TRADOC G-2

OPFOR/DATE

Leader's Smartbook

Victory Starts Here!

FOREWORD

This **Smartbook** on Opposing Forces (OPFOR) tactics and the Decisive Action Training Environment (DATE) is a quick reference guide that summarizes key aspects of exercise design for leaders and planners across the Army. For expansion on any of the topics presented herein, readers should reference the TRADOC Circular (TC) 7-100 series manuals, available via the Army Training Network (ATN) at https://atn.army.mil.

The Exercise Design Guide (TC 7-101) provides the foundation for exercise planners to determine how to create training *"conditions"* within exercises that reflect the complexities and dynamic nature of the operational environment (OE), as prescribed in the Army Doctrine Reference Publication 3.0 (ADRP 3.0). The Exercise Design Tool (EDT) presents planners an automated version for designing exercises, to include the selection of OPFOR counter-tasks, and is available via NIPR at https://tbr.army.mil or via SIPR at https://tbr.army.smil.mil. The EDT reduces the time-consuming process of searching for data from past training exercises to develop new training events by making use of a centralized repository of scenarios, orders, graphics and products that are doctrinally correct and easily manipulated. Among the features facilitated by the EDT are start-of-exercise data, mapping and graphics, storyline synchronization, higher headquarters order production, role player development, and (most importantly) data reuse to facilitate multi-year exercise refinement. The EDT is also the primary delivery vehicle for the DATE, which is the Army's unclassified composite representation of real-world OE conditions and threat capabilities for training AUTL tasks to a high level of proficiency. This Smartbook augments these digital tools as an on-the-go guide for quick reference, allowing leaders to refresh themselves on OPFOR doctrine and the DATE.

For additional information or support, users and exercise design planners can contact any of the below offices within the Training and Doctrine Command's G2:

- TRADOC G2, Ft. Eustis, VA. 757-501-6233, DSN: 501-6233
- DATE/OPFOR Doctrine: ACE-Threats, Ft. Leavenworth, 913-684-7968
- OE Training Support: G27, OE Training Support Center (OE-TSC), 757-878-9510
- OPFOR Program: G27, OPFOR Directorate (Smartbook POC), Ft. Eustis, 757-501-6168

This publication is approved for public distribution.

Table of Contents

Chapter 1 – Hybrid Threat

A. Hybrid Threat Definition. 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 Threat, 26 November 2010)

  1. Hybrid threats will use a strategic capability that forces any intervening power to adjust operations (WMD, special- purpose forces [SPF], etc.).

  2. 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.

B. 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 (rely on subversion/violence to change the status quo)
- Guerrilla units (irregular indigenous forces operating in occupied territory)
- Criminal organizations (such as gangs, drug cartels, or hackers)

C. Combatant versus Non-Combatant

  1. Combatants/Paramilitary Organizations. Organizations that accomplish their purpose, even partially, through the force of arms. Resemble regular military forces in organizations, equipment, training, or mission. The following are combatant paramilitary organizations.

    a. Insurgent Organizations. This 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.

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

    b. 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 best suited for irregular warfare and/or unconventional tactics.

    c. 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.

    d. Criminal Organizations. Entities that operate independently of nation-state control. Their large-scale organizations may extend beyond national boundaries to operate regionally or worldwide. Large-scale criminal organizations have the capability to adversely affect legitimate political, military, and judicial organizations. 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.

    e. Other Armed Combatants. Nonmilitary personnel who are armed but not part of an organized paramilitary or military structure.

    f. Unarmed Combatants. Any unarmed person who engages in hostilities or who purposely and materially supports hostilities against the United States or its co-belligerents. For example, technicians and workers who arm IEDs may not be armed.

2. Noncombatants. They are either friendly or neutral, they might provide support to combatants–either willingly or unwillingly. *Types of Noncombatants*

   a. 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; or they may be minor criminals who use their weapons for activities such as extortion and theft.

   b. Unarmed Noncombatants. Neutral or potential side-changers, depending on their perception of the United States actions. 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.

Chapter 2 – OPFOR Task Organization

A. 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.

B. 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 agree'nt

   1. 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.

   2. 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. 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.

   3. 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. In OPFOR plans and orders, the supporting command and support relationship is indicated by (SPT) next to a unit title or symbol.

   4. 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.

C. OPFOR Tactical Groups – The OPFOR forms tactical groups, at division or brigade-level by assigning 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).

1. Division Tactical Group (DTG) – The DTG is organized around an existing Divisional structure.
- The parent HQ normally augments the DTG with additional land resources as required.
- The 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 DTG normal has at least one ISC and IFC attached.
    o The **integrated fires command (IFC)** is a combination of a standing C2 structure and task organizing of constituent and dedicated fire support units.
    o The *integrated support command* **(ISC)** is the aggregate of combat service support units (and perhaps some combat support units) organic to a division and additional assets allocated from the AFS to a DTG.
- The Division is capable of exerting control over important geographic areas or medium size urban areas (population of 20,000 to 100,000).

2. Brigade Tactical Group (BTG) – The BTG is organized around an existing Brigade 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.

3. Battalions – In the OPFOR's force structure, the <u>basic unit of action is the *battalion*</u>. 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

4. 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. Companies are designed 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)

5. Detachments – A *detachment* is a BN or CO designated to perform a specific mission and allocated the forces necessary to do so. <u>Detachments are the smallest combined arms formations</u> and are, by definition, task-organized. BNs can form ***Battalion-size detachments* (BDETs)**, and companies can form ***Company-size detachments* (CDETs)**.

a. 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

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

c. 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

d. 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)

6. 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

## D. OPFOR Organization of the Tactical Battlefield

1. Area of Responsibility (AOR) – 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.

2. 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.
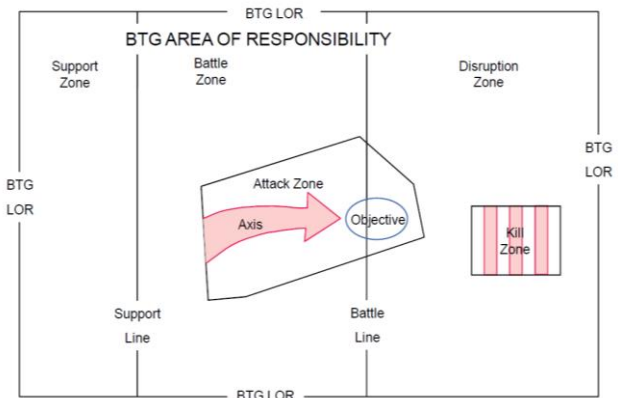
a. Offensive Battlefield Control Measures
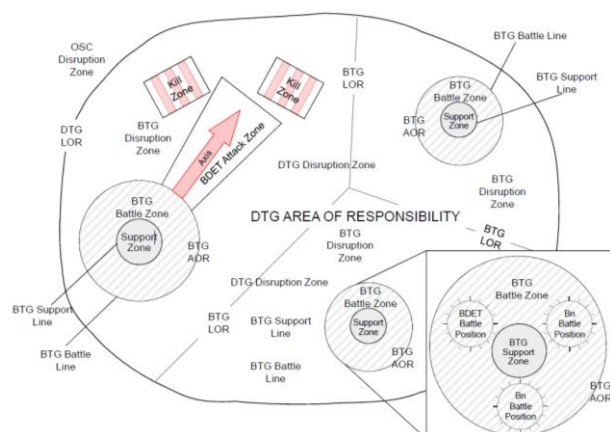
b. Defensive Battlefield Control Measures
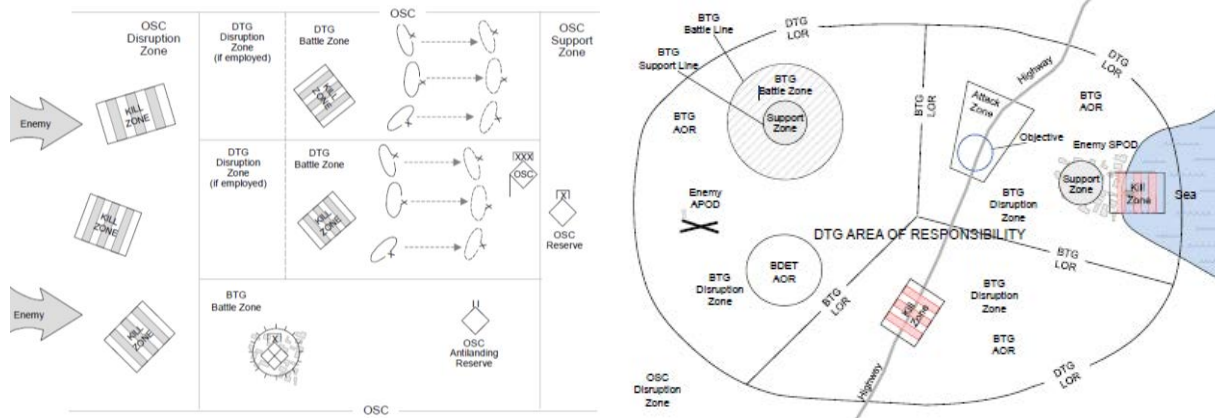
c. Battlefield Control Measure Definitions

(1) 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. The disruption zone is bounded by the battle line and the LOR of the overall AOR.

(2) Battle Zone – The *battle zone* is where the OPFOR, using fires and maneuver, engages 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:

The battle zone is separated from the disruption zone by the **battle line** and from the support zone by the **support line**.

(3) 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.

(4) 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.

(5) 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.

(6) Control Lines:
- **Support Line** – A control measure that separates the support zone from the battle zone.
- **Battle Line** – A control measure that separates the battle zone from the disruption zone.
- **Limit of Responsibility (LOR)** – A control measure that beyond which the organization may not operate or fire without coordination through the next-higher HQ

E. OPFOR Functional Organization of Forces and Elements

1. Forces and Elements:

a. Forces – Organizations at the brigade or BTG and above.

b. Elements – Organizations at the battalion or BDET and below or BTG and above.

2. ACTION FORCES AND ELEMENTS – The part of the unit or grouping of units conducting a particular offensive or defensive action that is responsible for performing the primary function or task that accomplishes the overall mission goal or objective. In most cases, however, the higher unit commander will give the action force or element a more specific designation that identifies the specific function or task it is intended to perform, which equates to achieving the objective of the higher command's mission.

a. Offensive Examples:
- Raiding Element

- Exploitation Force

b. Defensive Examples
- Main Defense Force
- In a maneuver defense, the main defensive action is executed by a combination of two functional forces: the *contact force* and the *shielding force*.

3. ENABLING FORCES AND ELEMENTS – In relation to the action force or element, all other parts of the organization conducting an offensive or defensive action provide *enabling* functions of various kinds.

However, each subordinate force or element with an enabling function can be more clearly identified by the specific function or task it performs. For example:

- **Clearing element –** An element that *clears* obstacles to permit an action element to accomplish a detachment's tactical task.
- **Disruption force or element –** A unit that operates in the disruption zone; disrupts enemy preparations or actions; destroys or deceives enemy reconnaissance; begins reducing the effectiveness of key components of the enemy's combat system.
- **Fixing force or element –** A unit that fixes the enemy by preventing a part of his force from moving from a specific location for a specific period of time, so it cannot interfere with the primary OPFOR action.
- **Security force or element –** A unit that provides security for other parts of a larger organization, protecting them from observation, destruction, or becoming fixed.
- **Deception force or element –** A unit that conducts a deceptive action (such as a demonstration or feint) that leads the enemy to act in ways prejudicial to enemy interests or favoring the success of an OPFOR action force or element.
- **Support force or element –** A unit that provides support by fire; other combat or combat service support; or C2 functions for other parts of a larger organization.

F. OPFOR Command Posts

1. Main Command Post – The *main CP* generally is located in a battle zone or in a key sanctuary area or fortified position. It contains the bulk of the staff. The COS directs its operation. Its primary purpose is to simultaneously coordinate the activities of subordinate units not yet engaged in combat and plan for subsequent missions.

2. IFC Command Post – The Deputy Commander of a DTG or division directs the IFC from the *IFC CP*. The IFC CP possesses the communications, airspace control, and automated fire control systems required to integrate RISTA means and execute long-range fires. Each secondary staff subsection and some functional staff subsections have an element dedicated to the IFC CP. The IFC CP includes liaison teams from fire support, army aviation, and long-range reconnaissance elements. The IFC CP is typically separated from the main CP.

3. Forward Command Post – A *forward CP is staffed* with a small group of selected staff members. Its purpose is to provide the commander with information and communications that facilitate his decisions. The forward CP is deployed at a point from which he can more effectively and personally observe and influence the battle.

4. Sustainment Command Post – The resources officer establishes and controls the sustainment CP. This CP is deployed in a position to permit the supervision of execution of sustainment procedures and the movement of support troops, typically in the support zone. It contains staff officers for fuel supply, medical support, combat equipment repair, ammunition supply, clothing supply, food supply, prisoner-of-war, and other services.

5. Airborne Command Post – A*irborne CP* enable the commander to maintain control in very fluid situations, when subordinates are spread over a wide area, or when the other CPs are moving, a commander may use an. This is very common in DTG- or division-level commands, typically aboard helicopters.

6. Alternate Command Post – A*lternate CP* provides for the assumption of command should the CP containing the commander be incapacitated. The alternate CP is a designation given to an existing CP and is not a separately established element.

7. Auxiliary Command Post – The *auxiliary CP* provides C2 over subordinate units fighting on isolated or remote axes.

8. Deception Command Post – The OPFOR very often employs deception CPs as part of the overall INFOWAR plan. These are complex, multi-sensor-affecting sites integrated into the overall deception plan.

G. Communications Nets – C2 of OPFOR organizations relies on extensive and redundant communications. The OPFOR primarily uses—
- UHF and SHF SATCOM.
- Radio relay multichannel.
- HF radio stations.
- HF and VHF single-channel radios.
- Wire or cable.

1. Command nets. The commander normally controls the *primary command net* from the forward CP, while the COS maintains control of the *alternate net* from the main CP. Depending on the distances involved, the primary net may be either HF or VHF. All of the command's constituent and dedicated units monitor the command nets. The DTG or division IFC CP also monitors the command nets.

2. Operations Net. The operations officer maintains an *operations net* monitored by the commander, subordinate and supporting units, and any alternate or auxiliary CP created. The resources officer also monitors this net from the sustainment CP.

3. Integrated Fires Net. The DTG or division Deputy Commander, as IFC commander, maintains the integrated fires net. This net is monitored by the elements of the IFC.

