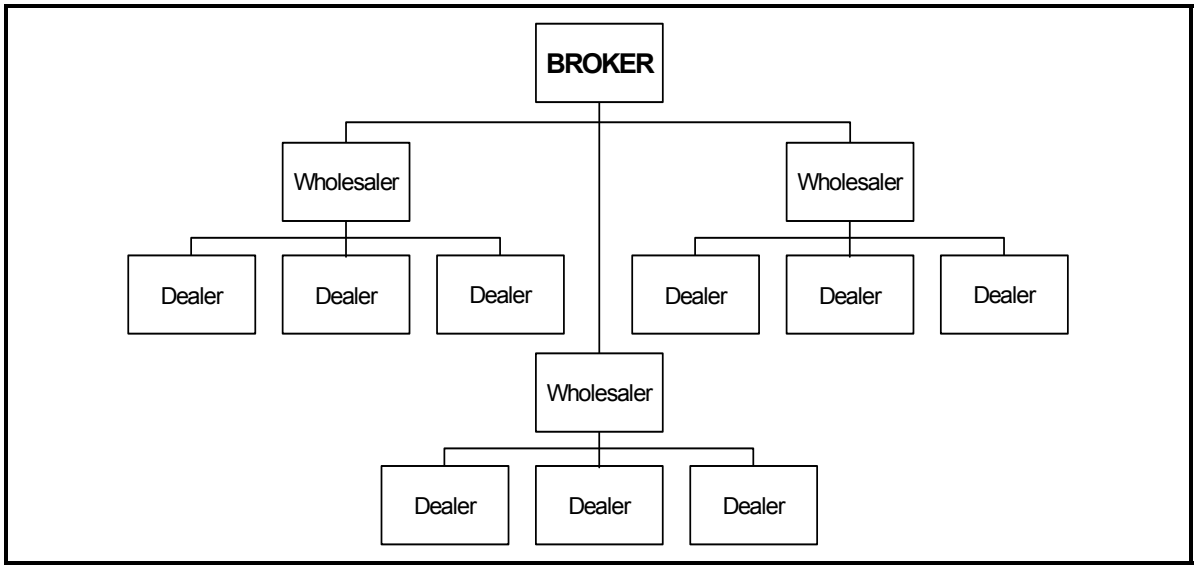

Figure 6-5. Example Structure of the Distribution Cell

6-45. Each level is dependent on the level above it, but each element within a level operates independently. A dealer, for example, depends on his wholesaler for drugs, but he operates independently of other dealers. Although there is no command structure per se, each level responds to the requests of its next higher level. Brokers are individuals who coordinate with the transportation cells to deliver drugs. Wholesalers deliver drugs to dealers who, in turn, deliver them to users. Brokers, wholesalers, and dealers receive and store drugs, break down large quantity of drugs into smaller quantities,

and distribute drugs. The size of their activities is directly related to the quantity of drugs distributed. For example, brokers handle larger quantities of drugs than wholesalers, and wholesalers deal with larger quantities than dealers. Similarly, the facilities for storage and the number of security personnel required at each level are proportional to the quantity of drugs handled.

6-46. The facilities used to store and distribute drugs range from large warehouses to small apartments or even vehicles. The facilities are inconspicuous and blend in with the environment. Abandoned buildings or front companies offer good protection for the organization's activities. Security measures, such as lookouts, simplistic sensors, and rudimentary barriers, attempt to warn of intrusions or prevent observation. The crafty members of the organization alter their movements and their storage and distribution facilities to lessen the chance of compromise.

6-47. Typically, members of the distribution cell arm themselves for protection. An extra security detail would draw attention to group members, so they provide security for themselves. The weapons of choice for include small arms and light assault weapons. The members employ communications security measures, such as codes, cellular telephones, and beepers, to avoid detection.

Money Laundering

6-48. The money laundering cell includes a variety of personnel, including accountants, bankers, tellers, and couriers. As in the support cells, some money laundering cell members are willing participants in the money laundering process and accept bribes for their services. Extortion and intimidation keep unwilling members active in the process. Members of money laundering organizations also establish and operate front companies.

6-49. Some members, such as accountants and bankers, perform their normal functions as in a legal business; however, they may conduct illegal acts on behalf of the organization. Because of banking regulations, members must conduct activities that do not draw attention to themselves. As an example, couriers deposit less than $10,000 in bank accounts to avoid federal banking regulations. However, not all countries have such regulations, making it easier to launder large sums of money.

6-50. Couriers conduct many transactions with financial institutions. They travel from bank to bank making deposits, or converting money into checks and money orders to prepare for smuggling activities. Couriers perform functions in the same manner described previously, except that cash, checks, or money orders replace drugs. The money laundering cell may also use electronic fund transfers which makes tracking of illegal transactions much more difficult, especially when the country has lax banking laws.

