ST 7-100
Version 1.0

OPFOR Battle Book for the Operational Environment

June 2013

U.S. Army TRADOC G-2
TRADOC-Intelligence Support Activity (TRISA) – Threats
Complex Operational Environment and Threat Integration Directorate (CTID)
Fort Leavenworth, Kansas

INTRODUCTION

OPERATIONAL ENVIRONMENT (OE)

Opposing Force (OPFOR) doctrine is the fighting method used by the Combat Training Centers (CTC) and other training OPFORs. It is to be a composite model of the strategic environment based on existing and projected threats (named "hybrid threat"), artificial training, and notional training. This doctrine provides for OPFOR organizations and fighting methods across the spectrum of potential training scenarios, objectives and BLUE force mixes. Doctrinal tenets of the OE focus on the reasoning behind the use of particular tactics, techniques and procedures (TTP) and do not prescribe specific battlefield geometries, formations or time schedules. The doctrine is a composite of real world models, taking its basis in reality, but keying on the focus to challenge task execution. Old Soviet doctrine concepts were removed. However, if a concept remained sound and is in use by potential adversaries of the U.S., it will appear in the doctrine under another name. Army Regulation (AR) 350-2, *Opposing Force (OPFOR) Program*, dated 09 April 2004 specifically prohibits the use of real-world countries in an unclassified training environment.

Joint Publication 3-0 defines *operational environment* as "a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of commanders." This environment includes land, maritime, space and associated threats presence, as well as friendly and neutral systems. The Decisive Action Training Environment (DATE) document was developed to provide the U.S. Army training community with a detailed description of the conditions of five OEs in the Caucasus region; specifically the countries of Ariana, Atropia, Gorgas, Minaria, and Donovia. It presents trainers with a tool to assist in the construction of scenarios for specific training events but does not provide a complete scenario. The DATE offers discussions of OE conditions through the Political, Military, Economic, Social, Information, Infrastructure, Physical Environment, and Time (PMESII-PT) variables.

COMPLEX OPFOR / HYBRID THREAT

In training for the realities of the OE, the Army needs a different type of OPFOR than that of the 1970s, 80s, and 90s which incorporates the hard lessons learned in Afghanistan, Iraq, and the Philippines. The Training Circular (TC) TC 7-100 series defines this complex 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." In the training environment, the OPFOR is a training tool that represents the nature and capabilities of various kinds of forces the U.S. Army might face in the OE.

This Student Text is not comprehensive concerning the OE or the OPFOR. You can download complete information in the following regulations, manuals, circulars, and documents the Army Training Network (ATN) at https://atn.army.mil/dsp_template.aspx?dpID=311.

OPFOR RESOURCES
(Current and future)

AR 350-2, *OPFOR Program*, 09 APR 2004

TC 7-100, *Hybrid Threats*, November 2010

FM 7-100.1, *Opposing Forces Operations*, 27 Dec 2004 (to be re-written as a TC)

TC 7-100.2, *Opposing Forces Tactics* (Approved final draft, August 2011)

TC 7-100.3, *Irregular Opposing Forces* (to be published)

FM 7-100.4, *Opposing Forces Organization Guide*, 03 May 2007(to be re-written as a TC)

TC 7-101, *Exercise Design*, November 2010

TC 7-102, *Operational Considerations for Training and Education Development*, Approved Final Draft June 2013

Worldwide Equipment Guide (WEG), September 2012

Decisive Action Training Environment (DATE) version 2, December 2011

PREFACE

ST 7-100 OPFOR Battle Book for the Operational Environment is a reference guide prepared under the direction of the U.S. Army Training and Doctrine Command, Intelligence Support Activity (TRISA) - Complex OE & Threat Integration Directorate (CTID). This student text, using the PMESII-PT variables of the OE, outlines a methodology for integrating the OPFOR into training exercises. This student text replaces ST 7-100 dated June 2005.

Purpose. To provide an overview of the OE Estimate, the eight OE variables, Hybrid threats, Decisive Action Training Environment (DATE), OE assessments, the OPFOR organization guide, tactical level OPFOR tactics, and the Worldwide Equipment Guide (WEG). It supports operational missions, institutional training, and professional military education for U.S. military forces. This student text is a supplement to the 7-100 series of OPFOR documents and is not a replacement document.

Intended Audience. This student text exists primarily for U.S. military students. Compiled from open source material, this student text promotes an OPFOR perspective in a composite-model training environment and is not a replacement document.

Using ST 7-100. Study and integration of the OPFOR in the OE improves the readiness of U.S. military forces. As a living document, TRISA updates this student text as necessary to ensure it remains a current and relevant resource. Each of the student text chapters contains specific information designed to assist the student in developing a realistic and challenging OPFOR. Links within the student text provide expanded information and ease of use. Unless stated otherwise, masculine nouns and pronouns do not refer exclusively to the male gender.

Proponent Statement. Headquarters, U.S. Army Training and Doctrine Command (TRADOC) is the proponent for this publication. Periodic updates will accommodate emergent user requirements. Send comments and recommendations on DA Form 2028 directly to TRADOC TRISA-Threats at the following address: TRADOC TRISA-Threats, ATTN: ATIN-T, 803 Harrison, Drive, Bldg 467, Fort Leavenworth, Kansas 66027-1323.

TABLE OF CONTENTS:

Chapter 1

The OE Estimate

The OEs we will encounter in the future will not be like the OEs of Iraq and Afghanistan. Although there may be similarities, each conflict is inherently unique in situations, circumstances, and events from the collision of differing interests and desires. We must be wary of believing that history does anything more than provide a general azimuth toward likely futures. Three assumptions drive this:

- First, U.S. military dominance will shape how potential adversaries perceive us and plan to mitigate existential risks as they pursue their objectives.
- Second, the U.S. Army is one of the elements of national power and must be prepared to answer the call of the nation's leaders no matter what the task. There is no acceptable excuse for not being trained and ready when called.
- Third, our adversaries will likely embrace an ideology that blinds them to what we might consider irrational decisions based on a clear understanding of outcomes. This may put the U.S. Army at a disadvantage, even when present in overwhelming strength. Adversaries will seek to deny the U.S. the advantages of our preferred way of war, by denying the advantage of our standoff precision strike and finely honed Intelligence, Surveillance and Reconnaissance (ISR) capabilities. Opportunistic enemies will use the sheer complexity of all the elements interacting in an OE to frustrate commanders (CDR) and confound senior policy makers.

The OE is the combination of eight variables (political, military, economic, social, information, infrastructure, physical environment, and time, or PMESII-PT), not just military and threat dimensions. Actors within the OE create the conditions, circumstances, and influences that can affect military operations. This environment exists today and for the clearly near future.

In August 2012, TRISA-Threats published "Operational Environments to 2028: The Strategic Environment for Unified Land Operations". In this publication, TRADOC G-2 identified potentially contentious OEs and missions our Army could face, including the OEs of Iran, China, Yemen, North Korea, Pakistan, and Nigeria as *possible* environments. This publication went on to elaborate on the conditions of the strategic environment and its military implications. Annexes included specificity concerning each of the combatant commands areas of responsibility.

In training environments, the OE provides the framework to create conditions to replicate the complexity of the real world and thus provide realistic and relevant training. It provides a non-specific capabilities-based approach. If training consists of task, condition, and standard, then the OE is the condition(s), in which the Army can train mission essential tasks to the desired standard. If the training event is a mission rehearsal exercise (MRX) or a regionally aligned force (RAF), then the trainers will apply the OE of a specific theater resulting in an operational environment assessment (OEA) of that selected environment.

Chapter 2

Political, Military, Economic, Social, Information, Infrastructure, Physical Environment, and Time (PMESII-PT) Variables

Composite-model training developers define the OE in terms of PMESII-PT variables. The linkage among variables is critical to successful analysis – it is the links that set or create the conditions of each environment. Trainers and scenario writers must understand this synergy and be able to adapt actions based upon the dynamic nature of this relationship.

The variables represent a "system of systems" meaning that all of the variables are multi-faceted, complex and inter-relational in nature. Study of the variables helps to achieve and maintain an understanding of the context of the environment.

The start point for understanding the OE must be those critical factors that reside in all OEs, and have the greatest impact on the military, PMESII-PT. The conceptual template for any future military operation must incorporate the expected characteristics of these variables.

While these variables can be useful in describing the overall (strategic) environment, they are also useful in defining the nature of a specific OE. Each of these conditions will vary according to a specific situation. 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 critical variables are different.

Political Variable

The political variable focuses on political power within a given OE.

Understanding the political circumstances within an OE will help the CDR recognize key actors and visualize their explicit and implicit aims, their capabilities to achieve their goals, and their possible allegiances. These actors can mobilize group identity, ideas, beliefs, action and violence to enhance their power and control over society, people, territory and resources; the sources of political mobilization may lie in the political leadership; religious, ethnic or economic communities; or in the indigenous security institutions such as the military or police.

Nation-state and non-state actors often enter into relationships (formal and informal) with other actors or organizations. Understanding the implications of these relationships requires analysis of all relevant political, economic, military, religious, or cultural mergers and/or partnerships of the key entities of a given OE. This analysis also captures the presence and significance of external organizations and other groups in an OE. Examples include groups united by a common cause, such as non-governmental organizations (NGO), private voluntary organizations, private security organizations, transnational corporations, and international organizations that conduct humanitarian assistance operations.

Finally, political analysis of an OE addresses the concept of 'will.' Will encompasses a unification of values, morals, agendas, effort, and the probability of acting on them. Through this unity, participants are willing to sacrifice individually for the achievement of the unified goal. Understanding the will of key groups (political, military, insurgent, and terrorist) in the OE will help further define various groups' goals and their willingness to support and achieve their ends.

Military Variable

Military capabilities may be the most critical and most complex variable that affects military operations. The Military variable explores the military capabilities of all relevant actors within a given OE. It includes equipment, military doctrine, manpower, training levels, resource constraints and leadership issues. Military leadership is especially important in gaining and understanding of the individual leaders and the human characteristics of their forces is vital to success. Analysis should focus on an actor's ability to field forces and leverage them for use domestically, regionally, or globally. Our enemies will be flexible, thinking, and adaptive.

The military variable does not exist in isolation from the other variables that help determine the overall OE. It interacts with the other variables: it affects them and is affected by them.

Nation-state or non-state actors measure military capabilities in relative terms in comparison to the capabilities of other actors against which they are applied. Most of the military forces in the world continue to operate in conventional ways, which remains sufficient against other local or regional actors. Once the United States becomes

involved, however, these same conventional forces may have to use adaptive and asymmetric approaches. When confronted with a stronger military power, weaker forces will employ irregular capabilities and methods, using indirect approaches to achieve their aims. As such, militaries and violence are instruments of their respective political systems.

Economic Variable

The economic variable encompasses individual behaviors and aggregate phenomena related to the production, distribution, and consumption of resources in an OE. Specific factors may include the influence of industrial organization, international trade, development (foreign aid), finance, institutional capabilities, geography and the rule of law. Though the world economy becomes more and more linked each year, nation-state economies differ in various ways. These differences significantly influence political choices.

Other factors include unofficial economies or black market/underground economies, which are alternative structures indicating weaknesses in the mainstream economy. These economies conduct legal and illegal activity within an economic environment. Their existence is based upon many factors which may include: high tax burdens, weak banking systems, business regulations and legislation, inefficiency of government institutions, and high unemployment rate.

Unofficial economies tend to develop more in transitioning countries due to the presence of more corruption and lower incomes. However, the desire to engage in an unofficial economy differs between emerging, affluent or rich economies. In affluent or rich economies the driving force to engage in an unofficial economy tends to be an effort to evade taxes. In emerging economies the desire to engage in an unofficial economy tends to be centered on an effort to evade the law.

Two examples of unofficial economic activities are: unrecorded legal income (such as cash paid for service) and cash received as a result of illicit activities such as drug dealing, money laundering, loan sharking and prostitution.

Economic deprivation is also a major cause of conflict. One actor may have economic superiority over another for many reasons, including access to natural resources or power. Military personnel operating in this complex environment may need to look beyond political rhetoric to discover a fundamental economic disparity among groups.

The economic variable establishes the boundaries between the "haves" and "have-nots." Economic superiority, rather than military superiority, may be the key to regional or global dominance.

Social Variable

The social variable describes the cultural, religious, and ethnic makeup within an OE. A social system consists of the people, groups, and institutions that exhibit shared identity, behaviors, values, and beliefs. Social groups consist of groups organized, integrated, and networked by relationships, interacting within their environment.

Social demographics refer to the trends and impact of human population, and its cultural, religious and ethnic make-up. Extreme devotion to a particular cause or significant hatred of a particular group provides the enemy with an unshakable will and a willingness to die for a cause.

Information Variable

We now live in an information-based society that uses computers and other information systems throughout the military and civilian sectors. This variable describes the nature, scope, characteristics, and effects of individuals, organizations, and systems that collect, process, disseminate, or act on information.

Information involves the access, use, manipulation, distribution, and reliance on data, media, and knowledge systems-civilian and military-by the global community.

CDRs must understand and engage the information environment to achieve their operational and strategic objectives. Understanding whatever communication infrastructure exists is important because it controls information flow and influences local, regional, national, and international audiences.

Our potential adversaries understand the value of information and information warfare (INFOWAR). Many of them see this as the most productive avenue to offset U.S. conventional capabilities. We can expect these adversaries to expand their efforts to attack our computer networks and other information systems and disrupt information flow. They will use psychological warfare and deception at every level.

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

In developing countries, information may flow by less sophisticated means- couriers, graffiti, rumors, cultural symbols, art, literature, radio, and local print media. Understanding whatever communication infrastructure exists is important because it controls information flow and influences local, regional, national, and international audiences.

Infrastructure Variable

Infrastructure is composed of the basic facilities, services, and installations needed for the functioning of a community or society. The degradation or destruction of infrastructure will affect the entire OE especially the political, military, economic, social, and information variables.

This variable also reflects the technological sophistication of all the actors mentioned. Technological capability encompasses an actor's ability to conduct research and development and then capitalize on the results for civil and military purposes. The infrastructure variable reflects the technological level of the OE in terms of sectors or technological success or advancement, scientific and research institution, technology acquisition policies, and the education and training facilities which support the acquisition of technology.

Physical Environment Variable

The physical environment defines the physical circumstances and conditions that influence the execution of operations throughout the domains of air, land, sea and space. The defining factors are urban settings (super-surface, surface, and subsurface features), other types of complex terrain, weather, topography, hydrology, and environmental conditions.

Potential enemies understand that less complex and open environments expose their military weaknesses. Operations in open environments favor a U.S. force with long-range, precision-guided weapons and sophisticated reconnaissance capability. Therefore, adversaries/OPFOR may choose to operate in urban environments or other complex terrain and during weather conditions that may adversely affect U.S. military operations and mitigate technological advantages. By 2030, current projections show 60% of all people (approximately 4.9B) will live in an urban area, mostly mega cities with populations of 10M or more.

Time Variable

Time is one of, if not the most significant, planning factors driving decision-cycles, operational tempo and planning horizons. Time may also influence endurance or protraction of military operations since popular support for extended operations may diminish over time.

Time is both an operational planning factor and a tool to manipulate tactical and strategic advantages. In most cases, potential adversaries of the United States view time as being to their advantage. For example, the time it takes to deploy U.S. forces into the region gives opponents an opportunity to find ways of adjusting the nature of the conflict into something for which U.S. forces are not prepared.

Adversaries will also seek to control the tempo of operations to influence early-entry operations or prolong operations with the desire to increase friendly casualties. CDRs and staffs must consider time as a threat course of action (COA) when developing friendly operations.

OEA

OE Assessment Methodology process provides a methodology for examining and understanding any potential OE. It is an analysis of the critical variables and their impacts on any possible combat operations. A four-step process using is recommended for developing this assessment prior to training. Once developed, the OE Assessment can be applied to the training scenario. Helpful and complete OE Assessments are available on the Army Training Network at https://atn.army.mil. Once you are on ATN click on Links Tab. Then scroll across to the Training Resources Tab and click. Then scroll down to the " TRADOC G2 Intelligence Support Activity (TRISA) - Threats" tab and click. You may be prompted to log into AKO via your CAC or AKO alias and password at this point.

Summary

For planners to be successful in composite model training or real world missions, they must correctly identify the PMESII-PT variables. The variables of the OE 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 encounter. In order to provide realistic training, trainers and scenario writers must attempt to simulate this synergistic effect to the maximum extent.

The OE variables and their interaction provide an environment and conditions for all training. The complexity of a specific OE in training can be adjusted to ensure training objectives are met through the utilization of the OE Assessment Methodology.

Chapter 3

Hybrid Threat

"A *hybrid threat* is the diverse and dynamic combination of regular forces, irregular forces, and/or criminal elements all unified to achieve mutually benefitting effects."

--TC 7-100, *Hybrid Threats*

The hybrid threat components include two or more of the following:

- Military forces
- Nation-state paramilitary forces (such as internal security forces, police, or border guards)
- Insurgent organizations (movements that primarily rely on subversion and violence to change the status quo)
- Guerrilla units (irregular indigenous forces operating in occupied territory)
- Criminal organizations (such as gangs, drug cartels, or hackers)

Hybrid threats will use a strategic capability that forces any intervening power to adjust operations (WMD, special-purpose forces [SPF], etc). This capability may not be fully developed or developed at all. This will not affect the transition between regular and irregular operations, and the threat of the capability still provides a tool for manipulating the intervening force (e.g. Iraq's WMD capability circa 2001).

Hybrid threats have the ability to combine and transition between regular, irregular, and criminal forces and operations and to conduct simultaneous combinations of various types of activities that will change and adapt over time. Such varied forces and capabilities enable hybrid threats to capitalize on perceived U.S. vulnerabilities. Perhaps even more confusing will be when those combinations of threats are uncoordinated and simply seek to maximize their own organizational goals rather than any overarching objective.

Combatant versus Non-Combatant

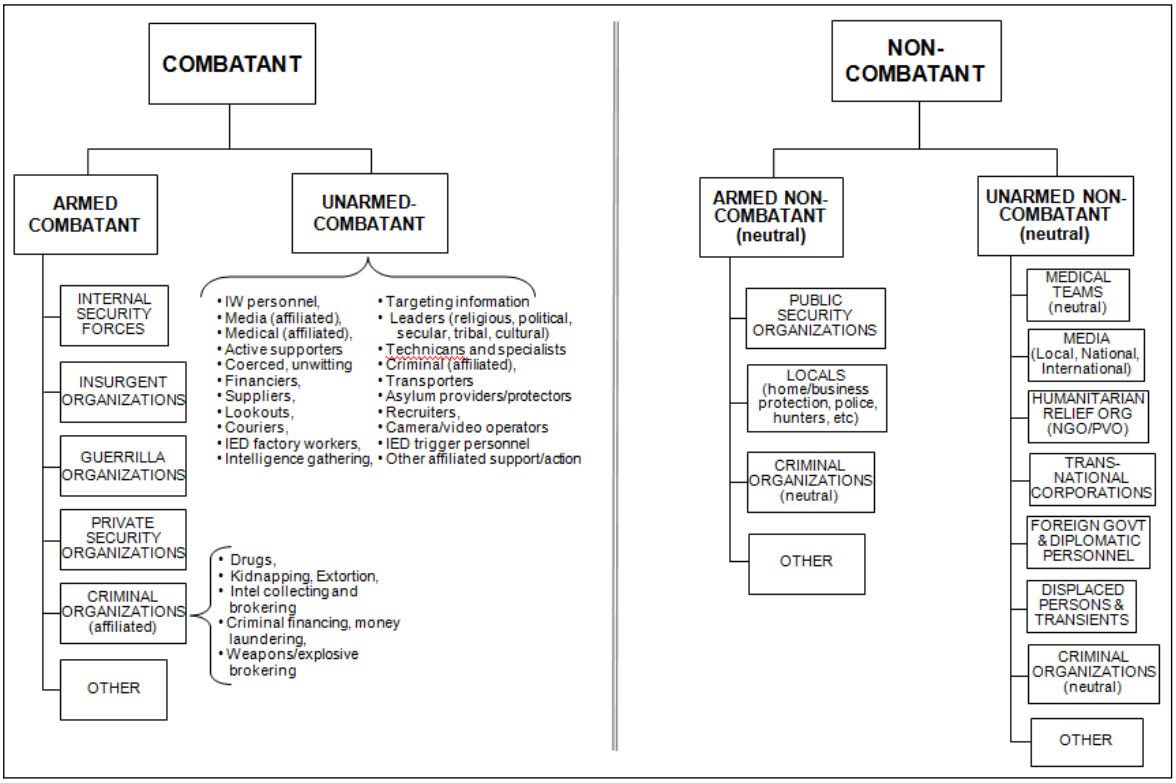


Figure 3-1. Combatant versus Noncombatant

In training environments such as CTCs, educational institutions within the military, and other agencies, role-players portray actors of the OE. In training exercises, role-players portray characters of an existing or fictitious country/region that constitutes the physical environment of the OE simulated for training purposes. In an MRX and RAF exercise, role-players depict characters in an actual country/region (specified real-world OE). Role-players will frequently portray non-state actors, either combatant or noncombatant. Figure 3-1 identifies the sub-elements within both combatants and noncombatants.

Combatants

Paramilitary Organizations. A variety of non-state paramilitary organizations/actors may be present in the OE. Non-state paramilitary organizations/actors distinguish themselves from regular armed forces of the State or any other country but resemble them in organizations, equipment, training, or mission. Basically, any organization that can accomplish its purpose, even partially, through the force of arms can be considered a paramilitary organization. The following are combatant paramilitary organizations.

Insurgent Organizations. This particular type of organization does not have a regular "fixed" organization or structure. Their mission and other variables of the OE determine their configuration and the composition of each subordinate cell. Their composition varies from organization to organization, mission to mission, OE to OE. (For more information on higher and local insurgent organizations, refer to Field Manual (FM) 7-100.4.

Insurgent organizations may have a relationship with guerrilla organizations, criminal organizations, or other OE actors based on similar or shared goals and/or interests.

Guerrilla Organizations. The structure of this organization depends on the critical variables (PMESII-PT) of the OE. Guerrilla organizations may be as large as a brigade (BDE) and small as a platoon and/or independent hunter/killer (H/K) teams. They resemble military structure with similar weapon types. They might be affiliated with forces from other countries or external organizations. Some may constitute a paramilitary arm of an insurgent movement, while others may pursue guerrilla warfare independently from or loosely affiliated with an insurgent organization. Fire and maneuver tactics along with terror tactics are typical. They are however, best suited for irregular warfare and/or unconventional tactics. For more information on guerrilla BDEs, battalions (BN) and companies, refer to FM 7-100.4 (see links above).

Private Security Organizations (PSO). 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. Teams of PSOs may consist of bodyguard teams, patrol teams, stationary guard teams, or information and investigation teams.

Criminal Organizations. Entities that usually operate independently of nation-state control. Their large-scale organizations often extend beyond national boundaries to operate regionally or worldwide. Small-scale criminal organizations do not have the capability to adversely affect legitimate political, military, and judicial organizations-but the large-scale organizations do. The weapons and equipment mix varies, based on type and scale of criminal activity. Criminal organizations at the higher end of the scale can take on characteristics of paramilitary organizations. Either by mutual agreement or coincidental interests, criminal organizations may become affiliated with other non-state paramilitary actors, such as insurgents, or guerrilla forces. They may exchange security for financial assistance or arms when operating in the same area.

Other Armed Combatants. Nonmilitary personnel who are armed but not part of an organized paramilitary or military structure. They may be disgruntled or hostile. Some of the nonaffiliated personnel may possess small arms legally to protect their families, homes, and/or businesses. Some might be opportunists looking to make a profit by attacking a convoy, vehicle or emplacing an IED. Some armed combatants are just angry at the United States. The reasons are immaterial-armed civilians are ubiquitous. This type of combatant may represent a large portion of the undecided in a population. They may not have determined which side they are on or if they will change sides in the future. They might change sides several times depending on the circumstances directly affecting their lives. Those who form a cohesive group, and then commit themselves to a particular COA can then be categorized according to the aims they pursue, as insurgents, guerrillas, PSO (perhaps of the informal "neighborhood watch" variety), or perhaps criminals.

Unarmed Combatants. Any unarmed person who engages in hostilities or who purposely and materially supports hostilities against the United States or its co-belligerents. This includes support that takes place off the battlefield. For example, technicians and workers who arm IEDs may not be armed.

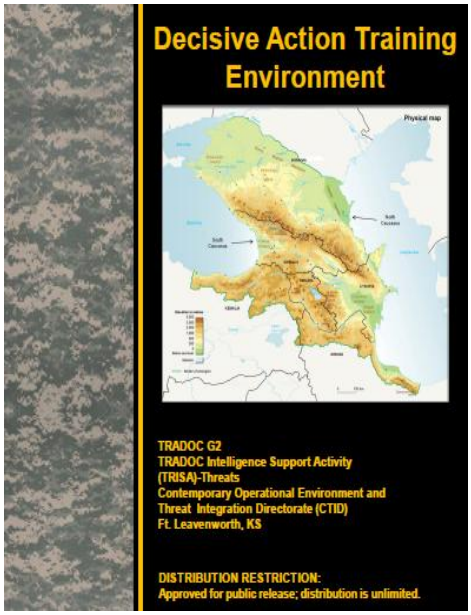
Noncombatants.

A variety of nonmilitary actors not part of the OPFOR might present in an OE. They are either friendly or neutral. They can be either armed or unarmed, and have the potential to become combatants in certain conditions. They might provide support to combatants–either willingly or unwillingly.

Armed Noncombatants. Persons with no affiliation with any military or paramilitary organization. They may be completely neutral or may lean towards support of one side or several sides. For example, some may use weapons as part of their occupation (hunters, security guards, or local police). Or they may be minor criminals who use their weapons for activities such as extortion and theft. Given the fact that these individuals are already armed, it would be easy for them to move from noncombatant status to combatant, if their situation changes.

Unarmed Noncombatants. Neutral or potential side-changers, depending on their perception of the United States actions. Changes in their situation may cause some previously unarmed noncombatants to become combatants and perhaps take up arms. Medical teams, media, humanitarian relief organizations, transnational corporations, internally displaced persons (IDP), transients, foreign government and diplomatic personnel, and local populace are a few examples of unarmed non-combatants.

The media include local, national, and international journalists, reporters, and associated support personnel. Their primary job is to report newsworthy events. Although most media personnel may try to remain objective and report accurately, there are those who have positive or negative biases which affect their reporting of events. Opposing sides in a conflict will seek to control and exploit the media in order to enhance their own positions. With or without manipulation by other parties, the media can have a great effect on public opinion and national will of the opposing sides.



Decisive Action Training Environment (DATE)

The purpose of the DATE document is to provide the U.S. Army training community with a detailed description of the conditions of five OEs in the Caucasus region; specifically the countries of **Ariana**, **Atropia**, **Gorgas**, **Minaria**, and **Donovia**. It presents trainers with a tool to assist in the construction of scenarios for specific training events but does not provide a complete scenario. The DATE offers discussions of OE conditions through the PMESII-PT variables. The DATE applies to all U.S. Army units (Active Army, Army National Guard, and Army Reserve) that participate in an Army or joint training exercise.

The DATE is a composite model that sets the conditions for a wide range of training events, to include decisive operations. Section 2: Variables of the OE and Orders of Battle (OBs) provides the bulk of these details. The variable discussion explores the complex and ever-changing combination of conditions, circumstances, and influences that could affect military operations within a given OE. The PMESII-PT variables offer insight into each country's independent, dynamic, and multi-dimensional environment. By defining these variables' makeup and interoperability as they relate to a specific country, a picture emerges of the environment's nature and characteristics.

Figure 3-2. DATE Countries (Caucasus Region outlined in Blue)

How to use the DATE

The DATE is a tool for the training community to use across training events ranging from rotations at the CTCs to individual home station training (HST) events. It is the baseline document for all the conditions and characteristics of the five OEs in the region. Exercise planners should use this document for all exercise and scenario design requirements.

The DATE was developed and designed to allow for flexibility and creativity in its application. Not all conditions in the document need to be represented during each training event. Specific training requirements should drive the scenario development and conditions replicated. If additional description or detail is need for a given condition, each exercise planner can add that narrative to the condition. The goal is to keep the baseline conditions stable, while allowing for any additional narrative to be added as required by the training tasks.

DATE Sections

The DATE contains four sections.

• Section 1: Strategic Setting describes the strategic situation of each actor across the Caucasus region and provides an overview of some key strategic issues. This section sets the stage for the document and presents a starting point for discussing the strategic environment and developing a specific scenario. A particular exercise or training event may need to add more discussion or specific strategic issues to this discussion to support the training requirements necessary for scenario construction and exercise execution.

• Section 2: Variables of the OE and Orders of Battle provides a comprehensive and complementary look at the PMESII-PT variables as they apply to the region, specifically **Ariana**, **Atropia**, **Gorgas**, **Minaria**, and **Donovia**. This section enables the scenario writers and exercise designers to better understand the regional conditions. Detailed OBs, derived from the TC 7-100 series, are provided to adequately stress U.S. Army units across the spectrum of operations.

• Section 3: Events provides a list of non-country specific events that can be used to test the mission essential task list (METL) of various friendly elements.

• Section 4: Orders of Battle Appendices is comprised of three parts. Organizational equipment tables of selected units are in an online version of Appendix A at https://www.us.army.mil/suite/files/26501220 . Appendix B provides instructions on how to task organize OPFOR units for combat. Appendix C consists of the OPFOR equipment tier tables from the WEG.

Chapter 4

OPFOR Organization Guide

FM 7-100.4 states "the administrative force structure to be used as the basis for OPFOR organization in all Army training, except real-world-oriented MRXs. This includes the forces of nation-state actors as well as key non-state actors. In most cases, the organizations found in the AFS will require task-organizing (see chapter 3) in order to construct an OPFOR order of battle (OB) appropriate for a training event." The following explanations and illustrations are administrative force structures as a start-point for trainers to task organize/tailor an effective sparring partner for training units.

Administrative Force Structure (AFS)

The State's Armed Forces have an AFS that manages military forces in peacetime. This AFS is the aggregate of various military headquarters (HQ), organizations, facilities, and installations designed to man, train, and equip the forces. Within the AFS, tactical-level commands have standard organizational structures (as depicted in the organizational directories). However, these AFS organizations normally differ from the OPFOR's wartime fighting force structures that are the result of task organizing for a mission.

The AFS includes all components of the Armed Forces not only regular, standing forces (active component), but also reserve and militia forces (reserve component). For administrative purposes, both regular and reserve forces come under the HQ of their respective service component. There are six components: Army, Navy, Air Force (which includes the national-level Air Defense Forces), Strategic Forces (with long-range rockets and missiles), Special-Purpose Forces (SPF) Command, and Internal Security Forces (ISF). Each of the six service components is responsible for manning, equipping, and training of its forces and for organizing them within the AFS.

The Strategic and Operational levels are discussed in detail in the 7-100 series of TCs. The focus of this student text will be the tactical level.

Tactical Level

In the OPFOR's AFS, the largest *tactical-level* organizations are divisions (DIV) and BDEs. In peacetime, they are often subordinate to a larger, operational-level administrative command. However, a service of the Armed Forces might also maintain some separate single-service tactical-level commands (DIVs, BDEs, or BNs) directly under the control of their service HQ. For example, major tactical-level commands of the Air Force, Navy, Strategic Forces, and the SPF Command often remain under the direct control of their respective service component HQ. The Army component HQ may retain centralized control of certain elite elements of the ground forces, including airborne units and Army SPF. This permits flexibility in the employment of these relatively scarce assets in response to national-level requirements.

For these tactical-level organizations (DIV and below), the AFS organizational directories contain standard table of organization and equipment (TOE) structures. However, these administrative groupings normally differ from the OPFOR's go-to-war (fighting) force structure.

Divisions (DIV)

In the OPFOR's AFS, the largest tactical formation is the DIV. DIVs are designed to be able to serve as the basis for forming a division tactical group (DTG), if necessary. However, a DIV, with or without becoming a DTG, could fight as part of an operational-strategic command (OSC) or an organization in the AFS (such as army or military region) or as a separate unit in a field group (FG).

Maneuver BDEs

The OPFOR's basic combined arms unit is the maneuver BDE. In the AFS, some maneuver BDEs are constituent to DIVs, in which case the OPFOR refers to them as ***divisional BDEs***. However, some are organized as ***separate BDEs***, designed to have greater ability to accomplish independent missions without further allocation of forces from a higher tactical-level HQ. Separate BDEs have some subordinate units that are the same as in a divisional BDE of the same type (for example, the HQ), some that are especially tailored to the needs of a separate BDE [marked "(Sep") in the organizational directories], and some that are the same as units of this type found at DIV level [marked "(Div)"].

Maneuver BDEs are designed to be able to serve as the basis for forming a BDE tactical group (BTG), if necessary. However, a BDE, with or without becoming a BTG, can fight as part of a division or DTG, or as a separate unit in an OSC, an organization of the AFS (such as army, corps, or military district), or an FG.

Battalions
In the OPFOR's force structure, the basic unit of action is the battalion. Battalions are designed to be able to execute basic combat missions as part of a larger tactical force. A battalion most frequently would fight as part of a BDE, brigade tactical group (BTG), or DTG. A battalion can also serve as the basis for forming a battalion detachment (BDET), if necessary.

Companies
OPFOR companies most frequently fight as part of a BN or BTG. However, companies are designed to be able to serve as the basis for forming a company-size detachment (CDET), if necessary.

Platoons
In the OPFOR's force structure, the smallest unit typically expected to conduct independent fire and maneuver tactical tasks is the platoon. Platoons are designed to be able to serve as the basis for forming a reconnaissance or fighting patrol. A platoon typically fights as part of a company (CO), BN, or detachment.

Aviation Units
The OPFOR has a variety of attack, transport, multipurpose and special-purpose helicopters that belong to the ground forces (Army) rather than the Air Force. Hence the term *army aviation*. Army aviation units are organized into BDEs, BNs, and COs.

Air Force organizations are grouped on a functional, mission-related basis into DIVs, regiments, squadrons, and flights. For example, a bomber DIV is composed primarily of bomber regiments, and a fighter regiment is composed mainly of fighter squadrons. The Air Force also has some mixed aviation units with a combination of fixed- and rotary-wing assets; these follow the normal Air Force organizational pattern, with mixed aviation regiments and squadrons. However, rotary-wing subordinates of these mixed aviation units would be BNs and companies (rather than squadrons and flights), following the pattern of similar units in army aviation. Various fixed- and/or rotary-wing Air Force assets may be task-organized as part of a joint, operational-level command in wartime.

Nondivisional Units
Units listed as "*nondivisional*" [marked "(Nondiv")] in the AFS organizational directories might be found in any of the operational-level commands discussed above, or in a theater command, or directly subordinate to the appropriate service HQ. The OPFOR force structure contains BDE- and BN-size units of single arms such as SAMS, artillery, surface-to-surface missiles (SSM), antitank (AT), combat helicopter, signal, and EW. In wartime, these nondivisional units can become part of a task-organized operational- or tactical-level command. These units almost always operate in support of a larger formation and only rarely as tactical groups or detachments, or on independent missions.