4. Support Net. The resources officer maintains the *support net*. Materiel support, maintenance, and medical units monitor this net. Subordinate combat arms units may also use this net when requiring additional, immediate assistance that constituent support assets are unable to provide.

5. Intelligence Net. The chief of reconnaissance maintains an *intelligence net,* monitored by reconnaissance units, maneuver units, the commander, DC, COS, and resources officer.

6. Airspace Control Net. The CAO maintains the *airspace control net* for the purpose of controlling the command's airspace. Elements on this net include aviation units, air defense assets, and army aviation liaison teams.

7. Special Mission Net. When required, the commander will create a *special mission net*, monitored by the COS, that is employed to control the activities of units conducting a special mission. Examples could be a reconnaissance detachment or an airborne or heliborne landing force deployed behind enemy lines. Specific communications systems employed depend on the depth and type of mission.

8. Air Defense and CBRN Warning Nets. The command maintains an *air defense and CBRN warning communications net,* monitored by all constituent, dedicated, and supporting units. This net is used for passing tactical alerts and CBRN and air warning notices. The COS maintains a watch on the DTG- or division-level warning nets at the main CP; he then disseminates warning where appropriate.

9. Deception Net(s). The chief of INFOWAR may also control one or more deception nets designed to mislead enemy signals intelligence analysis.

Chapter 3 – OPFOR Offensive Tactics

A. Purpose of the Offense. The OFFENSE is the decisive form of combat and the ultimate means of imposing the OPFOR's will on the enemy. OPFOR CDRs seek to create and exploit opportunities to take offensive action whenever possible. Six general **purposes of the offense:**
- Attack to gain freedom of movement
- Attack to restrict freedom of movement
- Attack to gain control of key terrain, personnel, or equipment
- Attack to gain information
- Attack to dislocate
- Attack to disrupt

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

OPFOR BDE level and above CDRs organize and designate various *forces* according to their *function*.

1. Enabling Forces – Various types of *enabling forces* are employed to create the conditions that allow the action force the freedom to operate.

- **Disruption Force** – BNs and below can serve as disruption forces for BDEs or BTGs. When transitioning to the offense, the disruption force typically includes the preexisting defensive disruption force.
- **Fixing Force** – the OPFOR force fixes the enemy preventing freedom of maneuver. Planners identify the target enemy forces, engagement method, and length of time the enemy must be fixed. The fixing force may consist of a number of units separated in time and space. BNs and below often serve as fixing forces for BTGs.
- **Assault Force**- one or more OPFOR detachments assigned to destroy an enemy force or seize a position.
- **Security Force** - The security force prevents or mitigates the effects of hostile actions against the overall tactical-level command and/or its key components. 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.
- **Deception Force -** OPFOR combat forces designated to take some action in support of the INFOWAR plan.
- **Support Force** – The support force provides fire support; other combat or combat service support; and/or C2 functions for other parts of the tactical group.

2. Action Forces - The OPFOR force responsible for performing the primary function or task that accomplishes the overall goal or objective of the tactical group. There are three basic types: exploitation force, strike force, and mission force.

- **Exploitation Force** – An exploitation force is assigned the task of achieving the objective of the mission by exploiting an opportunity created by an enabling force.
- **Strike Force** - A strike is an offensive COA that rapidly destroys an enemy's will and ability to fight through a synergistic combination of massed fires and maneuver. A strike is planned and coordinated at the operational level, but executed by a tactical-level force. The strike force accomplishes the final destruction of the targeted enemy force.
- **Mission Force** - In those non-strike offensive actions where the mission can be accomplished without the aid of external enabling forces, 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 designation IAW its specific function.

3. Reserves - OPFOR offensive reserve formations are given priorities based on the likelihood of acting as an enabling force or action force. The size and composition of an offensive reserve are situation-dependent.

C. Functional Organization of Elements for the Offense—Detachments, Battalions, and Below. An OPFOR detachment is a BN or CO task organized to perform a specific mission. CDRs organize their subordinate units according to the specific functions assigned to each. While CDRs at BDE and higher use the term "forces" when designating functional organizations, **CDRs at detachment, BN, and below use the term "element."** Elements are categorized into: action elements, enabling elements, or specialist elements. Often, the distinction between action and enabling elements is blurred because, as the mission progresses, conditions change or evolve and require modification.

1. Action Elements - The *action element* conducts the primary action of the overall organization's mission. The CDR normally gives this element a functional designation that more specifically describes the desired activity. For example, the action element in a raid is called the *raiding element*. If an element accomplishes its mission by exploiting an opportunity created by another element, it may be called the *exploitation element*.

2. Enabling Elements - Elements that enable the primary action in various ways; typically security elements and support elements. The *security element* provides tactical security for the overall organization and prevents the enemy from influencing mission accomplishment. The *support element* provides combat support, CSS, and C2 for the organization.

3. Specialist Elements - Specialist elements are typically formed around a unit with a specific capability, such as obstacle-clearing, reconnaissance, or deception.

4. Preparation and Execution of the Offense

The **principles of *preparation*** are: The **principles of *execution*** are:

- Establish contact;
- Make thorough logistics arrangements;
- Modify the plan when necessary;
- Rehearse critical actions in priority.

- Maintain contact;
- Implement battle drills;
- Modify the plan when necessary;
- Seize opportunities;
- Dominate the tempo of combat.

D. Types of Offensive Action—Tactical Groups, Divisions, and Brigades - Offensive action types are both tactical methods and guides for designing COAs. Subordinate units may execute different offensive and defensive COAs within the overall offensive mission framework.

   1. Attack - An offensive operation that destroys and/or defeats enemy forces, seizes and secures terrain. It seeks to defeat the enemy's military power by military means. Defeat is achieved through the disruption, dislocation, and subsequent paralysis that occurs when the loss of capability or the will to fight renders combat forces irrelevant. There are two types of attack: *integrated attack* and *dispersed attack*. Exploitation is considered a central part of all integrated and dispersed attacks.
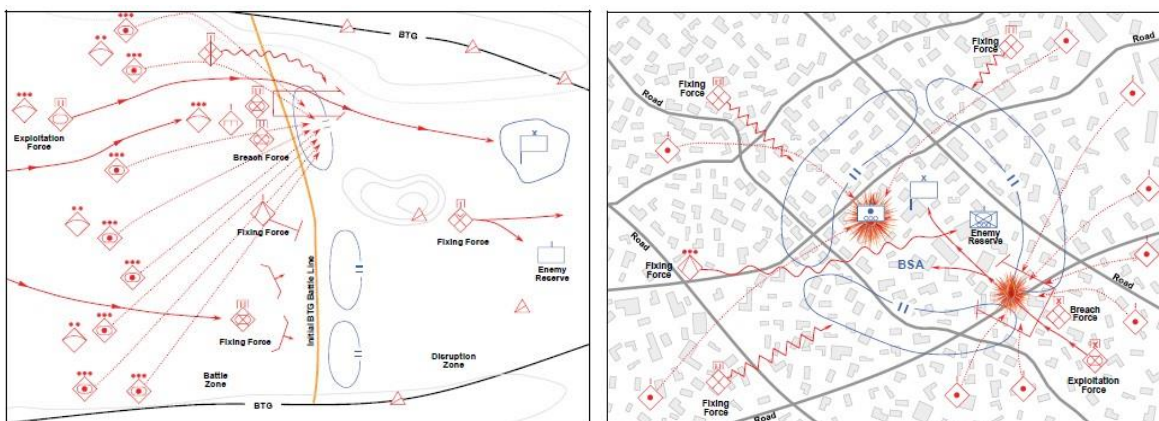
   a. Integrated Attack - an offensive action where the OPFOR seeks military decision by destroying the enemy's will and/or ability to continue fighting through the application of combined arms effects. It is often employed when the OPFOR overmatch**es** its opponent and is able to bring all elements of offensive combat power to bear. It may also be employed against a more sophisticated and capable opponent, if the appropriate opportunity is created or available**.** An integrated attack often employs **fixing**, **assault**, and **support forces**.

   (1) Integrated attacks are characterized by:
- Focusing on destruction of enemy combat power, mission command, and logistics.
- Fixing the majority of the enemy's force with the minimum force necessary.
- Isolating the 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 the OPFOR.
- Using flank attack and envelopment, particularly when enemy forces that have been fixed.

   (2) The OPFOR prefers 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.

   b. 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 for an attack. The primary objective of dispersed attack is to bring enough combined arms force to bear to destroy the enemy's will and/or capability to continue fighting. Dispersed attack relies on INFOWAR and a dispersion of

forces to conduct tactical offensive actions while overmatched by enemy precision standoff weapons and ISR. The dispersed attack is continuous and comes from multiple directions. It employs multiple means and capabilities interdependently working together, dispersed in time as well as space.

(1) 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 C2 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.

(2) The OPFOR must **create several conditions** that are critical to a successful dispersed attack:

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

(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.

(a) Enabling Forces - A dispersed attack employs fixing, assault, and support forces to support the primary assault. A disruption force may exist, but not specifically created. Deception forces play an important role in a dispersed attack.

• **Fixing Force.** The fixing force is primarily focused on fixing enemy response forces (reserves, quick response forces, precision fire systems) that are 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 enemy units and systems. OPFOR CDRs often 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 is charged with destroying a particular part of the enemy force or seizing key positions. Such assaults create favorable conditions for the exploitation force to rapidly move from dispersed locations and penetrate/infiltrate enemy defenses. An assault force may infiltrate infantry to pre-selected points to assist the exploitation force in its penetration. OPFOR CDRs often use multiple assault forces separated in time and/or space.

• **Support Force -** provides support to the attack by fire; other combat support, combat service support; and C2 functions. Smoke and suppressive artillery and rocket fires, combat engineer units, and air-delivered weapons are well suited to this function.

(b) Action Forces - The most common type of action force is the exploitation force. Such a force must be capable, through inherent capabilities or positioning, of destroying the attack target. OPFOR CDRs often use multiple exploitation forces separated in time and/or space, but often oriented on the same objective or objectives.
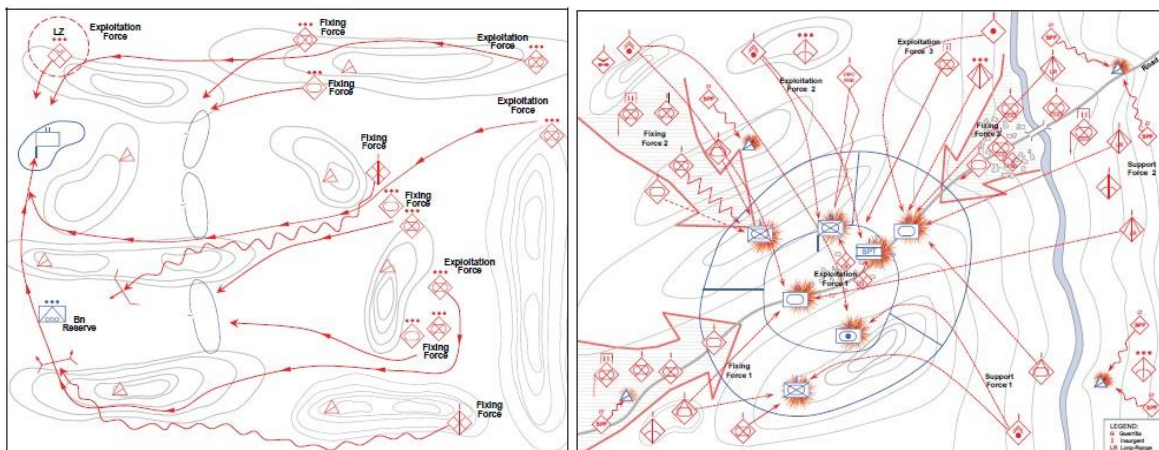
2. Limited-Objective Attack - seeks to destroy or deny the enemy key capabilities through primarily military means. The primary objective is a particular enemy capability (may be a man-made system, or group of systems, or a capability key to maintaining tempo. Limited-objective attacks are common while fighting a stronger enemy with the objective of preserving forces and wearing down the enemy.

a. Limited-objective attacks are characterized by-
- Focusing on destruction of enemy mission command and logistics capability.
- 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.

There are two types of tactical limited-objective attack: *spoiling attack* and *counterattack*.

b. Spoiling Attack - The purpose of a spoiling attack is to preempt or seriously impair an enemy attack while he is in the process of planning or preparing to attack. It is designed to disrupt the tempo of enemy operations. The primary objective of a limited-objective attack is a particular enemy capability.

(1) 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 create an opportunity for other combat actions.

(2) The OPFOR seeks the following conditions 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.

(3) Functional Organization for a Spoiling Attack - If enabling forces are required, then an *exploitation force* is designated to execute the spoiling attack (otherwise, it is called the *mission force*). The exploitation or mission force comes from a part of the tactical group that is capable of acting quickly and independently.

c. Counterattack - A *counterattack* is a form of attack by part or all of a defending force with the general objective of causing an enemy offensive to culminate. A successful counterattack returns the initiative to the OPFOR.

(1) 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.

(2) Functional Organization for a Counterattack - Functional organization for a counterattack is influenced by the fact that the counterattack usually originates from a defensive posture.

(a) *Enabling Forces* - Fixing, assault, and support forces are created while the disruption force is left over from the previous defensive functional organization.
- **Fixing Force -** part of the force assigned to ensure specified enemy forces/capabilities are not able to re-orient, break contact, and/or reposition. Additionally, the fixing force has the mission of destroying enemy reconnaissance forces and any combat forces that may have penetrated the OPFOR defense.
- **Assault Force -** If the enemy has a reserve, the assault force's mission is to force the enemy to commit it.
- **Support Force -** provides fire support, other CS or CSS, and C2 functions.

(b) *Action Forces* - The most common type of action force is an exploitation force, and there may be more than one. The exploitation force bypasses engaged enemy forces to destroy the enemy's CS and CSS before he has time to react.

E. Tactical Offensive Actions—Detachments, Battalions, and Below: At the tactical level, units execute one combat mission at a time, but OPFOR units, elements, and even plans are dynamic and adapt very quickly to the situation.

   1. Assault - An attack that destroys an enemy through firepower and physical occupation and/or destruction of his position. The OPFOR views all assaults as combined arms actions.