EXAMPLE DRUG ORGANIZATION

6-51. Figure 6-6 shows an example drug organization capable of conducting discussed activities.

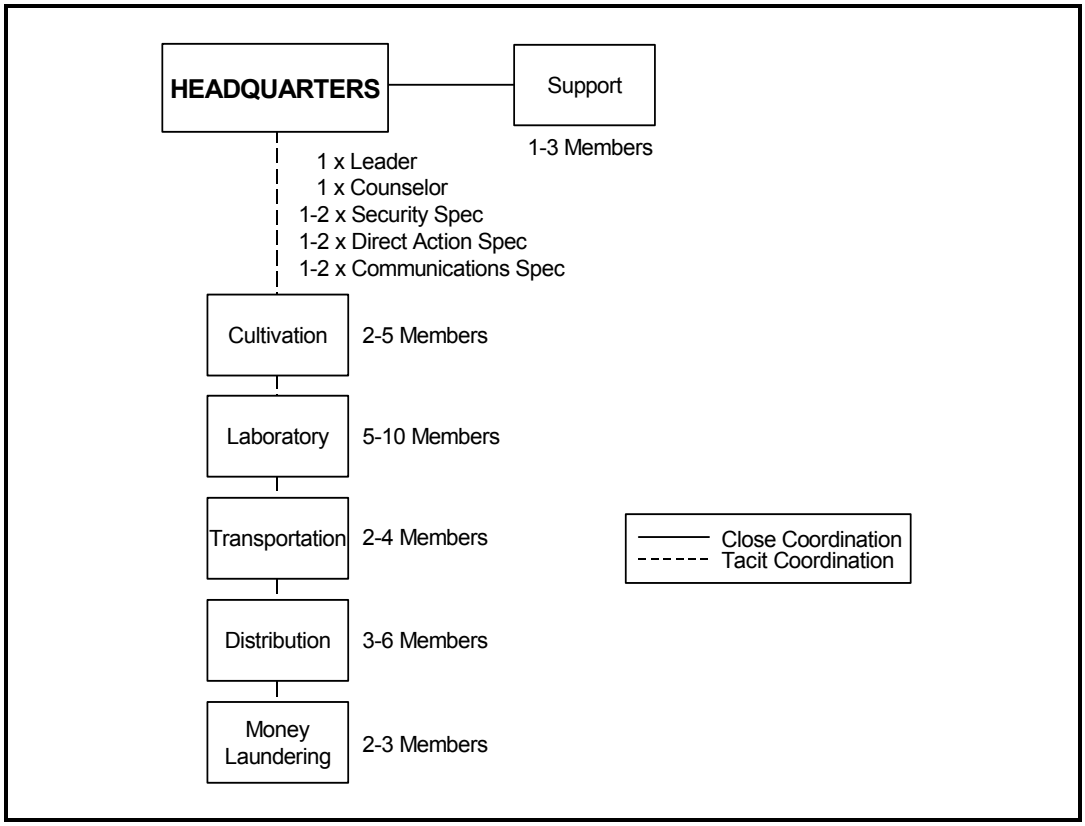

Figure 6-6. Example of a Drug Organization

ACTIVITIES

6-52. Drug and criminal organizations conduct many of the activities discussed below. The level of sophistication with which the organizations execute these actions depend on their size and the resources available. An organization with great wealth, for example, may conduct these activities on a grand scale using the latest technology.

SECURITY

6-53. For both drug and criminal organizations, security is paramount to their activities. The members of these organizations may use the highest degree of sophistication available to conduct intelligence collection and counterintelligence activities. These activities are a priority, can be well funded. In many cases, intelligence sources extend to high levels within government and law enforcement agencies. The local citizenry may willingly provide ample intelligence collection, counterintelligence, and security support. Intelligence and security can also be the result of bribery, extortion, or coercion.

6-54. Most members of drug and criminal organizations are capable of protecting themselves and their assets. Typically, they carry small-caliber weapons, such as handguns, pistols, rifles, and shotguns. They are lightly armed out of necessity or convenience, not for lack of resources. When greater force of arms is necessary to control people, protect vital resources, or obtain information, these organizations typically have "enforcers" who can use heavier arms, such as machineguns and assault weapons, if necessary.

SMUGGLING

6-55. Smuggling is the act of transferring illegal goods. In this case, it means transporting drugs or money in violation of the enemy's laws. Members of the transportation and money laundering elements conduct smuggling activities. Couriers conceal drugs, money, and other materiel either on their body or within conveyances. Individuals build special compartments within conveyances to conceal drugs or money to avoid detection. The hidden compartments must not draw attention and must protect the stored items. Only the creativity of the smuggler limits concealment possibilities. (See Figures 6-3 and 6-4 for examples of concealment techniques.)