Non-State Actors

Aside from the military and/or paramilitary forces of a nation-state, the OPFOR might consist of or include the forces of non-state paramilitary actors. The OE also includes various types of nonmilitary actors, although they are not part of the OPFOR.

Paramilitary Organizations
Non-state paramilitary organizations are distinct from the regular armed forces of the State or any other country, but resemble them in organization, equipment, training, or mission. Therefore, the AFS organizational directories include baseline organizations for insurgent and guerrilla forces.

Insurgent Organizations
Insurgent organizations have no regular, fixed "table of organization and equipment" structure. The mission, environment, geographic factors, and many other variables determine the configuration and composition of each insurgent organization and its subordinate cells. Their composition varies from organization to organization, mission to mission, environment to environment. The structure, personnel, equipment, and weapons mix all depend on specific mission requirements. So do the size, specialty, number, and type of subordinates.

There are several factors that differentiate the structure and capability of an insurgent organization (direct action cells) from the structure and capability of a guerrilla organization. Since the insurgent organization is primarily a

covert organization, it typically has a cellular structure to prevent compromise of the overall organization. By comparison, the guerrillas' organization reflects their kinship to a more formal military structure (BN, CO, platoon, squad, and fire team or task-organized H/K BN, H/K CO, H/K group, H/K section, and H/K team).

Insurgent organizations generally do not have much of the heavier and more sophisticated equipment that guerrilla organizations can possess. The weapons of the insurgents are generally limited to small arms, antitank grenade launchers (ATGL), and improvised explosive devices (IEDs) with very few crew-served weapons. In the event the insurgents require heavier weapons or capabilities they might obtain them from guerrillas, or the guerrilla organization might provide its services depending on the relationship between the two organizations at the time.

Higher Insurgent Organizations
The term *higher insurgent organization* includes any insurgent organization at regional, provincial, district, or national level, or at the transnational level. Cities, towns, or villages with a large population or covering a large geographic area are considered regions and may therefore control several local insurgent and/or guerrilla organizations. Higher insurgent organizations usually contain a mix of local insurgent and guerrilla organizations. Each of these organizations provides differing capabilities.

Local Insurgent Organizations
Local insurgent organizations are typically composed of from three to over 30 cells. All of the direct action cells could be multifunction (or multipurpose), or some may have a more specialized focus. The single focus may be a multifunction direct action mission, assassination, sniper, ambush, kidnapping, extortion, hijacking and hostage taking, or mortar and rocket attacks. Each of these may be the focus of one or more cells. More often, the direct action cells are composed of a mix of these capabilities and several multifunction cells. There are also a number of types of supporting cells with various functions that provide support to the direct action cells or to the insurgent organization as a whole. Thus, a particular insurgent organization could be composed of varying numbers of multifunction or specialty direct action cells, supporting cells, or any mix of these.

Guerrilla Organizations
Guerrilla organizations come in various shapes and sizes. They may be as large as several BDEs or as small as a platoon and/or independent H/K teams. The structure of the organization depends on several factors including the physical environment, sociological demographics and relationships, economics, and support available from external organizations and countries. In any case, a guerrilla organization might be affiliated with forces from other countries or external organizations. Some guerrilla organizations may constitute a paramilitary arm of an insurgent movement, while others may pursue guerrilla warfare independently from or loosely affiliated with an insurgent organization.

Compared to insurgent organizations as a whole, guerrilla organizations have a more military-like structure. Within this structure, guerrilla organizations have some of the same types of weapons as a regular military force. The guerrilla organization contains weapons up to and including 120-mm mortars, antitank guided missiles (ATGM), and man-portable air defense systems (MANPADS), and can conduct limited mine warfare and sapper attacks. Other examples of equipment and capability the guerrillas have in their organizations that the insurgents generally do not have are 12.7-mm heavy machineguns (MG); .50-cal antimateriel rifles; 73-, 82-, and 84-mm recoilless guns; 100- and 120-mm mortars; 107-mm multiple rocket launchers (MRL); 122-mm rocket launchers; global positioning system (GPS) jammers; and signals intelligence capabilities.

While both insurgent and guerilla organizations are very effective and lethal in close and populated terrain, the guerrilla organizations can perform more typical fire and maneuver tactics. The guerrilla organization can, and often does, use terror tactics; however it is best suited to conduct irregular or unconventional warfare tactics.

Guerrilla BDEs
The composition of the guerrilla BDE may vary. A basically rural, mountainous, or forested area with no major population centers might have a guerrilla BDE with only one or two BNs (or five or six companies) with little or no additional combat support or combat service support. A guerrilla BDE operating astride a major avenue of approach, or one that contains several major population (urban) or industrial centers, might be a full guerrilla BDE with additional combat support or combat service support (CSS) elements.

Guerrilla BNs
Often a BDE-sized guerrilla force may not be appropriate—a guerrilla BN or a task-organized BN may be sufficient. A guerrilla BN may be any combination of guerrilla companies or guerrilla H/K companies. When a BN consists predominantly of guerrilla H/K companies, it may be considered a guerrilla H/K BN. A typical task-organized-BN

might have four or five guerrilla H/K companies, organic BN units, and a weapons battery from BDE (with mortar, AT, and rocket launcher platoons) and possibly intelligence and electronic warfare (IEW) support.

Guerrilla Companies

The guerrilla CO fights unconventionally with platoons, squads, and fire teams. When organized for combat as a guerrilla H/K CO, it also fights unconventionally, but with H/K groups, sections, and teams. The guerrilla H/K CO is simply a restructured guerrilla CO. Therefore, they both contain the same number of personnel and similar numbers of equipment. Complete BNs and BDEs—or any part thereof—can be organized for combat as H/K units.

The typical guerrilla H/K CO is broken into three H/K groups. Each group has four sections of three H/K teams each. Thus, the CO contains a total of 36 H/K teams. There are actually 39 H/K teams, if the two sniper teams and the CO scouts in the CO's HQ and command section are counted.

The guerrilla H/K CO or BN is especially effective and lethal in close environments (such as urban, forest, or swamp). The task-organized H/K team structure is ideal for dispersed combat. The structure that makes H/K teams virtually impossible to isolate and kill in a dispersed fight also allows them to melt into the population and terrain whenever necessary.

PSO

Private security organizations (PSO) 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. PSO teams may consist of bodyguard teams, patrol teams, stationary guard teams, or information and investigation teams.

PSOs are diverse in regard to organizational structure and level of capability. The weapons and equipment mix is based on team specialization/role and varies. Other example equipment includes listening and monitoring equipment, cellular phones, cameras, facsimiles, computers, motorcycles, helicopters, all-terrain vehicles, AT disposable launchers, submachine guns, and silenced weapons.

CRIMINAL ORGANIZATIONS

Criminal organizations are normally independent of nation-state control and large-scale organizations often extend beyond national boundaries to operate regionally or worldwide. Individual drug dealers and criminals or small-scale criminal organizations (gangs) do not have the capability to adversely affect legitimate political, military, and judicial organizations—but the large-scale organizations do. The weapons and equipment mix varies, based on type and scale of criminal activity. Criminal organizations at the higher end of the scale can take on the characteristics of a paramilitary organization.

By mutual agreement, or when their interests coincide, criminal organizations may become affiliated with other non-state paramilitary actors, such as insurgent or guerrilla forces. Insurgents or guerrillas controlling or operating in the same area can provide security and protection to the criminal organization's activities in exchange for financial assistance or arms. Guerrilla or insurgent organizations can create diversionary actions, conduct reconnaissance and early warning, money laundering, smuggling, transportation, and civic actions on behalf of the criminal organization. Their mutual interests can include preventing U.S. or local government forces from interfering in their respective spheres.

At times, criminal organizations might also be affiliated with nation-state military and/or paramilitary actors. In time of war, for instance, the State can encourage and materially support criminal organizations to commit actions that contribute to the breakdown of civil control in a neighboring country.

OTHER ARMED COMBATANTS

In any OE, there are likely to be nonmilitary personnel who are armed but not part of an organized paramilitary or military structure. Nevertheless, they may be disgruntled and hostile. Some of these nonaffiliated personnel may possess small arms legally to protect their families, homes, and/or businesses. When a catalyst occurs, they can use their "defensive" weapons to attack. Some might only be opportunists who decide to attack a convoy, a vehicle, or a soldier in order to make a profit. Their motives might be religious, racial, or cultural differences, or revenge, hatred, or greed. Some are just angry at the U.S. The reasons are immaterial—armed civilians are ubiquitous.

Such armed combatants may represent a large portion of the undecided in a population—those who have yet to determine which side they are on. They may also be those who are going to change sides. They might be completely neutral one minute, and the next they might be on the side of the enemy. Any number of catalysts might cause them to change sides. The event causing the change might be the injury or death of a family member, loss of property, or

the perceived disrespect of their culture, religion, or tribe. Their decision will probably not remain permanent. They might change sides several times depending on the circumstances directly affecting their lives. Once they commit themselves to a side, they are easier to categorize.

UNARMED COMBATANTS

The local populace contains various types of unarmed nonmilitary personnel who, given the right conditions, may decide to purposely and materially support hostilities against the United States. This active support or participation may take many forms, not all of which involve possessing or using weapons. In an insurgent organization, for example, unarmed personnel might conduct recruiting, financing, intelligence-gathering, supply-brokering, transportation, courier, or INFOWAR functions (including videographers and camera operators). Technicians and workers who fabricate IEDs might not be armed. The same is true of people who provide sanctuary for combatants. Individuals who perform money-laundering or operate front companies for large criminal organizations might not be armed. Individual criminals or small gangs might be affiliated with a paramilitary organization and perform support functions that do not involve weapons. Unarmed religious, political, tribal, or cultural leaders might participate in or actively support a paramilitary organization. Unarmed media or medical personnel may become affiliated with a military or paramilitary organization. Categorize even unarmed individuals who are coerced into performing or supporting hostile actions and those who do so unwittingly as "combatants". Thus, various types of unarmed combatants can be part of the OPFOR. In short, an unarmed combatant is any unarmed person who engages in hostilities or who purposely and materially supports hostilities against the United States or its co-belligerents. This includes support that takes place off the battlefield.

Noncombatants

Nonmilitary actors that are not part of the OPFOR may be present in the OE. As noncombatants, they are currently either friendly or neutral. They can be either armed or unarmed, and have the potential to become combatants in certain conditions. They might provide support to combatants—either willingly or unwillingly.

ARMED NONCOMBATANTS

There are likely to be armed noncombatants who are not part of any military or paramilitary organization. Some may be in possession of small arms legally to protect their families, property, and/or businesses. Some may use weapons as part of their occupation (for example, hunters, security guards, or local police). Some may be minor criminals who use their weapons for activities such as extortion and theft; they might even steal from U.S. forces, to make a profit. They may be completely neutral or have leanings for either side, or several sides. However, they are not members of or directly affiliated with a hostile faction. Such armed noncombatants are ubiquitous. Their numbers vary from one individual to several hundred.

UNARMED NONCOMBATANTS

At a minimum, other actors in the OE include unarmed noncombatants. They are an integral part of the OE and cannot be excluded. Examples include medical teams, media, humanitarian relief organizations, transnational corporations, displaced persons, transients, foreign government and diplomatic personnel, and local populace. These nonmilitary actors may be neutral or potential side-changers, depending on their perception of U.S. actions.

Chapter 5

OPFOR Task Organization for Combat

This chapter provides an overview of TC 7-100.2, OPFOR Tactics.

This chapter introduces the baseline tactical doctrine for the complex OPFOR. It explains how the OPFOR directs tactical forces and actions, and provides insight into the OPFOR's theory and practice of commanding and controlling forces in war.

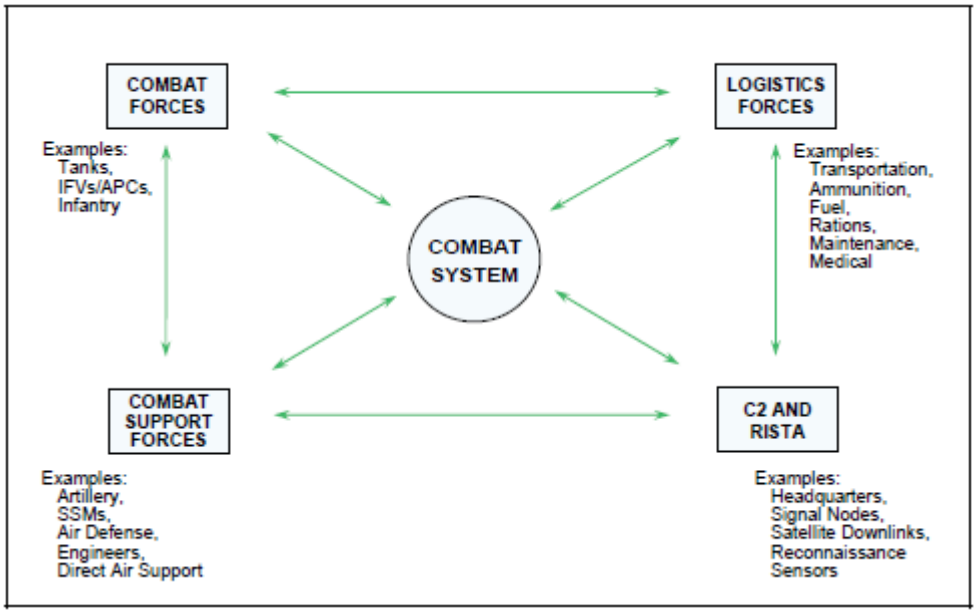


Figure 5-1. Systems Warfare

Systems Warfare

A *combat system* is the result from the synergistic combination of four basic subsystems that are integrated to achieve a military function. The subsystems are:

- **Combat forces**— main battle tanks, infantry fighting vehicles (IFV), armored personnel carriers (APC), or infantry
- **Combat support forces**— artillery, SSM, air defense, engineers, and direct air support
- **Logistics forces**— transportation, ammunition, fuel, rations, maintenance, and medical
- **Command and control, and reconnaissance, intelligence, surveillance and target acquisition (RISTA)** — HQ, signal nodes, satellite downlink sites, and reconnaissance sensors.

The OPFOR believes that a qualitatively and/or quantitatively weaker force can defeat a superior foe, if the lesser force can dictate the terms of combat. It believes that the systems warfare approach allows it to move away from the traditional attrition-based approach to combat. It is no longer necessary to match an opponent system-for-system or capability-for-capability. CDRs and staffs will locate the critical component(s) of the enemy combat system, patterns of interaction, and opportunities to exploit this connectivity. The OPFOR will seek to disaggregate enemy combat power by destroying or neutralizing single points of failure in the enemy's combat system. Systems warfare has applications in both offensive and defensive contexts.

S2 NOTE: OPFOR uses C2, not mission command.

OPFOR COMMAND AND CONTROL (C2)

Principles of Command and Control. The OPFOR defines command and control as the actions of CDRs, command groups, and staffs of military HQ to maintain continual combat readiness and combat efficiency of forces,

to plan and prepare for combat operations, and to provide leadership and direction during the execution of assigned missions. It views the C2 process as the means for assuring both *command* (establishing the aim) and *control* (sustaining the aim). The OPFOR's tactical C2 concept is based on:

- **Mission tactics.** OPFOR tactical units focus on the purpose of their tactical mission, and use initiative to act on that purpose despite enemy action or unforeseen events.
- **Flexibility through battle drills**. True flexibility comes from Soldiers understanding basic battlefield functions to such a degree they are second nature. Battle drills are not considered restrictive.
- **Accounting for mission dynamics**. Enemy action and battlefield conditions may make the original mission irrelevant and require a new mission without a planning session. Tactical staffs constantly evaluate the situation and make recommendations accordingly. CDRs at every level act flexibly, relying on their battlefield judgment to what best meets and sustains the aim of his superior.

The state accepts that **decentralized planning** is essential to controlling the tempo of the operation. Consequently, the OPFOR organization provides for initiative within the bounds of mission guidance. To help mitigate the risks of decentralized execution, the OPFOR employs a **deliberate decision-making process** that produces plans supporting each unit's role in the operation. These plans also identify branches and sequels to provide CDRs with sufficient guidance so they can use their initiative when necessary. This flexibility to subordinates is essential for meeting the needs of the OPFOR in the OE.

OPFOR Command and Support Relationships

The OPFOR uses four command relationships to task organize for operations:

Relationship	Commanded by	Logistics from	Positioned by	Priorities from
Constituent	Gaining	Gaining	Gaining	Gaining
Dedicated	Gaining	Parent	Gaining	Gaining
Supporting	Parent	Parent	Supported	Supported
Affiliated	Self	Self or Parent	Self	Mutual agreement

Constituent. Constituent units are those forces assigned directly to a unit and forming an integral part of it. They may be organic to the TOE of the AFS forming the basis of a given unit, assigned at the time the unit was created, or attached to it after its formation.

Dedicated. Dedicated is a command relationship identical to constituent with the exception that a dedicated unit still receives logistics support from a parent HQ of similar type. An example of a dedicated unit would be the case where a specialized unit, such as an attack helicopter CO, is allocated to a BTG. The base BDE does not possess the technical experts or repair facilities for the aviation unit's equipment. However, the dedicated relationship permits the CO to execute missions exclusively for the BTG while still receiving its logistics support from its parent organization. In OPFOR plans and orders, the dedicated command and support relationship is indicated by (DED) next to a unit title or symbol.

Supporting. Supporting units continue to be commanded by and receive their logistics from their parent HQ, but are positioned and given mission priorities by their supported HQ. This relationship permits supported units the freedom to establish priorities and position supporting units while allowing higher HQ to rapidly shift support in dynamic situations. An example of a supporting unit would be a MRL BN supporting a BTG for a particular phase of an operation but ready to rapidly transition to a different support relationship when the BTG becomes the DTG reserve in a later phase. The supporting unit does not necessarily have to be within the supported unit's area of responsibility (AOR). In OPFOR plans and orders, the supporting command and support relationship is indicated by (SPT) next to a unit title or symbol.

Affiliated. Affiliated organizations are those operating in a unit's AOR that the unit may be able to sufficiently influence to act in concert with it for a limited time. No "command relationship" exists between an affiliated organization and the unit in whose AOR it operates. Affiliated organizations are typically nonmilitary or paramilitary groups such as criminal cartels or insurgent organizations. In some cases, affiliated forces may receive

support from the DTG or BTG as part of the agreement under which they cooperate. Although there will typically be no formal indication of this relationship in OPFOR plans and orders, in rare cases (AFL) is used next to unit titles or symbols.

OPFOR Tactical Groups

The OPFOR often forms a tactical group, which is a DIV or BDE that has been assigned additional land forces necessary to accomplish the mission. A tactical group differs from higher-level task organizations in that it is built around the structure of an already existing organization. Normally, these assets are initially allocated to an OSC or FG, which further allocates these forces to subordinate units. The purpose of these groups is to ensure unity of command for all land forces in a given AOR. Tactical groups formed from DIVs are called division tactical groups (DTG) and those formed from brigades are called brigade tactical groups (BTG).

DTG

The DTG is organized around an existing DIV or BDE structure. Although a DIV or BDE may fight as originally organized, the parent HQ normally augments the group with additional land resources as required. Thus, a DTG is not a joint command.

The DTG is task organized to perform both offensive and defensive operations. BDEs, BTGS, and interagency organizations can all be assigned. The DIV is capable of exerting control over important geographic areas or medium size urban areas (population of 20,000 to 100,000).

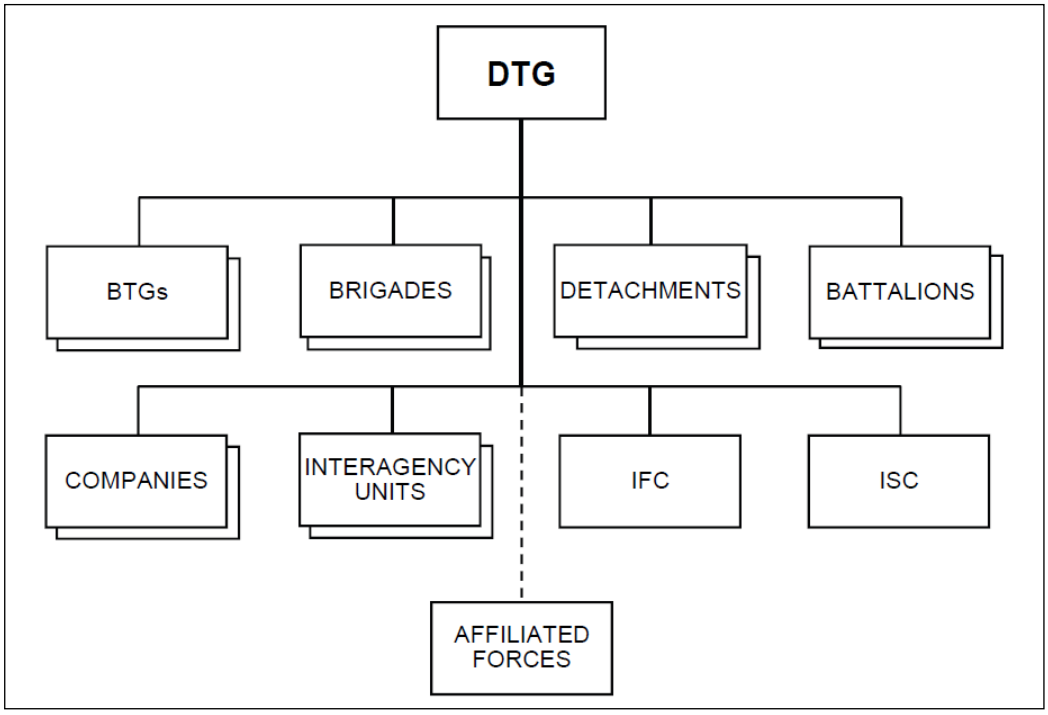


Figure 5-2. Possible DTG

Some of the units constituent to the DTG are part of the DIV on which it is based. Note that some BDEs are task organized into BTGs, while others may not be and have structures that come straight out of the organizational directories for the AFS. Likewise, some BNs and companies may become detachments.

Besides what came from the original DIV structure, the rest of the organizations shown come from a pool of assets the parent OSC has received from the AFS and has decided to pass down to the DTG. All fire support units that were organic to the DIV or allocated to the DTG (and are not suballocated down to a BTG) go into the integrated fires command (IFC). Likewise, CSS units go into the integrated support command (ISC). As shown here, DTGs can also have affiliated forces from paramilitary organizations.

Brigade Tactical Group (BTG)

Like the DTG, the BTG is organized around an existing BDE and is not a joint organization. Interagency organizations may be assigned up to BN size, and may include land forces from other services. Unlike higher-level commands, OPFOR BDEs and BTGs do not have an IFC or an ISC.

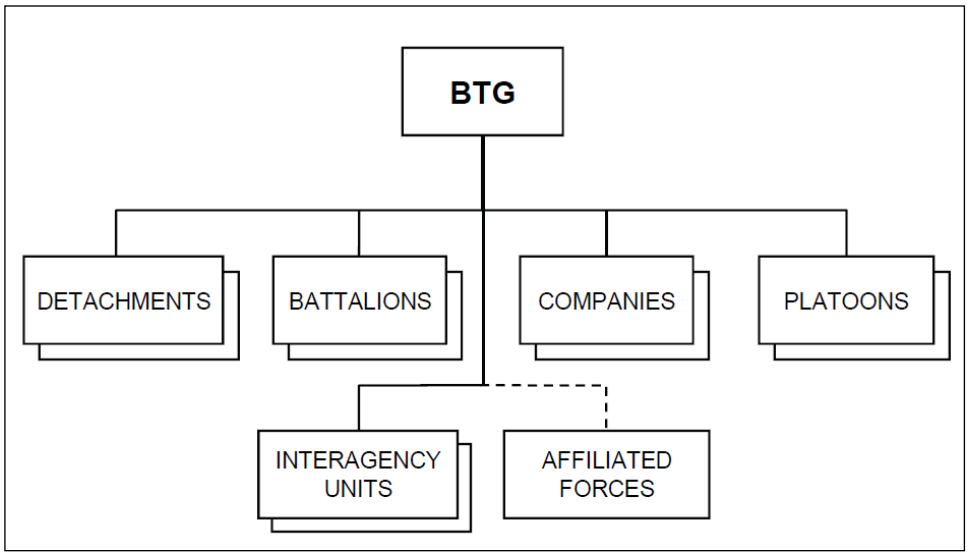


Figure 5-3. Possible BTG

This example shows that some BNs and companies of a BTG may be task-organized as detachments, while others are not. BTGs (and higher commands) can also have affiliated forces from paramilitary organizations.

Battalions

In the OPFOR's force structure, the basic unit of action is the *battalion*. Battalions are designed to be able to

- Serve as the basis for forming a BDET, if necessary
- Fight as part of a BDE, BTG, DIV, or DTG
- Execute basic combat missions as part of a larger tactical force
- Plan for operations expected to occur 6 to 24 hours in the future
- Execute all of the tactical actions

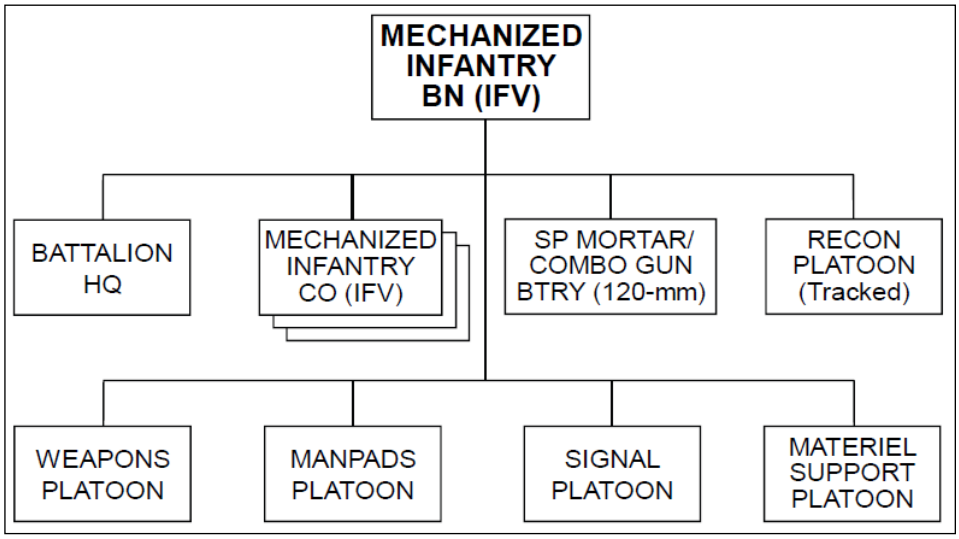


Figure 5-4. BN example

Companies

In the OPFOR's force structure, the largest unit without a staff is the CO. In fire support units, this level of command is commonly called a battery (see example below). Companies are designed to be able to–

- Serve as the basis for forming a CDET, if necessary.
- Fight as part of a BN, BDET, BDE, BTG, DIV, or DTG.
- Execute tactical tasks (a CO will not normally be asked to perform two or more tactical tasks simultaneously)

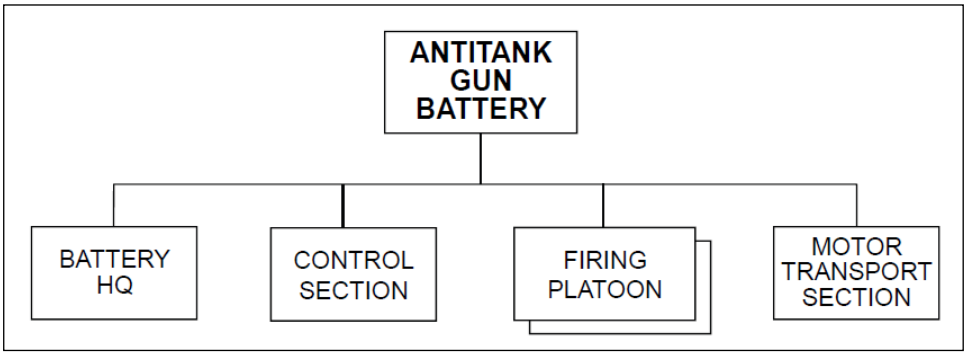


Figure 5-5. CO (Battery) example

Detachments

A *detachment* is a BN or CO designated to perform a specific mission and allocated the forces necessary to do so. Detachments are the smallest combined arms formations and are, by definition, task-organized. To further differentiate, detachments built from BNs can be termed *battalion-size detachments* (BDETs), and those formed from companies can be termed *company-size detachments* (CDETs). The forces allocated to a detachment suit the mission expected of it. They may include:

- Artillery or mortar units
- Air defense units
- Engineer units (with obstacle, survivability, or mobility assets)
- Heavy weapons units (including heavy MGs, automatic grenade launchers, and ATGMs)
- Units with specialty equipment such as flame weapons, specialized reconnaissance assets, or helicopters
- Interagency forces up to CO size for BDETs, or platoon size for CDETs
- Chemical defense, AT, medical, logistics, signal, and electronic warfare (EW) units

BDETs can accept dedicated and supporting SPF, aviation (combat helicopter, transport helicopter), and unmanned aerial vehicle (UAV) units

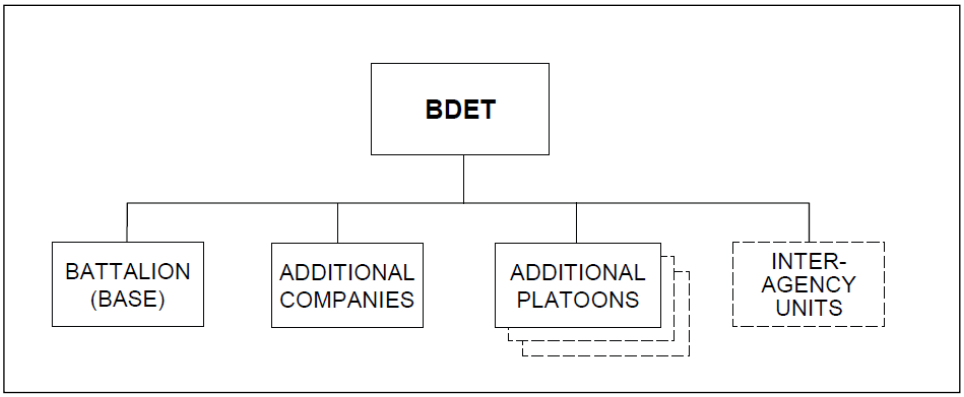


Figure 5-6. BDET example

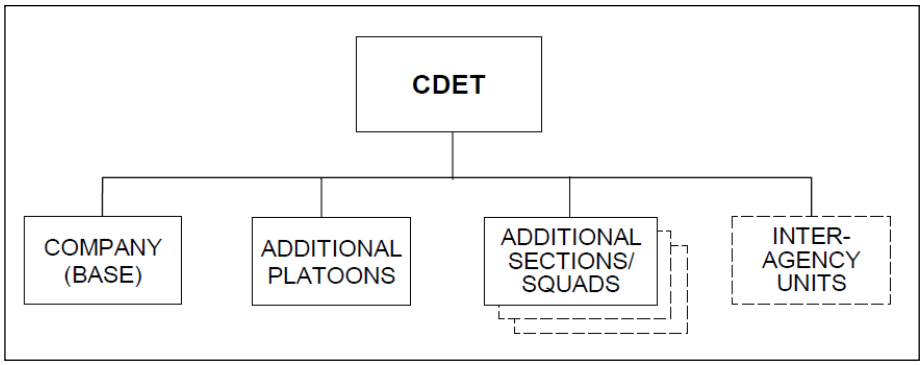


Figure 5-7. CDET example

The basic type of OPFOR detachment—whether formed from a BN or a CO—is the *independent mission detachment* (IMD). IMDs are formed to execute missions that are separated in space variety of missions, some of which are listed here as examples:

- Seizing key terrain
- Linking up with airborne or heliborne forces
- Conducting tactical movement on secondary axes
- Pursuing or enveloping an enemy force
- Conducting a raid or ambush

Other types of detachments and their uses are described in subsequent chapters of TC 7-100.2. These detachments include—

- Counterreconnaissance detachment (CRD). (See chapter 5)
- Urban detachment (UD). (See chapter 5)
- Security detachment (SD). (See chapter 5)
- Reconnaissance detachment (RD). (See chapter 7)
- Movement support detachment (MSD). (See chapter 12)
- Obstacle detachment (OD). (See chapter 12)

Platoons and Squads

In the OPFOR's force structure, the smallest unit typically expected to conduct independent fire and maneuver is the platoon. Platoons are designed to be able to-

- Serve as the basis for forming a functional element or patrol
- Fight as part of a CO, BN, or detachment
- Execute tactical tasks. (a platoon will not be asked to perform two or more tactical tasks simultaneously)
- Exert control over a small riot, crowd, or demonstration

Platoons and squads within them can be task-organized for specific missions

OPFOR Organization of the Tactical Battlefield

The OPFOR organizes the battlefield in such a way that it can rapidly transition between offensive and defensive actions and between linear and nonlinear operations. This flexibility enables the OPFOR change the nature of the conflict into something for which the enemy is not prepared.

Area of Responsibility (AOR)

OPFOR organizations are given a specific *area of responsibility*. An OPFOR AOR is the geographical area and associated airspace within which a CDR has the authority to plan and conduct combat operations.

An AOR is bounded by a *limit of responsibility* (LOR) beyond which the organization may not operate or fire without coordination through the next-higher HQ. AORs may be linear or nonlinear in nature. Linear AORs may contain subordinate nonlinear AORs and vice versa.

A combat order normally defines AORs (and zones within them) by specifying boundary lines in terms of distinct local terrain features through which a line passes. The order specifies whether each of those terrain features is included or excluded from the unit's AOR or zones within it.

Zones

AORs typically consist of three basic *zones*: *battle*, *disruption*, and *support*. An AOR may also contain one or more *attack* and/or *kill* zones. The various zones in an AOR have the same basic purposes within each type of offensive and defensive action. Zones may be linear or nonlinear in nature. The size of these zones depends on the size of the OPFOR elements involved, engagement ranges of weapon systems, the terrain, and the nature of the enemy's operation. Within the limits of responsibility or LOR, the OPFOR normally refers to two types of control lines. The *support line* separates the support zone from the battle zone. The *battle line* separates the battle zone from the disruption zone.