A detachment conducting an assault typically is organized into three elements: the *assault element*, the *security element*, and the *support element*. An assault is the most violent action the OPFOR undertakes, demanding an integrated combined-arms approach. 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 permitting the assault element to move without receiving destructive fire.
- Violent fire and maneuver against the enemy.

   a. *Assault Element*
The assault element must be able to maneuver from its assault position to the objective and destroy the enemy. Speed of execution is critical and the OPFOR prefers as much simultaneous action as possible. Additionally, the assault element uses surprise; limited visibility; complex terrain; and/or C3D. Typical tactical tasks expected of the assault element are:

Assault Element tasks:	Clear	Destroy	Occupy	Secure	Seize

   b. *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:

Security Element tasks:	Screen	Ambush	Contain	Disrupt	Isolate
	Guard	Block	Delay	Fix	
	Cover	Canalize	Destroy	Interdict	

   c. *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 success requires that he lead the assault element personally. The support element controls all supporting fires, combat support, and CSS functions. **Typical support element tasks are**:

Support Element tasks:	Attack by fire	Disrupt	Fix	Neutralize	Support by fire	Canalize	Contain
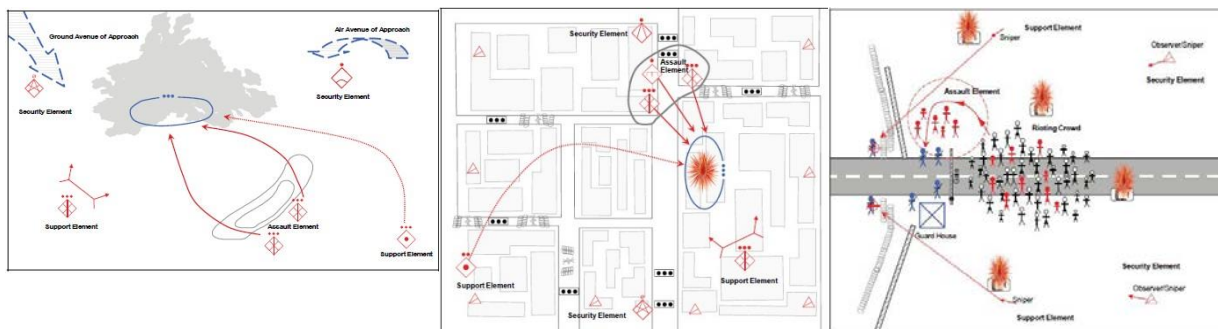
   2. Ambush - An ambush is a surprise attack from a concealed position, used against moving or temporarily halted targets. In an ambush, enemy activity determines the time, and the OPFOR sets the place. Ambushes are conducted to:
- Destroy or capture personnel and supplies.

- 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 on the enemy is magnified by the use of multi-tiered ambushes. A common tactic is to also ambush the reaction force and/or attack enemy medical evacuation assets. Successful ambushes force the enemy to allocate combat power to the security of principal roads, railroads, or waterways. **Key factors in an ambush** are:

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

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

(1) *Ambush Element* - attacks and destroys enemy in designated kill zone(s). The ambush element is responsible for halting the column, killing/capturing personnel, recovering supplies and equipment, and destroying everything else.

(2) *Security Element* - secures the ambush element from other enemy forces. These elements isolate the ambush site using roadblocks, outposts, and other ambushes; and cover the withdrawal of the ambush element from the ambush site.

(3) *Support Element* - The support element of an ambush has the same basic functions as that of an assault and often supports the ambush element with direct and/or indirect fires.

b. Types of Ambush – The three types of OPFOR ambush - annihilation, harassment, or containment - are conducted to kill/capture personnel, destroy or capture equipment/supplies, restrict enemy movement, and collect information.

(1) *Annihilation Ambush* - The purpose of an annihilation ambush is to destroy the enemy force. The support and ambush elements kill enemy personnel and destroy equipment within the kill zone by concentrated
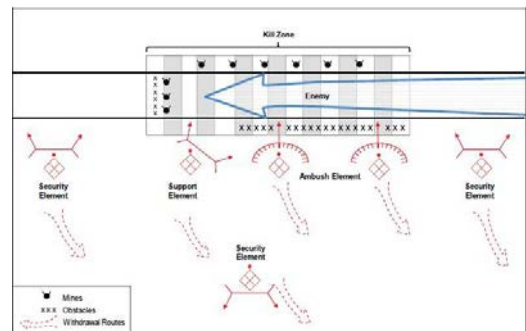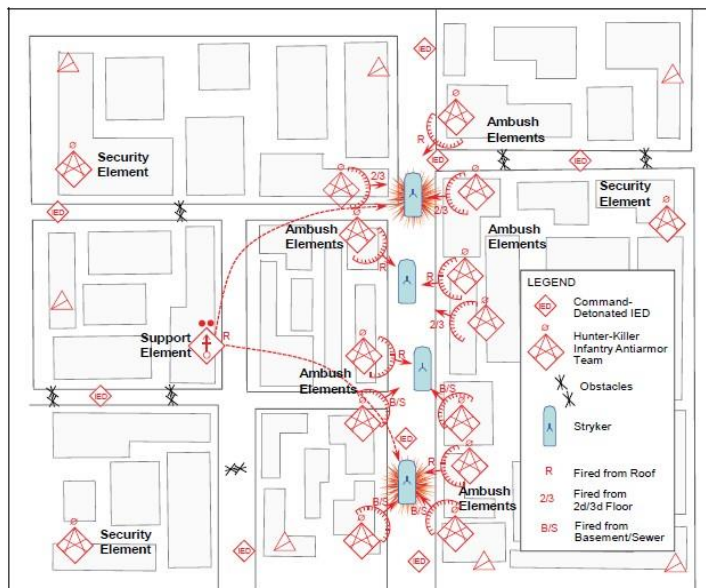
direct and indirect fires. The ambush element secures the kill zone and eliminates any remaining enemy personnel. The ambush element thoroughly searches for any usable information and equipment, which it takes or destroys.

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 element withdraws first, then the support element, and finally the security element. The entire ambush force reassembles at a designated location.

Annihilation ambushes in complex terrain often involve task organizations of "hunter-killer (HK) teams." HK antiarmor teams are composed of antiarmor gunners, machinegunner, sniper, and one or more

riflemen.

(2) *Harassment Ambush* - If the enemy has superior combat power, the OPFOR executes a harassment ambush at a significant distance from the enemy. A harassment ambush disrupts and psychologically impacts routine enemy activities/personnel.

(3) *Containment Ambush* - A security measure that is part of a larger action used to prevent the enemy from using an avenue of approach or interdicting a friendly action (i.e. raid or another ambush). The ambush force may erect multiple, mutually supporting obstacles covered by direct and indirect fires to fix the enemy for the necessary amount of time.

3. Raid - A raid is an attack against a stationary target for the purpose of its capture or destruction that ends with a planned withdrawal of the raiding force to safety. Raids are also 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.

a. Raids are characterized by:

• Destroying or damage key systems or facilities (i.e. command posts, 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 and to cause the enemy to deploy additional units to protect critical sites.

• OPFOR reconnaissance and sensors with capability to find and track the target.

• A C2 method to link the raiding force and sensors.

• Supporting operations (primarily INFOWAR) create opportunities for the raiding force to operate.
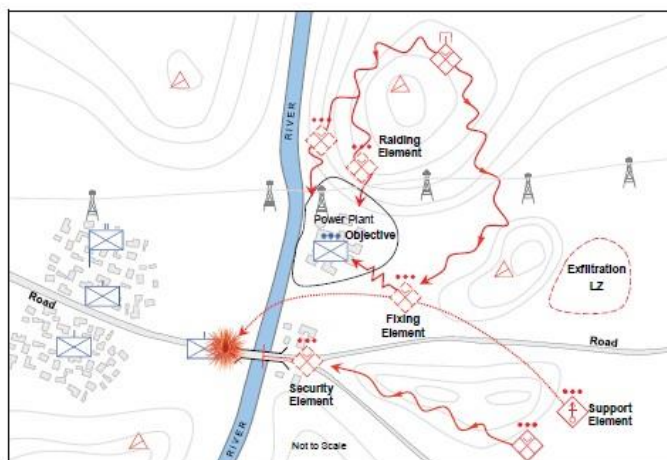
b. Functional Organization for a Raid - The size of the raiding force depends upon its mission, the nature and location of the target, and the enemy situation. Regardless of size, the raiding force typically consists of three elements: raiding, security, and support. It may involve other functional elements, such as a fixing element.

(1) *Raiding Element(s)* - The raiding element executes the destruction or seizure of the raid target.

(2) *Security Element(s)* - The security element is primarily focused on distracting and fixing enemy security and response forces in the objective area. The security element is equipped and organized to detect and fix enemy forces and then cover the withdrawal of the raiding element. The security element is normally assigned the following tactical tasks:
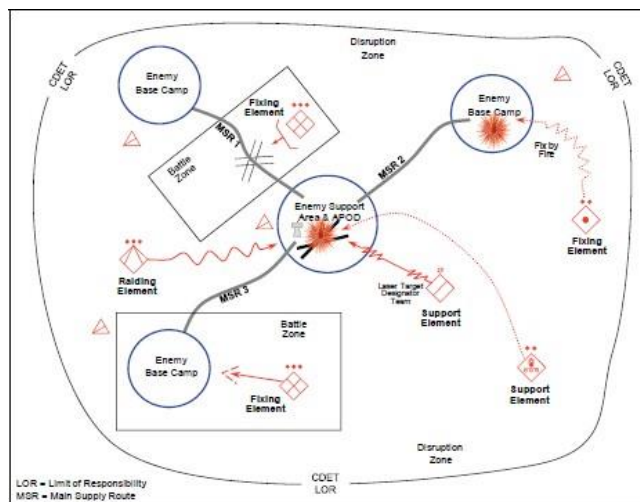
| Security Element tasks:	Screen	Ambush	Contain	Disrupt	Isolate
	Guard	Block	Destroy	Fix	
	Cover	Canalize	Delay	Interdict	

(3) *Support Elements* - 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:

Support Element tasks:	• Eliminating guards. • Breaching and removing obstacles to the objective. • Conducting diversionary or holding actions.	• Canalizing enemy forces. • Providing fire support.

4. 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, disposition, military capabilities, and intentions. 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 other action elements. There may be more than one of each type. The CDR may also form various types of support elements.
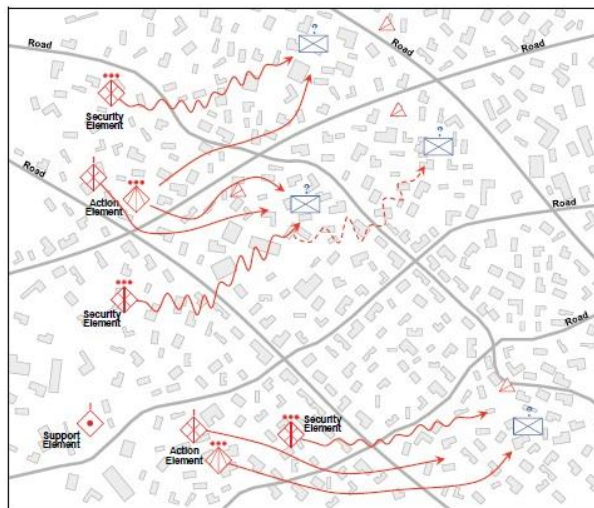
Chapter 4 – OPFOR Defensive Tactics

A. Planning the Defense – 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

B. Planned Defense – 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.

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

1. Maneuver Defense – When the OPFOR is not completely overmatched, the OPFOR may employ a maneuver defense. The maneuver defense uses fires and maneuver to destroy key elements of the enemy's combat system and deny enemy forces their objective while preserving the friendly forces.

a. Method – The maneuver defense trades terrain for the opportunity to destroy portions of the enemy formation and render the enemy's combat system ineffective. The force typically uses a contact force to engage the enemy. The shielding force covers the contact force during the contact force's disengagement/withdrawal.
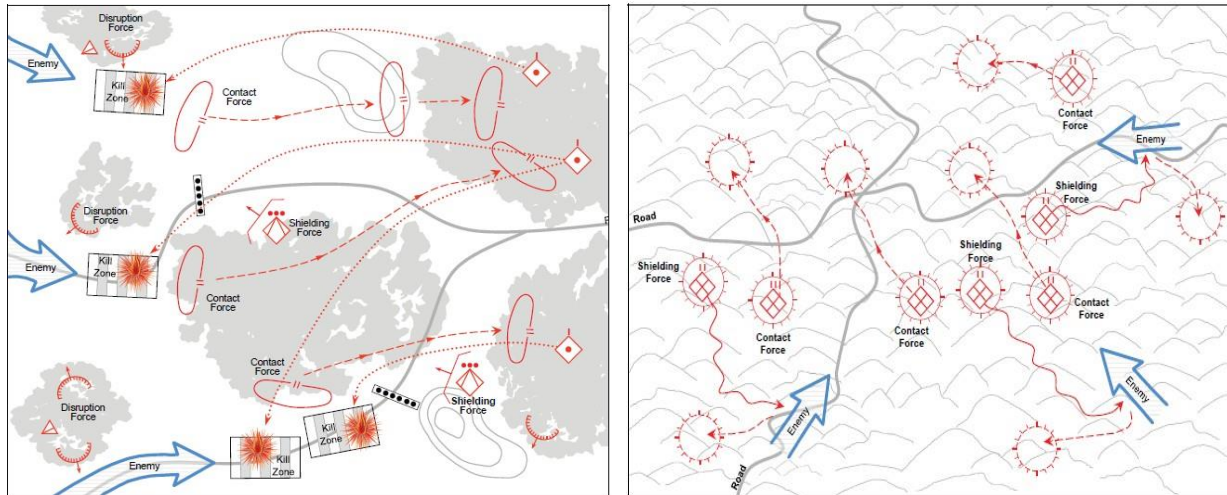

b. Disruption Force – Targets and destroys critical enemy subsystems before the enemy enters the main battle zone. Often fights from successive BPs to force the enemy to fight on disadvantageous ground and at the tempo of the OPFOR's choosing. The BPs should be far enough apart to force the enemy to reposition their assets to continue to place fires on the OPFOR. The disruption force seeks to set conditions for spoiling attacks or counter attacks. The disruption force may become part of the main defense force or become a reserve.

c. Main Defense Force – The main defense force's mission is to complete the defeat of the enemy. Basic elements of the main battle zone include BPs, firing lines, and reposition routes.

d. Reserves – The reserves can be any number in types and strengths. The maneuver reserve should be strong enough to defeat the enemy's exploitation force. The reserve must have sufficient air defense coverage and mobility assets to allow maneuver.