MONEY LAUNDERING

6-56. The organization conducts money-laundering activities to transfer funds into the legitimate international financial system. Because of the legal restrictions levied by the enemy, the organization must have a way of transferring "dirty," or illegally earned, money into "clean" money. The organization smuggles some currency back to its country of origin. However, large sums of enemy currency are not feasible for the organization because it must use the legal currency of its government to make transactions. For example, a farmer cannot receive payment for his crops in the enemy's currency because he would be unable to use it.

6-57. A more productive way to transfer funds into the legitimate financial system is to operate through front companies. Front companies are legitimate businesses that provide a means to distribute drugs and launder money. The organization establishes its own front companies or approaches legal companies to act as intermediaries. Some front companies, such as an import or export business, may operate for the sole purpose of laundering money. Other companies, which are targets of extortion, operate as profit-making activities and launder money as a service to the organization. Drug and criminal organizations operate front companies in their host country, as well as in other countries.

EXTORTION

6-58. Extortion is the act of obtaining support by force or intimidation. Organizations use extortion to obtain information or to protect members. Members of the headquarters element conduct extortion on behalf of the organization; other cells may extort as part of their activities. Examples of extortion include intimidating politicians to vote in a manner favorable to the organization, intimidating judges to free an organization member, and forcing a farmer to grow drug-producing crops.

BRIBERY

6-59. Bribery is the practice of giving money or other favors to influence someone. Organizations give money to people in power who make or influence decisions. For example, law enforcement officials receive bribes, which causes them to make decisions that favor the organization. Law enforcement officials or enemy reconnaissance patrols may avoid the organization's infiltration routes to allow drugs to enter enemy territory. If the organization is unable to bribe someone, it employs harsher methods, such as extortion, assassination, or murder, to gain cooperation.

RECRUITING

6-60. Drug or criminal organizations do not recruit for the same reasons or in the same manner as other paramilitary organizations. They do not try to increase their membership or build their organizations. They increase their numbers only if it is profitable to do so. For example, the organization may need more chemists to process drugs, so it recruits chemists. When the organization no longer requires their service, it dismisses them. The drug or criminal organization may bribe, extort, or simply pay for services, whereas another paramilitary organization may appeal to an individual's ideological desires. While other forces recruit and indoctrinate, drug and criminal organizations hire people to perform a given function.

CIVIC ACTIONS

6-61. Drug and criminal organizations conduct programs of patronage under the guise of civic actions. These programs are only indirectly intended to benefit the general populace. Rather, the main intent of the drug and criminal organizations is to gain and maintain support, reward their supporters, and facilitate their continued activities. They may build a school, improve a road, or supply food and medicine. These projects benefit the local population because they improve the people's quality of life and may improve their standard of living. For example, road building makes it easier to transport goods to market and creates jobs. Some of the jobs may be temporary, such as those in construction, while others may be permanent, such as those in education and clinics. Through its propaganda efforts, the organization ensures that the population knows who is making the improvements.

6-62. Sometimes the organization cooperates with an insurgent force to conduct civic actions. Both groups want to create chaos or increase instability within the enemy government. They do not cooperate for ideological reasons. Their sole purpose is to inhibit the enemy's ability to affect their activities by gaining the inherent security a grateful public can provide.

INFORMATION WARFARE

6-63. Drug and criminal organizations may have the resources to conduct a variety of information warfare activities (see Chapter 2). However, their focus is often on a well-orchestrated perception management (propaganda) effort. This can be a powerful tool for intimidating enemies and encouraging support of the organization's moneymaking efforts. The use of perception management techniques can ensure that the population knows who is

making improvements in the local environment and allow the organization to take credit for other benefits it provides to the local population.

6-64. The organization can also use counterpropaganda to spin events against the enemy. For example, the enemy may burn a farmer's drug-producing crop and then broadcast announcements that the action is a direct result of the farmer's involvement with an illegal activity. However, the drug organization can counter this by instilling the idea that the enemy does not have programs to help the farmer make profits legally and reminding the populace of the new medical clinic it built.

CRIMINAL ACTIVITIES

6-65. Drug organizations may conduct other criminal activities (such as murder, theft, prostitution, arms trafficking, and racketeering) that support their goals. However, these are secondary to the organization's main money-making activity. These actions occur infrequently, since they are generally not worth the risk. However, the significance of these actions relates to gaining and maintaining support.

MUTUAL INTERESTS

6-66. When mutual interests exist, drug and criminal organizations may combine efforts with insurgent and/or terrorist organizations controlling or operating in the same area. Such allies can provide security and protection or other support to the drug or criminal organization's activities in exchange for financial assistance, arms, and protection from government forces or other common enemies. The amount of mutual protection depends on the size and sophistication of each organization (drug/criminal or insurgent/terrorist) and the respective level of influence with the government and/or local population. Terrorist or insurgent groups can create diversionary actions or conduct reconnaissance and early warning, money laundering, smuggling, transportation, and civic actions on behalf of the drug or criminal organization.