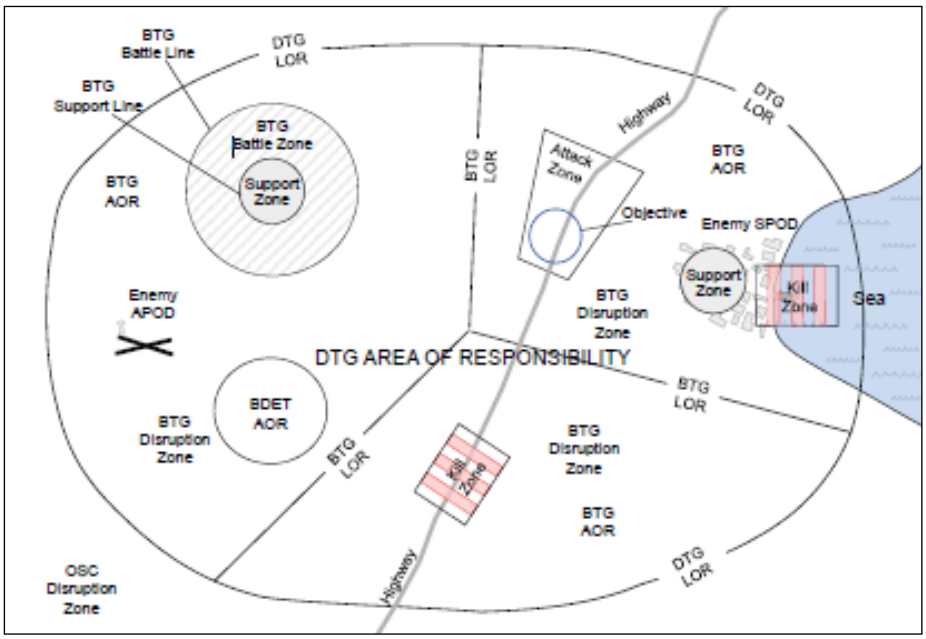


Figure 5-8. Example of a non-linear AOR with graphic control measures.

Disruption Zone

The *disruption zone* is the AOR of the disruption force. It is that geographical area and airspace in which the unit's disruption force will conduct disruption tasks. This is where the OPFOR will set the conditions for successful combat actions by fixing enemy forces and placing long-range fires on them. Units in this zone begin the attack on specific components of the enemy's combat system, to begin the disaggregation of that system. Successful actions in the disruption zone will create a window of opportunity that is exploitable in the battle zone. Specific actions in the disruption zone can include—

- Attacking the enemy's engineer elements. This can leave his maneuver force unable to continue effective operations in complex terrain exposing them to destruction by forces in the battle zone.
- Stripping away the enemy's reconnaissance assets while denying him the ability to acquire and engage OPFOR targets with deep fires. This includes an air defense effort to deny aerial attack and reconnaissance platforms from targeting OPFOR forces.
- Forcing the enemy to deploy early or disrupting his offensive preparations
- Gaining and maintaining reconnaissance contact with key enemy elements
- Deceiving the enemy as to the disposition of OPFOR units

The disruption zone is bounded by the battle line and the LOR of the overall AOR. In linear offensive combat, the higher HQ may move the battle line and LOR forward as the force continues successful offensive actions. Thus, the boundaries of the disruption zone will also move forward during the course of a battle. The higher CDR can push the disruption zone forward or outward as forces adopt a defensive posture while consolidating gains at the end of a successful offensive battle and/or prepare for a subsequent offensive battle. Disruption zones may be contiguous or noncontiguous. They can also be "layered," in the sense that one command's disruption zone is part of the disruption zone of the next-higher command. BNs and below do not typically have their own disruption zones. However, they may conduct actions within the disruption zone of a higher command.

Battle Zone

The *battle zone* is where the OPFOR expects to conduct decisive actions. Forces in the battle zone will exploit opportunities created by actions in the disruption zone. Using all elements of combat power, the OPFOR will engage the enemy in close combat to achieve tactical decision in this zone. In the battle zone, the OPFOR is trying to accomplish one or more of the following:

- Create a penetration in the enemy defense through which exploitation forces can pass
- Draw enemy attention and resources to the action
- Seize terrain
- Inflict casualties on a vulnerable enemy unit to prevent the enemy from moving a part of his force to impact OPFOR actions elsewhere on the battlefield

A DIV or DTG does not always form a DIV- or DTG-level battle zone per se. That zone may be the aggregate of the battle zones of its subordinate units. In nonlinear situations, there may be multiple, noncontiguous BDE or BTG battle zones, and within each the DIV or DTG would assign a certain task to the unit charged to operate in that space. The BDE or BTG battle zone provides each of those subordinate unit CDRs the space in which to frame his actions. BN and below units often have AORs that consist almost entirely of battle zones with a small support zone contained within them.

The battle zone is separated from the disruption zone by the battle line and from the support zone by the support line. In the offense, the CDR may adjust the location of these lines in order to accommodate successful offensive action. In a linear situation, those lines can shift forward during the course of a successful attack. Thus, the battle zone would also shift forward.

Support Zone

The *support zone* is that area of the battlefield designed to be free of significant enemy action and to permit the effective logistics and administrative support of forces. Security forces will operate in the support zone in a combat role to defeat enemy special operations forces. Camouflage, concealment, cover, and deception (C3D) measures will occur throughout the support zone to protect the force from standoff RISTA and precision attack. A DIV or DTG

support zone may be dispersed within the support zones of subordinate BDEs or BTGs, or the DIV or DTG may have its own support zone that is separate from subordinate AORs. If the battle zone moves during the course of a battle, the support zone would move accordingly. The support zone may be in a sanctuary that is noncontiguous with other zones of the AOR.

Attack Zone

An *attack zone* is given to a subordinate unit with an offensive mission, to delineate clearly where forces will be conducting offensive maneuver. Attack zones are often used to control offensive action by a subordinate unit inside a larger defensive battle or operation.

Kill Zone

A *kill zone* is a designated area on the battlefield where the OPFOR plans to destroy a key enemy target. A kill zone may be within the disruption zone or the battle zone. In the defense, it could also be in the support zone.

S2 NOTE: There is no "template" for the OPFOR, but well trained S-2s can explain their capabilities and intent.

Chapter 6

OPFOR Tactics - Offense

OPFOR Offense

This chapter describes the OPFOR's concept for tactical offensive operations. More information can be found in the 7-100 series manuals that can be downloaded from the Army Training Network at https://atn.army.mil/dsp_template.aspx?dpID=311 .

The OPFOR sees OFFENSE as the decisive form of combat and the ultimate means of imposing its will on the enemy. While conditions at a particular time or place may require the OPFOR to defend, defeating an enemy force ultimately requires shifting to the offense. Even within the context of defense, victory normally requires some sort of offensive action. Therefore, OPFOR CDRs seek to create and exploit opportunities to take offensive action whenever possible.

The aim of offense at the tactical level is to achieve tactical missions in support of an operation. A tactical command ensures that its subordinate commands thoroughly understand both the overall goals of the operation and the specific purpose of a particular mission they are about to execute. In this way, subordinate commands may continue to execute the mission without direct control by a higher HQ, if necessary.

Purpose of the Offense

All tactical offensive actions are designed to achieve the goals of an operation through active measures. However, the purpose or reason, of any given offensive mission varies with the situation, as determined through the decision-making process. The primary distinction among types of offensive missions is their purpose which is defined by what the CDR wants to achieve tactically. Thus, the OPFOR recognizes six general purposes of tactical offensive missions: **Gain freedom of movement**; **Restrict freedom of movement**; **Gain control of key terrain, personnel, or equipment**; **Gain information**; **Dislocate**; and, **Disrupt**.

An **attack to gain freedom of movement** creates a situation in an important part of the battlefield where other friendly forces can maneuver in a method of their own choosing with little or no opposition. Such an attack can take many forms.

An **attack to restrict freedom of movement** prevents the enemy from maneuvering as he chooses. Restricting attacks can deny key terrain, ambush moving forces, dominate airspace, or fix an enemy formation. Tactical tasks often associated with restricting attacks are ambush, block, canalize, contain, fix, interdict, and isolate. The attrition of combat elements and equipment may also limit the enemy units' ability to move.

An **attack to gain control of key terrain, personnel, or equipment** is not necessarily terrain focused—a raid with the objective of taking prisoners or key equipment is also an attack to gain control. Besides the classic seizure of key terrain that dominates a battlefield, an attack to control may also target facilities such as economic targets, ports, or airfields. Tactical tasks associated with an attack to control are raid, clear, destroy, occupy, retain, secure, and seize. Some non-traditional attacks to gain control may be information attack, computer warfare, EW, or other forms of INFOWAR.

An **attack to gain information** is not to locate to destroy, fix, or occupy but rather to gain information about the enemy. Quite often the OPFOR will have to penetrate or circumvent the enemy's security forces and conduct an attack in order to determine the enemy's location, dispositions, capabilities, and intentions.

An **attack to dislocate** employs forces to obtain significant positional advantage, rendering the enemy's dispositions less valuable, perhaps even irrelevant. It aims to make the enemy expose forces by reacting to the dislocating action. Dislocation requires enemy CDRs to make a choice: accept neutralization of part of their force or risk its destruction while repositioning. Turning movements and envelopments produce dislocation. Artillery or other direct or indirect fires may cause an enemy to either move to a more tenable location or risk severe attrition. Typical tactical tasks associated with dislocation are ambush, interdict, and neutralize.

An **attack to disrupt** is used to prevent the enemy from being able to execute an advantageous COA (COA) or to degrade his ability to execute that COA. It is also used to create windows of opportunity to be exploited by the OPFOR. It is an intentional interference (disruption) of enemy plans and intentions, causing the enemy confusion and the loss of focus, and throwing his battle synchronization into turmoil. The OPFOR then quickly exploits the result of the attack to disrupt. A spoiling attack is an example of an attack to disrupt.

Attacks to disrupt focus on a key enemy capability, intention, or vulnerability. They are also designed to disrupt enemy plans, tempo, infrastructure, logistics, affiliations, mission command, formations, or civil order. Attacks to disrupt often have a strong INFOWAR component and may disrupt, limit, deny, and/or degrade the enemy's use of the electromagnetic spectrum, especially the enemy's mission command. They may also take the form of computer warfare and/or information attack.

The attack to disrupt may not be limited by distance. It may be carried out in proximity to the enemy (as in an ambush) or from an extreme distance (such as computer warfare or information attack from another continent) or both simultaneously. The attack to disrupt may be conducted by a single component (an ambush in contact) or a coordinated attack by several components such as combined arms using armored fighting vehicles, infantry, artillery, and several elements of INFOWAR (for example, EW, deception, perception management, information attack, and/or computer warfare).

The OPFOR does not limit its attacks to military targets or enemy combatants. The attack to disrupt may be carried out against noncombatant civilians (even family members of enemy soldiers at home station or in religious services), diplomats, contractors, or whomever and/or whatever the OPFOR CDRs believe will enhance their probabilities of mission success.

Functional Organization of Forces for the Offense—Tactical Groups, Divisions, and Brigades

In planning and executing offensive actions, OPFOR CDRs at BDE level and above organize and designate various *forces* within his level of command according to their *function*. Thus, subordinate forces understand their roles within the overall battle. However, the organization of forces can shift dramatically during the course of a battle, if part of the plan does not work or works better than anticipated.

Each functional force has an identified CDR. This is often the senior CDR of the largest subordinate unit assigned to that force. The force CDR is responsible to the tactical group CDR to ensure that combat preparations are made properly and to take charge of the force during the battle. This frees the tactical group CDR from decisions specific to the force's mission. Even when tactical group subordinates have responsibility for parts of the disruption zone, there is still an overall tactical group disruption force CDR.

A BN or below organization can serve as a functional force (or part of one) for its higher command. At any given time, it can be part of only a single functional force or a reserve.

Enabling Force(s)

Various types of *enabling forces* are charged with creating the conditions that allow the action force the freedom to operate. In order to create a window of opportunity for the action force to succeed, the enabling force may be required to operate at a high degree of risk and may sustain substantial casualties. However, an enabling force may not even make contact with the enemy, but instead conduct a demonstration. BNs and below serving as an enabling force are often required to conduct breaching or obstacle-clearing tasks, However, it is important to remember that the requirements laid on the enabling force are tied directly to the type and mission of the action force.

Disruption Force

In the offense, the *disruption force* would typically include the disruption force that already existed in a preceding defensive situation. It is possible that forces assigned for actions in the disruption zone in the defense might not have sufficient mobility to do the same in the offense or that targets may change and require different or additional assets. Thus, the disruption force might require augmentation. BNs and below can serve as disruption forces for BDEs or BTGs.

Fixing Force

OPFOR offensive actions are founded on the concept of fixing enemy forces so that they are not free to maneuver. In the offense, planners will identify which enemy forces need to be fixed and the method by which they will be fixed. They will then assign this responsibility to a force that has the capability to fix the required enemy forces with the correct method. The fixing force may consist of a number of units separated from each other in time and space, particularly if the enemy forces required to be fixed are likewise separated. A fixing force could consist entirely of affiliated irregular forces. BNs and below often serve as fixing forces for BTGs and are also often capable of performing this mission without significant task organization. This is particularly true in those cases where simple suppressive fires are sufficient to fix enemy forces.

Assault Force
At BTG level, the CDR may employ one or more *assault forces*. This means that one or more subordinate detachments would conduct an assault to destroy an enemy force or seize a position. However, the purpose of such an assault is to create or help create the opportunity for the action force to accomplish the BTG's overall mission.

Security Force
The *security force* conducts activities to prevent or mitigate the effects of hostile actions against the overall tactical-level command and/or its key components. If the CDR chooses, he may charge this security force with providing force protection for the entire AOR, including the rest of the functional forces; logistics and administrative elements in the support zone; and other key installations, facilities, and resources. The security force may include various types of units such as infantry, SPF, counter reconnaissance, and signals reconnaissance assets to focus on enemy special operations and long-range reconnaissance forces operating throughout the AOR. It can also include Internal Security Forces units allocated to the tactical-level command, with the mission of protecting the overall command from attack by hostile insurgents, terrorists, and special operations forces. The security force may also be charged with mitigating the effects of WMD.

Deception Force
When the INFOWAR plan requires combat forces to take some action, these forces will be designated as deception forces.

Support Force
A support force provides support by fire; other combat or combat service support; or C2 functions for other parts of the tactical group.

Action Force(s)
One part of the tactical group conducting a particular offensive action is normally responsible for performing the primary function or task that accomplishes the overall goal or objective of that *action*. In most general terms, therefore, that part can be called the *action force*. In most cases, however, the tactical group CDR will give the action force a more specific designation that identifies the specific function it is intended to perform, which equates to achieving the objective of the tactical group's mission. There are three basic types of action forces: exploitation force, strike force, and mission force.

Exploitation Force
In most types of offensive action at tactical group level, an *exploitation force* is assigned the task of achieving the objective of the mission. It typically exploits a window of opportunity created by an enabling force. In some situations, the exploitation force could engage the ultimate objective with fires only.

Strike Force
A strike is an offensive COA that rapidly destroys a key enemy organization through a synergistic combination of massed precision fires and maneuver. The primary objective of a strike is the enemy's will and ability to fight. A strike is planned and coordinated at the operational level, but executed by a tactical-level force. The force that actually accomplishes the final destruction of the targeted enemy force is called the *strike force*.

Mission Force
In those non-strike offensive actions where the mission can be accomplished without the creation of a specific window of opportunity, the set of capabilities that accomplish the mission are collectively known as a *mission force*. However, the tactical group CDR may give a mission force a more specific designation that identifies its specific function.

Reserves
OPFOR offensive reserve formations will be given priorities in terms of whether the staff thinks it most likely that they will act as a particular type of enabling or action force. The size and composition of an offensive reserve are entirely situation-dependent.

Functional Organization of Elements for the Offense—Detachments, Battalions, and Below

An OPFOR detachment is a BN or CO designated to perform a specific mission and task organized to do so. CDRs of detachments, BNs, and companies organize their subordinate units according to the specific functions they intend each subordinate to perform. They use a methodology of "functional organization" similar to that used by used by BDEs and above. However, one difference is that CDRs at BDE and higher use the term *forces* when designating functions within their organization. **CDRs at detachment, BN, and below use the term *element.*** Elements can be

broken down into two very broad categories: action and enabling. However, CDRs normally designate functional elements more specifically, identifying the specific action or the specific means of accomplishing the function during a particular mission. CDRs may also organize various types of specialist elements. Depending on the mission and conditions, there may be more than one of some of these specific element types.

The number of functional elements is unlimited and is determined by any number of variables, such as the size of the overall organization, its mission, and its target. Quite often the distinction between exactly which element is an action element or an enabling element is blurred because, as the mission progresses, conditions change or evolve and require adaptation.

Action Elements
The *action element* is the element conducting the primary action of the overall organization's mission. However, the CDR normally gives this element a functional designation that more specifically describes exactly what activity the element is performing on the battlefield at that particular time. For example, the action element in a raid may be called the *raiding element*. If an element accomplishes the objective of the mission by exploiting an opportunity created by another element, is may be called the *exploitation element*.

Enabling Elements
Enabling elements can enable the primary action in various ways. The most common types are security elements and support elements. The *security element* provides local tactical security for the overall organization and prevents the enemy from influencing mission accomplishment. (A security element providing front, flank, or rear security may be identified more specifically as the "front security element," "flank security element," or "rear security element.") The *support element* provides combat and CSSand C2 for the larger organization. Due to such considerations as multiple avenues of approach, a CDR may organize one or more of each of these elements in specific cases

Specialist Elements
In certain situations, a detachment may organize one or more specialist elements. Specialist elements are typically formed around a unit with a specific capability, such as an obstacle-clearing, reconnaissance, or deception. Detachments formed around such specialist elements may or may not have a security or support element depending on their specialty, their location on the battlefield, and the support received from other units. For example, a MSD typically has a reconnaissance and obstacle-clearing element, plus one or two road and bridge construction and repair elements. If an MSD is receiving both security and other support from the infantry or mechanized units preparing to move through the cleared and prepared area, it probably will not have its own support and security elements. In this case, all of the elements will be dedicated to various types of engineer mobility functions.

Preparation for and Execution of the Offense

In the preparation phase, the OPFOR focuses on ways of applying all available resources and the full range of actions to place the enemy in the weakest condition and position possible. CDRs prepare their organizations for all subsequent phases of the offense. They organize the battlefield and their forces and elements with an eye toward capitalizing on conditions created by successful attacks. The principles of preparation are: **Establish contact**; **Make thorough logistics arrangements**; **Modify the plan when necessary**; and, **Rehearse critical actions in priority**.

The degree of preparation often determines the nature of the offense in the execution phase. Successful execution depends on forces that understand their roles in the battle and can swiftly follow preparatory actions with the maximum possible shock and violence and deny the enemy any opportunity to recover. A successful execution phase often ends with transition to the defense in order to consolidate gains, defeat enemy counterattacks, or avoid culmination. In some cases, the execution phase is followed by continued offensive action to exploit opportunities created by the battle just completed. The principles of execution are: **Maintain contact**; **Implement battle drills**; **Modify the plan when necessary**; **Seize opportunities**; and, **Dominate the tempo of combat**.

Types of Offensive Action—Tactical Groups, Divisions, and Brigades

The types of offensive action in OPFOR doctrine are both tactical methods and guides to the design of COAs. An offensive mission may include subordinate units that are executing different offensive and defensive COAs within the overall offensive mission framework.

S2 NOTE: Any division or brigade receiving additional assets from a higher command becomes a DTG or BTG. Therefore, references to a tactical group throughout this chapter may also apply to division or brigade, unless specifically stated otherwise.

S2 NOTE: There is no "movement to contact" in OPFOR doctrine, but they do use the "reconnaissance attack".

Attack

An *attack* is an offensive operation that destroys or defeats enemy forces, seizes and secures terrain, or both. It seeks to achieve tactical decision through primarily military means by defeating the enemy's military power. This defeat does not come through the destruction of armored weapons systems but through the disruption, dislocation, and subsequent paralysis that occurs when combat forces are rendered irrelevant by the loss of the capability or will to continue the fight. Attack is the method of choice for OPFOR offensive action. There are two types of attack: *integrated attack* and *dispersed attack*.

The OPFOR does not have a separate design for "exploitation" as a distinct offensive COA. Exploitation is considered a central part of all integrated and dispersed attacks. The OPFOR does not have a separate design for "pursuit" as a distinct offensive COA. A pursuit is conducted using the same basic COA framework as any other integrated or dispersed attack. The fixing force gains contact with the fleeing enemy force and slows it or forces it to stop while the assault and exploitation forces create the conditions for and complete the destruction of the enemy's mission command and logistics structure or other systems. The OPFOR recognizes that moving forces that make contact must rapidly choose and implement an offensive or defensive COA. The OPFOR methodology for accomplishing this is through battle drills.

Integrated Attack

Integrated attack is an offensive action where the OPFOR seeks military decision by destroying the enemy's will and/or ability to continue fighting through the application of combined arms effects. Integrated attack is often employed when the OPFOR enjoys overmatch with respect to its opponent and is able to bring all elements of offensive combat power to bear. It may also be employed against a more sophisticated and capable opponent, if the appropriate window of opportunity is created or available. See examples below.

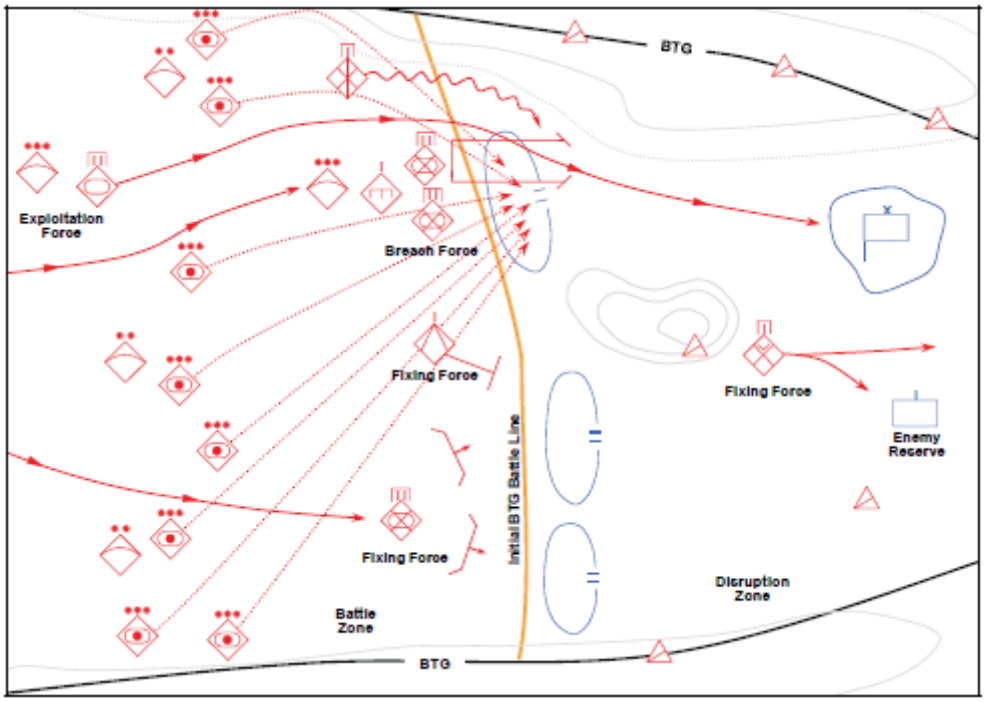


Figure 6-1. Integrated Attack, example 1

Integrated attacks are characterized by–

- Not being focused solely on destruction of ground combat power but often on mission command and logistics.
- Fixing the majority of the enemy's force in place with the minimum force necessary.
- Isolating the targeted subcomponent(s) of the enemy's combat system from his main combat power.

- Using complex terrain to force the enemy to fight at a disadvantage.
- Using deception and other components of INFOWAR to degrade the enemy's situational understanding and ability to target OPFOR formations.
- Using flank attack and envelopment, particularly of enemy forces that have been fixed.

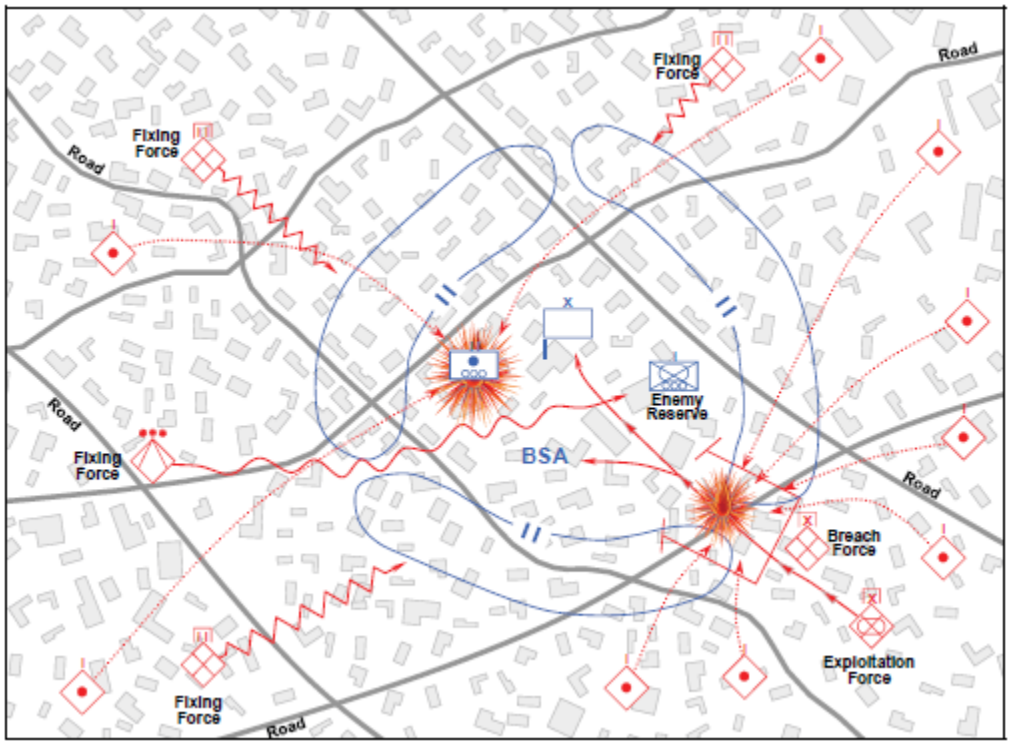


Figure 6-2. Integrated Attack, example 2

The OPFOR prefers to conduct integrated attacks when most or all of the following conditions exist:

- The OPFOR possesses significant overmatch in combat power over enemy forces.
- It possesses at least air parity over the critical portions of the battlefield.
- It is sufficiently free of enemy standoff reconnaissance and attack systems to be able to operate without accepting high levels of risk.

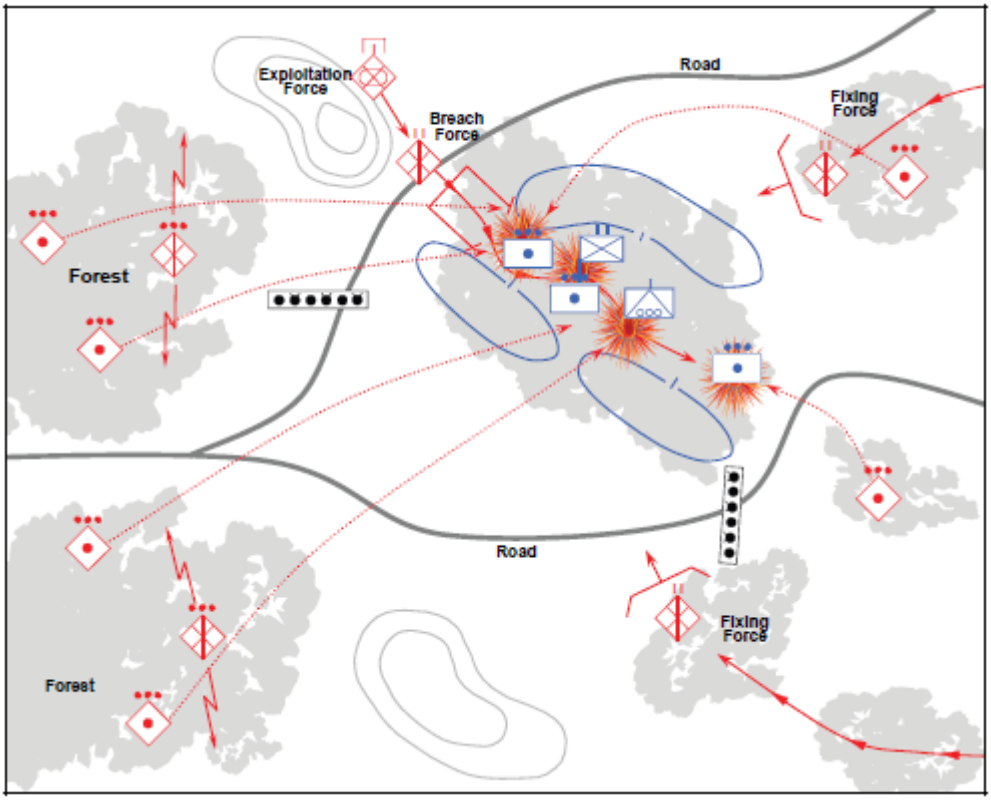


Figure 6-3. Integrated Attack, example 3

An integrated attack often employs fixing, assault, and support forces. A disruption force exists, but is not created specifically for this type of offensive action.

Dispersed Attack

Dispersed attack is the primary manner in which the OPFOR conducts offensive action when threatened by a superior enemy and/or when unable to mass or provide integrated C2 to an attack. This is not to say that the dispersed attack cannot or should not be used against peer forces, but as a rule integrated attack will more completely attain objectives in such situations. Dispersed attack relies on INFOWAR and dispersion of forces to permit the OPFOR to conduct tactical offensive actions while overmatched by precision standoff weapons and imagery and signals sensors. The dispersed attack is continuous and comes from multiple directions. It employs multiple means working together in a very interdependent way. The attack can be dispersed in time as well as space. See examples of dispersed attacks below.

The primary objective of dispersed attack is to take advantage of a window of opportunity to bring enough combined arms force to bear to destroy the enemy's will and/or capability to continue fighting. To achieve this, the OPFOR does not necessarily have to destroy the entire enemy force, but often just destroy or degrade a key component of the enemy's combat system.

Selecting the appropriate component of the enemy's combat system to destroy or degrade is the first step in planning the dispersed attack. This component is chosen because of its importance to the enemy and varies depending on the force involved and the current military situation. In example 1, an enemy force dependent on one geographical point for all of its logistics support and reinforcement would be most vulnerable at that point. Disrupting this activity at the right time and to the right extent may bring about tactical decision on the current battlefield, or it may open further windows of opportunity to attack the enemy's weakened forces at little cost to the OPFOR. In example 2, an enemy force preparing to attack may be disrupted by an OPFOR attack whose purpose is to destroy long-range missile artillery, creating the opportunity for the OPFOR to achieve standoff with its own missile weapons. In example 3, the key component chosen may be the personnel of the enemy force. Attacking and causing mass casualties among infantrymen may delay an enemy offensive in complex terrain while also being politically unacceptable for the enemy command structure.

Dispersed attacks are characterized by–

- Not being focused on complete destruction of ground combat power but rather on destroying or degrading a key component of the enemy's combat system (often targeting enemy mission command and logistics).
- Fixing and isolating enemy combat power.
- Using smaller, independent subordinate elements.
- Conducting rapid moves from dispersed locations.
- Massing at the last possible moment.
- Conducting simultaneous attack at multiple, dispersed locations.
- Using deception and other elements of INFOWAR to degrade the enemy's situational understanding and ability to target OPFOR formations.

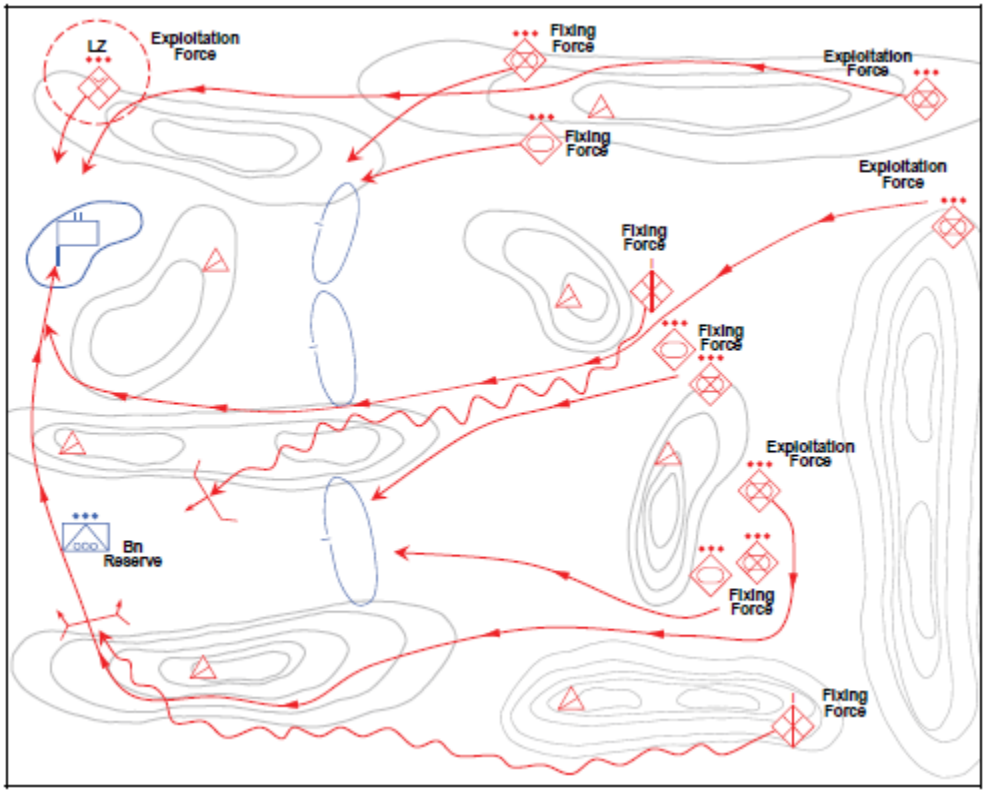


Figure 6-4. Dispersed Attack, example 1

The window of opportunity needed to establish conditions favorable to the execution of a dispersed attack may be one created by the OPFOR or one that develops due to external factors in the OE. When this window must be created, the OPFOR keys on several tasks that must be accomplished:

- Destroy enemy ground reconnaissance.
- Deceive enemy imagery and signals sensors.
- Create an uncertain air defense environment.
- Selectively deny situational awareness.
- Maximize use of complex terrain.