2. Area Defense – An Area Defense is used when key areas must be denied to the enemy, or when the enemy has overmatch capability. The OPFOR seeks to use the area defense to force the enemy offensive to culminate before the enemy can achieve their objectives, and/or deny the enemy his objectives while preserving the OPFOR's combat power. INFORWAR and deception are important to the execution of the area defense.

a. Method – Area defenses occupy complex battle positions and dominate the surrounding area with reconnaissance fires. The intent is to begin to disaggregate the enemy in the disruption zone, making the enemy incapable of synchronizing their combat operations against the main defense zone.
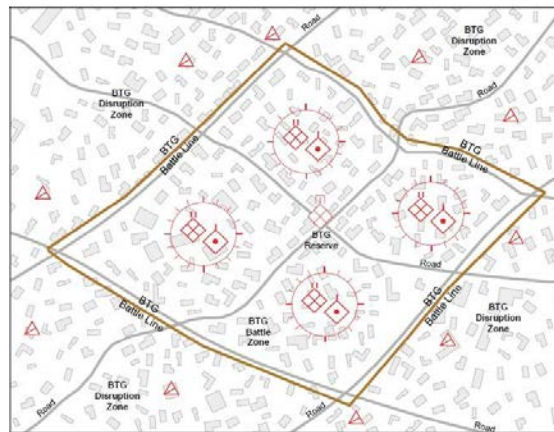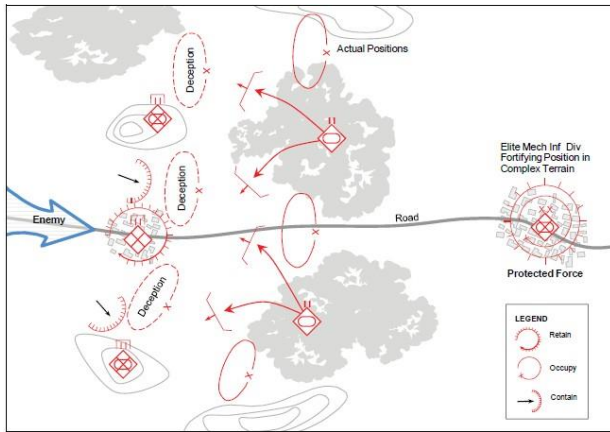
b. Disruption Force – The disruption force typically uses ambushes, precision fires, and raids to destroy key enemy systems without significantly exposing themselves. The disruption force may also use a maneuver defense concept to accomplish their mission. The disruption force is allocated a significant obstacle effort and mobility support. Typical disruption tasks are –

- Detect the enemy's main grouping.
- 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

c. Main Defense Force – The main defense typically uses CBPs to prevent the enemy's precision fires, and force the enemy to choose costly methods of attack. The OPFOR also seeks to deny the enemy the ability to operate in covered and concealed areas.

d. Reserves – There are number of reserve forces available to the OPFOR, based on the CDR's estimate. The reserves are typically placed in an AA of one or more of the BPs.

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

a. Disruption Force – The force in the disruption zone responsible for the counterreconnaissance fight, preventing the enemy from conducting an effective attack and maintaining contact with the enemy. A DTG's Disruption Force is typically a BTG. A BTG's Disruption Force is typically an IMD. Disruption forces normally have:

- Ambush Teams (ground and air defense)
- Long-range reconnaissance patrols and/or SPF teams
- RISTA assets and forces
- Combat Reconnaissance Detachments (CRD)
- Artillery systems
- Target designation teams
- Affiliated forces (guerillas, terrorists, insurgents, and/or criminals)
- Antilanding reserves

b. Main Defense Force – The force responsible for accomplishing the primary defensive mission. Operates in the Battle Zone. In a maneuver defense, the force may be broken down as a contact force and shielding force.

c. Protected Force- Is the force being kept from detection or destruction by the enemy. Typically the Counterattack Force or the Reserve.

d. Security Force – Has the mission to prevent or mitigate the effects of hostile actions against the overall command and/or its key components. May consist of infantry, SPF, counterreconnaissance, and signals reconnaissance to focus on enemy special operations and long-range reconnaissance forces

operating throughout the AOR.

e. Counterattack Forces – Has the mission of causing the enemy's offensive operation to culminate. Commits the force when the enemy is vulnerable for the action.

f. Types of Reserves:
- ***Maneuver Reserve*** – Composition and size is situation-dependent. Should be strong enough to respond to unforeseen opportunities and contingencies. Potential missions:
  - ***Conduct Counterattack***
  - ***Conduct Counterpenetration***
  - ***Conduct Antilanding missions***
  - ***Assist heavily engaged defending forces to break contact and withdraw***
  - ***Deception Force***
- ***Antitank Reserve (ATR)*** – Generally an AT unit, and often augmented by an Obstacle Detachment.
- ***Antilanding Reserve (ALR)*** – Include maneuver, Air Defense, and engineer units to prevent the vertical envelopment by the enemy.
- ***Special Reserves*** – Typically an Engineer Obstacle Detachment (OD) to strengthen defenses on a threatened axis. May serve as a chemical defense reserve if WMD is expected.
- ***Deception Force*** – The creation of nonexistent or partially existing formations. 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.

D. Tactical Defensive Actions—Detachments, Battalions, and Below

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

a. The standard functional organization of a detachment for defense is into four parts:
- **Disruption element –** The disruption element of a detachment provides 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.
- **Main defense element** – The main defense element accomplishes the detachment's tactical task.
- **Support element** – The support element provides combat and CSS and C2 for the detachment.
- **Reserve element** - The reserve element provides the defender with the tactical flexibility to influence unforeseen events or to take advantage of developing opportunities.
- **There may also be specialist elements.**
  - Obstacle-clearing element
  - Reconnaissance element
  - Deception element.

b. Detachments may be assigned one of several tasks while conducting a defense.
- 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

c. Preparing for the Defense – In the preparation phase, the 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)

d. Executing the Defense – Principles of executing a defense include**:**
- Maintain contact
- Implement battle drills
- Modify the plan when necessary
- Seize opportunities

2. 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.

a. 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**.**

(1) Defense of an SBP - 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.

(2) Functional Organization of Elements to Defend an SBP

(a) Disruption Element – Disruption unit(s) 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.

1 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.
- 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.
- CSOPs are typically assigned one or more of the following tactical tasks:
  - Ambush.
  - Attack by fire.
  - Delay.
  - Disrupt.
  - Fix.

2 Ambush Teams. Ambush teams (independent from CSOPs) identify and attack key enemy targets, they will engage them by   employing flanking or surprise close-range fire.

(b) 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.

(c) Reserve Element
The reserve element of an SBP exists to provide the OPFOR CDR with tactical flexibility. 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

(d) 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

(3) Organizing the Battlefield for an SBP – Battlefield Geometry

(a) 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.

(b) 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.

(c) Reverse Slope Defense. A reverse slope defense is positioned behind an intervisibility line that masks the OPFOR from enemy observation and direct fire. Reverse slope defensive position offer 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
- Maximize long-range weapons fires by emplacing the 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.
- Maintain observation of the enemy forward of intervisibility line with reconnaissance and OPs.

(d) Fire Planning. Fire is the basic means of destroying the enemy in the defense.
- Employ lethal and nonlethal weaponry in a unified manner, 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 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 appoint reconnaissance elements to identify targets and weapons systems to engage them.
- The BN or BDET 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 are covered by frontal and flanking or cross fires of the OPFOR BN's or BDET's and other supporting weapons systems. 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.

(e) Support Zone – The support zone may contain C2, CSS, indirect and direct support fire assets, and the reserve, as well as other supporting assets. Support zones are not typically found below the CO level.

(4) Executing Defense of an SBP

(a) Disruption Zone –
- Conduct aggressive counterreconnaissance.
- OPFOR EW assets attempt to detect the presence and location of enemy reconnaissance elements.

- The reserve element acts 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.

(b) 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.

(c) Support Zone – Defenders in the support zone will provide support to defenders in the disruption and battle zones as required.

(d) Deception – Establish dummy firing positions and BPs to keep the enemy from discovering the nature of the OPFOR defenses and to draw fire away from actual units. 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.

(e) Reconnaissance – 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.

(f) Armored Fighting Vehicles – Armored fighting vehicles 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.

(g) Fire Support – OPFOR 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

(h) Air Defense
- Employ active & passive air defense measures to protect the defender from air threats.
- Intersperse Antiaircraft guns and shoulder-fired surface-to-air missile systems (SAMS) throughout the SBP, including antilanding ambushes.

(i) Engineer
- Engineers support the SBP initially by preparing survivability positions and countermobility works that support the disruption and battle zones.
- Once these survivability and countermobility preparations are complete, engineer support shifts to mobility support for the reserve force.
- Engineer tasks are a shared responsibility throughout the OPFOR.
- SBP obstacles are 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. Use remotely delivered mine capability to reinforce pre-existing obstacles, block avenues of approach, or to re- seed breached obstacles.

(j) 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.

(k) 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.

(2) Complex Battle Position – 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

(a) Complex terrain is a topographical area consisting of an urban center larger than a village and/or of two or more types of restrictive terrain or environmental conditions occupying the same space. (Restrictive terrain or environmental conditions include but are not limited to slope, high altitude, forestation, severe weather, and urbanization.). Complex terrain, due to its unique combination of restrictive terrain and environmental conditions, imposes significant limitations on observation, maneuver, fires, and intelligence collection. (FM 7-100.1 Opposing Force Operations, 27 December 2004)

(b) Defense of a CBP – CBPs protect units from detection and attack, and deny their seizure and occupation by the enemy. CBP defenders engage only as long as they perceive an ability to w i n . Should the OPFOR CDR feel that his forces are decisively overmatched, he will withdraw in order to preserve combat power. CBPs use restrictive terrain and engineer countermobility efforts to deny enemy approaches, seizure, and occupation of the position. OPFOR makes maximum use of C3D and cultural standoff to deny the enemy the ability to detect and attack the position, and remain dispersed to negate the effects of precision ordinance strikes. Once the defense is established, non-combat vehicles are 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

(c) Functional Organization of Elements to Defend a CBP

1 Disruption Element – The disruption element of a CBP detect attackers and provide early warning. The disruption element may form CSOPs and ambush teams. The disruption element establishes observation posts and ground ambushes and can establish antilanding ambushes and ALRs.

When attacked, disruption elements will remain in position to provide a reconnaissance capability. The disruption element may include indirect fire assets, such as mortars, to provide immediate, observed, harassing fires.

2 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.

3 Reserve Element – The reserve element of a CBP provides the OPFOR CDR with tactical flexibility. During the counterreconnaissance battle, the reserve may augment disruption elements order to provide additional security to the main defense element. 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

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

- C2 & CSS
- Supporting direct fire (e.g. MG, ATGM, recoilless rifle, or automatic grenade launcher)

- Supporting indirect fire (mortar or artillery)
- Supporting nonlethal actions (e.g. jamming, psychological warfare, or broadcasts)
- Engineer support

(d) Organizing the Battlefield for a CBP

<u>1</u> **Disruption Zone –** The BN, CO, or detachment may send out CSOPs and/or ambush teams into the disruption zone.

<u>2</u> **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. 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.

<u>3</u> **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.

Chapter 5 - Battle Drills

A. Actions on Contact

1. Forms of Contact – The OPFOR recognizes seven forms of contact:
- Direct fire
- Indirect fire
- Obstacle
- Air
- Chemical, biological, radiological, and nuclear (CBRN)
- Electronic warfare (EW)
- Sensor

The actions on contact battle drill is primarily for use by a force making sensor and/or direct fire contact with an enemy force. When making undesired contact (indirect fire, air, CBRN, EW, or ground contact made by a noncombat unit), the break contact battle drill is employed instead. When making contact with an isolated obstacle, the situational breach battle drill may be selected.

2. Conditions:

- Expected contact in his course of action.
- Unexpected contact regarding time.
- Unexpected contact regarding location.
- Unexpected contact regarding the enemy.
- Unexpected contact regarding the any combination of the above.

Battle drill actions on contact are 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 the new circumstances.
This **flexibility is achieved by**:
- **Ensuring that contact is made with one or more security elements** before the remainder of the force becomes engaged.
- Employing one or more security elements to **shape the engagement area by either fixing or isolating the enemy** to avoid additionally committing the action element.
- **Providing the commander with the ability to make his own decisions** if communication with higher authority is impractical.
- Using cover camouflage, concealment, cover, and deception (C3D) to **prevent unwanted engagements**.

3. Execution – Execution of actions on contact varies depending on the situation and the commander's battle plan. The actions on contact battle drill is accomplished by performing one or a combination of the five subtasks below. Figure 5-1 shows an example of actions on contact involving some of these subtasks.

4. Fix – The security element making contact fixes the enemy. This security element is then known as the fixing element. It continues to provide early warning of approaching enemy forces and prevents them from gaining further information on the rest of the OPFOR force. Fixing elements often make use of terrain choke points, obstacles, ambushes, and other techniques to fix a larger force.
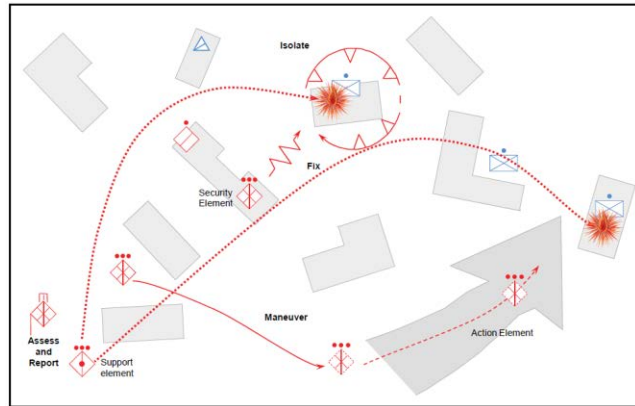
5. Assess and Report – Based on reports he receives from element(s) in contact, the detachment commander must make an assessment of the tactical situation that determines whether or not making contact in this manner and with this enemy constitutes a change in his course of action. This determination is the most vital step in successful execution of actions on contact because if it is performed incorrectly, the unit will subsequently be executing a course of action inappropriate to the mission and situation. Concurrent with his assessment, the commander reports to the chain of command what contact has been made with the enemy force, critical details of its composition, and his assessment.

6. Isolate – The detachment making contact maneuvers and deploys security elements to ensure additional enemy forces do not join the battle unexpectedly. Indirect fire and close air support can be used either individually or combined with other means to achieve the same effect.

7. Maintain Freedom to Maneuver – The commander of the contacting unit ensures he makes contact with the minimum part of his force necessary to fix the enemy. He makes use of C3D and the break contact battle drill to prevent his force from becoming decisively engaged. Security elements determine safe maneuver avenues for him to employ. Freedom to maneuver is also maintained by:
- Dominating avenues of approach into the engagement area.
- Determining location of enemy flanks or exposed areas of weakness.