6-67. The congruence of interests can also result in drug and criminal organizations having a close relationship with an established government. In some cases, the government may be the covert sponsor of these organizations. The government's main motivation for this may be for financial gain, but it could also intend on using these organizations against insurgent or terrorist groups or against a neighboring state in support of a broader strategy.

Chapter 7

Noncombatants

Noncombatants, in the strictest sense, are individuals who are in an area of combat operations but are not armed and are not participating in any activity in support of any of the factions or forces involved in combat. In actuality, however, some of these nonmilitary elements may support or otherwise affect the conflict, either wittingly or unwittingly. Some of them might actually be armed. That is the reality in the contemporary operational environment.

To varying degrees, the civilian population has an impact all other elements that compose the contemporary operational environment and to a large extent determines the nature of political and military action. Aside from military and paramilitary forces, the civilian population of a nation or region is often the single most important aspect of the environment.

TYPES OF NONCOMBATANTS

7-1. The media, humanitarian relief organizations, criminals, transnational corporations, private security organizations, and other civilians on the battlefield are the noncombatants discussed in this chapter. They represent a diverse grouping of individuals and organizations.

7-2. Virtually every country in the world has a demographically and socially diverse population. This diversity is based on such factors as religion, ethnicity, race, tribal affiliation, and class structure. The ability of a nation to harmonize these diverse elements goes far in determining its success as a nation. It is also the demographic and sociological aspects of a population that provide significant complexity to military operations. This situation can be further complicated by the presence of other noncombatants who are not indigenous to the country or region.

MEDIA

7-3. The media include local, national, and international journalists, reporters, and associated support personnel. Media personnel may be independent or affiliated with a particular news agency. Their primary job is to provide information. Although media personnel may seek to remain objective and report accurately, there are those who have a bias favoring a certain position. Some will resort to any means to obtain or publish their story at any cost.

7-4. The media use equipment, such as still cameras, video cameras, tape recorders, videocassette recorders, cellular telephones, laptop computers, general office equipment, and satellite-linked computer and video equipment. The sophistication of the equipment depends on the financial resources of the media element. A well-resourced reporter may have a cellular telephone, a notebook or laptop computer, assorted audio-visual equipment, and an all-

terrain vehicle equipped with the latest video manipulation technology. Alternatively, an independent reporter may only have a laptop computer. All media personnel carry credentials to indicate who they are and for whom they work.

7-5. Opposing sides in a conflict will seek to control the media internally and exploit them externally. The pervasive presence of the media provides a certain situational awareness that might not otherwise be available. Media may allow an opponent the opportunity to attack the national will of its enemy. They will most likely be used as an outlet for propaganda and psychological warfare campaigns. These sources of facts and opinions cannot be controlled by the chain of command. Media coverage of operations and real time dissemination will also dramatically affect international relations and strategic interaction. With or without manipulation by other parties, the media can have a great effect on public opinion and national will.

7-6. The balancing effect of multiple reporting sources tends to reduce the impact of any one outlet's bias or "spin." Democracies with freedom and widespread access to media and other information systems can be less susceptible to propaganda but are still susceptible to media influence. Populations that have only limited access to information are more vulnerable to slanted or manipulated reporting.

HUMANITARIAN RELIEF ORGANIZATIONS

7-7. Nongovernmental organizations (NGOs) and private volunteer organizations (PVOs) provide humanitarian assistance and disaster relief. These international organizations may offer assistance based on their unique goals regardless of the race, creed, or nationality of the recipients while remaining independent from any government style policies. Officially, they are not affiliated with a government, yet humanitarian relief organizations may be influenced by policies of their home country. Conversely, since no government in particular regulates these organizations, they may discriminate against race, creed, nationality, and political affliction. While there are several thousand of humanitarian relief organizations worldwide, Figure 7-1 provides an example organizational structure.

7-8. These humanitarian relief organizations are generally motivated by charity. They will be trying to help the local population deal with manmade and natural disasters and disease, hunger, and poverty. However, some organizations and individual participants may have motivations that differ from their public organizational mission statements. These can be economic, political, religious, cultural, or private motivations, such as revenge. There are both stated and hidden interests and objectives.