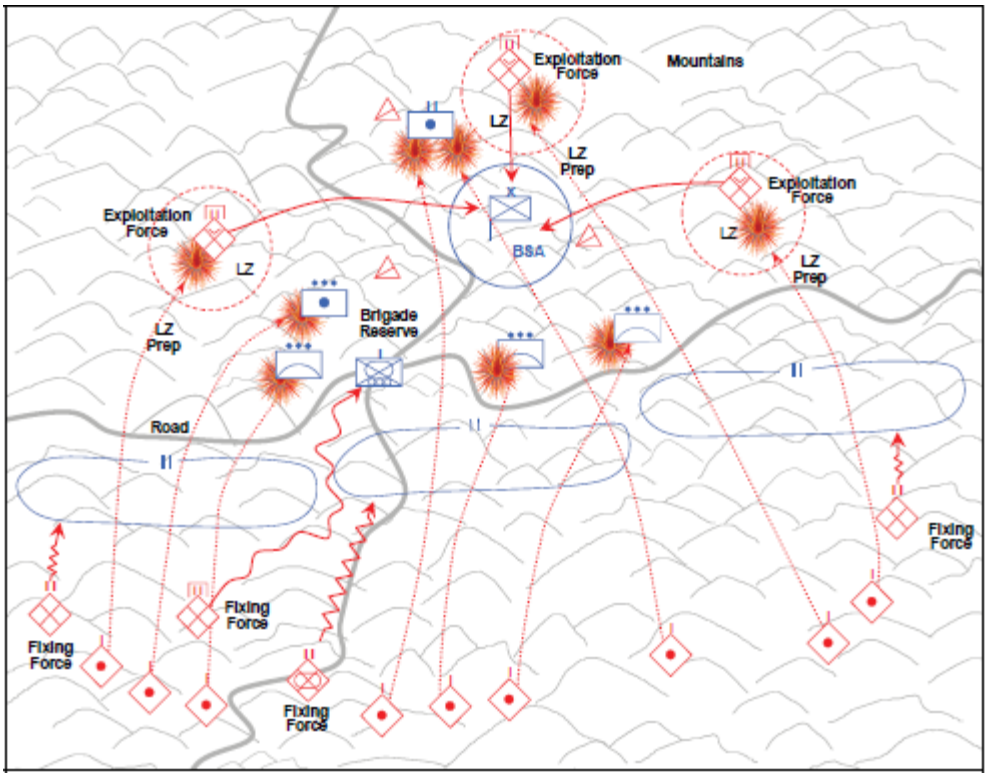


Figure 6-5. Dispersed Attack, example 2

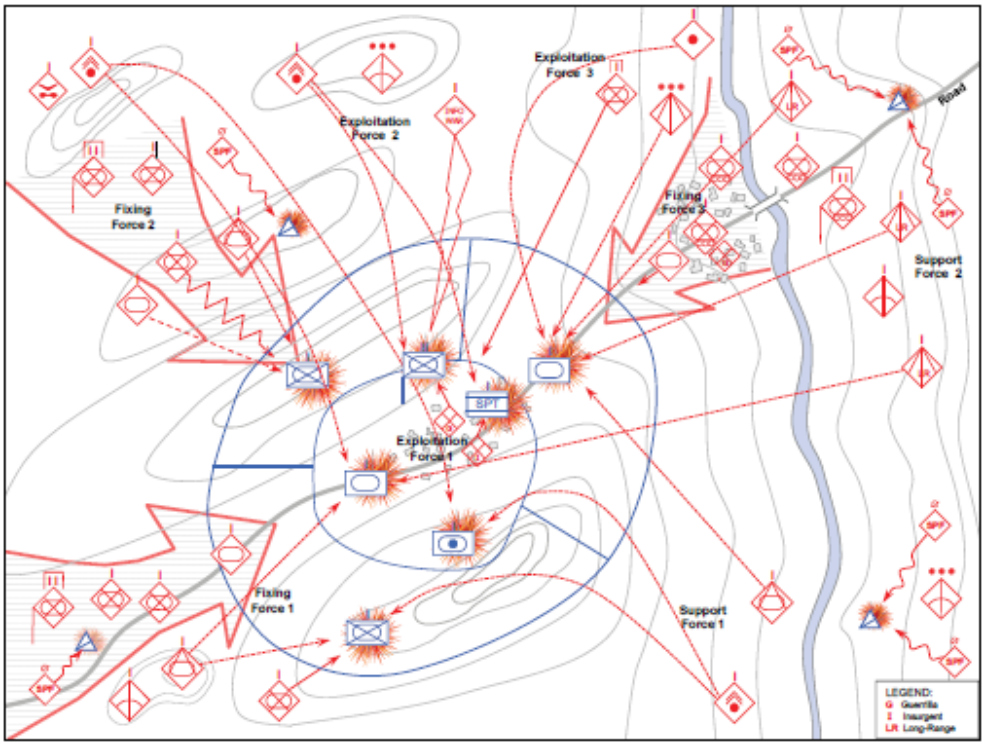


Figure 6-6. Dispersed Attack, example 3

Functional Organization for a Dispersed Attack

A dispersed attack employs various types of functional forces. The tactical group CDR assigns subordinate units functional designations that correspond to their intended roles in the attack.

Enabling Forces
A dispersed attack often employs fixing, assault, and support forces. A disruption force exists, but is not created specifically for this type of offensive action. Deception forces can also play an important role in a dispersed attack.

- **Fixing Force.** The fixing force in a dispersed attack is primarily focused on fixing enemy response forces. Enemy reserves, quick response forces, and precision fire systems that can reorient rapidly will be those elements most capable of disrupting a dispersed attack. Maneuver forces, precision fires, air defense and antiarmor ambushes, situational obstacles, chemical weapons, and EW are well suited to fix these kinds of units and systems. Dispersed attacks often make use of multiple fixing forces separated in time and/or space.
- **Assault Force.** At BTG level, the CDR may employ one or more *assault forces*. The assault force in an integrated attack is charged with destroying a particular part of the enemy force or seizing key positions. Such an assault can create favorable conditions for the exploitation force to rapidly move from dispersed locations and penetrate or infiltrate enemy defenses. An assault force may successfully employ infiltration of infantry to carefully pre-selected points to assist the exploitation force in its penetration. Dispersed attacks often make use of multiple assault forces separated in time and/or space.
- **Support Force.** A support force provides support to the attack by fire; other combat or combat service support; or C2 functions. Smoke and suppressive artillery and rocket fires, combat engineer units, and air-delivered weapons are well suited to this function.

Action Forces
The most common type of action force in an integrated attack is the *exploitation force*. Such a force must be capable, through inherent capabilities or positioning relative to the enemy, of destroying the target of the attack. In one set of circumstances, a tank BDE may be the unit of choice to maneuver throughout the battlefield as single platoons in order to have one CO reach a vulnerable troop concentration or soft mission command node. Alternatively, the exploitation force may be a widely dispersed group of SPF teams set to attack simultaneously at exposed logistics targets. Dispersed attacks often make use of multiple exploitation forces separated in time and/or space, but often oriented on the same objective or objectives.

Limited-Objective Attack

A *limited-objective attack* seeks to achieve results critical to the battle plan or even the operation plan by destroying or denying the enemy key capabilities through primarily military means. The results of a limited-objective attack typically fall short of tactical or operational decision on the day of battle, but may be vital to the overall success of the battle or operation. Limited-objective attacks are common while fighting a stronger enemy with the objective of preserving forces and wearing down the enemy, rather than achieving decision.

The primary objective of a limited-objective attack is a particular enemy capability. This may or may not be a particular man-made system or group of systems, but may also be the capability to take action at the enemy's chosen tempo.

Limited-objective attacks are characterized by-

- Not being focused solely on destruction of ground combat power but often on mission command and logistics.
- Denying the enemy the capability he most needs to execute his plans.
- Maximal use of the systems warfare approach to combat.
- Significant reliance on a planned or seized window of opportunity.

Quite often, the limited-objective attack develops as a situational offense. This occurs when an unclear picture of enemy dispositions suddenly clarifies to some extent and the CDR wishes to take advantage of the knowledge he has gained to disrupt enemy timing. This means that limited-objective attacks are often conducted by reserve or response forces that can rapidly shift from their current posture to strike at the enemy.

There are two types of tactical limited-objective attack: spoiling attack and counterattack. These share some common characteristics, but differ in purpose.

Spoiling Attack

The purpose of a spoiling attack is to preempt or seriously impair an enemy attack while the enemy is in the process of planning, forming, assembling, or preparing to attack. It is designed to control the tempo of combat by disrupting the timing of enemy operations. The spoiling attack is a type of attack to disrupt.

Spoiling attacks do not have to accomplish a great deal to be successful. Conversely, planners must focus carefully on what effect the attack is trying to achieve and how the attack will achieve that effect. In some cases, the purpose of the attack will be to remove a key component of the enemy's combat system. A successful spoiling attack can make this key component unavailable for the planned attack and therefore reduces the enemy's overall chances of success. More typically, the attack is designed to slow the development of conditions favorable to the enemy's planned attack.

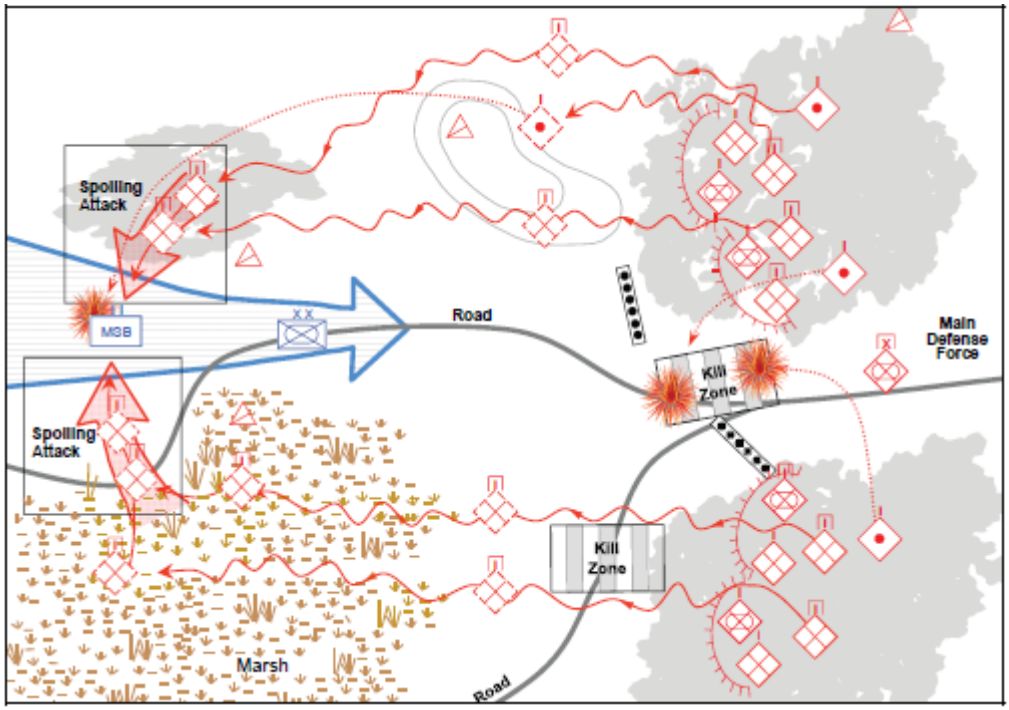


Figure 6-7. Spoiling Attack

Spoiling attacks are characterized by-

- A requirement to have a clear picture of enemy preparations and dispositions.
- Independent, small unit action.
- Highly focused objectives.
- The possibility that a spoiling attack may open a window of opportunity for other combat actions.

The OPFOR seeks to have the following conditions met in order to conduct a spoiling attack:

- RISTA establishes a picture of enemy attack preparations.
- Enemy security, reserve, and response forces are located and tracked.
- Enemy ground reconnaissance in the attack zone is destroyed or rendered ineffective.

Functional Organization for a Spoiling Attack

A spoiling attack may or may not involve the use of enabling forces. If enabling forces are required, the part of the tactical group that actually executes the spoiling attack would be an *exploitation force*. Otherwise, it may be called the *mission force*. The exploitation or mission force will come from a part of the tactical group that is capable of acting quickly and independently to take advantage of a fleeting opportunity. Since the spoiling attack is a type of

attack to disrupt, the exploitation or mission force might come from the disruption force. If more combat power is required, it might come from the main defense force, which would not yet be engaged. A third possibility is that it could come from the tactical group reserve.

Counterattack

A *counterattack* is a form of attack by part or all of a defending force against an enemy attacking force with the general objective of denying the enemy his goal in attacking. It is designed to cause an enemy offensive operation to culminate and allow the OPFOR to return to the offense. A counterattack is designed to control the tempo of combat by returning the initiative to the OPFOR. See figure below for an example of a counterattack.

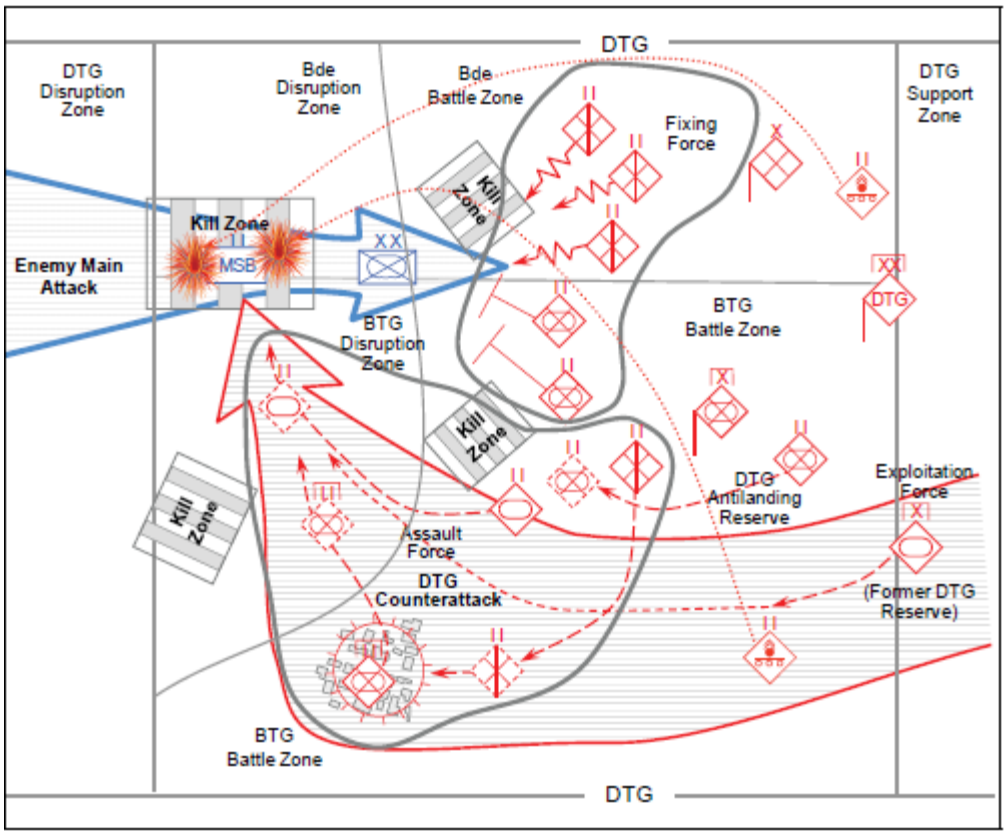


Figure 6-8. Counterattack

Counterattacks are characterized by-

- A shifting in command and support relationships to assume an offensive posture for the counterattacking force.
- A proper identification that the enemy is at or near culmination.
- The planned rapid transition of the remainder of the force to the offense.
- The possibility that a counterattack may open a window of opportunity for other combat actions.

The OPFOR seeks to set the following conditions for a counterattack:

- Locate and track enemy reserve forces and cause them to be committed.
- Destroy enemy reconnaissance forces that could observe counterattack preparations.

Functional Organization for a Counterattack

Functional organization for a counterattack involves many of the same types of forces as for an integrated or dispersed attack. However, the exact nature of their functions may differ due to the fact that the counterattack comes out of a defensive posture.

Enabling Forces
A counterattack often employs fixing, assault, and support forces. The disruption force was generally part of a previous OPFOR defensive posture.

- **Fixing Force.** The fixing force in a counterattack is that part of the force engaged in defensive action with the enemy. These forces continue to fight from their current positions and seek to account for the key parts of the enemy array and ensure they are not able to break contact and reposition. Additionally, the fixing force has the mission of making contact with and destroying enemy reconnaissance forces and any combat forces that may have penetrated the OPFOR defense.
- **Assault Force.** In a counterattack, the assault force (if one is used) is often assigned the mission of forcing the enemy to commit his reserve so that the enemy CDR has no further mobile forces with which to react. If the fixing force has already forced this commitment, the counterattack design may not have an assault force.
- **Support Force.** A support force can provide support to a counterattack by fire; other combat or combat service support; or C2 functions.

Action Forces
The most common type of action force in a counterattack is an exploitation force, and there may be more than one. The exploitation force in a counterattack bypasses engaged enemy forces to attack and destroy the enemy's support before he has time or freedom to react. An exploitation force must have mobility, protection, and firepower.

Tactical Offensive Actions—Detachments, Battalions, and Below

OPFOR CDRs of detachments, BNs, and below select the offensive action best suited to accomplishing their mission. Units at this level typically are called upon to execute one combat mission at a time. Therefore, it would be rare for such a unit to employ more than one type of offensive action simultaneously. At the tactical level, all OPFOR units, organizations, elements, and even plans are dynamic and adapt very quickly to the situation.

S2 NOTE: Any battalion or company receiving additional assets from a higher command becomes a battalion-size detachment (BDET) or company-size detachment (CDET). Therefore, references to a detachment may also apply to battalion or company, unless specifically stated otherwise.

Assault

An assault is an attack that destroys an enemy force through firepower and the physical occupation and/or destruction of his position. An assault is the basic form of OPFOR tactical offensive combat. Therefore, other types of offensive action may include an element that conducts an assault to complete the mission; however, that element will typically be given a designation that corresponds to the specific mission accomplished.

The OPFOR does not have a separate design for "mounted" and "dismounted" assaults, since the same basic principles apply to any assault action. An assault may have to make use of whatever units can take advantage of a window of opportunity, but the OPFOR views all assaults as combined arms actions. See figures below for examples of assault.

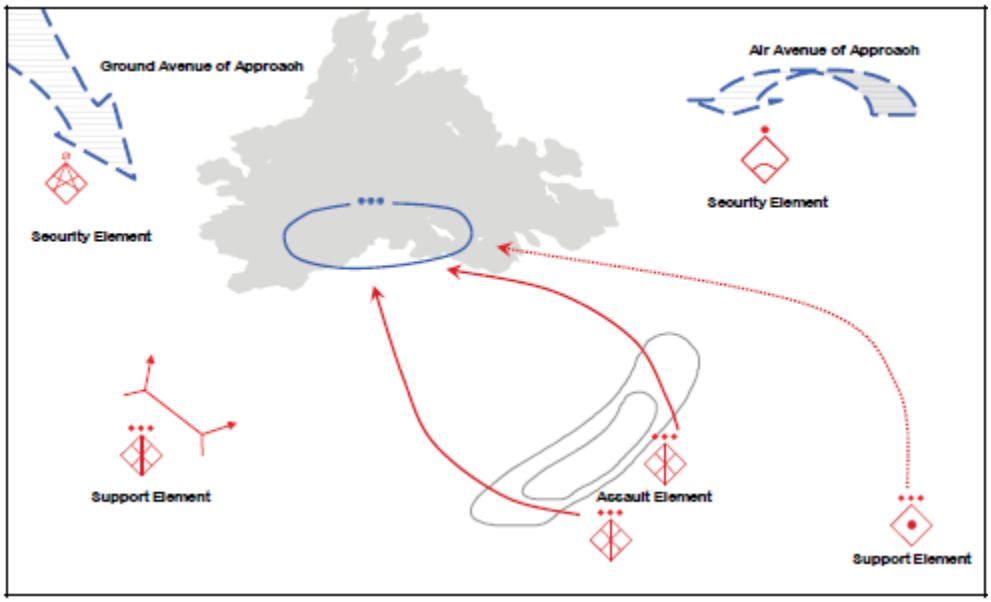


Figure 6-9. Assault, example 1

A detachment conducting an ambush typically is organized into three elements: the *assault element*, the *security element*, and the *support element*.

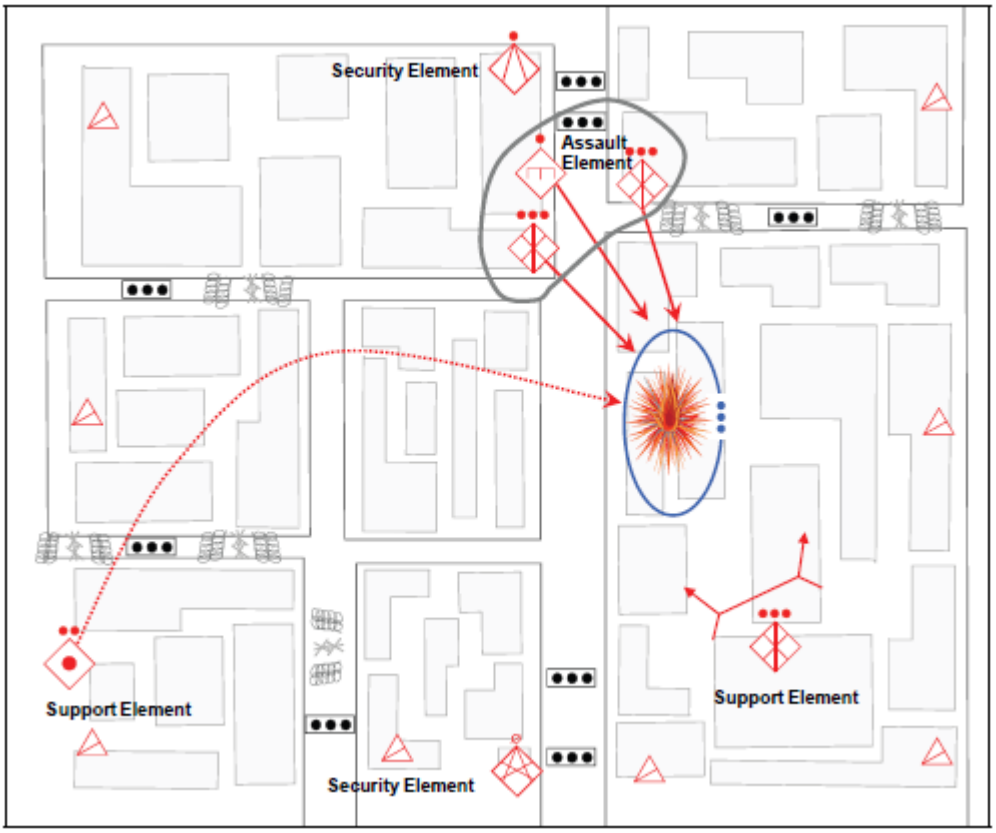


Figure 6-10. Assault, example 2

The detachment conducting an assault is given an AOR in which to operate. A key decision with respect to the AOR will be whether or not a higher HQ is controlling the airspace associated with the assault. The combat order, which assigns the AOR, will often identify the enemy position being assaulted as the primary objective, with associated attack routes and/or axes. Support by fire positions will typically be assigned for use by the support element. The

security element will have battle positions (BP) that overwatch key enemy air and ground avenues of approach with covered and concealed routes to and from those positions.

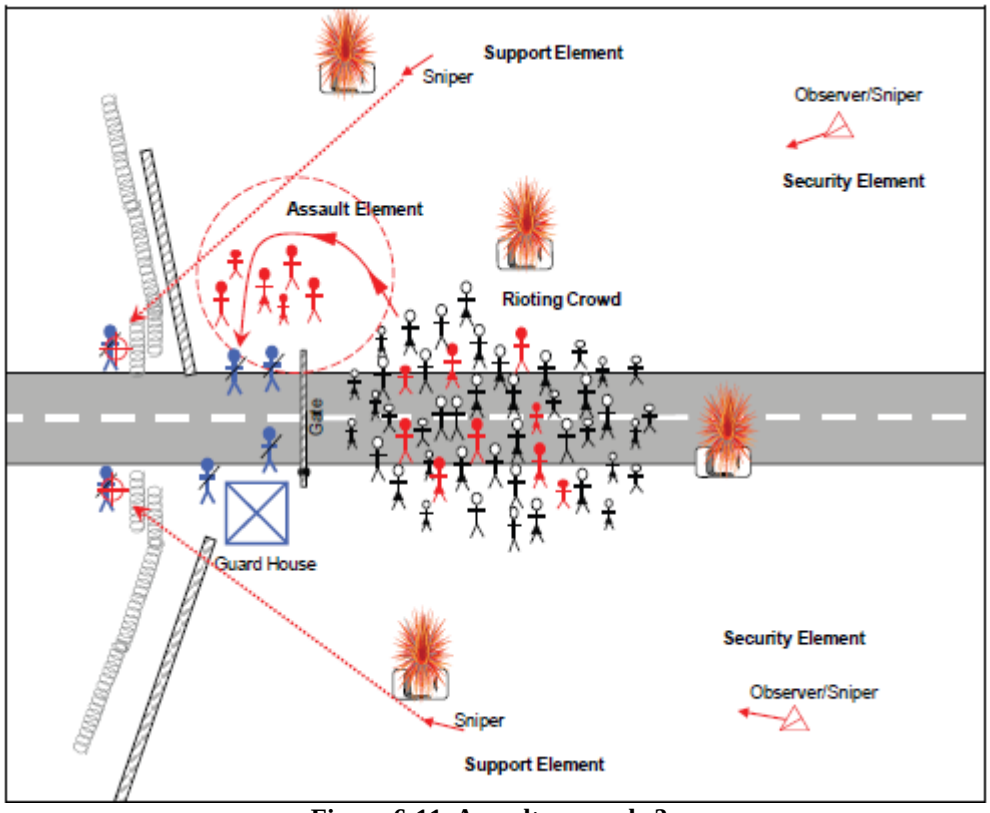


Figure 6-11. Assault, example 3.

Executing an Assault

An assault is the most violent COA a military force can undertake. The nature of an assault demands an integrated combined-arms approach. Indeed, a simple direct assault has a very low chance of success without some significant mitigating factors. Decisive OPFOR assaults are characterized by—

- Isolation of the objective (enemy position) so that it cannot be reinforced during the battle.
- Effective tactical security.
- Effective suppression of the enemy force to permit the assault element to move against the enemy position without receiving destructive fire.
- Violent fire and maneuver against the enemy.

Assault Element

The assault element must be able to maneuver from its assault position to the objective and destroy the enemy located there. It can conduct attack by fire, but this is not an optimal methodology and should only be used when necessary. Typical tactical tasks expected of the assault element are—

- Clear
- Destroy
- Occupy
- Secure
- Seize

Speed of execution is critical to an assault. At a minimum, the assault element must move with all practical speed once it has left its attack position. However, the OPFOR goal in an assault is for all the elements to execute their tasks with as much speed as can be achieved. The OPFOR prefers as much of the action of the three elements of an assault to be simultaneous as possible. OPFOR small units practice the assault continually and have clear battle drills for an assault.

In addition to speed, the assault element will use surprise; limited visibility; complex terrain; and/or C3D. These can allow the assault element to achieve the mission while remaining combat effective.

Security Element

The security element is typically the first element to act in an assault. The security element moves to a position (or positions) where it can deny the enemy freedom of movement along any ground or air avenues of approach that can reinforce the objective or interfere with the mission of the assault element. The security element is equipped and organized such that it can detect enemy forces and prevent them from contacting the rest of the detachment. The security element normally is assigned a screen, guard, or cover task, but may also be called upon to perform other tactical tasks in support of its purpose:

- Ambush
- Block
- Canalize
- Contain
- Delay
- Destroy
- Disrupt
- Fix
- Interdict
- Isolate

Support Element

The support element can have a wide range of functions in an assault. Typically the detachment CDR exercises C2 from within a part of the support element, unless his analysis deems success requires he leads the assault element personally. The support element controls all combat support (CS) and CSS functions as well as any supporting fires. The support element typically does not become decisively engaged but parts of it may employ direct suppressive fires. Tasks typically expected of support elements in the assault are—

- Attack by fire
- Disrupt
- Fix
- Neutralize
- Support by fire
- Canalize
- Contain

Command and Control of an Assault

Typically, the CDR positions himself with the support element and the deputy CDR moves with the assault element, although this may be reversed. The primary function of control of the assault is to arrange units and tasks in time and space so that the assault element begins movement with all capabilities of the support element brought to bear, the security element providing the detachment's freedom to operate and the objective isolated.

Support of the Assault
An assault typically requires several types of support. These can include reconnaissance, fire support, air defense, and INFOWAR.

Ambush

An ambush is a surprise attack from a concealed position, used against moving or temporarily halted targets. Such targets could include truck convoys, railway trains, boats, individual vehicles, or dismounted troops. In an ambush, enemy action determines the time, and the OPFOR sets the place. Ambushes may be conducted to—

- Destroy or capture personnel and supplies.
- Harass and demoralize the enemy.
- Delay or block movement of personnel and supplies.
- Canalize enemy movement by making certain routes useless for traffic.

The OPFOR also uses ambush as a primary psychological warfare tool. The psychological effect is magnified by the OPFOR use of multi-tiered ambushes. A common tactic is to spring an ambush and set other ambushes along the relief or reaction force's likely avenues of approach. Another tactic is to attack enemy medical evacuation assets, especially if the number of these assets is limited. The destruction of means to evacuate wounded instills a sense of tentativeness in the enemy soldiers because they realize that, should they become wounded or injured, medical help will not be forthcoming. Successful ambushes usually result in concentrating the majority of movements to principal roads, railroads, or waterways where targets are more vulnerable to attack by other forces. Key factors in an ambush are—

- Surprise.
- Control.
- Coordinated fires and shock (timing).
- Simplicity.
- Discipline.
- Security (and enemy secondary reaction).
- Withdrawal.

Functional Organization for an Ambush

Similar to an assault, a detachment conducting an ambush is typically organized into three elements: the *ambush element*, the *security element*, and the *support element*. There may be more than one of each of these types of element.

Ambush Element
The *ambush element* of an ambush has the mission of attacking and destroying enemy elements in the kill zone(s). The ambush element conducts the main attack against the ambush target that includes halting the column, killing or capturing personnel, recovering supplies and equipment, and destroying unwanted vehicles or supplies that cannot be moved.

Security Element
The *security element* of an ambush has the mission to prevent enemy elements from responding to the ambush before the main action is concluded. Failing that, it prevents the ambush element from becoming decisively engaged by providing early warning. Security elements are placed on roads and trails leading to the ambush site to warn the ambush element of the enemy approach. These elements isolate the ambush site using roadblocks, other ambushes, and outposts. They also assist in covering the withdrawal of the ambush element from the ambush site. The distance between the security element and the ambush element is dictated by terrain.

Support Element
The *support element* of an ambush has the same basic functions as that of an assault. It is quite often involved in supporting the ambush element with direct and/or indirect fires.

Types of Ambush

There are three types of OPFOR ambush - annihilation, harassment, or containment - based on the desired effects and the resources available. OPFOR frequently employ ambushes because they have a great chance of success and provide force protection. The OPFOR conducts ambushes to kill or capture personnel, destroy or capture equipment, restrict enemy freedom of movement, and collect information and supplies.

Annihilation Ambush

The purpose of an *annihilation ambush* is to destroy the enemy force. These are violent attacks designed to ensure the enemy's return fire, if any, is ineffective. Using direct, or indirect, 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 AT weapons.

The support and ambush elements kill enemy personnel and destroy equipment within the kill zone by concentrated fires. The ambush element remains in covered and concealed positions until the enemy is rendered combat ineffective. Once that occurs, the ambush element secures the kill zone and eliminates any remaining enemy personnel that pose a threat. The ambush 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 ambush element withdraws first, then the support element, and lastly the security element. The entire ambush force reassembles at a predetermined location and time. For examples of annihilation ambushes see figures below.

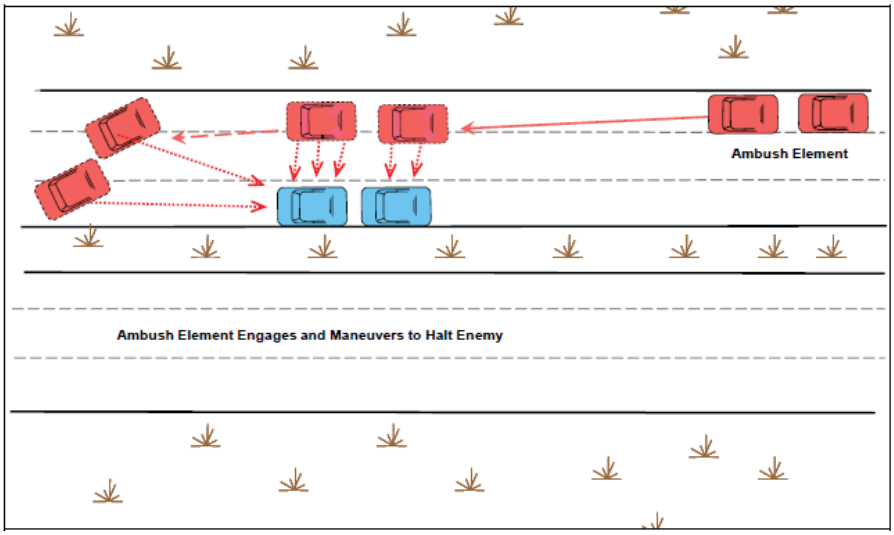


Figure 6-12. Annihilation Ambush, example 1

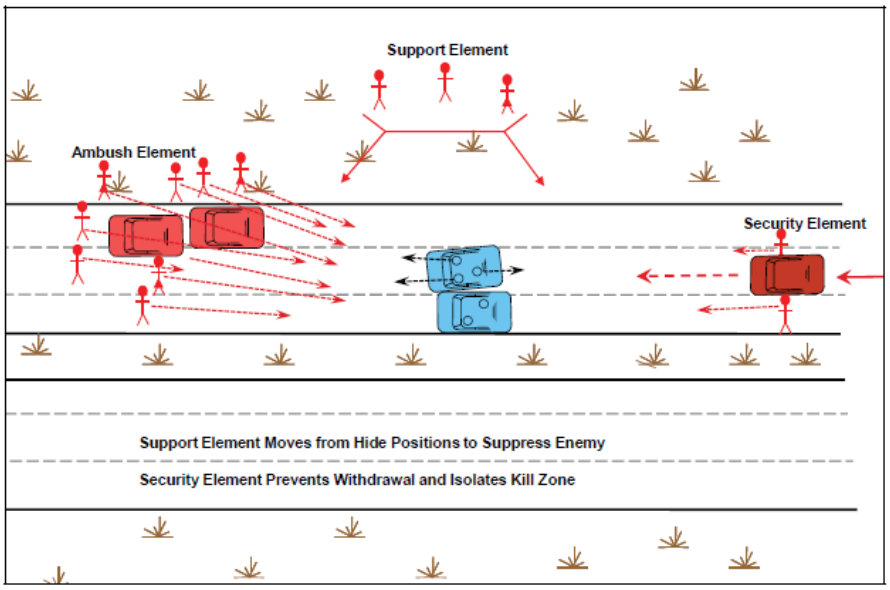


Figure 6-13. Annihilation Ambush, example 2

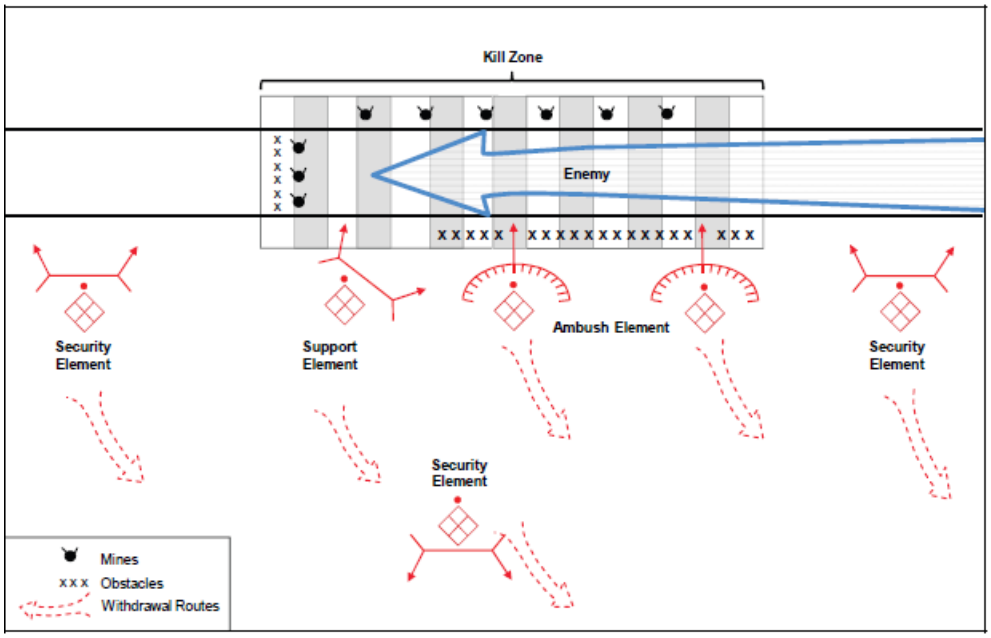


Figure 6-14. Annihilation Ambush, example 3

Annihilation ambushes in complex terrain, including urban environments, often involve task organizations that the OPFOR calls "hunter-killer (H/K) teams." The H/K team structure is extremely lethal and is especially effective for close fighting in such environments. Although other companies may be used as well, generally, infantry companies are augmented and task-organized into these H/K teams. When task organized to ambush armored vehicles, they may be called "antiarmor H/K teams" or "H/K infantry antiarmor teams."