8. Execute Course of Action – The contacting unit either continues with its original course of action if deemed appropriate or executes a new one that suits the situation. A new course of action could be one given to the unit based on the assessment it provide to its higher command or one chosen by the commander in absence of time or guidance. The unit making contact ensures follow-on units are aware of the contact and deconflict positioning, typically through the use of a standard marking system.

B. Breaking Contact – The primary objective 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, C3D, and countermobility. The OPFOR will routinely break contact in order to maneuver into predesignated defensive positions or to draw the enemy force into an ambush. In other cases, the OPFOR breaks contact when faced with no other tactical option.

1. Conditions:

- Included in the battle plan.
- Loss of time is especially critical.
- Loss of terrain is not critical.
- Enemy is too strong to engage with the force on hand.

2. Execution – Execution of the breaking contact battle drill varies depending on the situation and the commander's battle plan. The breaking contact battle drill is accomplished by performing the following subtasks. In most cases, all subtasks are part of the breaking contact battle drill. However, the first three subtasks may be executed in a variety of ways. Figure 5-2 shows an example of breaking contact.

3. Protect – The detachment commander takes immediate steps, using a variety of means, to protect his force while it maneuvers to a position out of contact. The security element fixes the enemy. It prevents the enemy force from maneuvering in order to remain in contact with the rest of the OPFOR force. It may employ INFOWAR to appear to be larger than it is or even to appear to be the entire OPFOR detachment.

The detachment commander employs fires as part of the break contact battle drill to suppress the enemy and prevent him from returning fire effectively and to fix him and restrict his maneuver. If available, he may use indirect fires, close air support, EW, and/or CBRN means to fix the enemy. C3D is employed to limit or remove the enemy's ability to maintain situational awareness of the OPFOR force. This may be as simple as placing obscuring smoke between the enemy and the detachment or as complex as a sophisticated deception plan making use of decoys and mock-ups. Countermobility actions, such as the emplacement of dynamic obstacles or the destruction of man-made structures can also restrict the enemy's ability to maneuver and maintain contact with the detachment.
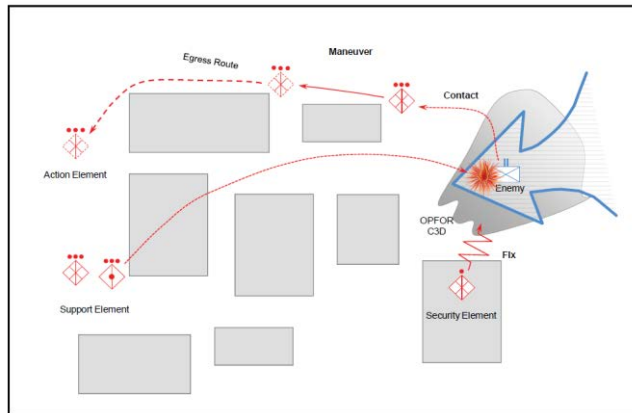
4. Retain Freedom to Maneuver - The commander reduces his elements in contact to only security element(s). For any other element(s) that originally made contact, he identifies egress routes. He selects one or more routes from his current location that enable his detachment to remain out of contact while permitting him to maneuver in support of his mission.

Once the rest of the force has maneuvered out of contact, the security element(s) that performed a fixing function can rejoin the rest of the force. Separating these fixing elements from the enemy may require further use of C3D, fires, and countermobility measures.

5. Assess and Report – The commander receives reports from the subordinate element(s) that first made contact and/or the fixing element(s) that remain in contact. Based on those reports, he must make an assessment of the tactical situation. Concurrent with his assessment, the commander reports to the chain of command what form of contact has been made with the enemy force, critical details of the enemy force's composition, and his assessment of the situation.

6. Continue or Change Course of Action – Once freedom to maneuver has been retained or regained, the OPFOR force executes the basic course of action. The course of action is usually the primary action of the unit's original tactical mission. However, the detachment commander makes an assessment of the tactical situation to determine whether or not making contact in this manner and with this enemy force dictates a change in the course of action.

C. 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. This allows the unit to maintain momentum rather than being stopped or impeded by the obstacle. The decision to attempt the situational breach is based on the OPFOR commander's knowledge of the enemy forces in the area and the expected tactical advantage in terms of key terrain and time.

1. Conditions:
- Included in the battle plan.
- Time constraints.
- Terrain is crucial.
- Exposes enemy weaknesses.

2. Execution – In order to execute the situational breach effectively, the OPFOR must be prepared to provide the necessary security to allow movement through the obstacle. This is accomplished by isolating the potential enemy avenues of approach while reducing the obstacle for the rest of the unit to pass through.

3. Isolate – The security element takes action to ensure enemy elements cannot reinforce those defending the obstacle. It might accomplish this through C3D measures, countermobility tasks, direct or indirect fire engagements, or a variety of other means.

4. Secure – support element establishes a support-by-fire position and takes action to ensure enemy elements defending the obstacle are neutralized. It also supports movement through the obstacle.

5. Penetrate – The reaching element reduces the obstacle such that it can complete its mission (as the action element) and/or enable a follow-on force to do so. All OPFOR organizations carry sufficient equipment, whether field expedient or constituent, to penetrate basic enemy obstacle systems and urban construction and debris.

6. Execute Course of Action – Once the obstacle has been penetrated and the lanes isolated and secured, the action element and/or a follow on force continues the mission, if that is deemed appropriate. However, based on the commander's assessment of the situation and/or guidance from a higher command, the unit may adopt a new course of action.
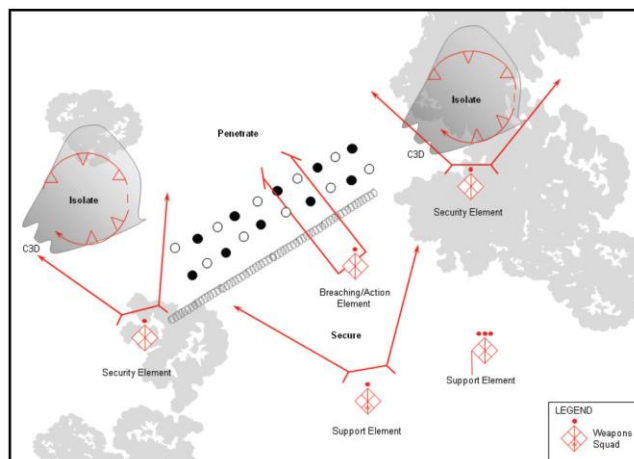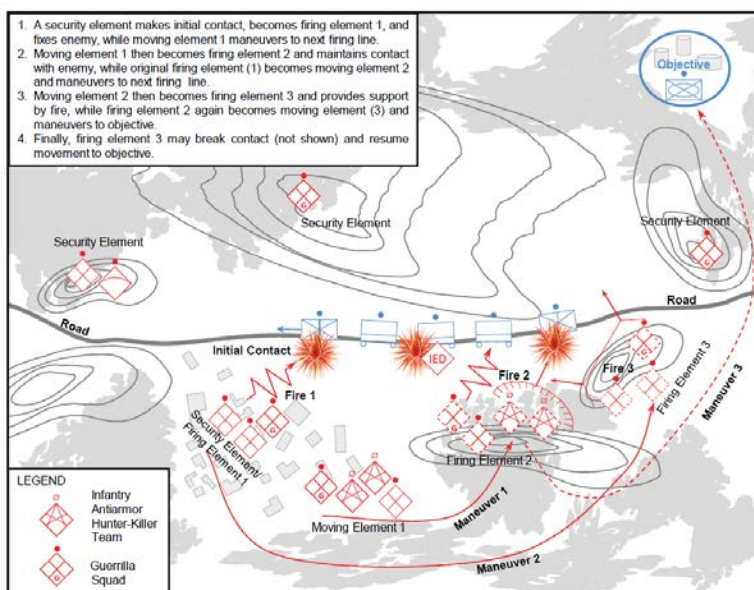
D. Fire and Maneuver – Fire and maneuver is the way in which OPFOR units move while in contact with the enemy. In such conditions, the OPFOR commander designates part of his force to be the *firing element* and part to be the *moving element*. The firing element fires from a position of concealment and/or cover in order to support the moving element. This is the most basic of all OPFOR battle drills.

1. Conditions:
- Included in the battle plan.
- Time constraints.
- Exposes enemy weaknesses.

2. Execution – The critical aspect of executing fire and maneuver is the commander's selection of the right amount of combat power and resources to assign to each of the elements of his force. The part of the force initially designated as the firing element directs suppressing fire against any enemy that has the ability to influence the movement of the moving element. The moving element then moves to the next firing line. Once the moving element reaches that new position, it becomes the new firing element, and the former firing element becomes the new moving element. This

continues until a moving element reaches the objective. See figure 5-4 on page 5-8 for an example of fire and maneuver.

3. Make Contact – Normally, a security element makes first contact with the enemy. It observes the enemy force and reports on its activity. Security element(s) continue to provide early warning of approaching enemy forces and prevent them from gaining further information on the rest of the OPFOR unit. If the enemy force attempts to move in a direction that could influence the movement of the OPFOR unit, the security element becomes a fixing element.

4. Fix – The security element making contact fixes the enemy. Once the firing element moves into a suitable position, it can also fix the enemy, often by delivering suppressing fires against an enemy force that has the ability to influence the movement of the moving element. (While performing this function, the firing element could be called a fixing element.)

5. Isolate – Security elements ensure additional enemy forces do not join the battle unexpectedly. Indirect fire and close air support can be used either individually or combined with other means to achieve the same effect.

6. Maneuver – The moving element maneuvers to a new position of advantage with respect to the enemy. On order, the moving element assumes the role of the new firing element. If further maneuver is required, the moving and firing elements continue alternation of fixing the enemy and maneuvering against the enemy.

E. 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. It is one of the most critical battle drills OPFOR units execute, and it is often a subtask in other battle drills. The ability to fix the enemy at crucial points is the fundamental way by which 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.
- He does not think he can move.

1. Conditions:
- Included in the battle plan.
- Time is required for follow-on forces.
- Enemy is located on a preplanned target.
- INFOWAR assets achieve desired effects.

2. Execution – fix the enemy using the method most likely to achieve the results with the minimum risk to its forces.

3. Fires – Fix the enemy by killing enemy soldiers or wounding them enough to prevent relocation (destructive fires) or by making it too dangerous for them to reposition (suppressive fires). Indirect fires and/or close air support are also employed to fix the enemy in situations where distance and terrain make it difficult to achieve the effect through direct fire alone. Fires are the main method for decisively engaging the enemy.

4. INFOWAR – Fixes the enemy by convincing the enemy he does not want to move or by making him think he cannot move. Use propaganda, deception, and/or information attack.

5. Countermobility – Countermobility actions fix the enemy primarily by physically restraining his movement.
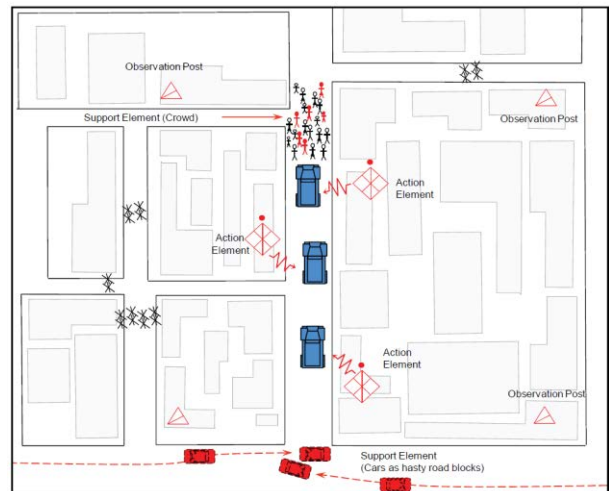
Chapter 6 – Information Warfare

A. Tactical Level INFOWAR

1. Purpose: The OPFOR defines *information warfare* as specifically planned and integrated actions taken to achieve an information advantage at critical points and times. The primary goals are to:

- Influence an enemy's decision-making through his collected and available information, information systems, and information-based processes.
- Retain the ability to employ friendly information and information-based processes and systems.

2. Tactical Effects:

- **Destroy**. To physically render an enemy's information systems ineffective; most effective before the enemy executes a C2 function or on a resource-intensive target that is hard to reconstitute.
- **Degrade**. Reduces the effectiveness of the enemy's information infrastructure, information systems, and information collection means.
- **Disrupt**. Disruption of observation and sensor capabilities at critical times and locations.
- **Deny**. Limit enemy's ability to collect or disseminate information or deny his collection efforts.
- **Deceive**. To mislead decision-makers and manipulate overall understanding of OPFOR activities
- **Exploit**. Use enemy's C2 or RISTA capabilities to the advantage of the OPFOR.
- **Influence**. Affect enemy's beliefs, motivation, perspectives, and reasoning capabilities; may be done through misinformation, manipulating or "spinning" information.

3. INFORWAR Elements, Objectives and Targets: Elements of INFOWAR do not exist in isolation from one another and are not mutually exclusive. The overlapping of functions, means, and targets requires that they all be integrated into a single, integrated INFOWAR plan.

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

4. INFORWAR Elements, objectives and Targets

INFOWAR Element	Objectives	Targets
Electronic Warfare	Exploit, disrupt, deny, and degrade the enemy's use of the electromagnetic spectrum.	C2 and RISTA assets and networks.
Deception	Mislead enemy decision-makers. Cause confusion and delays in the Decision-making process. Persuade the local population and/or international community to support OPFOR objectives.	Key military decision-makers. General population and international media sources and Internet sites.
Physical Destruction	Destroy the enemy's information infrastructures.	C2 nodes and links, RISTA assets, telecommunications, and power sources.
Protection and Security Measures	Protect critical assets.	Enemy RISTA assets.
Perception Management	Distort reality or manipulate information to support OPFOR goals.	Enemy RISTA assets. Local populace and leaders. Media sources (international and domestic).
Information Attack	Alter or deny key information.	Decision-makers and other users of information. Systems reliant on accurate information.
Computer Warfare	Disrupt, deny, or degrade the enemy's computer networks and information flow.	C2 and RISTA assets and networks.

B. Electronic Warfare (EW)

1. Purpose: To control or deny the enemy's use of the electromagnetic spectrum, while ensuring its use by the OPFOR. EW allows the OPFOR to exploit, deceive, degrade, disrupt, damage, or destroy sensors, processors, and C2 nodes.