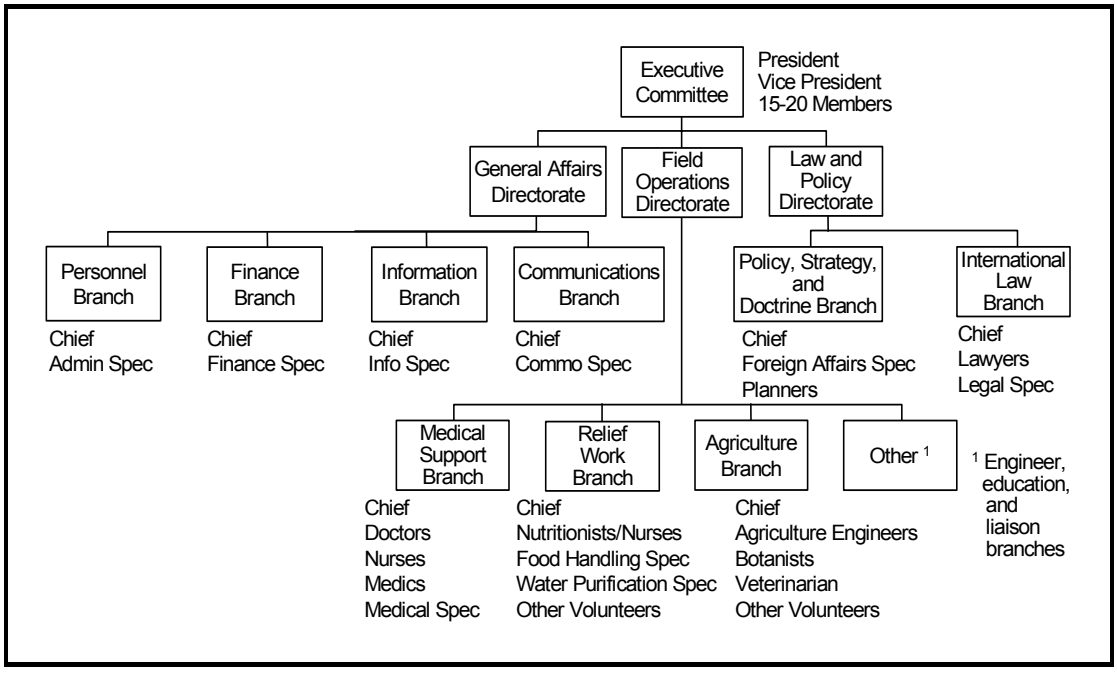

Figure 7-1. Humanitarian Relief Organization (Example)

7-9. When offering assistance in times or war or internal conflict, each organization or individual participant pursues its own interests and objectives, which are sometimes supporting but sometimes competing with those of the combatants:

- Some organizations are favorable to the efforts of one of the combatant sides and are willing to provide them assistance regarding the culture, languages, and peculiarities of the local population. In return, combatant forces can provide an environment in which these organizations can deliver goods and services to the population.
- An organization may have the same ideology as one of the combatant sides and may adversely affect the other's mission accomplishment or may create situations that lead to conflict. The combatants may use these outside elements to help them collect information or provide supplies.
- Some organizations may be working at cross purposes to all involved parties or combatants, not favoring one side or the other. Rather, they are actively pursuing agendas that favor third parties or alternative solutions.
- Another possibility is that such organizations may make mistakes based upon inexperience. Combatant forces may then have to divert troops and resources from their assigned missions to conduct rescues or provide security, and may be forced to elevate the level of conflict.

CRIMINALS

7-10. Criminals (other than those in large-scale drug and criminal organizations described in Chapter 6) operate outside a formal organizational structure. Some criminals may form loose organizations—called gangs or rings—that normally have no true formal structure. Individual criminals or small gangs may be a nuisance to local law enforcement personnel, but generally they do not have the power to influence legitimate institutions. They are not capable of bribing on a grand scale like a large-scale criminal organization can. Nevertheless, even low-capability criminals sometimes can impact events through opportunistic actions.

7-11. Criminals, bandits, or thieves are opportunists who commit crimes. Those civilians, media, or humanitarian relief personnel who commit crimes are considered to be criminals.

TRANSNATIONAL CORPORATIONS

7-12. Transnational corporations may enter into partnerships with transition states that are trying to increase their world economic position. Emerging states may invite such corporations to establish research and manufacturing facilities in their countries as a means of building infrastructure. The presence of these corporations can also enhance a country's security. However, their motivations are not always charitable; they may try to influence regional affairs or assist their host country in actions that promote their own economic gain.

7-13. When external forces become involved in a particular country or region, they must take into account transnational corporations conducting business there. The presence of these outside business interests can put additional pressure on the intervening extraregional forces to avoid collateral damage to civilian life and property. Some transnational corporations also have their own armed security forces to protect their own interests or perhaps also those of their host country.

7-14. With globalization of economies, the host country must also take into account transnational corporations conducting business within its borders or in its region. If the country's actions adversely affect these foreign enterprises, it could invite outside intervention.

PRIVATE SECURITY ORGANIZATIONS

7-15. Private security organizations (PSOs) are business enterprises or local ad hoc groups that provide security and/or intelligence services, on a contractual or self-interest basis, to protect and preserve a person, facility, or operation. A PSO sometimes acts as an adjunct to other security measures, and provides advisors, instruction, and personnel for host-nation military, paramilitary, and police forces, as well as for private individuals and businesses (including transnational corporations).