At a minimum, each H/K infantry antiarmor team is composed of gunners of infantry antiarmor weapons, a machinegunner, a sniper, and one or more riflemen. The H/K teams use command detonated, controllable, and side-attack mines (AT, anti-vehicle, and antipersonnel) in conjunction with predetermined artillery and mortar fires. The example below is an annihilation ambush conducted by H/K teams in a complex, urban environment.

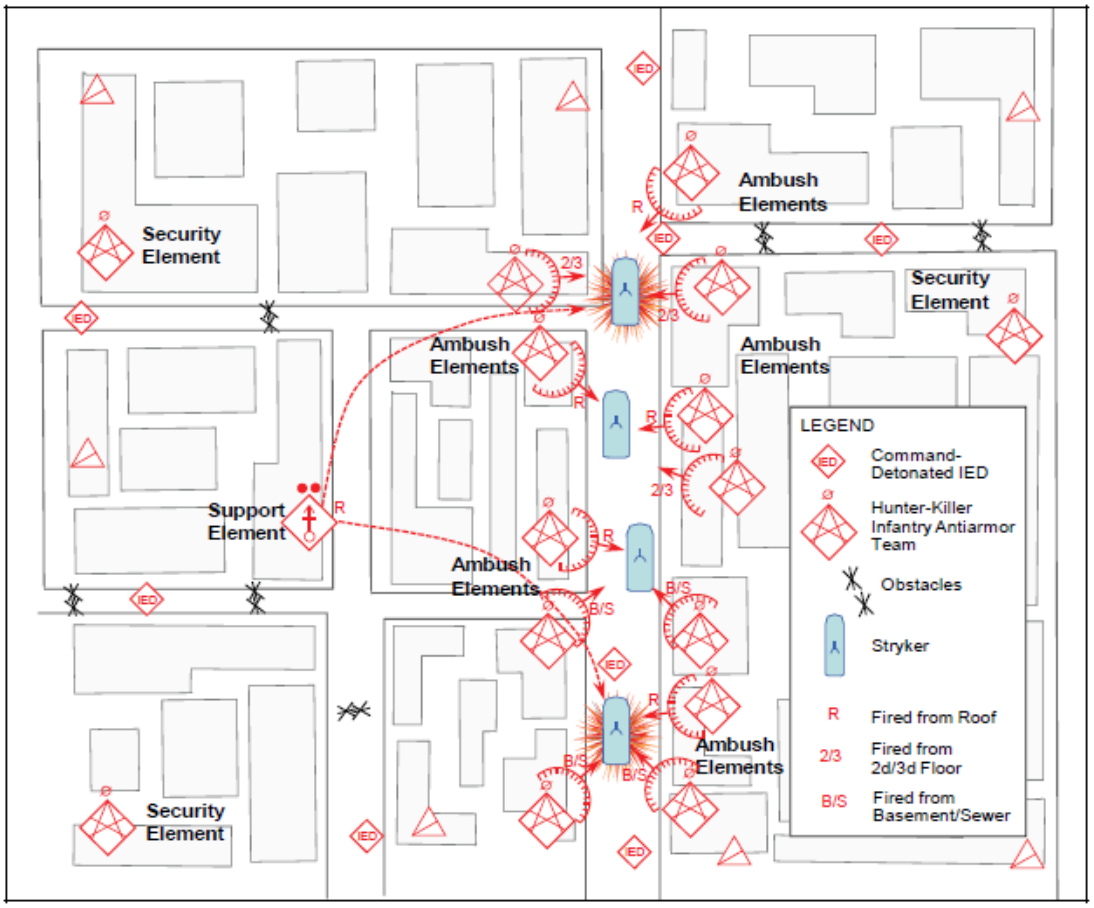


Figure 6-15. Annihilation Ambush using infantry antiarmor (hunter-killer) teams, example 4

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. The OPFOR 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. Compared to an annihilation ambush, the detachment typically conducts a harassment ambush at a greater distance from the enemy, up to the maximum effective range of its weapons. See the example of a harassment ambush below.

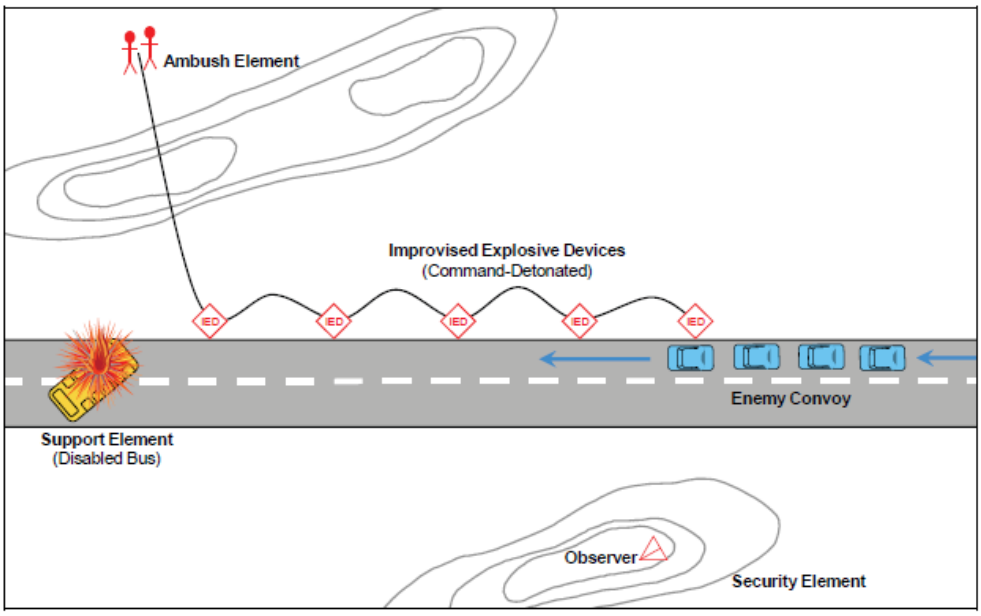


Figure 6-16. Harassment Ambush

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 or another ambush. The ambush element may 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.

Obstacles may be 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 ambush force may erect multiple, mutually supporting obstacles covered by direct and indirect fires.

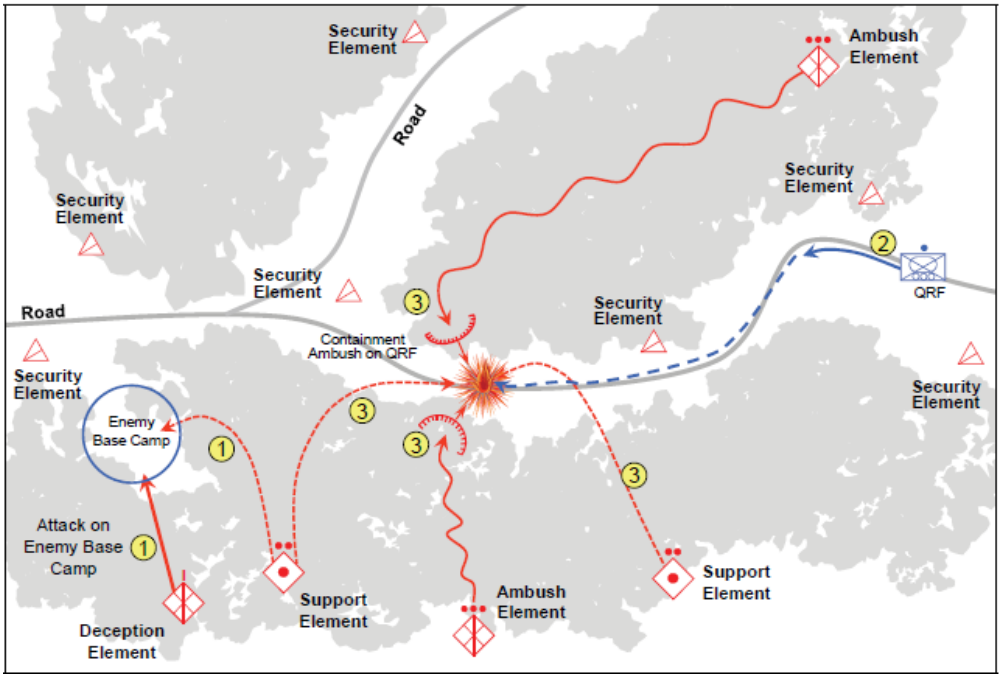


Figure 6-17. Containment Ambush, example 1

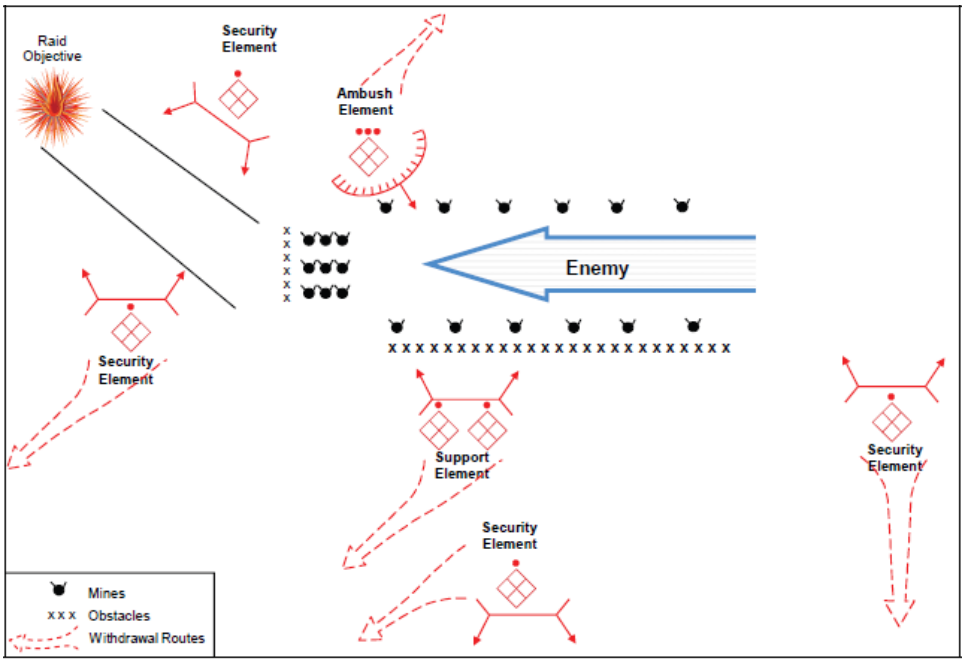


Figure 6-18. Containment Ambush, example 2

Raid

A raid is an attack against a stationary target for the purposes of its capture or destruction that culminates in the withdrawal of the raiding force to safe territory. Raids can also be used to secure information and to confuse or deceive the enemy. The keys to the successful accomplishment of any are raid surprise, firepower, and violence. The raid ends with a planned withdrawal upon completion of the assigned mission. Raids are characterized by-

- Destroying or damage key systems or facilities (such as command posts [CP], communication facilities, supply depots, radar sites), providing or denying critical information, or securing hostages or prisoners.
- Destroy, damage, or capture supplies or lines of communications (LOC).
- Support the INFOWAR plan. Raids can distract attention from other OPFOR actions, to keep the enemy off balance, and to cause the enemy to deploy additional units to protect critical sites.
- OPFOR sensor(s) with capability and mission to find and track the target. Sensors are often ground reconnaissance, but may include UAVs or satellites.
- A C2 method to link raiding force and sensors.
- Supporting operation(s) - usually primarily INFOWAR to create window of opportunity for raiding force to operate.

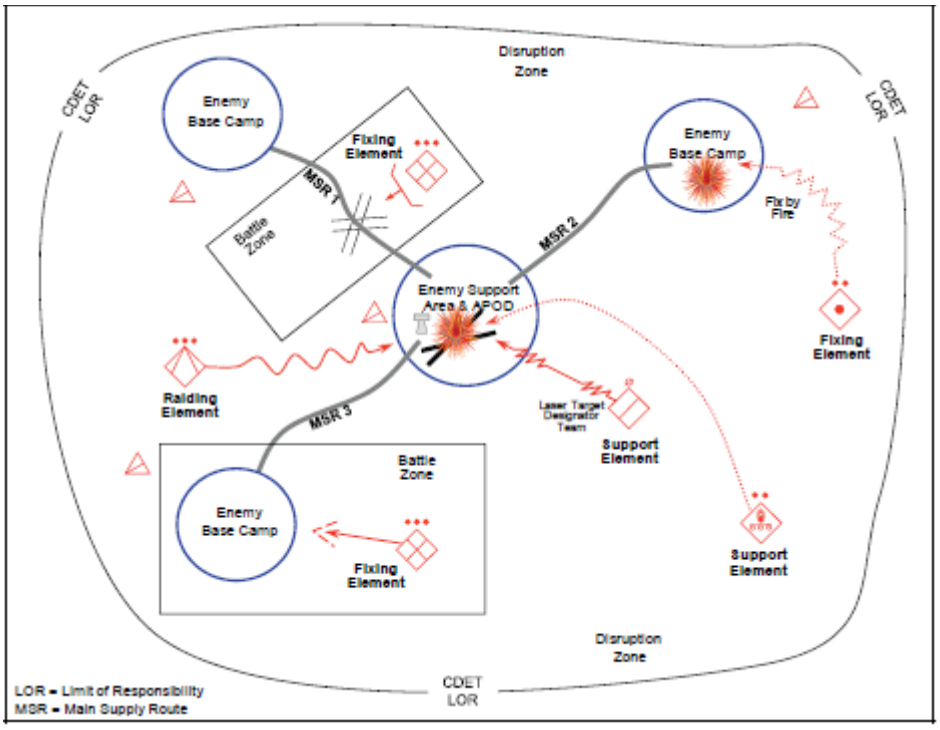


Figure 6-19. Raid, example 1

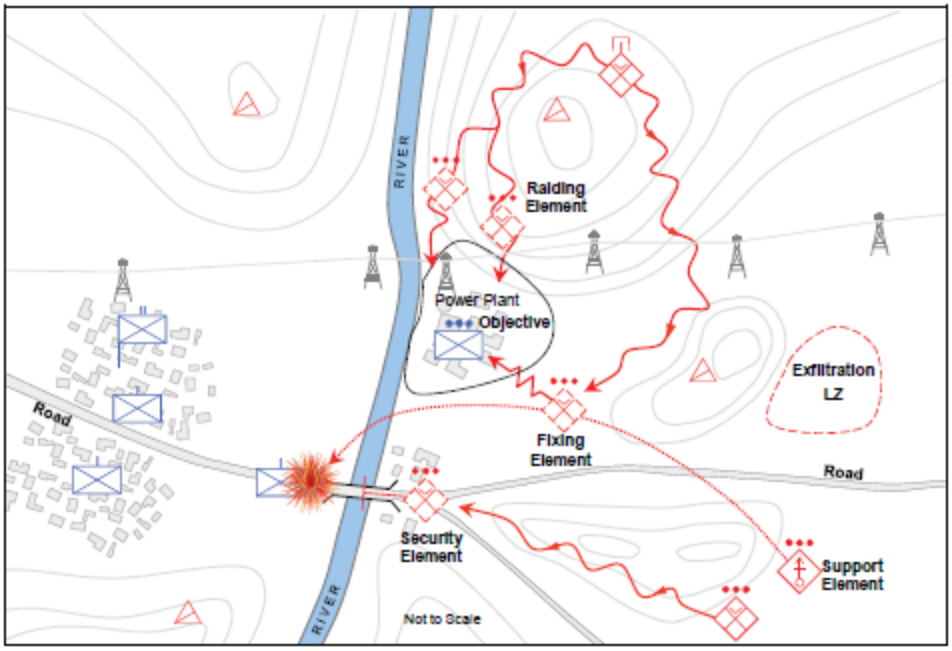


Figure 6-20. Raid, example 2

Functional Organization for a Raid

The size of the raiding force depends upon its mission, the nature and location of the target, and the enemy situation. The raiding force may vary from a detachment attacking a large supply depot to an SPF team attacking a checkpoint or a portion of unprotected railroad track. Regardless of size, the raiding force typically consists of three elements: raiding, security, and support. It may involve other functional elements, such as a fixing element.

Raiding Element(s)
The raiding element executes the major task ensuring the success of the raid. It is charged with the actual destruction or seizure of the target of the raid.

Security Element(s)
The primary threat to all elements of a raiding force is being discovered and defeated by enemy security forces prior to execution of the raid. The security element in a raid is primarily focused on fixing enemy security and response forces or the enemy's escape from the objective area. The security element is equipped and organized such that it can detect enemy forces and prevent them from contacting the rest of the detachment. The security element also covers the withdrawal of the raiding element and act as a rear guard for the raiding force. The size of the security element depends upon the size of the enemy's capability to intervene and disrupt the raid.

The task of a security element in a raid is to occupy enemy security and response forces and force the enemy to focus on parts of the battlefield away from the raid. Security elements deploy to locations where they can deny the enemy freedom of movement along any ground or air avenues of approach that can reinforce the objective or interfere with the mission of the raiding element. The security element normally gets a screen, guard or cover overall mission, but may also be called upon to perform other tactical tasks in support of its purpose:

- Ambush.
- Block.
- Canalize.
- Contain.
- Destroy.
- Delay.
- Disrupt.
- Fix.
- Interdict.
- Isolate.

Support Element(s)
The support element serves as an enabling function and assists in setting the conditions for the success of the raid. This support may take several forms. The support element provides fire support, logistics support, reinforcements, to the raiding and security elements. Support may also include armor, air defense, engineer, and INFOWAR. The detachment CDR normally controls the raid from within the support element. If needed, support elements may assist the raiding element(s) in reaching the target. They can also execute one or more complementary tasks, such as—

- Eliminating guards.
- Breaching and removing obstacles to the objective.
- Conducting diversionary or holding actions.
- Canalizing enemy forces.
- Providing fire support.

S2 NOTE: The reconnaissance attack is the most ambitious (and least preferred) method to gain information. When other means of gaining information have failed, a detachment can undertake a reconnaissance attack.

Reconnaissance Attack

A *reconnaissance attack* is a tactical offensive action that locates moving, dispersed, or concealed enemy elements and either fixes or destroys them. It may also be used by the CDR to gain information about the enemy's location, dispositions, military capabilities, and quite possibly his intentions. The OPFOR recognizes that an enemy will take significant measures to prevent the OPFOR from gaining critical intelligence. Therefore, quite often the OPFOR will have to fight for information, using an offensive operation to penetrate or circumvent the enemy's security forces to determine who and/or what is located where or doing what. Key factors in the reconnaissance attack are situational awareness, contact conditions, and tempo. Depending on the situation, the detachment CDR organizing a

reconnaissance attack may designate reconnaissance, security, and/or action elements. There may be more than one of each type. The CDR may also form various types of support elements.

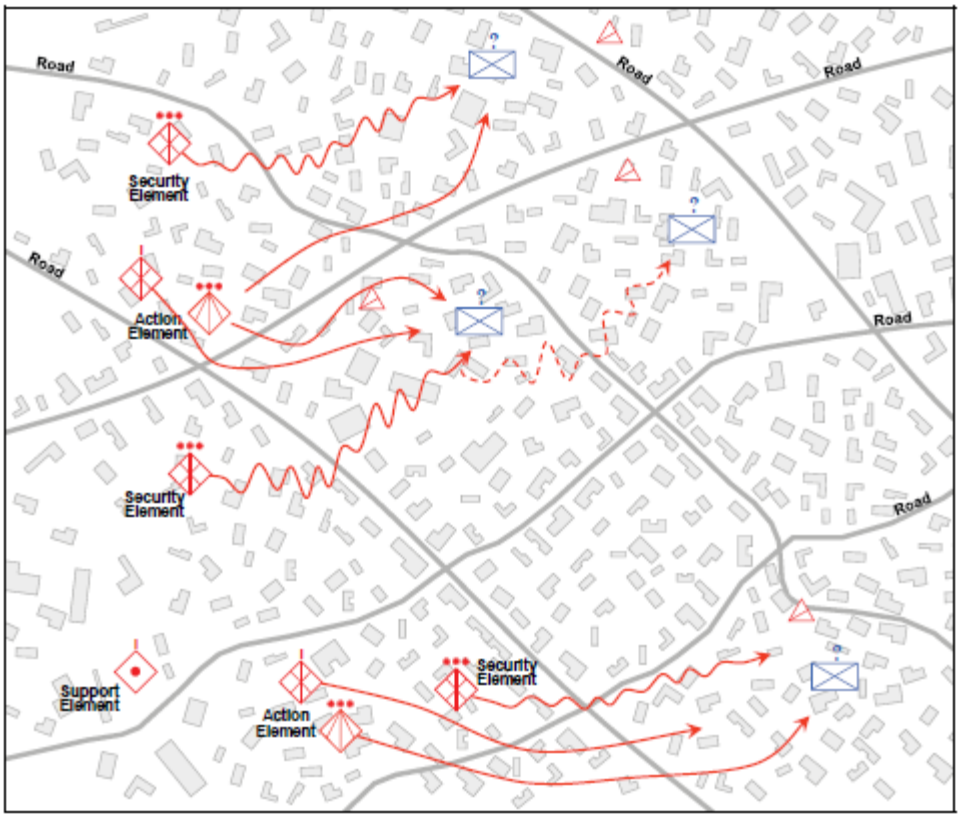


Figure 6-21. Reconnaissance attack

Chapter 7

OPFOR Tactics – Defense

This chapter describes the OPFOR's concept for tactical defensive operations. More information can be found in the 7-100 series manuals that can be downloaded from the Army Training Network at https://atn.army.mil/dsp_template.aspx?dpID=311.

While the OPFOR sees the offense as the decisive form of military action, it recognizes defense as the stronger form of military action, particularly when faced with a superior foe. It may be sufficient for the OPFOR simply not to lose. Even when an operational-level command as a whole is conducting an offensive operation, it is likely that one or more tactical-level subordinate units may be executing defensive missions to preserve offensive combat power in other areas, to protect an important formation or resource, or to deny access to key facilities or geographic areas. The same is true of subordinate units within a tactical-level command. CDRs and staffs do not approach the defense with preconceived templates.

Defensive battles are designed to achieve the goals of the battle or operation plan through active measures while preserving combat power. A tactical command ensures that its subordinate commands thoroughly understand both the overall goals of the battle plan and the specific purpose of a particular battle they are about to fight. In this way, subordinate commands can continue to fight the battle without direct control by a higher HQ. The purpose of any given defensive battle depends on the situation, resources, and mission—as determined through the decision-making process. The OPFOR recognizes four general purposes of tactical defensive missions:

- Protect personnel and equipment.
- Restrict freedom of movement.
- Control key terrain.
- Gain time.

These general purposes serve as a guide to understanding the design of a defensive mission and not as a limit placed on a CDR as to how he makes his intent and aim clear. These are not the only possible purposes of tactical missions but are the most common.

Planning the Defense

For the OPFOR, the key elements of planning defensive missions are–

- Determining the objective of the defensive action
- Determining the level of planning possible (planned versus situational defense)
- Organizing the battlefield
- Organizing forces and elements by function
- Organizing INFOWAR activities in support of the defense

Defensive actions are not limited solely to attrition-based tactics. Some actions against a superior and/or equal force will typically include the increased use of–

- Infiltration to conduct spoiling attacks and ambushes.
- Mitigation of enemy capabilities using INFOWAR, especially perception management and computer attack, in support of defensive operations.
- Use of affiliated forces for reconnaissance, counterreconnaissance, security, and attacks against key enemy systems and forces.

Planned Defense

A planned defense is a defensive mission or action undertaken when there is sufficient time and knowledge of the situation to prepare and rehearse forces for specific tasks. Typically, the enemy is in a staging or assembly area and in a known location and status. Key considerations in defensive planning are–

- Determining which enemy forces will attack, when, and how.
- Determining enemy weakness and how to create and/or exploit them.
- Determining key elements of the enemy's combat system and interdict them, thereby mitigating overall enemy capability.
- Determining defensive characteristics of the terrain. Selecting key positions in complex terrain from which to dominate surrounding avenues of approach.
- Determining the method that will deny the enemy his tactical objectives.
- Developing a plan for RISTA that locates and tracks major enemy formations, and determines enemy patterns of operations, intentions, timeframes, and probable objectives.
- Creating or taking advantage of a window of opportunity that frees friendly forces from any enemy advantages in precision standoff and situational awareness.
- Planning all aspects of an integrated counterattack making use of all means available, including INFOWAR, UAVs, SPF, and/or affiliated irregular forces.

Situational Defense

The OPFOR may also conduct a *situational* defense. It recognizes that the modern battlefield is chaotic. Circumstances will often change so that the OPFOR is not afforded the opportunity to conduct offensive action, as originally planned, thus forcing it to adopt a defensive posture. If the OPFOR determines that a fleeting, situational window of opportunity is closing, it may assume a situational defense. Although detailed planning and preparation greatly mitigate risk, they are often not achievable if enemy action has taken away the initiative. The following are examples of conditions that might lead to a situational defense:

- The enemy is unexpectedly striking an exposed key OPFOR unit, system, or capability.
- The enemy is conducting a spoiling attack to disrupt OPFOR offensive preparations.
- An OPFOR unit makes contact on unfavorable terms for subsequent offensive action.
- The enemy gains or regains air superiority sooner than anticipated.
- An enemy counterattack was not effectively fixed

In a situational defense, the CDR develops his assessment of the conditions rapidly and without a great deal of staff involvement. He provides a basic COA to the staff, which then quickly turns that COA into an executable combat order. Even more than other types of OPFOR defensive action, the situational defense relies on implementation of battle drills by subordinate tactical units.

Functional Organization of Forces for the Defense—Tactical Groups, Divisions, and Brigades

In his combat order, the CDR of a DIV, DTG, BDE, or BTG also specifies the initial functional organization of the forces within his level of command. However, the organization of forces can shift dramatically during the course of a battle. For example, a unit that initially was part of a disruption force may eventually occupy a BP within the battle zone and become part of the main defense force or act as a reserve.

Each of the separate functional forces has an identified CDR. The force CDR is responsible to the DIV, BDE, or tactical group CDR to ensure that combat preparations are made properly and to take charge of the force during the operation. This frees the higher-level CDR from decisions specific to the force's mission. Even when subordinates of a tactical group have responsibility for parts of the tactical group disruption zone, there is still an overall tactical group disruption force CDR.

Disruption Force

The OPFOR CDR may create a single cohesive disruption force with a single overall CDR or he may create multiple (probably dispersed) forces operating in the disruption zone with numerous CDRs. Activities in the disruption zone may be independent of each other, integrated, continuous, or sporadic.

The size and composition of forces in the disruption zone depends on the level of command involved, the CDR's concept of the battle, and the circumstances in which the unit adopts the defense. The function of the disruption

force is to prevent the enemy from conducting an effective attack. Therefore, the size of the disruption force is not linked to any specific echelon, but rather to the function. A tactical CDR will always make maximum use of stay-behind forces and affiliated forces existing within his AOR. Subordinate CDRs can employ forces in a higher command's disruption zone with tactical group approval.

While a DTG disruption force is typically a BTG, a BTG disruption force is typically an IMD. However, a disruption force has no set OB and will be whatever available unit(s) best fit the CDRs needs. The disruption force may contain–

- Ambush teams (ground and air defense)
- Long-range reconnaissance patrols and/or SPF teams
- RISTA assets and forces
- CRD
- Artillery systems
- Target designation teams
- Elements of affiliated forces (such as guerrillas, terrorists, insurgents, or criminals)
- Antilanding reserves

The purpose of the disruption force is to prevent the enemy from conducting an effective attack. The disruption force does this by initiating the attack on key components of the enemy's combat system. Successful attack of designated components or subsystems begins the disaggregation of the enemy's combat system and creates vulnerabilities for exploitation in the battle zone. Skillfully conducted disruption operations will effectively deny the enemy the synergy of effects of his combat system.

The disruption force may also have a counterreconnaissance mission. It may selectively destroy or render irrelevant the enemy's RISTA forces and deny him the ability to acquire and engage OPFOR targets with deep fires. It employs OPFOR RISTA assets to locate and track enemy RISTA forces and then directs killing systems to destroy them. For this purpose, the disruption force may include operational-level RISTA assets, SPF, and helicopters. There will be times, however, when the OPFOR wants enemy reconnaissance to detect something that is part of the deception plan. In those cases, the disruption force will not seek to destroy all of the enemy's RISTA assets.

The disruption force may deceive the enemy as to the location and configuration of the main defense in the battle zone, while forcing him to show his intent and deploy early. Some other results of actions in the disruption zone can include delaying the enemy to allow time for preparation of the defense or a counterattack, canalizing the enemy onto unfavorable axes, or ambushing key systems and vulnerable troop concentrations.

Main Defense Force

The main defense force is the functional force charged with execution of the primary defensive mission. It operates in the battle zone to accomplish the purpose of the defense. (During a maneuver defense, the main defense force is typically broken down into a contact force and a shielding force.)

Protected Force

The protected force is the force being kept from detection or destruction by the enemy. It may be in the battle zone or the support zone.

Security Force

The security force conducts activities to prevent or mitigate the effects of hostile actions against the overall command and/or its key components. If the CDR chooses, he may charge this security force with providing force protection for the entire AOR, including the rest of the functional forces; logistics and administrative elements in the support zone; and other key installations, facilities, and resources. The security force may include various types of units (infantry, SPF, counterreconnaissance, and signals reconnaissance) to focus on enemy special operations and long-range reconnaissance forces operating throughout the AOR. It can also include Internal Security Forces with the mission of protecting the overall command from attack by hostile insurgents, terrorists, and special operations

forces. The security force may also be charged with mitigating the effects of WMD. The security force CDR can be given control over one or more reserve formations, such as the antilanding reserve.

Counterattack Forces

A defensive battle may include a planned counterattack scheme. This is typical of a maneuver defense, but could also take place within an area defense. In these cases, the tactical CDR will designate one or more counterattack forces. He will also shift his task organization to create a counterattack force when a window of opportunity opens that leaves the enemy vulnerable to such an action. The counterattack force can have within it fixing, mission, and exploitation forces. It will have the mission of causing the enemy's offensive operation to culminate. The tactical group CDR uses counterattack forces to complete the defensive mission and regain the initiative for the offense.

Types of Reserves

At the CDR's discretion, forces may be held out of initial action so that he may influence unforeseen events or take advantage of developing opportunities. He may employ a number of different types of reserve forces of varying strengths, depending on the situation.

Maneuver Reserve
The size and composition of a reserve force is entirely situation-dependent. However, the reserve is normally a force strong enough to respond to unforeseen opportunities and contingencies at the tactical level. A reserve may assume the role of counterattack force to deliver the final blow that ensures the enemy can no longer conduct his preferred COA. Reserves are almost always combined arms forces.

A reserve force will be given a list of possible missions for rehearsal and planning purposes. The staff assigns to each of these missions a priority, based on likelihood that the reserve will be called upon to execute that mission. Some missions given to the reserve may include−

- Conducting a counterattack. (The counterattack goal is not limited to destroying enemy forces, but may also include recovering lost positions or capturing positions advantageous for subsequent combat actions.)
- Conducting counterpenetration (blocking or destroying enemy penetrations).
- Conducting antilanding missions (eliminating vertical envelopments).
- Assisting forces heavily engaged on a defended line to break contact and withdraw.
- Acting as a deception force.

Antitank Reserve (ATR)
OPFOR CDRs faced with significant armored threats may keep an ATR. It is generally an AT unit and often operates in conjunction with an OD. Based on the availability of AT and engineer assets, a DIV- or BDE-size unit may form more than one ATR.

Antilanding Reserve (ALR)
Because of the potential threat from enemy airborne or heliborne troops, a CDR may designate an ALR. While other reserves can perform this mission, the CDR may create a dedicated ALR to prevent destabilization of the defense by vertical envelopment of OPFOR units or seizure of key terrain. ALRs will be resourced for rapid movement to potential drop zones (DZs) and landing zones (LZs). The ALR CDR will have immediate access to the operational and tactical intelligence system for early warning of potential enemy landing operations. ALRs typically include maneuver, air defense, and engineer units, but may be allocated any unit capable of disrupting or defeating an airborne or heliborne landing, such as smoke or INFOWAR. ALRs assume positions prepared to engage the enemy primary DZ or LZ as a kill zone. They rehearse and plan for rapid redeployment to other suspected DZs or LZs.

Special Reserves
In addition to their ODs, units may form an engineer reserve of earthmoving and obstacle-creating equipment. A CDR can deploy this reserve to strengthen defenses on a particularly threatened axis during the course of the battle. A unit threatened by enemy use of WMD may also form a chemical defense reserve.

Deception Force
When the INFOWAR plan requires the creation of nonexistent or partially existing formations, these forces will be designated deception forces in close-hold executive summaries of the battle plan. Wide-distribution copies of the

plan will make reference to these forces according to the designation given them in the deception story. The deception force in the defense is typically given its own command structure, both to replicate the organization(s) necessary to the deception story and to execute the multidiscipline deception required to replicate an actual military organization. Tactical group CDRs can use deception forces to replicate subordinate tactical group and detachment command structures, in order to deny enemy forces information on battle plans for the defense.