2. Use: OPFOR employs both nonlethal and lethal EW, ranging from signals reconnaissance and electronic jamming to the deployment of corner reflectors, protective countermeasures, and deception jammers. The OPFOR can employ low-cost GPS jammers to disrupt enemy precision munitions targeting, sensor-to-shooter links, and navigation. Lethal EW activities include the physical destruction of high-priority targets supporting the enemy's decision-making, to include reconnaissance sensors, CPs, C2 systems, and air defense suppression measures.

3. Primary Target: Focus is on enemy's advanced C2 systems that provide real-time force synchronization and shared situational awareness. As such, the OPFOR also enhances its own survivability through disrupting the enemy's ability to mass fires with dispersed forces, while increasing enemy crew and staff workloads and disrupting his fratricide-prevention measures.

4. Electronic Reconnaissance & Attack (EA): Reconnaissance detects, identifies, locates, and tracks high-value targets (HVTs) that includes both intercept and direction finding, which may enable a near-real-time attack on the target. EA supports the disaggregation of enemy forces to disrupt coordination between and within units, especially when enemy units are achieving varying degrees of success. HVTs for reconnaissance and attack include:

- Maneuver unit CPs.
- Forward air controllers (FACs).
- Logistic CPs.

C. Deception

1. Purpose: The OPFOR integrates deception into every tactical action, ranging from physical decoys and electronic devices to tactical activities and behaviors. Successful deception activities depend on the identification and exploitation of enemy information systems and networks, as well as other conduits for introducing deceptive information. Enemy reconnaissance system is the primary information conduit and therefore receives the most attention, while international media and Internet sites may also be a target for deceptive information at the tactical level.

2. Deception Forces: INFOWAR plan may call for the creation of one or more deception forces or elements. This means that nonexistent or partially existing formations attempt to present the illusion of real or larger units. The deception force is typically given its own command structure to replicate the organization's signature and to execute the multidiscipline deception required to replicate an actual or larger military organization. Examples include:

- Executing feints and demonstrations to provide a false picture of where the main effort will be.
- Creating the false picture of a major offensive effort.
- Maximizing protection and security measures to conceal movement.
- Creating false high-value assets.

D. Protection & Security Measures

1. Purpose: Encompasses a wide range of activities, incorporating the elements of deception and EW to significantly enhance tactical survivability and preserve combat power. At the tactical level, protection and security measures focus primarily on:

- Counter-reconnaissance.
- C3D.
- Information and operations security.

2. Camouflage, Concealment, Cover, and Deception: the OPFOR employs a variety of C3D techniques throughout the disruption, battle, and support zones. The OPFOR employs a variety of signature-reducing or -altering materials and systems, to include infrared- and radar-absorbing camouflage nets and paints.

E. Perception Management: Involves measures aimed at creating a perception of truth that best suits OPFOR objectives.

It integrates a number of widely differing activities that use a combination of true, false, misleading, or manipulated information against a range of audiences to include the enemy forces, the local populace, and to world popular opinion. perception management activities include efforts conducted as part of:

- PSYWAR.
- Direct action.
- Public affairs.
- Media manipulation and censorship.
- Statecraft.
- Public diplomacy.
- Regional or international recruitment and/or fundraising for affiliated irregular forces.

F. Information Attack (IA)

1. Purpose: focuses on the intentional disruption or distortion of information in a manner that supports accomplishment of the OPFOR mission. Unlike computer warfare attacks that target the information systems, IAs target the information itself.

2. IA Manipulation: Data manipulation is potentially one of the most dangerous techniques available to the OPFOR. Data manipulation involves covertly gaining access to an enemy information system and altering key data items without detection. Examples are:

- **Navigation**. Altering position data for enemy units, soldiers, and systems, making them think they are in the right place when they are not.
- **Blue Force Tracking**. Altering position data of enemy units, soldiers, and systems to make others believe them to be in one place where they are not or to lose track of them altogether. Alternatively, data manipulation can make OPFOR units appear as enemy or vice versa.
- **Battlefield information systems**. Enhancing OPFOR success by the ability to mitigate and/or influence enemy activities controlled via battlefield information systems.
- **Survey and gun or mortar alignment**. Causing enemy weapons to fire on the wrong targets.
- **Targeting and sensors**. Misdirecting sensors to have false reads, locate false targets, or identify the enemy's own units as OPFOR targets.
- **Weapon guidance**. Sending weapons to the wrong location or wrong target.
- **Timing**. Changing internal clocks, thereby disrupting synchronization.
- **Logistics tracking**. Sending logistics packages to the wrong place or delaying their arrival. This can be done by altering bar codes on equipment or by hacking and altering logistics (delivery or request) data.
- **Aviation operations**. Changing altimeter readings, position location data, or identification, friend or foe codes.

3. IA Targets: targets for an IA are information residing in the critical tactical systems of the enemy. Such targets include:

- Telecommunications links and switches.
- Fire control.
- Logistics automation.
- RISTA downlinks.
- Situational awareness networks.
- C2 systems.

G. Computer Warfare

1. Purpose: Consists of attacks on the computer systems, networks, and/or nodes. This includes a wide variety of activities, including:

- Unauthorized access (hacking) of information systems for intelligence-collection purposes.
- Insertion of malicious software (viruses, worms, logic bombs, or Trojan horses).
- Distributed denial of service attacks use a network of slave computers to overwhelm target computers with packets of data and deny them outgoing access to networks.

2. IA Manipulation: OPFOR computer warfare activities may be conducted prior to or during a military action. For example, by damaging or destroying networks related to an enemy's projected force deployments and troop movements, the OPFOR can effectively disrupt planning and misdirect movement, producing substantial confusion and delays. As modern armies increasingly rely on "just-in-time" logistics support, targeting logistics-related computers and databases can produce delays in the arrival of critical materiel such as ammunition, fuel, and spare parts during critical phases of a conflict.

Chapter 6 – Decisive Action Training Environment (DATE) 2.2

The Decisive Action Training Environment (DATE) is a tool for the training community to use across training events ranging from rotations at the Combat Training Centers (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. All data below is extracted from DATE 2.2.

A. Ariana

Ariana, the area's second-largest and second-strongest nation militarily, possesses massive oil and gas reserves in its southwest region along the Persian Gulf. This area and the Strait of Hormuz comprise key terrain assets for the country. Ariana's government is aggressive, capable, revolutionary, and intent on spreading its vision of Islamic governance and the establishment of a new Arianian hegemony throughout the region. Ariana mobilizes target populations through politicization of Islam to accomplish its long-term goals.

1. Political – Theocracy.

- Ariana's government is a hostile, national-level, stable theocracy. Clerical authority over government structure
- Token representative government
- Strong influence of clerical class
- Wary of "Western Influence"
- Seeking regional dominance
- Strong relationship with Limaria
- Mutually beneficial unofficial relationship with Donovia
- Generally antagonistic relationship with Atropia
- The Arianian military plays a large role in Arianian society with its network of members and ex-members in prominent positions throughout the country.
- The heart of political power in Ariana is the Council of Guardians Revolution
- Supreme Leader Ayatollah Mahmood Mekhenei and the Arianian military are the centers of political power in Ariana. All political power to clerical authority is found in an ideology known as *Wilayat al Faqih,* or the Guardianship of the Islamist Jurist.
- The military fulfils the role as ideological guardian of the Revolution's Islamic ethos. The military believes it repr
- sents the most faithful representation of Council of Guardians Revolution ideals.
- The theocratic Arianian government contains three branches like the US, but the executive branch wields the lion's share of federal power.

Political Issues:
- The revolution remains popular in rural areas, but there is rising discontent for what is seen as "sham" elections.
- The Government uses the "Rule of Law" to squash threats to their regime and what they government sees as anti-social behavior.
- Corruption, especially in urban areas, to get access to government services. Military officers import hard to obtain items and resell at inflated prices.

2. Military – Large conventional force

- Three standing Armies consisting mostly Tier 2 capabilities with four Separate Army Divisions that are considered to be Tier 1
- Most capable military in the region after Donovia, large Army, small and agile Air Force and Navy.
- Faces small insurgencies in southeast
- Capable of a wide range of operations; conventional, hybrid, and adaptive
- Successful nuclear weapons program, has a capable and growing CBRN capability.
- Has increasingly robust satellite communications capabilities, the second most capable space power in the regions with at least one government owned and operated satellite for intelligence operations and navigation.
- Sees any attack on its nuclear program or hydrocarbon production as an act of war.

National Strategic Goals:
- Wants to become the dominant regional military power
- Be strong enough to defend its borders, control the Strait of Hormuz, and deny access to hostile powers
- Remains focused on maintaining weapons of mass destruction to deter conventional aggression by enemies and because they are the rightful possession of a great power, as Ariana views itself.
- Global deployment of smaller clandestine units (irregular forces) to train and equip other anti-Western factions.

Military Strategy – Ariana conducts overt and covert operations in order to maintain its position within the region. The country maintains strong relationships with Limaria and has ties with Donovia. Ariana also is focused on keeping Western influence out of the region and maintaining its current status as a regional strongman.

Threat	Type	OE	Activities	Targets
God's Helpers Brigade	Insurgent	SE Ariana	The largest foreign anti-Ariana insurgent group, has conducted a low-level pseudo-insurgency for two decades. Promotes violent populace opposition to the ruling political party.	Arianian government facilities and leaders
Other Anti-Ariana Insurgent groups	Insurgents	Primarily SE Ariana	Smaller anti-Ariana operations similar to the God's Helpers Brigade to include sporadic violence.	Arianian government facilities and leaders
Drug and Weapons Organizations	Criminal	Country-wide	Drug and weapons smuggling and sales. Certain Special Purpose Forces (SPF) elements have links to the black market and criminal organizations.	Arianian police and security forces
New Dawn of Freedom of Arianian Kurdistan	Potential Separatist Insurgent	NE Ariana	Potential for insurgent activities in support of separatist goals.	Arianian government facilities and leaders
Arianian Freedom Movement	Religious	Country-wide	Religious opposition to the Shia-dominated Ariana government over the Islamic concept of velayat-e-faqih or political rule by the Islamic clergy.	Arianian government facilities and leaders
Ethnic Arabs	Unorganized	SW Arianian-Iraqi Border	Potential ethnic and religious unrest.	Arianian government facilities and leaders
Baluchi Separatists	Potential Separatist Insurgent	Southern Ariana	Sunni Baluchis feel discriminated against by the Shia Islamic Ariana government and are agitating for secession from Ariana.	Arianian government facilities and leaders

3. Economic – Economy based on petroleum industry
- Owns large oil and natural gas (hydrocarbon) reserves, but effected by sanctions preventing the sale of products

- International sanctions depress economy
- Insufficient large-scale industrial production limits overall economic growth.
- Relies on Limaria for international trade
- High levels of corruption and heavy government involvement negatively affect the economy.
- Exports large amounts of military hardware
- Agriculture accounts for 10% of GDP and employs 25% of labor force.

4. Social – Persian Shia Muslim Culture
- 51% Persian
- 24% Atropian
- 77% literacy rate
- 1 million IDPs, 70% there over 20 years
- 68% of population is urban
- Government enforces Sharia law
- The belief in the superiority of the Persian culture and faith in Islam will manifest in Arianian soldiers willing to die for their cause.
- Ariana's belief in limited women's roles reduce the number of women available to serve in the military.
- Demonstrates high social volatility with open civil unrest, the rise of a political reform movement, and changes to its basic social fabric, such as the role of women in society.
- Long-simmering tensions continue between ethnic and religious groups, including tensions between the Shia and the non-Shia groups such as Ariana's Sunni Arabs, Baluchi separatists, and Kurds.
- **Languages spoken in Ariana**:
  - Persian Dialects: 58.0
  - Turkic Dialects: 26.0
  - Kurdish: 9.0
  - Luri: 2.0
  - Baluchi: 1.0
  - Arabic: 1.0
  - Kalarian: 1.0
  - Other: 2.0
- Smuggling, drugs and contraband, are significant in Ariana, and exploited by criminal gangs
- Centers of Social Power
- The family (immediate and extended) is a basic foundation of Ariana's social structure.
- Arianians condone favoritism or bias based on family relationships, and this remains a culturally accepted norm.
- **Tribal System.**
  - Tribal Confederation
  - Tribe
  - Sub-tribe
  - Clan
  - Branch
  - Family
- Honor in Arianian culture defines an individual's reputation and worth.
- A family's male head of household is responsible for protecting the family's honor.
- When someone's honor is compromised, Arianians seek revenge for themselves, their family, or their group.

5. Information – Tightly controlled information/media environment
- Good INFOWAR capabilities; superior in niche areas
- Public media is hostile to US interests and will associate anti-Arianian motives with any US Motive.
- Government repressively monitors and controls information in Ariana
- TV and Internet are the country's most dynamic and powerful mediaEnglish is rapidly replacing Donovian as a common language for trans-border communication
- Ariana's military is believed to use commercial L-band receivers which are reciprocal with GPS or GLONASS for navigation.

- Ariana's advancements in satellite communication services are rapidly developing. Ariana operates one government-owned telecommunication satellite which utilizes Ku-band transponders in a geostationary orbit.
- Arianians conduct influence operations throughout the Muslim world but attempt to play down the "Persian" and "Shia" origins of their revolutionary message.

6. Infrastructure – Relatively modern infrastructure
- Has the resources to maintain and improve infrastructure but priority is on nuclear and oil/natural gas programs, which require modernization
- International sanctions prevent substantial improvements
- Possesses nuclear power, but has inadequate distribution

7. Physical Environment – Located in key position on Persian Gulf and Strait of Hormuz
- Borders Atropia and Limaria – Land and Caspian Sea borders allow direct access to all countries except Gorgas
- Faces Caspian Sea
- Rugged mountainous terrain
- Mountains and Dessert form the majority of Ariana
- Controls the Strait of Hormuz
- It is assessed that the underground facilities (UGFs) managed by the Arianian government support national missile and nuclear enrichment and development programs.
- There is a significant network of underground tunnels created and used by the God's Helpers Brigade, an insurgent group that has been opposing leaders for nearly two decades in southeast Ariana.
- The climate ranges from subtropical in the south to sub-polar at high elevations. Summer and winter can generate extreme temperatures of hot and cold respectively. Rainfall mainly occurs in spring.

8. Time – Value planning over deadlines
- Uses the Solar, Lunar, and Gregorian (Western) calendars
- Harvest cycle is May to August
- 4-year election cycle, 6 for president, 8 for Forum of Proficiency; no term limit

B. Atropia

Atropia is vulnerable because of its natural resources and as a result of conflicts over the Lower Janga region. Atropia possesses significant oil and gas reserves in both the northeast and the Caspian Sea. Further, the Baku-Tbilisi-Ceyhan (BTC) pipeline, one of the most critical infrastructure components in the region, originates near its capital city. These rich natural resources generate potential threats from external forces.