7-16. The PSOs themselves may be legitimate, well-respected transnational corporations providing contract advisors and employees as part of a military nation-building program funded by a foreign government. PSOs may also be domestic firms, which supply contract guard forces. In its simplest form, a

PSO might be a local citizen organization that performs these actions on a volunteer basis.

7-17. PSOs are employed to prevent, detect, and counter intrusions or theft; protect property and people; enforce rules and regulations; and conduct investigations. They may also be used to neutralize any real or perceived threat in their area of responsibility.

7-18. The capabilities of PSO employees vary from highly trained former military members to uneducated, poorly trained recruits. The level of sophistication and competence of a PSO is often directly related to a client's ability to fund the contract. A PSO may provide services on a contract basis outside its country of origin. The allegiance of PSOs also varies from fanatical devotion to obligation for purely financial reasons. A PSO with wavering or conflicting loyalties is subject to corruption.

7-19. PSOs are most diverse in regard to organizational structure and level of capability. These, too, are often directly related to the client's ability to pay. For example, a transnational corporation or a large-scale drug or criminal organization can afford to pay more than many small countries. Figure 7-2 depicts a typical PSO. This example shows a fairly small force, but the same basic elements would be present in a larger force.

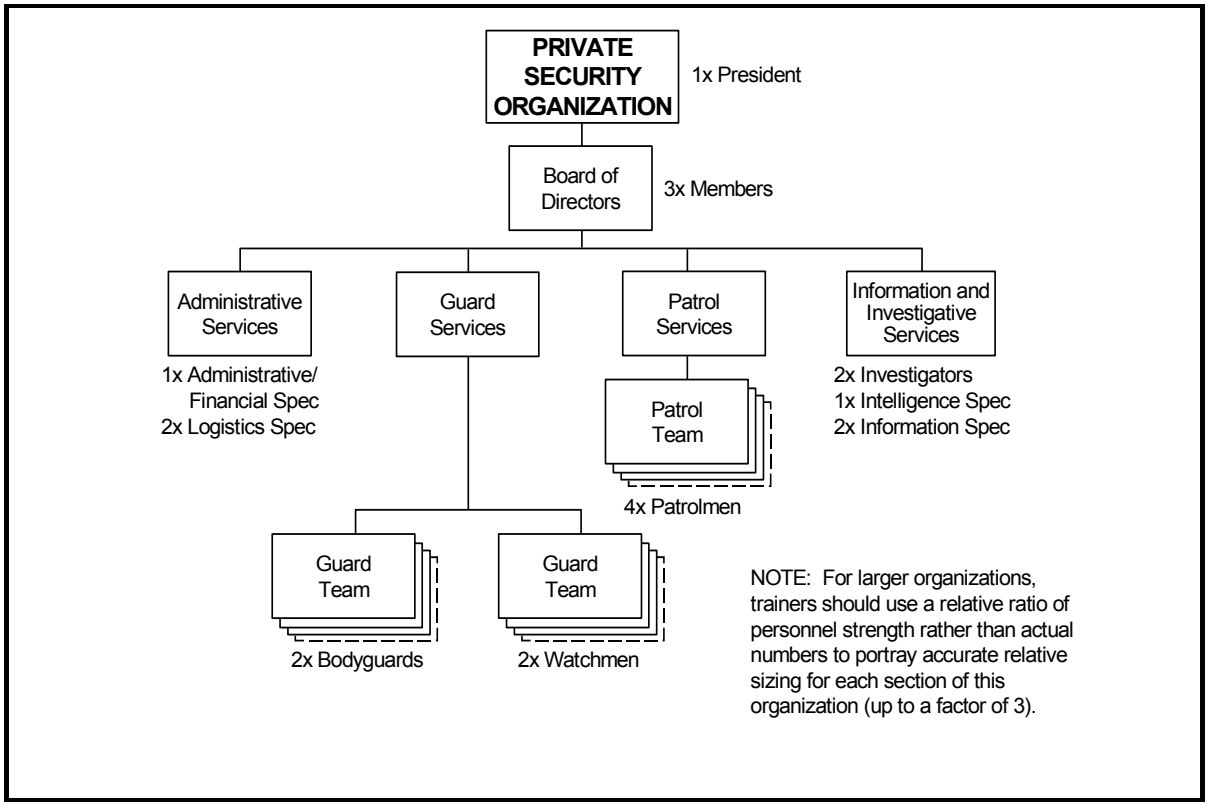

Figure 7-2. Private Security Organization (Example)

7-20. The board of directors acts much like a headquarters staff of a military organization. Administrative services provide all administrative, financial, and logistics support. Guard services provide bodyguards and perform surveillance. Patrol services conduct patrols and tactical actions, such as an ambush. Guard and patrol service members receive weapons training. Information and investigative services collect, analyze, and disseminate all types of information and intelligence, including economic intelligence. They also perform personnel security investigations and counterintelligence functions.