Functional Organization of Elements for the Defense—Detachments, Battalions, and Below

Detachments, BNs, and companies employ a similar but different scheme for organizing functional elements than the functional force methodology used by tactical groups. This is because the OPFOR tends to use detachments to accomplish a single tactical task rather than a multi-task mission.

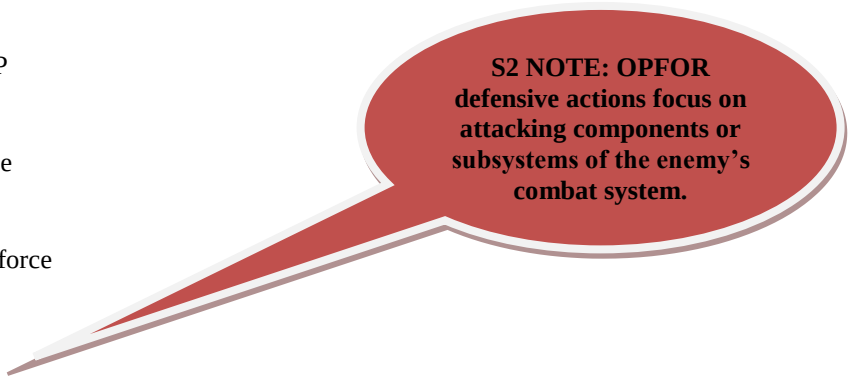
The standard functional organization of a detachment for defense is into four parts: the **disruption element**, the **main defense element**, the **support element**, and the **reserve element**. There may also be specialist elements.

The disruption element of a detachment can provide security for the detachment, prevents the enemy from influencing mission accomplishment, and prevents the enemy from conducting an effective attack by targeting key systems and subcomponents of the enemy's combat system in the disruption zone. The main defense element accomplishes the detachment's tactical task. The support element provides combat and CSS and C2 for the detachment. The reserve element provides the defender with the tactical flexibility to influence unforeseen events or to take advantage of developing opportunities.

In certain situations, a detachment may organize one or more specialist elements. Specialist elements are typically formed around a unit with a specific capability such as an obstacle-clearing element, reconnaissance element, or deception element.

At any given time, a detachment will only be associated with a single functional force (disruption, main defense, security, counterattack, or reserve force) of a higher command. If a higher command needs to divide a detachment to accomplish other tasks, it will require a change in task-organizing. Detachments may be assigned one of several tasks while conducting a defense. Some examples are—

- Defend a simple BP
- Defend a complex BP
- Act as CRD
- Act as deception force
- Act as security force
- Act as counterattack force
- Act as reserve



Preparing for the Defense

In the preparation phase, the OPFOR focuses on ways of applying all available resources and the full range of actions to conduct the defense in the strongest condition and strongest positions possible. The defensive dispositions are based on the application of the systems warfare approach to combat. Planning considerations include:

- Deny enemy information
- Make thorough countermobility and survivability preparations
- Make use of complex terrain
- Make thorough logistics arrangements
- Modify the plan when necessary
- Rehearse everything possible, in priority (counterreconnaissance plan, commitment of reserve, initiation of counterattack, fire support plan, INFOWAR plan)

Executing the Defense

Successful execution depends on forces and elements that understand their roles in the battle and can swiftly follow preparatory actions with implementation of the battle plan or rapid modifications to the plan, as the situation requires. A successful execution phase results in the culmination of the enemy's offensive action. It ideally ends with transition to the offense in order to keep the enemy under pressure and destroy him completely. Against a superior enemy force, however, a successful defense may end in a stalemate.

A successful defense sets the military conditions for a return to the offense or a favorable political resolution of the conflict. The OPFOR may have to surrender territory to preserve forces. Territory can always be recaptured, but the destruction of OPFOR major combat formations threatens the survival of the State. Destruction of the protected force is unacceptable.

Principles of executing a defense include:

- Maintain contact
- Implement battle drills
- Modify the plan when necessary
- Seize opportunities

S2 NOTE: The OPFOR derives great flexibility from battle drills, using minor, simple, and clear modifications to adapt to ever-shifting conditions. OPFOR does not write standard procedures into its combat orders and does not write new orders when a simple shift from current formations and organization will do.

Types of Defensive Action—Tactical Groups, Divisions, and Brigades

The two basic types of defense are **maneuver** and **area** defense. A tactical group CDR may use both forms of defense simultaneously across his AOR. A defensive battle plan may include subordinate units that are executing various combinations of maneuver and area defenses, along with some offensive actions, within the overall defensive mission framework.

Maneuver Defense

In situations where the OPFOR is not completely overmatched, it may conduct a tactical *maneuver defense*. This type of defense is designed to achieve tactical decision by skillfully using fires and maneuver to destroy key elements of the enemy's combat system and deny enemy forces their objective, while preserving the friendly force. Maneuver defenses cause the enemy to continually lose effectiveness until he can no longer achieve his objectives. They can also economize force in less important areas while the OPFOR moves additional forces onto the most threatened axes.

Even within a maneuver defense, the tactical group CDR may use area defense on some enemy attack axes, especially on those where he can least afford to lose ground. Conversely, he may employ maneuver defense techniques to conduct actions in the disruption zone if it enhances the attack on the enemy's combat system and an area defense in the battle zone.

Method

Maneuver defense inflicts losses on the enemy, gains time, and protects friendly forces. It allows the defender to choose the place and time for engagements. Each portion of a maneuver defense allows a continuing attack on the enemy's combat system. As the system begins to disaggregate, more elements are vulnerable to destruction. The maneuver defense accomplishes this through a succession of defensive battles in conjunction with short, violent counterattacks and fires. It allows abandoning some areas of terrain when responding to an unexpected enemy attack or when conducting the battle in the disruption zone. In the course of a maneuver defense, the tactical CDR tries to force the enemy into a situation that exposes enemy formations to destruction. See examples of maneuver defense below.

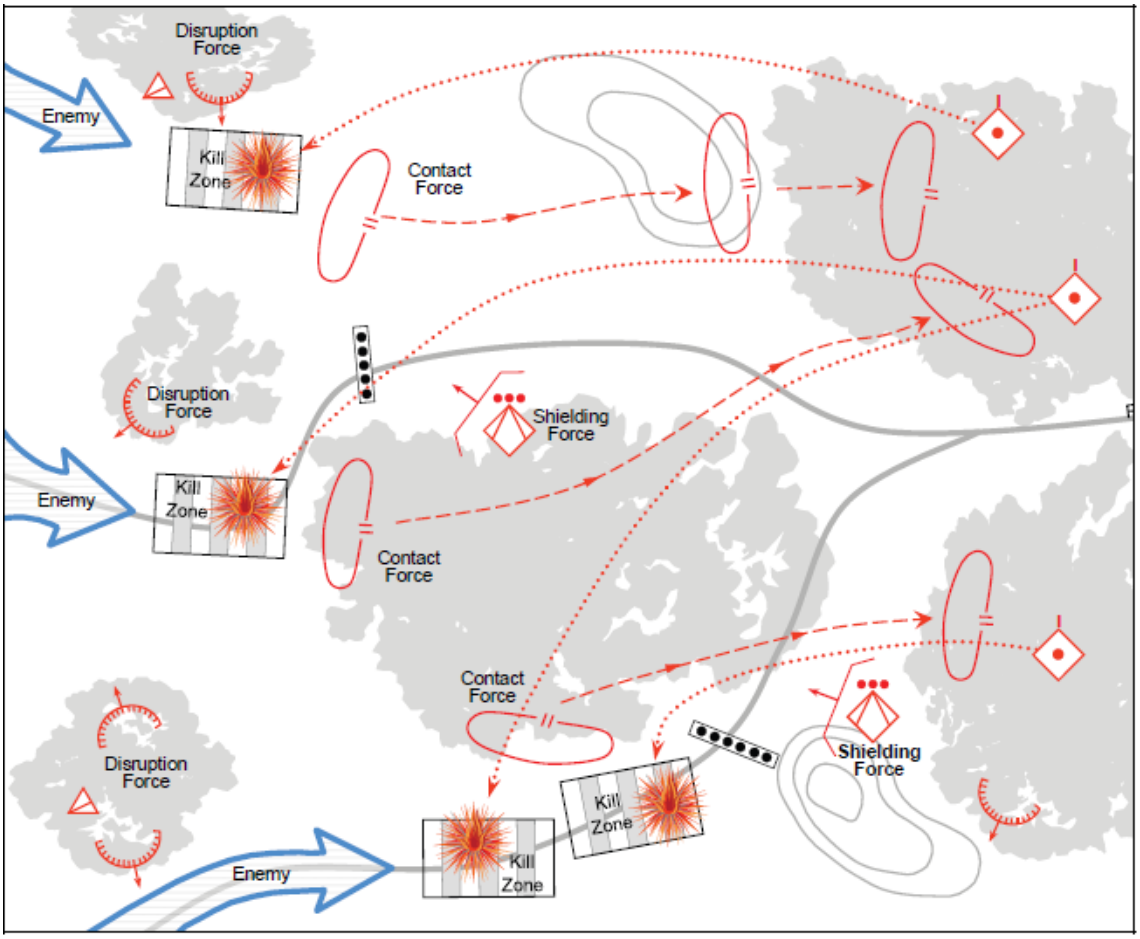


Figure 7-1. Maneuver Defense, example 1

Maneuver defense trades terrain for the opportunity to destroy portions of the enemy formation and render the enemy's combat system ineffective. The OPFOR might use a maneuver defense when (1) it can afford to surrender territory; (2) it possesses a mobility advantage over enemy forces; and, (3) conditions are suitable for canalizing the enemy into areas where the OPFOR can destroy him by fire or deliver decisive counterattacks.

Compared to area defense, the maneuver defense involves a higher degree of risk for the OPFOR, because it does not always rely on the inherent advantages of complex BPs. Units conducting a maneuver defense typically place smaller forces or elements forward in defensive positions and retain much larger reserves than in an area defense.

Defensive arrays are generally integrated into the terrain. In the spaces between arrays, the defenders typically execute disruption. Thus, it is difficult for the enemy to predict where he will encounter resistance.

The number of arrays and duration of defense on each array depend on the nature of the enemy's actions, the terrain, and the condition of the defending units. Arrays are selected based on the availability of obstacles and complex terrain.

Defensive Maneuver

Defensive maneuver consists of movement by bounds and the maintenance of continuous fires on enemy forces. A disruption force and/or a main defense force (or part of it) can perform defensive maneuver. In either case, the force must divide its combat power into two smaller forces: a contact force and a shielding force. The contact force is the force occupying the defensive array in current or imminent contact with the enemy. The shielding force is the force occupying a defensive array that permits the contact force to reposition to a subsequent array.

The contact force ideally forces the enemy to deploy his maneuver units and perhaps begin his fires in preparation for the attack. Then, before the contact force becomes decisively engaged, it maneuvers to its next preplanned array, protected by the array occupied by the shielding force. While the original contact force is moving, the shielding

force is able to keep the enemy under continuous observation, fires, and attack. When the original contact force assumes positions in its subsequent defensive array, it becomes the shielding force for the new contact force. In this manner, units continue to move by bounds to successive arrays, preserving their own forces while delaying and destroying the enemy.

Subsequent arrays are far enough apart to permit defensive maneuver by friendly units. The distance should also preclude the enemy from engaging two arrays simultaneously without displacing his indirect fire weapons. This means that the enemy, having seized a position in one array, must change the majority of his firing positions and organize his attack all over again in order to get to a position in the next array. However, the arrays are close enough to allow the defending units to maintain coordinated, continuous engagement of the enemy while moving from one to the other. It is possible that not all of the forces executing contact and shielding functions have the same number of arrays.

OPFOR CDRs may require a unit occupying an array to continue defending, even if this means the unit becomes decisively engaged or enveloped. This may be necessary in order to allow time for the construction of defenses farther from contact with the enemy. This may be the case when a unit is conducting maneuver defense in the disruption zone while the main defense force is preparing for an area defense in the battle zone. At some point, a unit conducting maneuver defense as part of the main defense force may be ordered to continue to defend an array, if conditions are favorable for defeating the enemy or repelling the attack at that array.

The shielding force does not necessarily have to remain in place to do its job. It can go out to meet the enemy (perhaps in an ambush) and then maneuver into another array. This type of maneuver can force the enemy into a nonlinear fight.

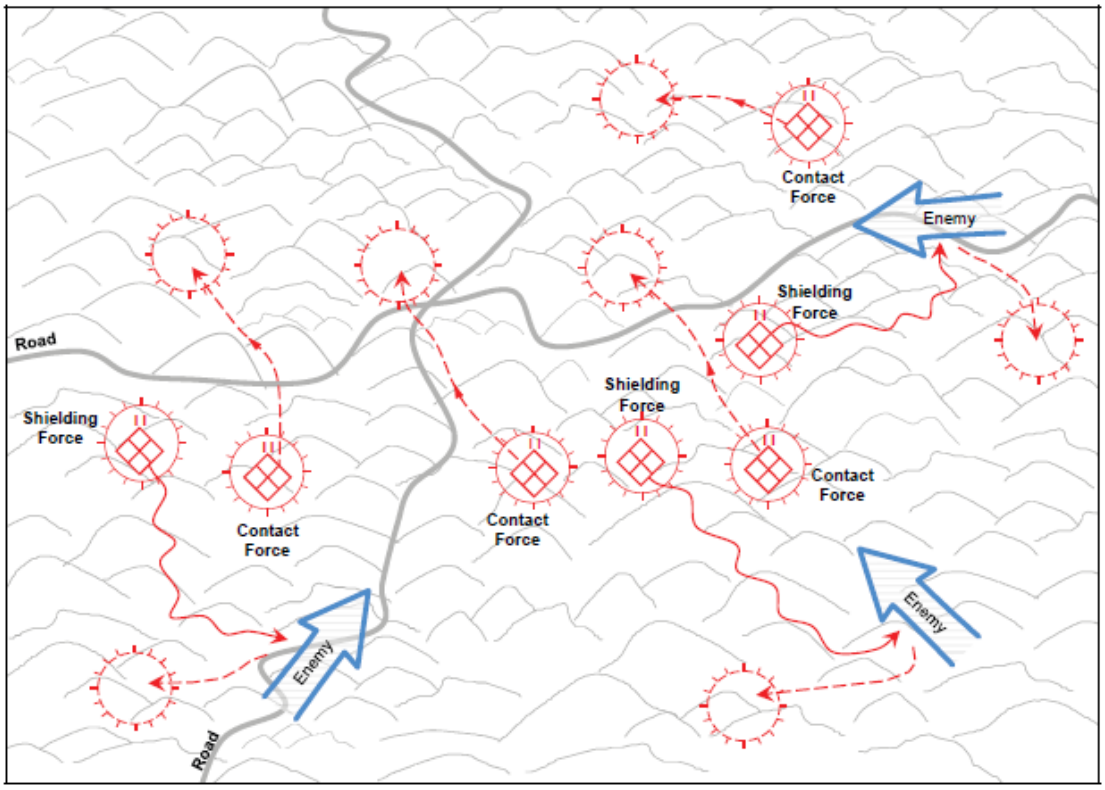


Figure 7-2. Maneuver Defense, example 2

Disruption Force

The disruption force initiates the attack on the enemy's combat system by targeting and destroying subsystems that are critical to the enemy. If successful, the disruption force can cause culmination of the enemy attack before the enemy enters the battle zone. In the worst case, the enemy would enter the battle zone unable to benefit from an integrated combat system and vulnerable to defeat by the main defense force.

In a maneuver defense, the disruption force often occupies BPs in the disruption zone and seeks to force the enemy to fight on disadvantageous ground and at a tempo of the OPFOR's choosing. A maneuver defense disruption force also can set the conditions for a spoiling attack or counterattack. The disruption force mission includes disaggregating the enemy attack and, if possible, destroying the enemy force.

Maneuver units conduct the defense from successive BPs. Intervals between these positions provide space for deployment of mobile attack forces, precision fire systems, and reserves.

The distance between successive positions in the disruption zone is such that the enemy is forced to displace the majority of his supporting weapons to continue the attack on the subsequent positions. This aids the force in breaking contact and permits time to occupy subsequent positions. Long-range fires, ODs, and ambushes to delay pursuing enemy units can assist units in breaking contact and withdrawing.

If the disruption force has not succeeded in destroying or halting the attacking enemy, but is not under too great a pressure from a pursuing enemy, it may occupy prepared BPs in the battle zone and assist in the remainder of the defensive mission as part of the main defense force. A disruption force may have taken losses and might not be at full capability; a heavily damaged disruption force may pass into hide positions. In that case, main defense or reserve forces occupy positions to cover the disruption force's disengagement.

Main Defense Force

The mission of the main defense force is to complete the defeat of the enemy by engaging portions of the force exposed by actions of the disruption force and by enemy reactions to contact. This may involve resubordination of units and in some cases attacks by fire or maneuver forces across unit limits of responsibility.

The main defense force in a maneuver defense divides its combat power into contact and shielding forces. These forces move in bounds to successive arrays of defensive positions.

The basic elements of the battle zone are BPs, firing lines, and repositioning routes. BPs use the terrain to protect forces while providing advantage in engagements.

The CDR may order a particular unit to stand and fight long enough to repel an attack. He may order this if circumstances are favorable for defeating the enemy at that point. The unit also might have to remain in that position because the next position is still being prepared or a vertical envelopment threatens the next position or the route to it.

Reserves

A CDR in the maneuver defense can employ a number of reserve forces of varying types and strengths. The maneuver reserve is a force strong enough to defeat the enemy's exploiting force. The CDR positions this reserve in an assembly area using C3D to protect it from observation and attack. From this position, it can transition to a situational defense or conduct a counterattack. The reserve must have sufficient air defense coverage and mobility assets to allow maneuver. If the CDR does not commit the reserve from its original assembly area, it maneuvers to another assembly area, possibly on a different axis, where it prepares for other contingencies

Area Defense

In situations where the OPFOR must deny key areas (or the access to them) or where it is overmatched, it may conduct a tactical area defense. Area defense is designed to achieve a decision in one of two ways:

- By forcing the enemy's offensive operations to culminate before he can achieve his objectives.
- By denying the enemy his objectives while preserving combat power until decision can be achieved through strategic operations or operational mission accomplishment.

The area defense does not surrender the initiative to the attacking forces, but takes action to create windows of opportunity that permit forces to attack key components of the enemy's combat system and cause unacceptable casualties. Area defense can set the conditions for destroying a key enemy force. Extended windows of opportunity permit the action of maneuver forces to prevent destruction of key positions and facilitate transition to a larger offensive action. INFOWAR is particularly important to the execution of the area defense. Deception is critical to the creation of complex BPs, and effective perception management is vital to the creation of the windows of opportunity needed to execute maneuver and fires.

Method

Area defense inflicts losses on the enemy, retains ground, and protects friendly forces. It does so by occupying complex BPs and dominating the surrounding area with reconnaissance fire. These fires attack designated elements of the enemy's combat system to destroy components and subsystems that create an advantage for the enemy. The intent is to begin disaggregating the enemy combat system in the disruption zone. When enemy forces enter the battle zone, they should be incapable of synchronizing combat operations.

S2 NOTE: *Reconnaissance fire* is the integration of RISTA, fire control, and weapon systems into a closed-loop, automated fire support system that detects, identifies, and destroys critical targets in minutes. Reconnaissance fire enables the OPFOR to deliver rotary-wing air, SSM, cruise missile, and artillery fires (including precision munitions) on enemy targets within a very short time after acquisition.

Area defense creates windows of opportunity in which to conduct spoiling attacks or counterattacks and destroy key enemy systems. In the course of an area defense, the tactical CDR uses terrain that exposes the enemy to continuing attack.

An area defense trades time for the opportunity to attack enemy forces when and where they are vulnerable. A skillfully conducted area defense can allow a significantly weaker force to defeat a stronger enemy force. However, the area defense relies to a significant degree on the availability of complex terrain and decentralized logistics. Units conducting an area defense typically execute ambushes and raids in complex terrain throughout the AOR to force the enemy into continuous operations and steadily drain his combat power and resolve.

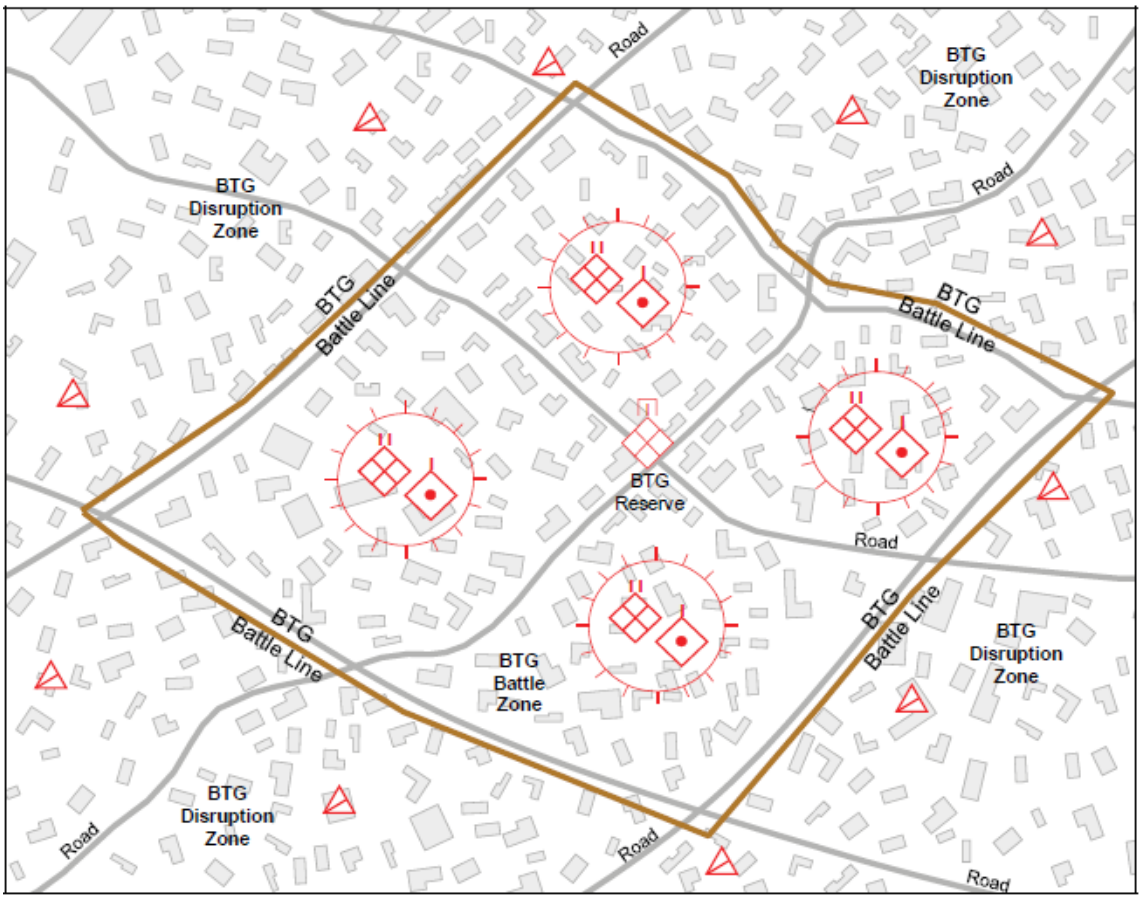


Figure 7-3. Area Defense, example 1

Disruption Force

In an area defense, the disruption zone is the area surrounding its battle zone(s) where the OPFOR may cause continuing harm to the enemy without significantly exposing itself. The disruption zone of an area defense is designed to be an area of uninterrupted battle. OPFOR RISTA elements contact with enemy forces, and other parts of the disruption force attack them incessantly with ambush and precision fires. The disruption force has many missions. The most important mission at the tactical level is destruction of appropriate elements of the enemy's combat system, to begin its disaggregation. The following list provides examples of other tasks a disruption force may perform:

- Detect the enemy's main groupings
- Force the enemy to reveal his intentions
- Deceive the enemy as to the location and configuration of BPs
- Delay the enemy, allowing time for preparation of defenses and counterattacks
- Force the enemy into premature deployment
- Attack lucrative targets (key systems, vulnerable troops)
- Canalize the enemy into situations unfavorable to him

The disruption force mission also includes maintaining contact with the enemy and setting the conditions for successful reconnaissance fire and counterattacks.

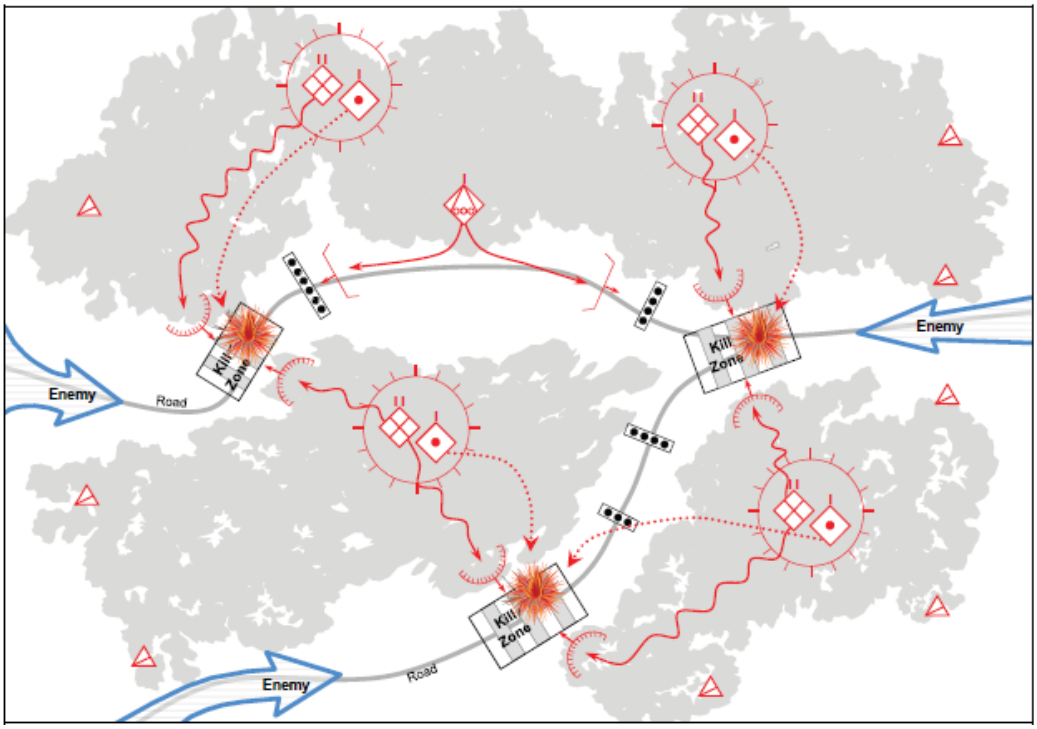


Figure 7-4. Area Defense, example 2

In an area defense, the disruption force often occupies and operates out of battle positions in the disruption zone and seeks to inflict maximum harm on selected enemy units and destroy key enemy systems operating throughout the AOR. An area defense disruption force permits the enemy no safe haven and continues to inflict damage at all hours and in all weather conditions.

Disruption force units break contact after conducting ambushes and return to BPs for refit and resupply. Long-range fires, ODs, and ambushes to delay pursuing enemy units can assist units in breaking contact and withdrawing.

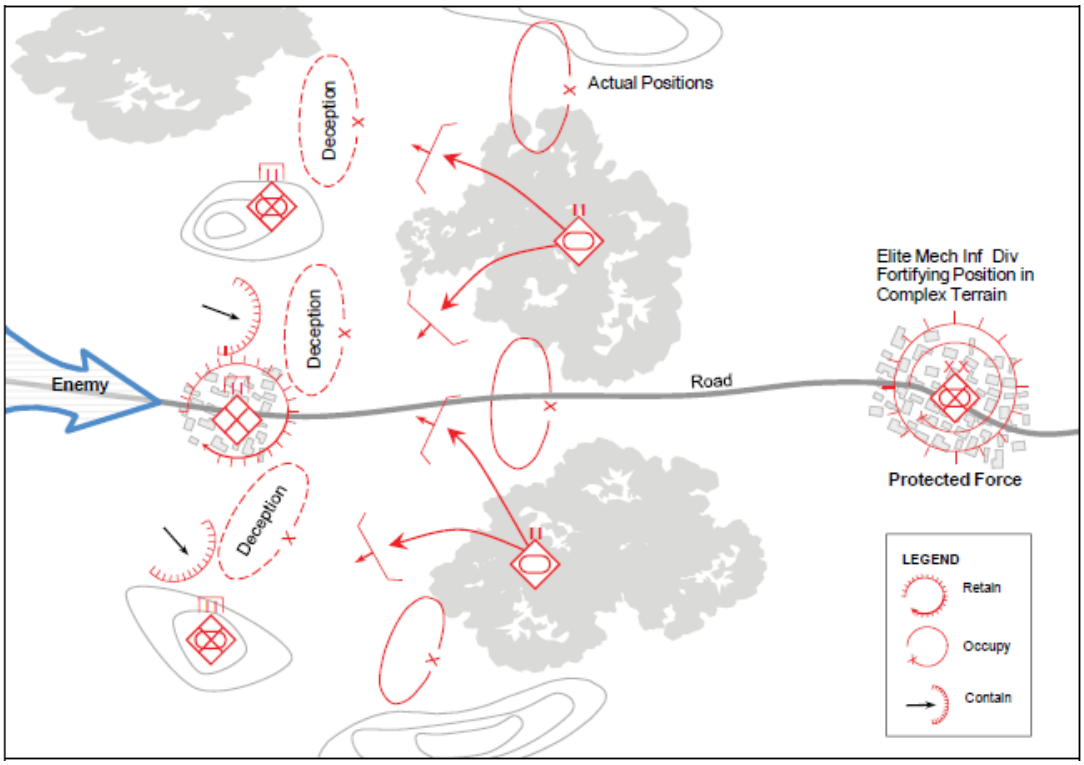


Figure 7-5. Area Defense, example 3

Even within the overall context of an area defense, the disruption force might employ a maneuver defense. In this case, the distance between positions in the disruption zone is such that the enemy will be forced to displace the majority of his supporting weapons to continue the attack on the subsequent positions. This aids the force in breaking contact and permits time to occupy subsequent positions.

The disruption zone will often include a significant obstacle effort. Engineer effort in the disruption zone also provides mobility support to portions of the disruption force requiring maneuver to conduct attacks or ambushes. Especially when overmatched by enemy forces, the OPFOR may use booby traps and other types of improvised obstacles.

Within the overall structure of the area defense, the disruption force seeks to conduct highly damaging local attacks. Units selected for missions in the disruption zone deploy on likely enemy avenues of approach. They choose the best terrain to inflict maximum damage on the attacking enemy and use obstacles and barriers extensively. They defend aggressively by fire and maneuver. When enemy pressure grows too strong, these forces can conduct a maneuver defense, withdrawing from one position to another in order to avoid envelopment or decisive engagement.

Since a part of the disruption force mission is to attack the enemy's combat system, typical targets for attack by forces in the disruption zone are–

- C2 systems
- RISTA assets
- Precision fire systems
- Aviation assets in the air and on the ground at attack helicopter forward arming and refueling points (FARPs) and airfields
- Logistics support areas
- LOCs
- Mobility and countermobility assets

S2 NOTE: Air defense ambushes are particularly effective in the disruption zone.

- Casualty evacuation routes and means

In some cases, the disruption force can have a single mission of detecting and destroying a particular set of enemy capabilities. This does not mean that no other targets will be engaged. It simply means that, given a choice between targets, the disruption force will engage the targets that are the most damaging to the enemy's combat system.

Main Defense Force

The units of the main defense force conducting an area defense occupy complex battle positions (CBPs) within the battle zone. The complex terrain is reinforced by engineer effort and C3D measures. These CBPs are designed to prevent enemy forces from being able to employ precision standoff attack means and force the enemy to choose costly methods in order to affect forces in those positions. They are also arranged in such a manner as to deny the enemy the ability to operate in covered and concealed areas himself.

The main defense force in an area defense conducts attacks and employs reconnaissance fire against enemy forces in the disruption zone. Disruption zone forces may also use the CBPs occupied by the main defense force as refit and rearm points.

Reserves

A CDR in an area defense can employ a number of reserve forces of varying types and strengths. In addition to its other functions, the maneuver reserve in an area defense may have the mission of winning time for the preparation of positions. This reserve is a unit strong enough to defeat the enemy's exploitation force in a maneuver battle during a counterattack. The CDR positions its reserve in an assembly area within one or more of the BPs, based on his concept for the battle.

Tactical Defensive Actions—Detachments, Battalions, and Below

OPFOR detachments, BNs, and companies generally participate as part of a maneuver or area defense organized by a higher command, as opposed to conducting one independently. CDRs of OPFOR detachments, BNs, or companies select the defensive action they deem to be best suited to accomplishing their mission. OPFOR detachments and below are typically called upon to execute one combat mission at a time. Therefore, it would be rare for such a unit to employ more than one of these methods simultaneously. As part of either an area defense or maneuver defense, such units often conduct tactical defensive actions employing simple battle positions (SBPs). Alternatively, as part of an area defense, they may employ CBPs.

Battle Positions

A battle position (BP) is a defensive location oriented on a likely enemy avenue of approach. A BP is designed to maximize the occupying unit's ability to accomplish its mission. A BP is selected such that the terrain in and around it is complementary to the occupying unit's capabilities and its tactical task. There are two kinds of BPs: simple and complex.

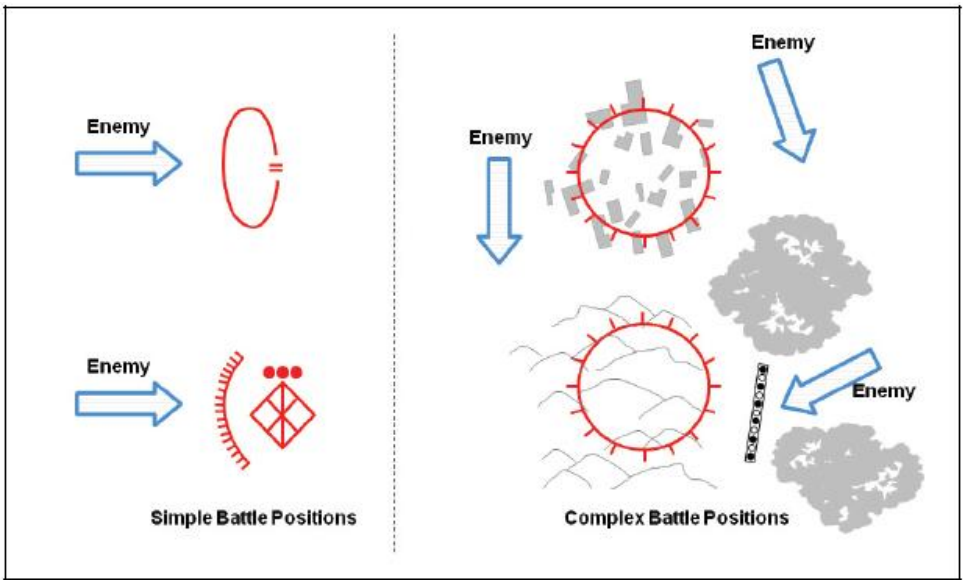


Figure 7-6. Simple and Complex BPs

Simple Battle Position

A simple battle position (SBP) is a defensive location oriented on the most likely enemy avenue of approach. SBPs are not necessarily tied to complex terrain. However, they often employ as much engineer effort and/or C3D measures as time allows.