Limaria currently occupies Atropia's Lower Janga region, an area fought over by Atropia and Limaria for over a quarter of a century. At present, over 95% of the Lower Janga region population belongs to the Limarian ethnic group. Refugees displaced from the Lower Janga dispute amount to over one million people. An estimated 400,000 Atropian Limarians and 30,000 Lower Janga Limarians fled to Limaria or Donovia to avoid the conflict. An estimated 800,000 Atropians from Limaria or Lower Janga sought refuge in Atropia. Various other ethnic groups in Lower Janga also evacuated to refugee camps in Atropia or Ariana. All efforts to settle the dispute since 1997 have failed. Ariana contains a large internal Atropian ethnic minority and disagrees with Atropia over the delineation of Caspian Sea oil and gas fields. Atropia, a majority Shia nation, resists Arianian-sponsored attempts to politicize Islam within Atropia.

1. Political – Dictatorship
- Power belongs to a small, elite group "one family" under President Salam Ismailov
- Looks to the West for support, but is considered "neutral."
- Sees Ariana, Donovia, and Limaria as threats
- US willing to support because the US sees Atropia as a counterbalance to Ariana and Donovia
- Attempts to follow a secular-Muslim model, few civil liberties exist
- South Atropia People's Army (SAPA) is the largest insurgency
- Bears much unfocused anger about the Lower Janga region, which is controlled by Limaria.

2. Military – Small army, navy, and air force
- Tier 2 conventional forces (10-20 years old) that has tier 1 niche capability
- Fields a capable Army Corps, with a small Air Force, and smaller Navy
- Limited offensive capabilities
- Tensions continue with Limaria over Lower Janga region, with continual skirmishes Defense of hydrocarbon resources and infrastructure paramount
- Has the capability to produce chemical, biological, radioactive, and nuclear (CBRN) munitions, but does not have the weapons in their inventory.
- Leases satellites to aid in achieving its strategic goals. Imagery intelligence is derived from commercially purchased imagery assets.
- The Army can conduct large-scale operations with the ability to fluctuate between adaptive tactics and hybrid operations.
- Two main and several small insurgent groups
- **National Strategic Goals**:
  o Resolution of territorial disputes, especially those with Limaria
  o Defense of Atropia's sovereignty and hydrocarbon resources
  o Economic expansion
  o Destruction of insurgent groups, especially those in the Lower Janga region

Threat	Type	OE	Activities	Targets
Salasyl	Insurgent	SE Atropia with Nation-wide capabilities	Possible ties to transnational criminal and terrorist actors. Engaged the Atropian regime in a low-level insurgency for the past 20 years. Promotes violent populace opposition to state taxation policies, unreliable public services, substandard medical preventive services, inaccessible state education programs for working class citizens, and a judicial system that illegally favors the ruling political party. Salasyl and South Atropian People's Army (SAPA) insurgents often clash violently over ideology, limited resources, and similar recruiting pools.	Atropian government facilities and leaders
South Atropian People's Army (SAPA)	Insurgent	Focuses on eight provinces in the south with cultural ties to Ariana	Primary goal is to create a separate country composed of southern Atropia and Ariana's northwestern provinces. Receives most of its training, equipment, and supplies from Ariana. SAPA and Salasyl insurgents often clash violently over ideology, limited resources, and similar recruiting pools.	Atropian government facilities and leaders
Bilasuvar Freedom Brigade (BFB)	Insurgent	Northern Vetlia and Erdabil Provinces	Donovia supports the BFB, creating political tension between Donovia and Atropia.	Atropian government facilities and leaders
Provisional Army of Lezgin (PAL)	Insurgent	Southern Erdabil and Western Sirvaki Prov.	Small insurgent group with limited regional activities.	Atropian government facilities and leaders
Bocyowicz Crime Family	Criminals	Ungoverned Territories	Acquires political power in poorly-governed regions, eventually gaining control of geographic space. These political actions are intended to provide security and freedom of movement for the criminal organization's activities. As a result, the third-generation criminal organization and its leadership challenge the legitimate state authority.	Atropian Police and security forces
Atropian Organized	Criminal	Baku	Illegal narcotics, smuggling, and human trafficking. Many of those involved in Atropian	Police and security forces

Crime (AOC)			illegal activities live in communities of displaced Atropians from Lower Janga and persons who fled Donovia. Atropia serves as a transit point for narcotics travelling to Donovia and Western countries.	
Al Iksir Cartel	Criminal	Northern Atropia and Southern Donovia	Illegal narcotics, smuggling, and human trafficking. Many of those involved in Atropian illegal activities live in communities of displaced Atropians who fled Donovia. Atropia serves as a transit point for narcotics travelling to Donovia and Western countries.	Police and security forces

3. Economic – Hydrocarbon extraction dependent economy
- Owns large oil and natural gas reserves and will remain a hydrocarbon-based economy
- Political patronage depresses economic growth
- Will attempt to keep good relations with neighbors to maintain export channels for its petroleum and gas and to import hydrocarbon industrial equipment and consumer goods

4. Social – Shia Muslim Culture
- 89% Shia Muslim
- 91% Atropian
- 99% literacy rate
- 1/2 million IDPs
- 52% of population is urban
- A social chasm exists between poor rural residents who rely primarily on agriculture and richer urban residents who work in industries
- Any major conflict in the Lower Janga Region will give Atropia a pretense to recover its lost territory and revenge its previous defeats by Limaria
- The difference between potential government benefits for any new internally displaced persons and those initially received by persons displaced two decades earlier may cause a rift between groups internal to Atropia.
- Society possesses elements of both European and Middle Eastern culture, through the emphasis on education with social conservatism
- Atropians consider themselves a branch of Kalarian people and spoke Atropian is linguistically similar to Kalarian.
- Atropians have links to Ariana through the large Atropian minority in Ariana
- **Languages spoken in Atropia**:
  - Atropian (Atropian): 90.3
  - Lezgi: 2.2
  - Donovian: 1.8
  - Limarian: 1.5
  - Other: 3.3
- The Lower Janga War forced the movement of hundreds of thousands of ethnic Atropian refugees from the Lower Janga province into Atropia,
- Atropia is almost entirely ethnically Atropian with a few non-Atropians who primarily reside in border areas or Baku.
- The percent of Atropians who consider themselves Muslim is 93.4, but polls suggest that only about 21% of Atropians believe religion plays an important factor in their daily life. Eighty-nine percent of Atropians are of the Shia denomination. Additionally, 2.5% are Donovian Orthodox and 2.3% are Limarian Orthodox.
- A growing concern among law enforcement within Atropia is the increase in trafficking tunnels from Ariana and Limaria. These underground networks were created to shield criminal groups and their nefarious smuggling activities from law enforcement agencies on both sides of the border.

5. Information – Free but monitored information/media environment
- Growing INFOWAR capabilities; focus on Limaria and Ariana
- Social media is growing in importance
- Atropian media is generally aligned with government and political leaders
- Atropia relies on third party satellite services, leasing commercial Ku-band transponders from larger, more developed republics.

- Atropian hackers actively attack Limarian websites

6. Infrastructure – Unable to maintain infrastructure
- Focus is on oil/natural gas programs
- Road system incapable of handling military traffic
- Rural areas lack modern water, electricity, and sewage system
- Baku International Sea Port on the Caspian Sea
- Has limited subterranean environment to defend against Limaria and facilitate movement between itself and Donovia. About 20 operational tunnels, and most if not all are also used for criminal operations.

7. Physical – Vital transportation corridor between east and west
- Access to Caspian Sea
- Varied terrain ranging from high rugged mountains to fertile lowlands
- Troop movement is difficult in the mountains, but unhampered in the central lowlands
- The Mingachevir Reservoir supplies the country with water for both agriculture and hydroelectric power.
- Atropia is a strategic transport corridor between Asia and Europe
- Atropia exhibits a wide variety of climates dependent on location, elevation, and proximity to the Caspian Sea. Based on altitude and distance from the Caspian Sea coastline, parts of Atropia enjoy dry-subtropical, wet-subtropical, temperate, and alpine climates.

8. Time – Punctuality not important
- Uses Gregorian calendar, but uses the lunar calendar for Muslim holidays
- Atropia has become more westernized in its business dealings in regards to time and punctuality.
- Harvest cycle is April to October, depending on climatic zone
- 2-year election cycle for legislature, four consecutive-term limit; 6-year presidential cycle, no term limit.

c. Donovia

Donovia is a resurgent nation that, prior to the early 1990s, was the region's dominant political, economic, military, and social player. Internal turmoil lessened Donovia's influence during the period from the 1990s to around 2000. Now, riding a wave of higher oil prices, a reinvigorated Donovia seeks to rebuild its prior levels of regional and international influence through a combination of assertive diplomacy and military power. However, the desire for independence among the other states in the region creates friction between them. Ultimately, Donovia's neighbors wish to accommodate Donovian power without jeopardizing their core equities.

1. Political – Authoritarian Republic
- Regionally dominant
- Figurehead elected President
- Power rests with small group of elites, the United Donovian (UD) Party controls the government
- Weakening legitimacy of ruling political party
- Typically neutral to US power and forces; will protect regional position of power
- Adversarial toward Atropia, maintains a positive relation with Ariana. Relations with Gorgas are "frost" at best and Donovia supports two breakaway provinces (Zabzimek and South Ostremek) in Gorgas. Limaria receives considerable assistance.
- High levels of crime and corruption
- Donovians view all political and diplomatic interaction as a zero-sum game.
- Donovians will integrate political, military, diplomatic, and economic power in all decision-making.
- The UD co-opted religious authority within Donovia, generally favoring religious leaders who support the UD, or at the very least do not challenge its authority.

2. Military – Large conventional force
- Three standing armies with mainly Tier 1 capabilities
- Most capable and modern military in region, considered to be well trained and equipped
- Capable of a wide range of operations, conventional, peace enforcement, and irregular warfare
- Successful nuclear weapons program enhances Donovia's robust CBRN capability. Some CBRN material may have been sold to terrorist organizations

- State of the art (tier 1) integrated air defense system complimented with tactical all-arms air defense capabilities
- Anti-satellite capabilities
- Strong INFOWAR capabilities
- Donovia is a major producer of military equipment and vehicles for its own use and for export to other countries.
- Regionally, has the strongest, technologically superior satellite capabilities with four commercial and two military satellites in operations. It will lease more, though, when needed.
- Donovia has an arse\nal of nuclear weapons, but is heavily concerned with nuclear power production. It is building ten additional nuclear reactors.
- **Strategic Goals**:
  - Defense of Donovia's sovereignty
  - Economic expansion
  - Preclusion or elimination of outside intervention
- **Army warfighting principles**:
  - Control access into the region
  - Employ operational shielding
  - Control the tempo
  - Cause [politically unacceptable casualties to the enemy
  - Neutralize technological overmatch

Threat	Type	OE	Activities	Targets
Bilasuvar Freedom Brigade (BFB)	Insurgent	Southern Donovia & northern Atropia	The Donovian government supports this group as its intent is to overthrow the current Atropian government. Donovia's support for the BFB creates political tension between the countries.	Atropian government facilities and leaders
Small Anti-Government Groups		Country-wide	Attacks and violence tend to be minimal and, unless these groups join forces, will remain an insignificant threat to the Donovian government. None of the groups has more than 50 individuals, and the names of these groups change randomly as members come and go.	Donovian government facilities and leaders
Jinat Crime Family	Criminal	Country-wide	Produced the infamous Traitor Ismail Jinat and is heavily invested in the mining trade.	Donovian police and security forces
Donovian Mafia	Criminal	Country-wide	The organization is well-organized and has branches and contacts in many nations, including the United States and the European Union. With former security service and military personnel among its members, the Donovian Mafia possesses a wide range of capabilities, including electronic surveillance, human intelligence networks, explosives and firearms expertise, and associations with government officials in Donovia and neighboring countries.	Donovian police and security forces
Al Iksir Cartel	Criminal	Southern Donovia & Northern Atropia	A local criminal gang, operates primarily in southern Donovia and northern Atropia.	Donovian police and security forces

3. Economic – Dominant energy sector
- Owns large oil and natural gas reserves
- Large hydrocarbon-related service sector
- Major international military equipment exporter
- Current economy resultant from an internal economic
- GDP is heavily skewed toward energy-related industry and services
- Corruption is integral to the economic system

4. Social – Arab Sunni Hanafi Culture

- 70% Arabic
- **Language is Donovian** (official, although there are many minority languages spoken)
- 98% literacy rate
- 67% of population is urban
- Although it is a Muslim-majority country, it is secular
- Donovia struggles with severe social issues and its population is in decline
- Criminal activity includes arms-trafficking, human trafficking, money laundering, extortion, fraud, and black marketeering. The Donovian Mafia controls smuggling tunnels into neighboring countries. The military can also use these tunnels

5. Information – Controlled information/media environment
- Tier 1 INFOWAR capabilities, with heavy government investment
- Most capable in region
- Government maintains almost total control over content within the informational environment
- Possesses a wide range of dual-use satellites, and two military imaging satellites

6. Infrastructure – Modern infrastructure
- Western standards in terms of railroads and ports
- Energy infrastructure is top priority
- Possesses both nuclear power and nuclear weapons
- Most infrastructure suffers from a lack of maintenance due to insufficient government funds

7. Physical Environment – Greater Caucasus Mountains separate country from southern neighbors
- Access to Black and Caspian Seas
- Varied terrain
- North Caucus area is separated from the rest of the Caucasus region by the Greater Caucasus Mountains, creating a formidable barrier to ground movement between Donovia and its southern neighbors

8. Time – Expect punctuality from Westerners but may not reciprocate
- Uses Gregorian calendar
- Expect punctuality
- Harvest cycle is year round
- 6-year election cycle for president, two consecutive-term limit; 4-year cycle for parliament

D. Gorgas

Gorgas, like Atropia, is a small yet fiercely independent state in a fragile and dangerous area, but without Atropia's hydrocarbon assets. The country's primary strength is geographical—its Black Sea ports and land border with Kalaria make it a logical pipeline route and regional outlet to the outside world. Gorgas remains among the smallest and least economically developed nations in the region. It currently exists in a state of "frozen conflict" with Donovia over Donovian attempts to block Gorgas from NATO and EU membership, as well as Donovian support for Zabzimek and South Ostremek—two breakaway regions formerly part of Gorgas.