7-21. Each organization is tailored to serve its customer's needs. For example, the leader of an insurgent or criminal organization may employ a PSO to provide bodyguards or conduct surveillance or a search prior to his arrival. Another group, such as a drug organization, may contract a PSO to guard its facilities. The PSO may erect a fence or employ roving, armed guards to protect the facilities. Private security organizations use both active and passive measures that may be either rudimentary or employ advanced technology, such as surveillance, identification devices, and alarms. (Figure 7-3 shows possible equipment that may be present in a PSO.) During the conduct of their duties, members of a PSO may take offensive actions. A patrol, for example, may conduct a small-scale ambush to counter an intrusion.

Principal Items of Equipment: Private Security Organization	**Administrative Services**	**Bodyguard Team**	**Stationary Guard Team**	**Patrol Team**	**Info. and Invest. Services**
WEAPONS					
Handgun	X	X	X	X	X
Submachine gun		X	X	X	
Sniper rifle				X	
Special weapons sight			X	X	
COMMUNICATIONS					
Radio	X	X	X	X	X
Cellular telephone	X	X			X
Facsimile	X				
Computer	X				
Encryption capability		X			X
Concealed capability		X			X
VEHICLES					
Patrol car				X	
All-terrain vehicle	X	X	X	X	X
Armored vehicle				X	
Motorcycle				X	
Helicopter				X	
SURVEILLANCE EQUIPMENT					
Camera			X	X	X
Binocular		X	X	X	X
Scope			X	X	X
Night-vision device			X	X	X
Listening device			X		X
Monitoring equipment					X

Figure 7-3. Example Private Security Organization Equipment List

OTHER CIVILIANS

7-22. Other civilians on the battlefield (COBs) can include government officials, businesspeople, the local population, transients, internally displaced civilians, or refugees. Government officials, such as police (see Chapter 5), mayors, town council members, and emergency service personnel, may be elected, appointed, or hired to perform duties. These officials are generally associated with a defined geographical area. Some officials, such as emergency service personnel, have specialized equipment and standard uniforms while other officials, such as mayors and town council members, wear clothing appropriate to the locale and do not require specialized equipment to perform their duties. Although a part of the civilian population, these groups and individuals are to varying degrees connected to the state and its governmental infrastructure. On the other hand, business people, farmers, lawyers, doctors, the clergy, tradesmen, and shopkeepers provide a wide range of services and conduct their daily routine without direct connection to the government. All these types of COBs have varied concerns and their own agendas.

7-23. During peace and war, a tension exists between various interests as they compete to gain the support of the population to achieve their objectives. Support from the civilian population is a key doctrinal tenant common to all insurgent movements. It is from the population that an insurgent organization recruits its manpower, gains intelligence, and receives safe haven and materiel support. No true insurgency can exist for an extended period without significant support from the civilian population. It is also from this population that terrorist groups are spawned and grow. Although the requirement for popular and material support is not as great as that for insurgents, some element of support is required to operate successfully. On the other side of the spectrum are the government and its concomitant military and internal security forces that seek support in order to maintain legitimacy.

INFORMATION WARFARE

7-24. Perception management and manipulation of information are important tools for gaining and maintaining support. Not just military and paramilitary organizations, but also the various types of noncombatants can employ these tools. Everyone wants their own organization or group portrayed in a favorable light and the opposition or its actions in an unfavorable light.

7-25. The media are in the business of providing information, but this is subject to manipulation. Elements of the media may be controlled by the local government or come under the influence of a nongovernment or antigovernment organization. Humanitarian relief organizations typically have an information branch. In transnational corporations, this may be called public relations. PSOs have information services. During war, it is virtually certain that information warriors representing various interests will use civilian suffering and casualties to shape local, national, and international perception and opinion.

EXPLOITING NONCOMBATANTS

7-26. A local government, insurgent, terrorist, drug, or criminal organization may exploit various noncombatant elements for its own purposes. For example, it might persuade an international humanitarian relief organization to provide assistance to only a certain group of people. In order to adequately exploit such elements, an organization must know—

- How they are organized.
- What motivates them.
- What activities they conduct or what services they provide.
- Any constraints that may limit their actions or services.

MOTIVATION

7-27. Motivation is the need or desire that causes these noncombatant elements to take action. Like a paramilitary force, these elements have a specific motivation, which may include altruism (unselfish, humanitarian), personal dissatisfaction, job satisfaction, or greed. For example, dislocated civilians who complain about living conditions may be dissatisfied with their present standard of living, whereas a humanitarian relief organization devotes its resources to helping those in need. An individual's actions often indicate his motivation. For example, a government official or member of the media may just be interested in doing his job well. A criminal who conducts black marketing is motivated by greed. An organization's motivation is often implied or stated in published documents under mission statements, mandates, or objectives. However, some organizations or individual members may have motivations that differ from their public statements.