Complex Battle Position

A complex battle position (CBP) is a defensive location designed to employ a combination of complex terrain, C3D, and engineer effort to protect the unit(s) within them from detection and attack while denying their seizure and occupation by the enemy. CBPs typically have the following characteristics that distinguish them from SBPs:

- Limited avenues of approach (CBPs are not necessarily tied to an avenue of approach)
- Any existing avenues of approach are easily observable by the defender
- 360-degree fire coverage and protection from attack (This may be due to the nature of surrounding terrain or engineer activity such as tunneling)
- Engineer effort prioritizing C3D measures; limited countermobility effort that might reveal the CBP location
- Large logistics caches
- Sanctuary from which to launch local attacks

Defense of an SBP

An SBP is typically oriented on the most likely enemy avenue of approach. SBPs may or may not be tied to restrictive terrain but will employ as much engineer effort as possible to restrict enemy maneuver. Defenders of SBPs will take all actions necessary to prevent enemy penetration of their position, or defeat a penetration once it has occurred.

Functional Organization of Elements to Defend an SBP

The CDR of a detachment, BN, or CO defending an SBP designates his subordinate units as functional elements. The name of the element describes its function within the defensive action.

Disruption Element

Unit(s) assigned to the disruption element have the mission of defeating enemy reconnaissance efforts; determining the location, disposition, and composition of attacking forces; and in some cases they will also target designated

subsystems of the attacking enemy's combat system. To accomplish these tasks, the disruption element may form combat security outposts (CSOPs) and ambush teams.

CSOPs. CSOPs prevent enemy reconnaissance or small groups from penetrating friendly positions and force the enemy to prematurely deploy and lose his momentum in the attack. CSOPs are generally composed of task-organized platoon- or squad-size elements. In a BN or BDET, the platoon or squad(s) forming the CSOP is generally drawn from the BN reserve element. Companies or CDETs may also form their own CSOPs. CSOPs are positioned forward of the battle zone on key terrain or along key avenues of approach. They typically will not be positioned directly astride avenues of approach into kill zones, but may cover them with fire. If decisively overmatched by enemy combat power, CSOPs may withdraw to the battle zone. An OPFOR BN or BDET may employ more than one CSOP. During the counterreconnaissance battle, other forces may augment CSOPs, covering those avenues of approach that the CSOPs do not cover. CSOPs are typically assigned one or more of the following tactical tasks:

- **Ambush.** A CSOP with this task generally will avoid contact with superior enemy forces and only engage key enemy targets. When assigning this task, the OPFOR CDR must also describe desired effects on the enemy (such as destroy, fix, or suppress).
- **Attack by fire.** A CSOP with this task is normally attempting to shape the battlefield in some fashion, either by turning an attacking enemy force into a kill zone or by denying the enemy a key piece of terrain. A CSOP with this task may also be required to target a key element of the enemy force.
- **Delay.** A CSOP with this task will attempt to buy time for the OPFOR to accomplish some other task such as defensive preparations, launch a counterattack, or complete a withdrawal. Normally, the CSOP will withdraw (remaining in the disruption zone, or moving to the battle or support zone) after engaging for a set amount of time.
- **Disrupt.** A CSOP with this task will attempt to weaken an enemy attack by using fires to cause premature commitment of the enemy, break apart his formation, and desynchronize his plan.
- **Fix.** A CSOP with this task will use fires to prevent a key element of the enemy force from moving from a specific place or halt them for a specific amount of time.

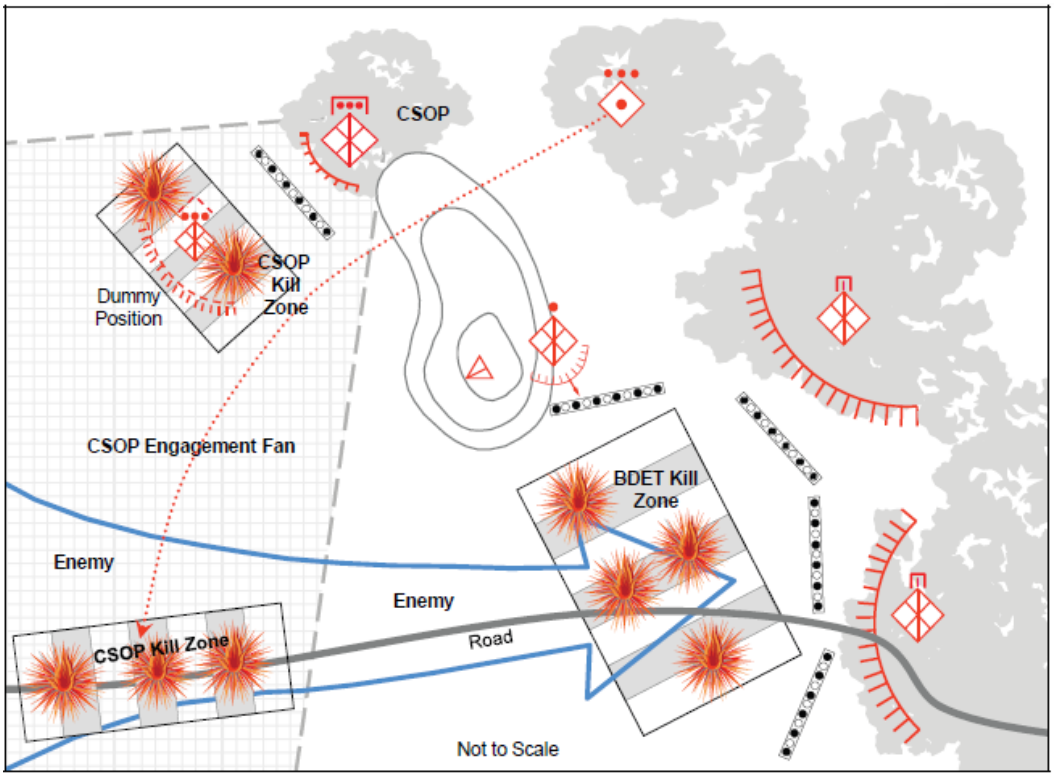


Figure 7-7. CSOP

Ambush Teams. Ambush teams (independent from CSOPs) remain concealed forward of the battle zone, and may allow some enemy forces to bypass their position. Once they identify key enemy targets, they will engage them by employing flanking or surprise close-range fire.

Main Defense Element
The main defense element of an SBP is responsible for defeating an attacking force, and for maneuvering to defeat the penetration or seizure of other SBPs.

Reserve Element
The reserve element of an SBP exists to provide the OPFOR CDR with tactical flexibility. During the counterreconnaissance battle, the reserve may augment forces in the disruption zone, in order to provide additional security to the main defense element. During this time, the reserve element will also rehearse potential counterattack routes, although to avoid detection it will rarely do so en masse. Once a significant attacking force is detected, the reserve element will withdraw to a covered and concealed position, conduct resupply, and prepare for additional tasks. Some typical additional tasks given to the reserve may include—

- Conducting a counterattack
- Conducting counterpenetration (blocking or destroying enemy penetration of the SBP)
- Conducting antilanding defense
- Assisting engaged forces in breaking contact
- Acting as a deception element

Support Element
The support element of an SBP has the mission of providing one or more of the following to the defending force:

- CSS
- C2
- Supporting direct fire (such as heavy MG, ATGM, recoilless rifle, or automatic grenade launcher)
- Supporting indirect fire (mortar or artillery)
- Supporting nonlethal actions (for example, jamming, psychological warfare, or broadcasts)
- Engineer support

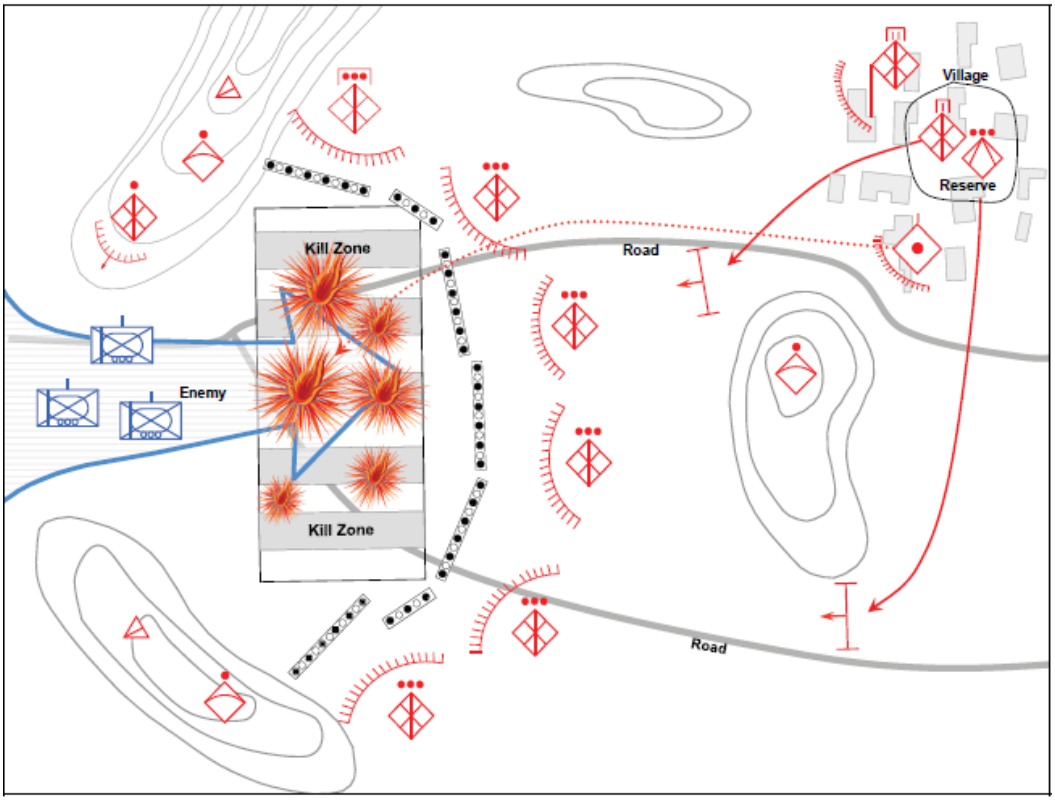


Figure 7-8. CDET in an SBP, example 1

Organizing the Battlefield for an SBP

A detachment, BN or CO CDR specifies the organization of the battlefield from the perspective of his level of command. As at higher levels, this normally consists of a battle zone and a support zone. It may also include a disruption zone.

Disruption Zone

The disruption zone is the area forward of the battle zone where the defenders will seek to defeat enemy reconnaissance efforts, detect attacking forces, disrupt and delay an attackers approach, and destroy key attacking elements prior to engagement in the battle zone. A defense of an SBP may or may not include a disruption zone.

Battle Zone

The battle zone is the area where the defending CDR commits the preponderance of his force to the task of defeating attacking enemy forces. Generally, an SBP will have its battle zone fires integrated with those of any adjacent SBPs. Fires will orient to form kill zones where the OPFOR plans to destroy key enemy targets. When possible, kill zones will be placed on the reverse slope of intervisibility lines within the battle zone.

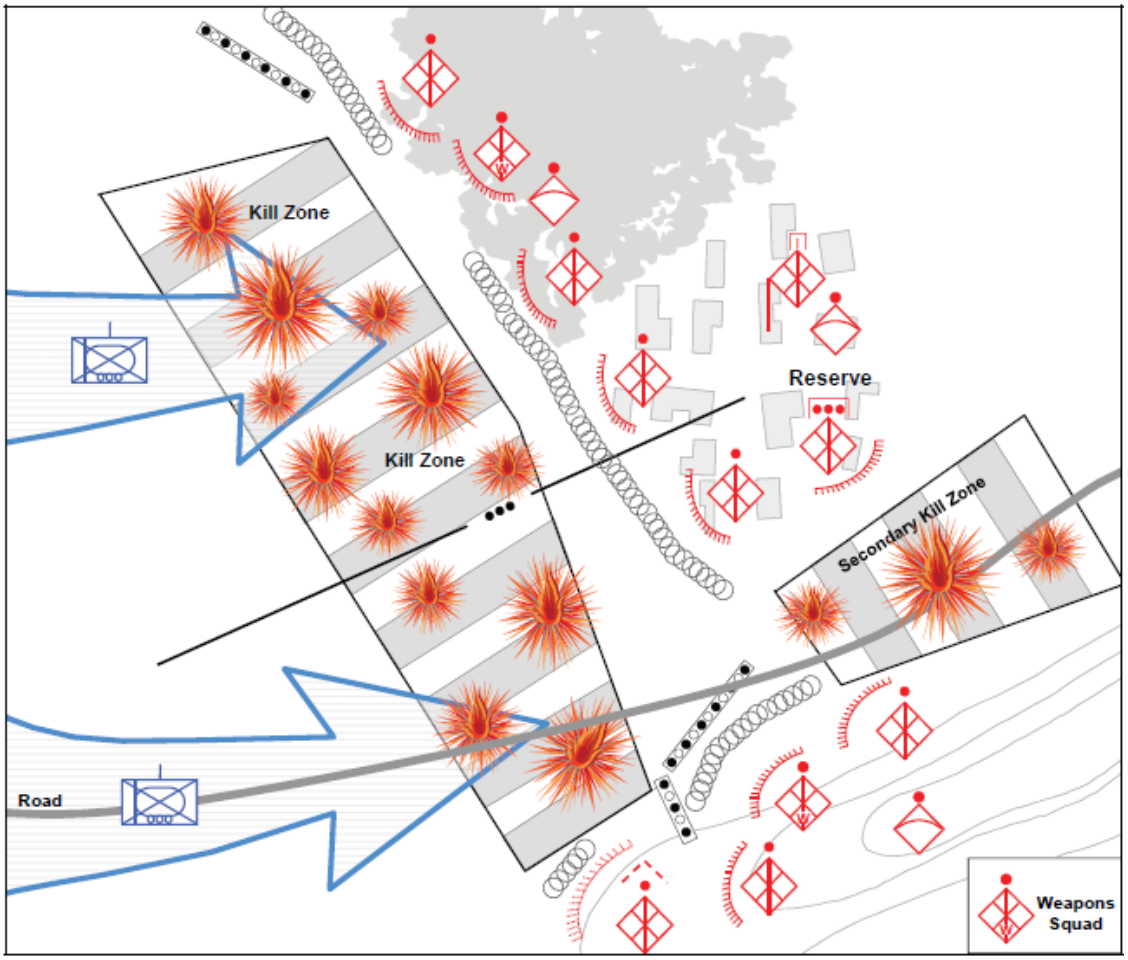


Figure 7-9. CDET in an SBP, example 2

Reverse Slope Defense. The OPFOR CDR will seek a defensive position behind a terrain feature(s) that, in addition to providing an intervisibility line, canalizes attackers into narrow attack frontages that lead into the kill zone. A reverse slope defense is positioned behind an intervisibility line so that is masked from enemy observation and direct fire. The defense is based upon employing the intervisibility line to protect friendly forces and isolate portions of the attacking force as they cross the crest. Although the OPFOR may not occupy the crest in strength, it will control it by fire. OPFOR CDRs prefer a reverse slope defensive position because it confers the following advantages:

- It hinders or prevents enemy observation of the defensive position
- Attacking forces are not able to receive direct fire support from follow-on forces
- It can negate an enemy stand-off fire advantage
- Attacking enemy forces are silhouetted while crossing the crest of the intervisibility line
- Engineers can conduct their work out of direct fire and observation from the enemy

In some cases, the adoption of a reverse slope defense can prevent the defender's weapon systems from exploiting their maximum range. However, skilful OPFOR CDRs will select defensive terrain that allows them to maximize their weapons stand-off range. They do so by emplacing their systems at their maximum effective range behind the crest of the intervisibility line that supports their kill zone. This may mean placing a weapon system on the counterslope behind the terrain forming the intervisibility line.

Maintaining observation of the enemy while on the forward slope of an intervisibility line can be difficult. To alleviate this disadvantage, OPFOR CDRs will employ reconnaissance assets to observe forward of the reverse slope defensive position.

Fire Planning. Fire is the basic means of destroying the enemy in the defense. To perform this task, the OPFOR will employ lethal and nonlethal weaponry in a unified manner, often directed into a kill zone. The normal basis of a BN's or BDET's system of fire is the AT fire of its companies (and any additional units task-organized into the BDET) and supporting artillery. In areas that are not accessible to vehicles, the basis of fire will primarily be MG, grenade launcher, mortar, and artillery fires. In this case, where possible, AT systems will be employed in an antipersonnel role.

During the OPFOR fire planning process, the CDR and staff delineate key enemy targets. The planners then appoint reconnaissance elements to identify targets and weapons systems to engage them. The OPFOR BN's or BDET's fire planning includes sectors of concentrated fire and barrier fire lines of artillery and mortars in the disruption zone, on flanks, and throughout the depth of the battle zone. Subordinate units and weapons are expected to coordinate with each other as well as flanks units in the coverage of kill zones.

Kill zones will be covered by frontal and flanking or cross fires of the OPFOR BN's or BDET's and other supporting weapons systems. The OPFOR will employ obstacles and fire concentrations to halt and hold the enemy within kill zones. Terrain considerations and available weaponry will dictate the size of the kill zone and the width of the OPFOR defense.

Support Zone
The support zone may contain C2, CSS, indirect and direct support fire assets, and the reserve, as well as other supporting assets. The support zone will normally be located in the SBP. Support zones are not typically found below the CO level.

Executing Defense of an SBP

SBP defenders will conduct aggressive counterreconnaissance throughout their occupation of the BP. Such counterreconnaissance will occur primarily in the disruption zone, but measures will also be taken in the battle and support zones. OPFOR EW assets will attempt to detect the presence and location of enemy reconnaissance elements. The reserve element may act as a quick-response force to destroy any enemy reconnaissance assets discovered in the battle or support zones. Once a significant attacking force is detected, the OPFOR will employ fires (direct or indirect) to delay and attrite attackers in the disruption zone.

Battle Zone
Defenders in the battle zone will attempt to defeat attacking forces. Should the enemy penetrate the main defenses or capture a position, defenders will take measures to defeat the penetration or recapture the position, to include the commitment of reserves and repositioning forces from other areas within the SBP.

Support Zone
Defenders in the support zone will provide support to defenders in the disruption and battle zones as required. In the event of the defeat or penetration of the SBP, they will maneuver as needed to avoid destruction or to support counterattacks.

Deception
To keep the enemy from discovering the nature of the OPFOR defenses and to draw fire away from actual units, defenders will establish dummy firing positions and BPs. In addition to enhancing force protection, the OPFOR will employ deception positions as an economy-of-force measure to portray strength. These measures will include the creation of false entrenchments, heat signatures, and dummy vehicles.

Command and Control of an SBP

To maintain security during defensive preparations, defenders will make all possible use of secure communications, such as couriers and wire. However, once the main battle is joined, communications measures will tend to be those that support maneuver, such as radio and cellular technology.

Support of an SBP

Depending on the situation, the SBP will require support. This support may include combat support (CS) and/or CSS or a mixture of both. While some of this support will be provided from within the parent organization, other support may be from other organizations.

Reconnaissance
SBP defenders will perform aggressive counterreconnaissance activities to prevent the enemy from remaining in reconnaissance contact with the SBP. The OPFOR will observe avenues of approach to provide early warning; determine location, composition, and disposition of attackers; and direct fires against key enemy systems or components of systems.

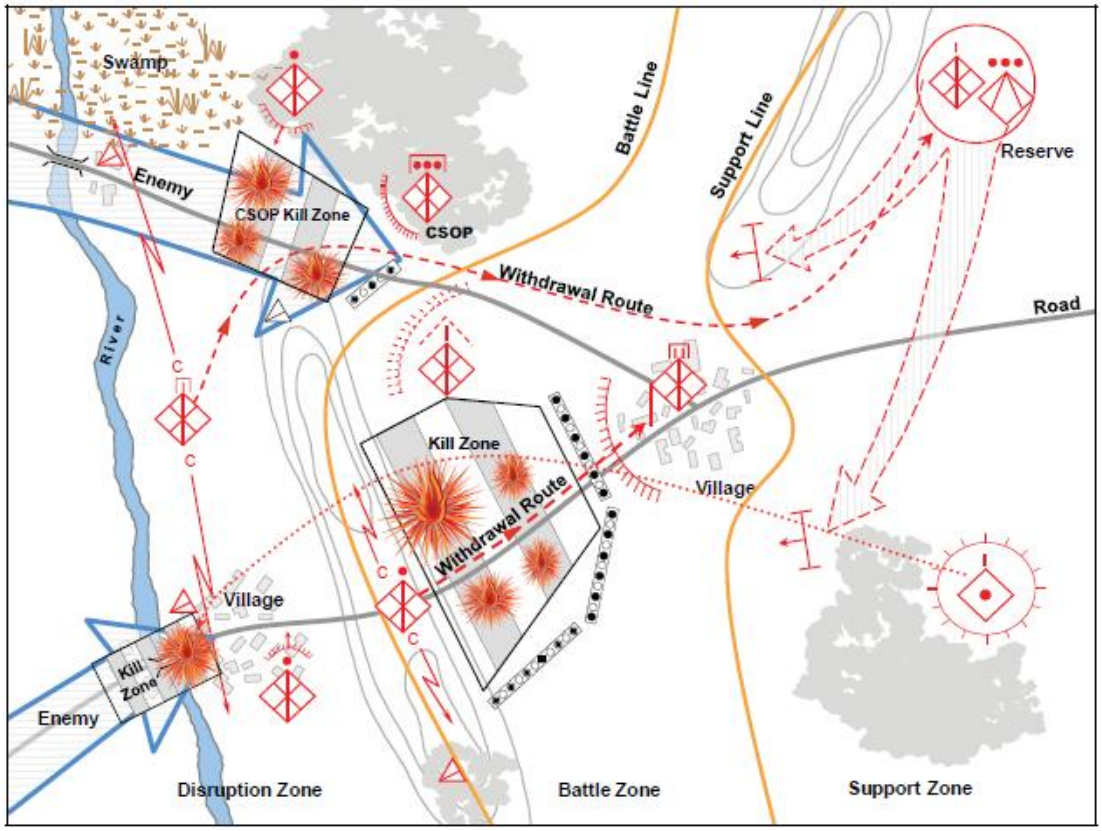


Figure 7-10. Reconnaissance Support to an SBP

Armored Fighting Vehicles
When employed within an SBP, armored fighting vehicles will typically serve an anti-armor role, but can also serve as in an anti-infantry role. They may also be massed as a counterattack reserve. Defending armored vehicles will be in two-tier (turret defilade) vehicle fighting positions to provide maximum cover and concealment, or will fight above ground to take maximum advantage of maneuver capabilities. Armored vehicles defending SBPs do not prefer single-tier (hull defilade) vehicle fighting positions, since they provide insufficient cover and concealment against precision munitions and restrict vehicular mobility.

Fire Support
SBPs may receive fire support both from constituent assets and from higher echelon supporting forces. Fire support is integrated with other adjacent units to ensure appropriate coverage. Defenders will employ fires to—

- Attrite attackers along the avenues of approach and in LZs
- Defeat attackers in the battle zone
- Defeat penetrations of BPs
- Support counterattacking forces

Air Defense
SBPs employ both active and passive air defense measures to protect the defender from air threats. Antiaircraft guns and shoulder-fired surface-to-air missile systems (SAMS) may be found interspersed throughout the SBP, including

antilanding ambushes. Electronically integrated air defense systems may be present when allocated to the defending force from higher-echelon supporting units.

Engineer

When available, engineers support the SBP initially by preparing survivability positions and countermobility works that support the disruption and battle zones. Once these preparations are complete, engineer support will shift to mobility support for the reserve force to ensure that it maintains freedom of maneuver.

Engineer tasks are a shared responsibility throughout the OPFOR. Although engineers have the bulk of specialized equipment for constructing fortified positions, this work exceeds the capability of organic constituent engineers and even those likely allocated from higher command. Therefore, the OPFOR uses all available personnel and equipment.

SBP obstacles are normally employed to shape the battlefield by disrupting the enemy's approach march, blocking avenues of approach, and turning the enemy into and fixing him in kill zones. Should the OPFOR have a remotely delivered mine capability, it will be used to reinforce pre-existing obstacles, block avenues of approach, or to re-seed breached obstacles.

First priority preparation tasks for a BN or BDET BP

Tasks of Combat Troops and Engineers

- Clear fields of observation and fire.
- Emplace obstacles integrated with CSOPs and platoon positions.
- Dig one- or two-man foxholes for riflemen, MG crews, snipers, and operators of grenade launchers, man-portable ATGMs, and shoulder-fired SAMs.
- Connect foxholes into a squad trench (open slit trench).
- Prepare a continuous trench in platoon and CO positions.
- Prepare emplacements at primary firing positions for IFVs/APCs, tanks, ATGM launchers, and other weapons in the platoon or CO position.
- Build basic positions (covered slit trenches) for platoon, CO, and BN or BDET CPs.
- Build basic positions (covered slit trenches) for BN or CO medical points.
- Dig and prepare covered slit trenches for each squad, crew, or team.
- Camouflage positions, weapons, and vehicles against reconnaissance and for protection against enemy precision weapons.

Tasks of Engineers

- Emplace additional obstacles on the most likely axes of enemy attack, in gaps between units, on their flanks, and in the depth of the BP.
- Deepen sections of trenches and communication trenches, and provide covered shelters for equipment on terrain that provides concealment from enemy observation and fire and permits the use of engineer mechanized equipment.
- Prepare lines of firing positions for reserve counterattack forces and prepare forward movement routes to these lines and to lines of deployment for counterattacks.
- Prepare routes for movement to the lines of deployment for the counterattack, lines of deployment of reserves, and firing positions.
- Set up water supply or distribution points.

Second-priority preparation tasks for a BN or BDET BP

Tasks of Combat Troops and Engineers

- Improve CO and platoon positions, adding overhead cover if possible.
- Finish building or improve CPs and medical points.
- Dig emplacements at alternate and temporary firing positions of IFVs/APCs, tanks, and other weapons.
- Dig emplacements at firing lines and assembly areas for IFVs/APCs, tanks, and other weapons.
- Dig communication trenches to primary and alternate firing positions for IFVs/APCs, tanks, and other weapons; to shelters; to CPs; and to the rear.
- Prepare dugouts on the basis of one per platoon and one for each CO, BN, or BDET medical point.
- When possible, make covered slit trenches or dugout shelters for each squad, weapon crew, or team.
- Create and upgrade the system of trenches and communication trenches from a combat and housekeeping standpoint. Housekeeping and sanitary preparation or trenches includes making niches for storing food, water, and equipment and making latrines, sumps, soakage pits, and drainage ditches.

Tasks of Engineers

• Connect individual emplacements into emplacements for squads with sections of trench dug with mechanized equipment.
• Prepare a continuous trench in the BN or BDET BP.
• Make bunkers for each CO/battery and at BN or BDET CPs.
• Make shelters for vehicles, weapons, equipment, missiles, ammunition, and other supplies.
• Prepare main dummy objects in the CO position or BN or BDET BP.
• Prepare for demolition of roads, bridges, overpasses, and other important objectives in the depth of the defense.
• Prepare routes for maneuver, resupply, and evacuation.

Third-priority preparation tasks for a BN or BDET BP

Tasks of Combat Troops and Engineers

• Finish building or improving communication trenches and preparing positions.
• Improve engineer preparation of CO positions and the BN or BDET BP.
• Improve the platoon positions and squad and weapon positions in a tactical and housekeeping respect.
• Connect squad trenches in the platoon and CO positions with one another, if this has not already been done.
• Build a system of engineer obstacles.
• Develop a system of trenches and communication trenches in the CO position or BN or BDET BP.
• Establish shelters for personnel and continue building shelters for equipment and deepening trenches and communication trenches.
• Adapt the communication trenches for conducting fire.
• Cover some parts of the trenches.
• Prepare dugout shelters at platoon CPs.
• Set up shelters (one per CO and per BN or BDET CP).
• Dig communication trenches to the rear (first with a depth of 0.6 m and then 1.1 m).
• Equip the trenches and communication trenches with alternate (lateral and forward) foxholes and emplacements for firing MGs and grenade launchers and with embrasures, overhead protection, and niches or recesses for ammunition.
• Prepare dummy firing positions and BPs.

Tasks of Engineers

• Develop or improve a network of routes for unit maneuver, supply, and evacuation.
• Expand the system of obstacles.
• Improve fighting positions, firing lines, lines of deployment for counterattack, lines of deployment of reserves, CPs, assembly areas of reserves, and logistics elements.

Logistics

When present, logistics units will normally be found with the support element, to the rear of the SBP. Units in the disruption zone and battle zone will locally stockpile supplies, including multiple basic loads of ammunition, to ensure that they remain self-sufficient during the battle.

INFOWAR

The SBP is supported by INFOWAR, primarily by deceiving the enemy as to the defenders' actual location. The OPFOR will conduct deception operations that portray inaccurate defender locations and strengths. Such measures will attempt to convince the attacker to strike areas where he will inflict minimal damage to the defenders, or maneuver himself to a position of disadvantage, such as the center of a kill zone.

Defense of a CBP

CBPs are designed to protect the units within them from detection and attack while denying their seizure and occupation by the enemy. CDRs occupying CBPs intend to preserve their combat power until conditions permit offensive action. In the case of an attack, CBP defenders will engage only as long as they perceive an ability to defeat aggressors. Should the defending CDR feel that his forces are decisively overmatched, he will attempt a withdrawal in order to preserve combat power.

Units defending in CBPs will use restrictive terrain and engineer countermobility efforts to deny the enemy the ability to approach, seize, and occupy the position. They will also make maximum use of C3D and cultural standoff to deny the enemy the ability to detect and attack the position.

C3D measures are critical to the success of a CBP, since the defender generally wants to avoid enemy contact. Additionally, forces within a CBP will remain dispersed to negate the effects of precision ordinance strikes. Generally, once the defense is established, non-combat vehicles will be moved away from troop concentrations to reduce their signature on the battlefield.

To reduce exposure to enemy standoff fires and RISTA, cultural standoff can be used in conjunction with CBPs. Cultural standoff is the fact that protection from enemy weapon systems can be gained through actions that make use of cultural differences to prevent or degrade engagement. Examples of cultural standoff are—

- Using a religious or medical facility as a base of fire
- Firing from within a crowd of noncombatants
- Tying prisoners in front of BPs and onto combat vehicles

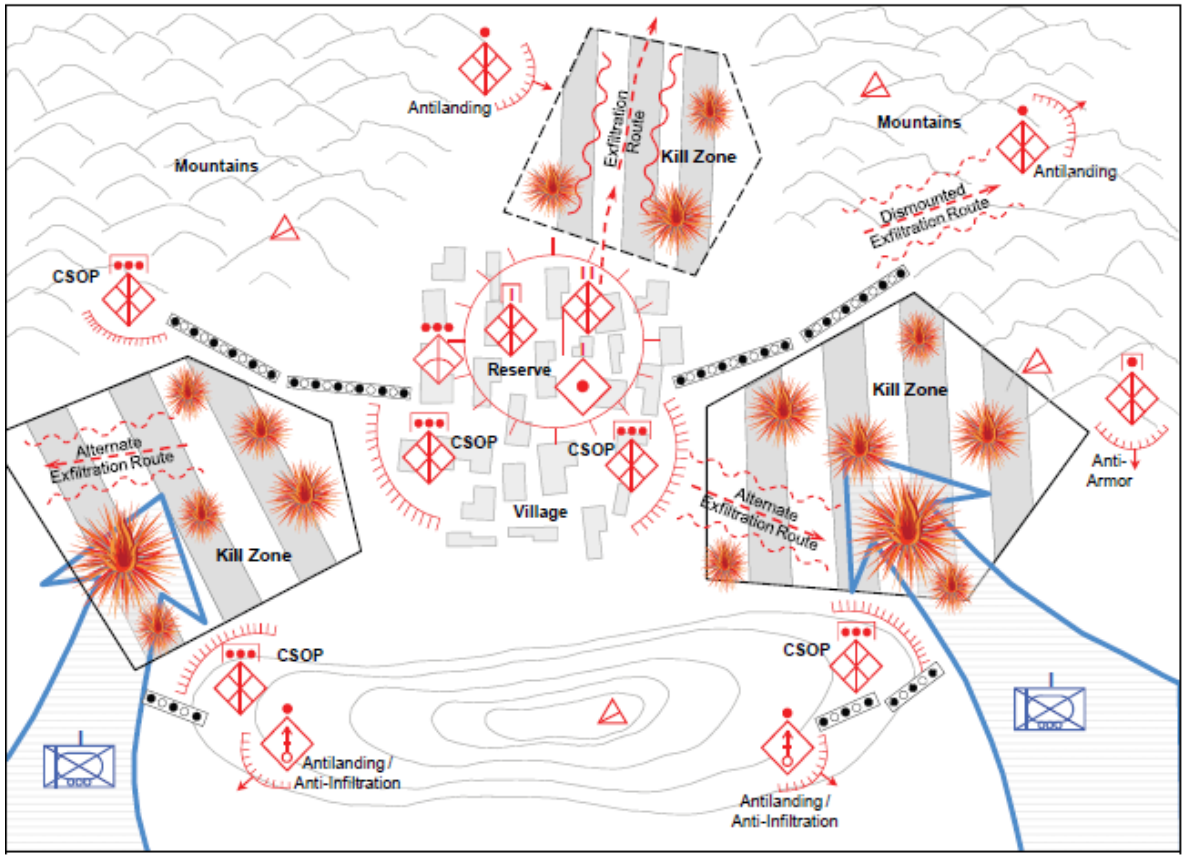


Figure 7-11. Defense of a CBP

Functional Organization of Elements to Defend a CBP

The CDR of a detachment, BN, or CO defending a CBP designates his subordinate units as functional elements. The name of the element describes its function within the defensive action.

Disruption Element

The disruption element of a CBP is primarily concerned detecting attackers and providing early warning to the defending force. To accomplish these tasks, the disruption element may form CSOPs and ambush teams. In addition to observation posts and ground ambushes, the disruption element can establish antilanding ambushes and ALRs. When the CBP is attacked, disruption elements will remain in position to provide the OPFOR CDR with a reconnaissance capability. The disruption element may also include indirect fire assets, such as mortars, to provide immediate, directly observed, harassing fires.

Main Defense Element
The main defense element of a CBP is responsible for defeating an attacking force. It can also cover the withdrawal of the support element in the case of an evacuation of the CBP.