The breakaway territory Zabzimek is located in northwest Gorgas and borders Donovia. Currently, a ceasefire and line of separation exist between Gorgas and Zabzimek, but the Zabzimek militia poses a threat to the port of Poti and lines of communication from the Black Sea to the Gorgan capital city of Tbilisi. Zabzimek achieved de facto independence after the conflict with Gorgas in 1992, but only Donovia and Nicaragua recognize the country internationally. Strong criminal elements operate in Zabzimek.

South Ostremek, in north-central Gorgas, also wants independence from Gorgas. Like Zabzimek, South Ostremek achieved *de facto* independence after the 2008 Donovia-Gorgas War, but only Donovia and Nicaragua recognize the new country internationally. South Ostremek wants to reunite with North Ostremek, a Donovian province. Currently, a ceasefire remains in effect between Gorgas and South Ostremek, primarily monitored by Donovian peacekeepers.

1. Political – Emerging Democracy

- Representative republic, although nascent in development of their institutions
- Values Western principles
- Looks to distance itself from Donovia
- Seeks NATO and EU membership
- The Gorgan Orthodox Church possesses a very real, albeit unofficial, political influence
- Zabzimek and South Ostremek have broken away from Gorgas and those provinces rely on Donovia for protection. Zabzimek conducted significant "ethnic cleansing."
- Jarie has also broken away from Gorgas, and has destroyed bridges linking it to Gorgas

2. Military – Smallest military in region
- Tier 2 conventional forces with niche tier 1 capability
- Armed forces are small but capable and can conduct conventional and adaptive operations
- Army consists of 3 Infantry BDEs (4,800 to 6,000 per BDE), 1 Artillery BDE, 1 separate tank BDE, on AT bn, and the National Guard
- Defensive capabilities with limited offensive capabilities
- Tensions continue with Zabzimek and South Ostremek (breakaway Gorgan republics) Donovian-sponsored paramilitaries are current threat, along with the Donovian military
- Must lease satellites, but commercially purchases global positioning receivers for both commercial and military use.
- IMINT capability is limited to from Western allies for most IMINT applications
- **National Strategic Goals**:
  - Defense of Gorgan sovereignty
  - Recovery of breakaway territories
  - Economic expansion
  - Elimination of insurgent groups
- A number of years ago, a civil war erupted in both Zabzimek and South Ostremek, where the territory still remains in the hands of separatists. Gorgas launched numerous operations in an attempt to bring the disputed areas back under Gorgan control. Donovia crossed the northern Caucasus to support the breakaway regions, counterattacked the Gorgan military forces, and recognized the breakaway regions as independent states. The Gorgan military failed in its mission to maintain the country's boundaries in both of these territories.

Threat	Type	OE	Activities	Targets
Zabzimek Separatists	Separatist Insurgents	Zabzimek	Maintains an armed military force. Zabzimek declared independence, Gorgas did not recognize this and fought the Zabzimek separatists to reinstate control. Donovia intervened on behalf of Zabzimek and oversaw the ceasefire agreement that left Zabzimek independent. A few years later, another six-day confrontation took place between the Zabzimek military and Gorgan militia units and Zabzimek recovered its territory occupied by the People's Liberal Republican Martyrs Group and the Falcon Brothers, two pro-Gorgan groups.	Gorgan government facilities and leaders
South Ostremek Separatists	Separatist Insurgents with conventional force capabilities	South Ostremek	South Ostremek declared its independence after Zabzimek, Gorgas attempted to bring it back under control. Gorgas failed due to Donovian intervention. Gorgas contributes an infantry battalion to the Donovian-led peacekeeping force in South Ostremek. South Ostremek also supports a small military force of an unknown number of military personnel, tanks, APCs, and artillery pieces.	Gorgan government facilities and leaders
People's Liberal Rep. Martyrs Grp	Pro-Gorgan Guerrillas	Zabzimek-Gorgas border	Conducts low-level guerrilla warfare in an attempt to reunite Zabzimek with Gorgas.	Zabzimek Separatist leaders and infrastructure
Falcon Brothers	Pro-Gorgan Guerrillas	Zabzimek-Gorgas border	Conducts low-level guerrilla warfare in an attempt to reunite Zabzimek with Gorgas.	Zabzimek Separatist leaders & infrast.

Zabzimek Irregular Forces	Separatist Insurgents with conventional force capabilities	Zabzimek	Operate freely within Zabzimek and occasionally conduct cross-border operations in Gorgas. They coordinate with and receive support from the Donovian and Zabzimeki regular and SPF units. Their goal is to insure an independent Zabzimek and harass and intimidate ethnic Gorgan civilians. They are capable of conducting small unit operations, dependent on support from Donovian SPF or regular units. Capabilities of these units include disruption, fixing, physical destruction, intimidation, and Reconnaissance, intelligence, surveillance, and target acquisition (RISTA).	Gorgan government facilities and leaders
Criminal Organizations	Criminal	Country-wide	A prime transshipment point for drugs from Central Asia. Gorgas lacks the resources to effectively tackle crime, especially in the mountainous north-eastern border with the Republic of Failaq in Donovia. Much of the support provided to anti-Donovian elements in Failaq comes from criminal and terrorist organizations that operate in this region. Zabzimek and South Ostremek are also dangerous, and organized crime permeates both areas	Gorgan police and security forces

3. Economic – Primarily service economy
- Large agricultural sector, lacks any major industry, and is dependent on trans-border trade
- Dependent on trans-national trade routes and pipelines
- Growth limited due to attempt to cut ties with Donovia

4. Social – Christian Culture
- 84% Gorgan Orthodox Christian, tolerant of other religions
- 100% literacy rate
- 1/4 million IDPs.
- 53% of population is urban with a stark difference in the standards of living between Tbilisi and the rest of the country
- Gorgas' national honor revolves around the return of its breakaway regions to governmental control; most Gorgans support this ultimate goal.
- Gorgans dislike the Donovians and will do almost anything to reduce Donovian influence in the Caucasus region.
- **Languages**:
  - Gorgan: 71.0 %
  - Donovian: 9.0 %
  - Limarian: 7.0 %
  - Atropian: 6.0 %
  - Other: 7.0 %

5. Information – Most free information/media environment in region
- Growing and integrated INFOWAR capabilities, generally along NATO doctrine, and mostly focused on Donovia
- INFOWAR based on NATO standards
- Public communications is growing, relatively free, and dynamic
- Relies on 3rd party satellites

6. Infrastructure – Unable to maintain infrastructure
- 1/3rd of population lives in Tbilisi
- Lacks raw materials for its factories
- Pipelines top priority
- Port of Poti on the Black Sea is key terrain for the region
- The tunnels in Gorgas were created and are used by insurgents, guerrillas and criminals.

7. Physical Environment – Controls much of Caucasus Mountains and routes through them
- Access to Black Sea
- Largely mountainous terrain

- Gorgas controls much of the Caucasus Mountains and routes through them
- Frequent earthquakes

8. Time – No urgency to complete tasks
- Uses Gregorian calendar
- Harvest cycle is April to October
- 4-year election cycle for all offices
- Gorgans lack a sense of urgency

E. Limaria

Limaria, a small and poor country, neighbors Atropia, Ariana, Gorgas, and Kalaria and also occupies the Lower Janga region. Limaria currently enjoys a strong economic and military relationship with Donovia and a good economic relationship with Ariana. Tensions still exist with Atropia over the disputed Lower Janga region, an Atropian province that is currently occupied by ethnic Limarians. Additionally, Ariana's and Limaria's improved trade relations have created tension with the US. Limaria will attempt to maintain relations with all the Caucasus powers due to its precarious economic development and isolated geopolitical position.

1. Political – Autocracy
- A neutral, provincial, recovering government
- A small, elite group controls Limarian politics
- Values alliance with Donovia
- Past genocide of Limarian civilians influences all decisions
- Sees Atropia as a threat
- Limarian Christian Church is the official church, and the church is not separated from government and is considered part of "being Limarian"
- Welcomes US trade

2. Military – Small military with army and air forces only
- Tier 2 conventional forces with limited tier 1 niche capabilities
- Consists of a skilled Army corps and a small, agile air force capable primarily of defensive operations. Limarian ground forces, primarily armor and mechanized infantry units are roughly equal to the Atropian military
- Capable of conventional and adaptive operations
- Tensions continue with Atropia over Lower Janga region, which Limaria controls
- Focused on Atropian military and support for allied Lower Janga military forces
- Terrorist groups present. Reports are that either the LLF or FLJM is attempting to acquire a dirty bomb
- Reports indicate possession of 2-5 nuclear weapons; government denies
- Uses Donovian satellite systems and commercially purchases global positioning receivers. Donovia would provide support if a large-scale conflict started in Limaria
- **National Strategic Goals**:
  - Defense of Limarian sovereignty
  - Protection of a Limarian population in the Lower Janga region
  - Annexation of territory, especially Lower Janga region in Atropia
  - Economic expansion
  - Destruction of insurgent groups against the government
- Limarian military strategy revolves around the Lower Janga region, and the military considers themselves to be the guarantor of security for the Lower Janga populace.

Threat	Type	OE	Activities	Targets
Limarian Liberation Front (LLF)	Pro-Limaria Guerrillas	Lower Janga Region	LLF consists of a number of independent Limarian groups, fused together by ideology and their common opposition to their Free Lower Janga Movement (FLJM). The goal of LLF is to control Lower Janga and push non-Limarians from the region. LLF will cooperate with Arianian special forces when it is in the group's best interest, but resists a permanent relationship. The group can conduct small cross-border attacks and has links to other global radical groups. Reporting indicates the possibility that it may attempt to smuggle dirty bomb(s) into the region.	FLJM and Atropian civilians
Free Lower Janga Movement (FLJM)	Pro-Atropia Guerrilla	Lower Janga Region	FLJM conducts military activities in the Lower Janga region to intimidate the Limarian population into leaving the region. The ultimate objective is to establish Lower Janga as an Islamic territory under the government of Atropia and displace the Limarian population in the region. Atropia is believed to provide assistance to the FLJM.	LLF and Limarian civilians
Criminal Orgs: - Limarian United Labor - Limarian Democratic Socialist Party - Abgar Bozian's Bozian	Criminal	Country-wide	Part of the *akhperutyuns* (brotherhoods), running robust human and drug trafficking operations. Due to official corruption, this clan operates nearly openly, mainly in Yerevan, and control much of the country's economy.	Limarian police and security forces

3. Economic – Service and agricultural based economy
- International trade window for Ariana
- Limaria will tie its economic fortunes to Ariana and Donovia
- Due to economic sanctions on Ariana, Limaria will increasingly operate as Ariana's export window to the rest of the world
- Lacks any extractive resources, but does have a modern industrial sector that supplies machine tools, textiles, and other manufactured goods
- Agriculture sector suffers from the lack of long-term investment, requiring Limaria to import their foodstuffs

4. Social – Christian Culture
- 98% Limarian, one of the most homogenous populations in the Caucasus region
- 99% literacy rate
- 300,000 IDPs
- 64% of population is urban
- 95% belong to the Limarian Apostolic Church
- Most Limarians feel culturally superior to their neighbors
- Genocide and persecution against them from their Muslim neighbors reverberates through Limarian culture. Limarians always make political decisions to ensure ethnic cleansing never happens again
- Most Limarians would like to see the Lower Janga region be autonomous and annexed as part of Limaria
- **97.7% speak Limarian**, and 95% come from Limarian ancestry
- Possess extreme hatred for Atropians and Kalarians because of past ethnic cleansing

5. Information - Fairly free information/media environment
- Soft censorship
- Integrated with Donovia for INFOWAR support, but also looks to NATO for support in INFOWAR capabilities
- English is becoming common from trans-border communication
- Television is an effective medium for information dissemination
- Limarian media generally follows Limarian government lines on issues

6. Infrastructure – Unable to maintain infrastructure
- Atropia's recent blockade forced reduction of Limarian industrial output
- Relies on food imports
- Lacks modern running water, electricity, and sewage system for much of the population
- Tunnels in Limaria vary from simple (no electricity) to complex. They are heavily used by criminals for smuggling, although primarily created by the military for its useAtropia has blockaded goods and electricity from entering Limaria
- Most rural areas lack potable water, electricity, and modern sewage systems

7. Physical Environment – Landlocked
- Contains Lake Sevan, the largest lake in the region
- Mountainous terrain with limited arable land
- Land-locked
- The Limarian government has developed an extensive tunnel network in the Torrel and Laulor provinces that border the Lower Janga region in Atropia. LLF and FLJM have also developed tunnels to support movement of people and logistics in and out or Lower Janga

8. Time – Do not believe in punctuality but will attempt to be punctual for Westerners
- Uses Gregorian calendar
- Harvest cycle is year round
- 5-year election cycle for all offices; no term limit

F. POTENTIAL CONFLICT FLASHPOINTS
- Atropian blockade of goods and electricity to Limaria: Limaria remains dependent on Gorgas (despite a limited embargo) and Ariana—an international pariah—for access to much of its imports and power.
- Lower Janga (current ceasefire): Localized violence routinely disrupts the ceasefire agreement.
- South Ostremek (current ceasefire): The ceasefire simply stabilized the conflict lines, as the Donovians want to politically pry Gorgas away from EU or NATO membership, or even close cooperation with the Western world. Gorgas definitely seeks a return to its pre-war territorial boundaries.
- Zabzimek (current ceasefire): Like South Ostremek, Gorgas prefers a return to the pre-war status quo and boundaries, while Donovia wants to further isolate Gorgas from its Atropian and Western allies.
- Archeological sites and religious shrines in Ariana: Ariana controls significant Shia religious sites where many Muslims conduct pilgrimages for religious purposes.
- Transnational pipeline operations: The export of crude oil and natural gas to the world remains a significant challenge for Ariana and Atropia. Oil producers possess several pipeline projects that diversify their export options, but pipelines remain vulnerable to interdiction.
- Caspian Sea oil and natural gas reserves: The demarcation of Caspian Sea deposits remains a source of contention. Oil and gas fields are the lifeblood of the countries that possess them, and their exact demarcation leads to contentious arguments over the boundaries.
- Arianian nuclear program: The Arianian government's desire to maintain a robust WMD program causes strife with nearly all its neighbors, as the relative power of a WMD-armed Ariana complicates the delicate balance of power that currently exists in the region.

Index

Zabzimek Separatists, 53

References

TC 7-100 Hybrid Threat, November 2010

TC 7-100.2 Opposing Force Tactics, December 2011

TC 7-100.3 Irregular Opposing Forces, January 2014

TC 7-101 Exercise Design, November 2010

ST 7-100 Version 1.0 OPFOR Battle Book for the Operational Environment June 2013

Decisive Action Training Environment 2.2, March 2015

Worldwide Equipment Guide, 2014