ACTIONS AND SERVICES

7-28. Noncombatants can conduct activities, take action, or provide services described below. The following list is illustrative, not exhaustive.

- Civil disturbances: crowds, riots, strikes, marches, protests, and demonstrations.
- Media interviews.
- Humanitarian assistance: disaster relief, refugee protection, development and education, negotiation support, and logistics support, such as medical, materiel, or food support.
- Requests for support: food, supplies, medical attention, protection, or religious services.
- File complaints or grievances.
- Interfere with activities or operations, which may include civil disturbances and requests for support.
- Insurgent or terror-type tactics: extortion, harassment, information gathering and dissemination, hijacking, or bombing.
- Criminal acts: theft and black marketing.
- Sources of information and intelligence for various military or paramilitary forces.

Figure 7-4 depicts activities conducted, actions taken, or services provided by the various types of noncombatants.

Noncombatant Actions and Services	**Media**	**Humanitarian Relief Org**	**Criminals**	**Multinational Corporations**	**Private Security Org**	**Other Civilians**	Government Officials	Businesspeople	Local Population	Transients	Dislocated Civilians
Civil disturbances											
Crowds									X	X	X
Riots									X	X	X
Strikes	X						X	X	X		
Marches									X	X	X
Protests								X	X	X	X
Demonstrations								X	X	X	X
Interviews	X										
Humanitarian assistance											
Disaster relief		X									
Dislocated civilian protection		X									
Development & education		X		X							
Negotiation support		X					X	X			
Logistics support		X		X							
Request for support	X			X	X		X	X	X	X	X
Filing complaints or grievances	X	X	X	X	X		X	X	X	X	X
Interfering with operations	X	X	X	X	X		X	X	X	X	X
Insurgent- or terror-type tactics			X		X		X	X	X	X	X
Criminal acts			X								
Sources of info and intel	X	X	X	X	X		X	X	X	X	X

Figure 7-4. Noncombatant Actions and Services (Examples)

LIMITATIONS

7-29. Local and international laws and customs, armed conflict, an organization's mandate or mission, effects of weather and terrain, and lack of resources all may constrain a noncombatant element's activities. A humanitarian relief organization may not be able to move food because of armed conflict or very restrictive terrain. Similarly, local populations may not be able to conduct a demonstration because local law prohibits it.

EXAMPLES OF EXPLOITATION

7-30. In time of war, combatants may use civilian infrastructure and population density as a means to protect military assets from enemy attack. One side might create refugee situations, riots, or demonstrations that can impede the progress of its enemy. Military and paramilitary organizations can use civilian populations as shields, obstacles, or sanctuary. They can use the

presence of noncombatants to shape the battlefield and lure enemy units into kill zones or ambushes. Refugees and displaced persons can create a heavy demand on a military unit's supply and medical system. Frequently, bands of refugees serve as cover for intelligence or direct action elements. Often, a member of a paramilitary organization can approach and/or infiltrate his target by acting as an innocent noncombatant.

7-31. A military or paramilitary force can manipulate individuals or groups of noncombatants to its advantage by exploiting their weaknesses or by supplying their needs. For example, a military or paramilitary group may provide information to a reporter. In doing so, however, it may seek to highlight information favorable to its cause or "spin" information to the detriment of others.

7-32. A paramilitary organization may orchestrate a civil disturbance by encouraging civilians to meet at a public area at a certain time. Members of the paramilitary group then infiltrate the crowd and incite it to riot or protest. Sometimes, they may pay civilians to conduct a demonstration or march. Members provide placards, banners, and bullhorns with instructions on what to say if questioned by the media or authorities. Those in the crowd do not necessarily believe what they are saying; they are being paid for a service.

7-33. A terrorist, drug, or criminal organization may coerce a businessperson into running a front company on its behalf. It may also use bribery or extortion to induce civilians to act as couriers or otherwise support its activities. An insurgent organization could likewise coerce a noncombatant to supply it with goods and services.

Bibliography

The bibliography lists field manuals by new number followed by old number.

DOCUMENTS NEEDED

These documents must be available to the intended users of this publication.

JP 1-02. *Department of Defense Dictionary of Military and Associated Terms*. Available online: http://www.dtic.mil/doctrine/jel/doddict/

FM 1-02 (101-5-1). *Operational Terms and Graphics.* 30 September 1997.

READINGS RECOMMENDED

These sources contain relevant supplemental information.

ARMY PUBLICATIONS

Most Army doctrinal publications are available online: http://www.adtdl.army.mil

FM 7-100. *Opposing Force Doctrinal Framework and Strategy*. 1 May 2003.

FM 7-100.1. *Opposing Force Operations*. TBP.

FM 7-100.2. *Opposing Force Tactics*. TBP.

FM 7-100.4 *Opposing Force Organization Guide*. TBP.

FM 7-100.5. *Opposing Force: Worldwide Equipment Guide*. TBP.