Reserve Element
The reserve element of a CBP exists to provide the OPFOR CDR with tactical flexibility. During the counterreconnaissance battle, the reserve may augment disruption elements, in order to provide additional security to the main defense element. However, the reserve will rarely do so if such action would reveal the location of the CBP to the enemy. Some typical additional tasks given to the CBP reserve may include—

- Conducting a counterattack
- Conducting counterpenetration (blocking or destroying enemy penetration of the CBP)
- Conducting antilanding defense
- Assisting engaged forces in breaking contact
- Acting as a deception element

Support Element
The support element of a CBP has the mission of providing one or more of the following to the defending force:

- CSS
- C2
- Supporting direct fire (such as heavy MG, ATGM, recoilless rifle, or automatic grenade launcher)
- Supporting indirect fire (mortar or artillery)
- Supporting nonlethal actions (for example, jamming, psychological warfare, or broadcasts)
- Engineer support

Organizing the Battlefield for a CBP

A detachment, BN, or CO CDR specifies the organization of the battlefield from the perspective of his level of command. As at higher levels, this normally consists of a battle zone and a support zone. It may also include a disruption zone.

Disruption Zone
The BN, CO, or detachment defending in the CBP may send out CSOPs and/or ambush teams into the disruption zone.

Battle Zone
The battle zone is the area where the defending CDR commits a major part of his force to the task of defeating attacking enemy forces, or delaying them while the defenders withdraw. In the defense of a CBP, the battle zone is typically the area in and surrounding the CBP that the defending force can influence with its direct fires. It may be larger depending on the scheme for maneuver and indirect fires the defending CDR wishes to employ.

Support Zone
The support zone may contain C2, CSS, indirect and direct support fire assets, the reserve, and other supporting assets. The support zone is located within the CBP.

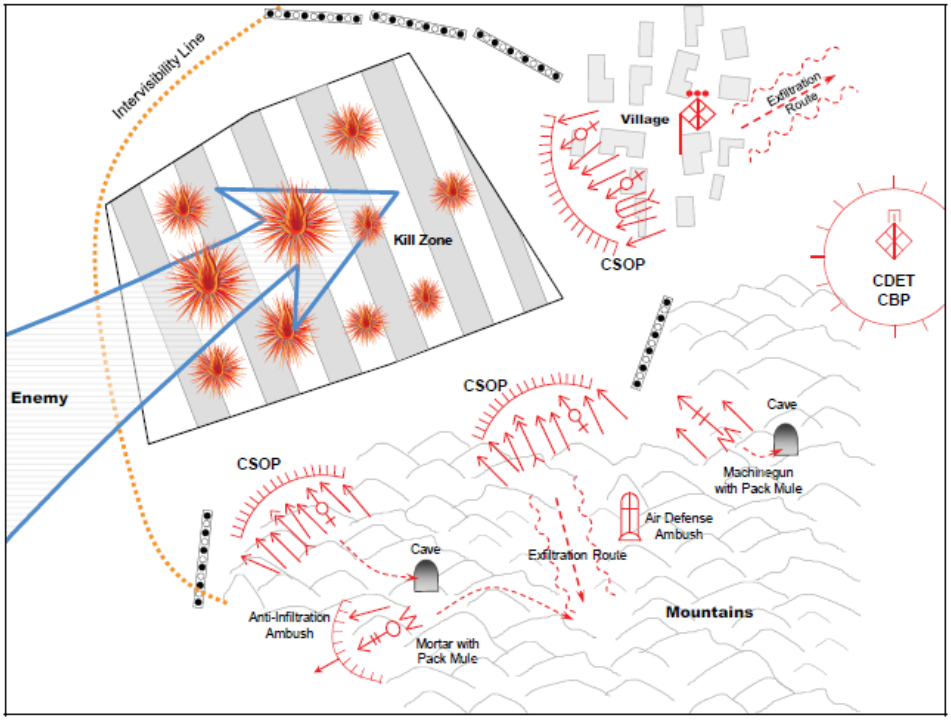


Figure 7-12. CSOPs in the disruption zone supporting a CBP, example 1

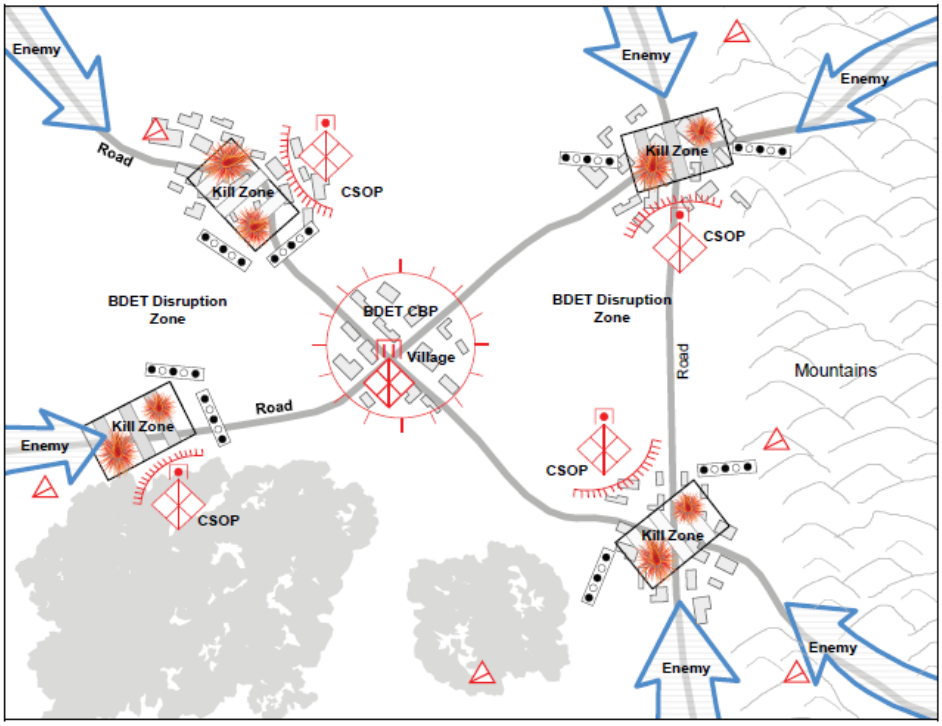


Figure 7-13. CSOPs in the disruption zone supporting a CBP, example 2

C2 of a CBP is difficult, and defenders will use secure communications including wire and couriers.

Support of a CBP may include reconnaissance, armor, fire support, air defense, engineer, logistics, and INFOWAR.

Chapter 8

OPFOR Weapons Systems and Equipment in the *Worldwide Equipment Guide (WEG)*

Introduction

In today's complicated and uncertain world, it is impossible to predict the exact nature of the next conflict that may involve U.S. forces. We must be ready to meet the challenges of any type of conflict, in all kinds of places, and against all types of threats in all OEs. As a training tool, the OPFOR must be a challenging, uncooperative sparring partner capable of stressing any or all warfighting functions and mission-essential tasks of the U.S. force.

The 7-100 series describes the doctrine, organizations, TTP, and equipment of such an OPFOR and how to combine it with other operational variables to portray the qualities of a full range of conditions appropriate to Army training environments.

The WEG was developed to support the 7-100 series and all OPFOR portrayal in training simulations (live, virtual, constructive, and gaming). The equipment portrayed in the WEG represents military systems, variants, and upgrades that U.S. forces may encounter now and in the near future. The authors continually analyze real-world developments, capabilities, and trends to guarantee the OPFOR remains relevant.

Published in three volumes, (Ground; Airspace & Air Defense Systems; and Naval & Littoral Systems) the WEG is the approved document for OPFOR equipment data used in U.S. Army training. Annual updates are posted on the TRISA Army Knowledge Online (AKO) website. Therefore, it is available for downloading and local distribution. Distribution is unlimited.

The WEG contains technical data on the capabilities of systems identified as "Principal Items of Equipment" in the AFS organizational directories and/or in the equipment tier tables or substitution matrices of the WEG. The WEG describes base models or upgrades of equipment base models, which reflect current capabilities. Many less common variants and upgrades are also addressed.

The WEG is organized by categories of equipment, in chapters. The format of the equipment pages is basically a listing of parametric data. This permits updating on a standardized basis as data becomes available. For meanings of acronyms and terms, see the Glossary. Please note that, although most terms are the same as U.S. terminology some reflect non-U.S. concepts and are not comparable or measurable against U.S. standards. For example, if an OPFOR armor penetration figure does not say RHA (rolled homogeneous armor), do not assume that is the standard for the figure.

The WEG and other OE training products are available for downloading at the TRISA CTID site at https://atn.army.mil/dsp_template.aspx?dpID=311

Equipment Tier Tables

OPFOR equipment is broken into four "tiers" in order to portray systems for adversaries with differing levels of force capabilities for use as representative examples of a rational force developer's systems mix. Equipment is listed in convenient tier tables for use as a tool for trainers to reflect different levels of modernity. Each tier provides an equivalent level of capability for systems across different functional areas. The tier tables are also another tool to identify systems in simulations to reflect different levels of modernity. The key to using the tables is to know the tier capability of the initial organizations to be provided. Tier 2 (default OPFOR level) reflects modern competitive systems fielded in significant numbers for the last 10 to 20 years.

Systems reflect specific capability mixes, which require specific systems data for portrayal in U.S. training simulations (live, virtual, and constructive). The OPFOR force contains a mix of systems in each tier and functional area which realistically vary in fielded age and generation. The tiers are less about age of the system than realistically reflecting capabilities to be mirrored in training. Systems and functional areas are not modernized equally and simultaneously. Forces have systems and material varying 10 to 30 years in age in a functional area. Often military forces emphasize upgrades in one functional area while neglecting upgrades in other functional areas. Force designers may also draw systems from higher or lower echelons with different tiers to supplement organizational assets. Our functional area analysts have tempered depiction of new and expensive systems to a fraction of the OPFOR force. The more common modernization approach for higher tier systems is to upgrade existing systems.

Some systems are used in both lower and higher tiers. Older 4x4 tactical utility vehicles which are 30 to 40 years old still offer effective support capability, and may extend across three tiers. Common use of some OPFOR systems also reduces database maintenance requirements.

> **Tier 1** systems are new or upgraded robust state-of-the-art systems marketed for sale, with at least limited fielding, and with capabilities and vulnerabilities representative of trends to be addressed in training. But a major military force with state-of-the-art technology may still have a mix of systems across different functional areas at Tier 1 and lower tiers in 2012.
>
> **Tier 2** reflects modern competitive systems fielded in significant numbers for the last 10 to 20 years, with limitations or vulnerabilities being diminished by available upgrades. Although forces are equipped for operations in all terrains and can fight day and night, their capability in range and speed for several key systems may be somewhat inferior to U.S. capability.
>
> **Tier 3** systems date back generally 30 to 40 years. They have limitations in all three subsystems categories: mobility, survivability and lethality. Systems and force integration are inferior. However, guns, missiles, and munitions can still challenge vulnerabilities of U.S. forces. Niche upgrades can provide synergistic and adaptive increases in force effectiveness.
>
> **Tier 4** systems reflect 40 to 50 year-old systems, some of which have been upgraded numerous times. These represent Third World or smaller developed countries' forces and irregular forces. Use of effective strategy, adaptive tactics, niche technologies, and terrain limitations can enable a Tier 4 OPFOR to challenge U.S. force effectiveness in achieving its goals. The tier includes militia, guerrillas, special police, and other forces.

Note: No force in the world has all systems at the most modern tier. Even the best force in the world has a mix of state-of-the-art (Tier 1) systems, as well as mature (Tier 2), and somewhat dated (Tier 3) legacy systems. Many of the latter systems have been upgraded to some degree, but may exhibit limitations from their original state of technology. Even modern systems recently purchased may be considerably less than state-of-the-art, due to budget constraints and limited user training and maintenance capabilities. Thus, even new systems may not exhibit Tier 1 or Tier 2 capabilities. As later forces field systems with emerging technologies, legacy systems may be employed to be more suitable, may be upgraded, and continue to be competitive. Adversaries with lower tier systems can use adaptive technologies and tactics, or obtain niche technology systems to challenge advantages of a modern force.

A major emphasis in an OPFOR is flexibility in use of forces and in doctrine. This also means OPFOR having flexibility, given rational and justifiable force development methodology, to adapt the systems mix to support doctrine and plans. The tiers provide the baseline list for determining the force mix, based on scenario criteria. The OPFOR compensates for capability limitations by using innovative and adaptive TTP. Some of these limitations may be caused by the lack of sophisticated equipment or integration capability, or by insufficient numbers. Forces can be tailored in accordance with OPFOR guidance to form tactical groups.

An OPFOR force developer has the option to make selective adjustments such as use of niche technology upgrades such as in tanks, cruise missiles, or rotary-wing aircraft, to offset U.S. advantages (see WEG Chapter 15, Equipment Upgrades). Forces may include systems from outside of the overall force capability level. A Tier 3 force might have a few systems from Tier 1 or 2. With savvy use of TTP and systems, all tiers may offer challenging OPFOR capabilities for training.

Below are examples of Tier Tables and Substitution matrices.

Equipment Tier Table (Example) from 2013.

Volume I: Ground Forces

	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
Dismounted Infantry				
Infantry Flame Launcher	Shmel-M	RPO-A	RPO	LPO-50
Lt AT Disposable Launcher	Armbrust	Armbrust	Armbrust	Rocket Propelled Grenade (RPG)22
AT Disposable Launcher	RPG-27	RPG-27	RPG-27	RPG-22
AT Grenade Launcher (ATGL)	Panzerfaust 3-IT600	Panzerfaust 3 T-600	Carl Gustaf M3	RPG-7V
Long-Range ATGL	PF-98 Mounted/Tripod (@ Bn)	RPG-29/Mounted/Tripod	SPG-9M (Imp)	SPG-9
Heavy ATGM Man-Portable	Eryx SR-ATGM	Eryx SR-ATGM	M79/Type 65-1 Recoilless	M67 Recoilless Rifle
Light Auto Grenade Launcher	QLZ-87	W-87	W-87	W-87
Auto Grenade Launcher	CIS-40 w/Air-Burst Munition	CIS-40	AGS-17	AGS-17
Heavy Machine Gun	NSV	NSV	NSV	DShK
General Purpose MG	PKM	PKM	PKM	PKM
Anti-Materiel Rifle	M82A1 .50 Cal	M82A1	M82A1	M82A1
Sniper Rifle	SVD	SVD	SVD	Mosin-Nagant
Assault Rifle	AK-74M	AK-74M	AKM	AKM
Carbine	AKS-74U	AKS-74U	AK-47 Krinkov	AK-47 Krinkov
CO-Dismount ATGM	Spike-LR ATGM Launcher	Spike-MR ATGM Launcher	AT-13	AT-7
BN-Dismount ATGMs	Kornet-E Launcher (1 team) Starstreak-SL AD/AT (1 team)	Kornet-E ATGM Lchr	AT-5B	AT-5

Systems Substitution Matrices

In each volume of the WEG, a Systems Substitution Matrix table provides comparative data for users who would like to substitute other systems for OPFOR systems listed in the baseline organizational directories. For each system, the table shows the system name, its tier level, and the WEG page on which data for that system begins. Within each functional area, systems are displayed in groups (with spaces separating the groups) of systems of like type that could be substituted for one another. Within each group, the system shown in *italics* is the one listed in TC 7-100.4 as the baseline system (normally Tier 2) in some OPFOR organization. Within each grouping by type, most systems are listed in tier order, and can be substituted to fit scenario requirements. Some systems span the boundary between two tiers (for example, "3-4"). Other systems can be used at more than one tier (for example, "3 and 4"). The Table below provides a sample from the Systems Substitution Matrix in volume 1 of the 2013 WEG.

Systems Substitution Matrix (Example) from 2013

Example from the WEG: AUG 2013 Volume 1, Chapter 02, Infantry

Chinese 120-mm ATGL PF-98 _____

PF-98 launcher CO version

PF-98 launcher BN version

Ammunition Types	Typical Combat Load
120-mm grenade Tandem HEAT Multipurpose	**5**

SYSTEM
Alternative Designations: Queen Bee
Date of Introduction: 2000
Proliferation: At least one country

Description:
Crew: 2, 3 if more rounds are needed
Caliber (mm):
Launch Tube: 120
Warhead: 120
Weight (kg): INA
Length (mm):
Firing Position: INA
Travel Position: INA
Rifling: None
Breech Mechanism Type: Rocket canister is attached to end of launcher, extending the launch tube.
Launcher mount: Shoulder for CO launcher, Tripod, shoulder, or pintle for BN launcher.
Rate of Fire (rd/min): 4-6
Fire From Inside Building: No

SIGHTS
Name: Y/MK/PF98(Y)-120
Type: Ballistic computer laser range-finder (LRF) sight for BN version, and optical telescope for CO sight
Magnification: 4 telescope for CO sight.
Location: Left side
Used With Range Finder: Yes
Night Sight: Thermal, range 500 m on BN sight
II night sight 300 m for CO sight

AMMUNITION
Name: HEAT, with time fuze
Caliber (mm): 120
Type: Tandem HEAT (shaped charge)
Range (m): 800 BN, 400-500 with CO level launcher
Penetration (mm CE): 800+
Weight (kg): 6.4
Time of Flight (sec): 10

Name: Multipurpose
Caliber (mm): 120
Type: Frag-HE-Incendiary (120 steel balls)
Range (m): 2,000
Penetration: 400 mm KE for steel balls, 25 m lethal radius
Weight (kg): 7.6

VARIANTS
CO and BN versions fire the same rounds. In subsequent years, these systems will proliferate throughout BNs in weapons units and into infantry platoons and lower. Over time the BN version will replace squad ATGLs.
BN system could be a representative OE Tier 1 ATGL for infantry units.

NOTES: The PF-98 appears to have employed propulsion principles from the Swedish Bofors Carl Gustaf 84-mm M2/M3 recoilless gun. The Carl Gustaf has a compact round with an expulsion charge to launch its grenade, a method which offers greater precision than more common rocket-propelled systems. But like the more recent and larger Gustaf rounds, the PF-98 added rocket assist to extend projectile ranges. Thus the producer refers to PF-98 as an "AT rocket launcher". By using sealed canisters to serve as launcher extensions, Queen Bee offers a trend-setting and effective way to increase lethality by growing ammunition to 120-mm, while retaining portability and extending range capability.

Israeli Mini-UAVs Skylark, Skylark II, and Skylark IV

SYSTEM
Alternative Designations:
Derived from the Skylark I (previously called Skylark)
Date of Introduction: 2004
Proliferation: Skylark I is used in at least 4 countries, and has been employed in Iraq and Afghanistan.

Description:
Engines: Electric, horsepower INA
Fuel (liters): Battery-powered
Propulsion: 2-blade pusher propeller
Weight (kg):
Takeoff: 5.5
Payload (combined): 0.5, 0.7 night
Speed (km/h):
Maximum (level): 74
Cruise: 74
Maximum Ceiling (m): 4,600
Endurance (hr): 2.0
Range (km): 10 mission radius
Dimensions (m):
Wing Span: 2.4
Deployment:
Crew: 2 (can be 3 dismounted). If vehicle carried, crewing is an alternate duty.
Number of aircraft: 3 per team
Carry: Breaks down for 2 backpacks
Launch Method: Hand launch. Other options are vehicle and aircraft
Recovery Method: One button for return flight and deep stall landing, without operator action.
Landing Method: Inflatable cushion

Survivability/Countermeasures:
It has a light composite structure, for low radar signature. The aircraft is extremely quiet. It has excellent flight dynamics for use in all **climates and severe weather.**

VARIANTS:
Skylark uses technologies from the Pointer program. Original Skylark is aka Skylark I. Skylark IV is a slightly improved version, ruggedized and gyro-stabilized.

Skylark II: **Slightly larger (35-kg) UAV which can be vehicle launched from a rail.**

SENSOR/OPTICS
Payload Type:
Day: Gimbaled gyro-stabilized daylight CCD camera with EO auto-tracker. The auto-tracker aids tracking moving vehicles.
Night: Thermal camera

FLIGHT CONTROL
Control System:
Hand-held Miniature Ground Control Station (GCS) with color TV console
Other terminals (photo left) can be used.

Flight control Method:
Continuous telemetry transmission with Spectralink data link. It can use one of various radio channels to avoid channel interference.
Programmed Mode Option: Yes. It can operate in "camera guide" mode, digitally tracing its map route with video recording for use in aircraft flight planning.

NOTES: Tactical UAVs sometimes crash. With a lower cost and volume production, they are more plentiful and more easily replaced than larger UAVs. A Skylark I crashed during operations in the West Bank, sustaining some damage. In one account, a Skylark experienced operational malfunctions in use by Canadian forces. Malfunctions have not been noted with Skylark IV.

Example from the WEG: AUG 2013 Volume 3, Chapter 3, Littoral Systems

Swedish Fast Assault Craft CB90H

Weapons	Combat Load
.50-cal Twin MG Fixed	1
.50-cal MG Pintle Mount	1
Alternatives for Pintle:	
Mk 19 40mm AGL	1
HELLFIRE ATGM	1
Other Options:	
Naval Mines or Depth Charges	4 6

SYSTEM
Alternative Designations: Combat Boat 90 H (Stridsbat 90, aka Strb 90 - Swedish). For designation, various spacings and forms are used, i.e., CB-90, CB 90 H, CB 90H, etc.
Date of Introduction: 1991 commissioned
Proliferation: At least 8 countries. Mexico produces CB90HM.
Description:
Crew: 4, plus 21-30 troops
Displacement (tons): 20 full load
Hull Materials: Aluminum
Length Overall (m): 14.9
Height of hull (m): 4.6
Beam (m): 3.8
Draft (m): .9

Performance:
Speed (knots): 50 (74 k/hr)
Range (nautical miles): 440
Propulsion: 2 x water jets and 2 x Scania DS114 diesel engines
At least 3other engine arrangements are used.
Protection:
Armor: See CB90HS variant
Buoyancy: Sealed compartment in aft area
NBC: Collective in forward-mid areas
Auxiliary Power Unit: Yes

FIRE CONTROL
Electro-Optics: EO sight for remote FCS on main gun
Radar: Naval patrol version

ARMAMENT
Main Armament:
Caliber, Type, Name: Twin .50 cal (12.7 x 99) MG , M2HB
Mount: Fixed forward firing, front hull, starboard side
Rate of Fire (rd/min): 900-1100 cyclic
Loader Type: Belt feed
Ready/Stowed Rounds: 750
Elevation (°): -20/+60
Fire on Move: Yes

Other Weapons:
1 x 12.7-mm MG M2HB on midway pintle mount. The gun can be replaced with a Mk 19 AGL.
Firing Ports: 6

VARIANTS
Variants include naval versions, riverine patrol craft, an ambulance version, and others.

CB90HS: Armored version with NBC protection, more engine hp, and protected against 7.62-mm rounds.

CB90HCG: Greek Coast Guard version with a raised structure, different engines, additional navigation, radars, and sonar.

CB90N: Naval patrol craft with superstructures and other crew accommodations.

CB90 patrol version

NOTES: Weapons, sensors, and countermeasures vary among vessels in the class. An option for future development is AMOS 120 mm mortar with twin auto-load direct fire. Another consideration is the RBS 17 MANPADS launcher.

Appendix A

OPFOR Tactical Task List

This appendix is from TC 7-101, *Exercise Design*, dated November 2010 that can be downloaded from the Army Training Network at https://atn.army.mil/dsp_template.aspx?dpID=311. This appendix is not a replacement document for TC 7-101, and is not comprehensive.

The OPFOR Tactical Task List is a listing of tactical tasks that are specific to the OPFOR. OPFOR tactical organizations and individuals perform these tasks instead of the comparable tasks in the Army Universal Task List (AUTL). OPFOR organizations and individuals perform tactical tasks in order to provide challenging conditions for the execution or attempted execution of mission essential tasks by training units.

Tactical Task 1.0 Assault. An assault is an attack that destroys an enemy force through firepower and the physical occupation and/or destruction of his position. An assault is the basic form of OPFOR tactical offensive combat.

Tactical Task 2.0 Raid. A raid is an attack against a stationary target for the purposes of its capture or destruction that culminates in the withdrawal of the raiding detachment to safe territory. Raids can also be used to secure information and to confuse or deceive the enemy. The keys to the successful accomplishment of any are raid surprise, firepower, and violence. The raid ends with a planned withdrawal upon completion of the assigned mission.

Tactical Task 3.0 Ambush (Annihilation). An ambush is a surprise attack from a concealed position, used against moving or temporarily halted targets. The purpose of an annihilation ambush is to destroy the enemy force. These are violent attacks designed to ensure the enemy's return fire, if any, is ineffective. Generally, this type of ambush uses the terrain to the attacker's advantage and 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.

Tactical Task 4.0 Reconnaissance Attack. A reconnaissance attack is a tactical offensive action that locates moving, dispersed, or concealed enemy elements and either fixes or destroys them. It may also be used to gain information. The reconnaissance attack may involve multiple security and assault elements.

Tactical Task 5.0 Reconnaissance. Reconnaissance represents all measures associated with organizing, collecting, and studying information on the enemy, terrain, and weather in the area of upcoming battles.

Tactical Task 6.0 Counterreconnaissance. Counterreconnaissance (CR) is a continuous combined arms action to locate, track and destroy all enemy reconnaissance operating in a given AOR. CR is conducted at all times and during all types of operations.

Tactical Task 7.0 Defend from Simple Battle Position (SBP). An SBP is a defensive location oriented on the most likely enemy avenue of approach or objective area. SBPs are not necessarily tied to restrictive terrain but will employ as much engineer effort as possible to restrict enemy maneuver. Defenders of SBPs will take all actions necessary to prevent enemy penetration of their position, or defeat a penetration once it has occurred. Unlike a complex battle position, which is typically independent, an SBP may form a larger integrated defense with other SBPs.

Tactical Task 8.0 Defend from Complex Battle Position (CBP). CBPs are designed to protect the units within them from detection and attack while denying their seizure and occupation by the enemy. They are not necessarily tied to an avenue of approach. CBPs protect forces while providing sanctuary from which to launch local attacks.

Tactical Task 9.0 Actions on Contact. Actions on contact are designed to ensure OPFOR units retain the initiative and fight under circumstances of their choosing. Actions on contact are also designed to provide the commander with the flexibility to either continue with the planned course of action or rapidly adopt a new course of action more suited to changed conditions.

Tactical Task 10.0 Situational Breach. A situational breach is the reduction of and passage through an obstacle encountered in the due course of executing another tactical task. The unit conducting a situational breach may have expected an obstacle or not, but in either case conducts a situational breach with the resources at hand and does not wait for specialized equipment and other support.

Tactical Task 11.0 Breaking Contact. The primary consideration in breaking contact is to remove the enemy's ability to place destructive or suppressive fires on the greater portion of the OPFOR force. This is accomplished by fixing the enemy, regaining freedom to maneuver and employing fires, counter-mobility and C3D.

Tactical Task 12.0 Fixing. Fixing is a tactical task intended to prevent the enemy from moving any part of his force from a specific location for a period of time. The ability to fix the enemy at crucial points is the fundamental way units maintain the freedom to maneuver and retain the initiative. An enemy becomes fixed in one of three basic ways: he cannot physically move, he does not want to move, or he does not think he can move. Suppressive fires, INFOWAR and countermobility are the primary methods by which an enemy is fixed in this way.

Tactical Task 13.0 Tactical Movement. Tactical movement is the method by which OPFOR units move on the battlefield. It is employed in any situation where enemy contact is possible. It is most often used in offensive operations, to move from attack position to the point of attack.

Tactical Task 14.0 Disruption. Disrupt is a tactical task intended to upset an enemy's formation or tempo, interrupt the enemy's timetable, cause the enemy to commit his forces prematurely, and/or cause him to attack in piecemeal fashion. The purpose of a disruption force is to significantly degrade the enemy's combat capability and to prevent the enemy from conducting an effective operation. The primary task of the disruption force is to initiate the attack against the enemy's combat system.

Tactical Task 15.0 Integrated Attack. Integrated attack is an offensive action where the OPFOR seeks military decision by destroying the enemy's will and/or ability to continue fighting through the application of combined arms effects. Integrated attack is often employed when the OPFOR enjoys overmatch with respect to its opponent and is able to bring all elements of offensive combat power to bear. It may also be employed against a more sophisticated and capable opponent, if the appropriate window of opportunity is created or available.

Tactical Task 16.0 Dispersed Attack. Dispersed attack is the primary manner in which the OPFOR conducts offensive action when threatened by a superior enemy and/or when unable to mass or provide integrated C2 to an attack. This is not to say that the dispersed attack cannot or should not be used against peer forces, but as a rule integrated attack will more completely attain objectives in such situations. Dispersed attack relies on INFOWAR and dispersion of forces to permit the OPFOR to conduct tactical offensive actions while overmatched by precision standoff weapons and imagery and signals sensors. The dispersed attack is continuous and comes from multiple directions. It employs multiple means working together in a very interdependent way. The attack can be dispersed in time as well as space.

Tactical Task 17.0 Fire and Maneuver. Fire and maneuver is the way in which OPFOR small units move while in contact with the enemy. When required to move while in contact with the enemy, the OPFOR commander selects a part of his force to be the support (or firing) element and part to be the action (or moving) element. The support element then directs suppressing fire against any enemy that has the ability to influence the movement of the action element. The action element then moves either to a firing line or to the objective. Once it reaches its new position, it becomes the new support element, and the former support element becomes the new moving element.

Tactical Task 18.0 All-Arms Air Defense. All-arms air defense is the simultaneous employment of several arms, in some cases including air defense systems, to achieve an effect against the enemy air threat that will render greater results than the use of air defense assets and systems alone. Thus, all OPFOR units possess some type of an organic air defense capability to differing degrees, depending on the type and size of the unit. The extent to which this capability can be applied is limited only by the commander and staff's knowledge of the enemy air threat, capabilities of their own systems, and their ability to apply that knowledge to come up with innovative solutions.

Tactical Task 19.0 Antilanding Actions. Antilanding actions are those methods used to prevent landings by airborne or heliborne troops or to destroy enemy landing forces on the ground as soon after landing as possible. Antilanding actions can and will be executed by any force with the capability to affect the aircraft or the landing forces. However, this is a combined arms action that primarily falls to the ALR for execution.

Tactical Task 20.0 Sophisticated Ambush. A sophisticated ambush is the linking in time and task of RISTA, attacking forces, and window of opportunity to destroy key enemy systems or cause politically unacceptable casualties. What makes a sophisticated ambush "sophisticated" is not the actual attack means. In fact, the actual ambush is executed by tactical-level forces. What makes it "sophisticated" is the linking of sensor, ambusher, window of opportunity, and a target that affects an enemy center of gravity.

Tactical Task 21.0 Maneuver Defense. A maneuver defense is a type of defensive action designed to achieve tactical decision by skillfully using fires and maneuver to destroy key elements of the enemy's combat system and deny enemy forces their objective, while preserving the friendly force. Within the enemy's combat system, the OPFOR would often target the enemy's C2 or logistics forces rather than his less vulnerable combat and combat support forces. Maneuver defenses cause the enemy to continually lose effectiveness until he can no longer achieve his objectives. They can also economize force in less important areas while the OPFOR moves additional forces onto the most threatened axes.

Tactical Task 22.0 Area Defense. Area defense is a type of defensive action designed to achieve a decision by either—

- Forcing the enemy's offensive operations to culminate before he can achieve his objectives or
- Denying the enemy his objectives while preserving combat power until decision can be achieved through strategic operations or operational mission accomplishment.

The area defense does not surrender the initiative to the attacking forces, but takes action to create windows of opportunity that permit forces to attack key elements of the enemy's combat system and cause unacceptable casualties.

Tactical Task 23.0 Information Warfare. Information warfare (INFOWAR) is defined as specifically planned and integrated actions taken to achieve an information advantage at critical points and times. The goal is to influence an enemy's decisionmaking 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.

Tactical Task 24.0 Insurgency. Insurgent forces are groups that conduct irregular or unconventional warfare within the borders or their country in order to undermine or overthrow a constituted government or civil authority. 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.

Appendix B

Glossary

ALR – Anti-Landing Reserve

AOR – Area of Responsibility

APC – Armored Personnel Carrier

AFS – Administrative Force Structure

AKO – Army Knowledge Online

AR – Army Regulation

AT – Antitank

ATGL – Antitank Grenade Launcher

ATGM – Antitank Guided Missile

ATR – Antitank Reserve

AUTL – Army Universal Task List

BDE - Brigade

BDET – Battalion Detachment

BN - Battalion

BP – Battle Position

BTG – Brigade Tactical Group

C2 – Command and Control

C3D – Camouflage, Cover, Concealment, and Deception

CBP – Complex Battle Position

CDET – Company Detachment

CDR - CDR

CFS – Chief of Fire Support

CO - Company

COA – Course of Action

CP – Command Post

CRD – Counterreconnaissance Detachment

CSOP – Combat Security Outpost

CSS – Combat Service Support

CTC – Combat Training Center

DATE – Decisive Action Training Environment

DIV - Division

DTG – Division Tactical Group

DZ – Drop Zone

EW – Electronic Warfare

FARP – Forward Arming and Refueling Points

FG – Field Group

FM - Field Manual

GPS – Global Positioning System

H/K – Hunter/Killer

HQ - Headquarters

HST – Home Station Training

ICT - Information and Communications Technology

IDP – Internally Displaced Person

IED – Improvised Explosive Device

IEW – Intelligence and Electronic Warfare

IFC – Integrated Fires Command

IFV – Infantry Fighting Vehicle

IMD – Independent Mission Detachment

ISC – Integrated Support Command

INFOWAR – Information Warfare

LOC – Line of Communications

LOR – Limit of Responsibility

LZ – Landing Zone

MANPADS – Man-Portable Air Defense System

METL – Mission Essential Task List

MG - Machinegun

MRL – Multiple Rocket Launcher

MRX – Mission Rehearsal Exercise

MSD – Movement Support Detachment

NGO – Non-Governmental Organization

OB – Order of Battle

OD – Obstacle Detachment

OE – Operational Environment

OEA – Operational Environment Assessment

OPFOR – Opposing Forces

OSC – Operational-Strategic Command

PMESII-PT – Political, Military, Economic, Social, Information, Infrastructure, Physical Environment, and Time

PSO – Private Security Organization

RAF – Regionally Aligned Force

RD – Reconnaissance Detachment

RISTA – Reconnaissance, Intelligence, Surveillance, and Target Acquisition

RPG – Rocket Propelled Grenade

SAMS – Surface-to-Air Missile System

SBP – Simple Battle Position

SD – Security Detachment

SPF – Special Purpose Force

SSM – Surface-to-Surface Missile

ST – Student Text

TC – Training Circular

TOE - Table of Organization and Equipment

TRISA – Training and Doctrine Command Intelligence Support Activity

TTP - Tactics, Techniques, and Procedures

UAV – Unmanned Aerial Vehicle

UD – Urban Detachment

WEG – Worldwide Equipment Guide

WMD – Weapons of Mass Destruction