OPFOR SMARTBOOK 5

thelightningpress.com

FIRST EDITION
(OPFOR5)

Irregular &
Hybrid Threat

Insurgents

Guerillas

Terrorists

Criminal
Organizations

Armed & Unarmed
Noncombatants

Foreign Security
Forces (FSF) Threat

Functional
Tactics

Irregular & Hybrid Threat

Forces, Operations & Tactics

The Lightning Press
Larsen & Wade

OPFOR SMARTBOOK

TheLightningPress.com

5

Irregular & Hybrid Threat

Forces, Operations & Tactics

The Lightning Press

Dr. Christopher Larsen
Norman M. Wade

The Lightning Press

2227 Arrowhead Blvd.
Lakeland, FL 33813
24-hour Order / Voicemail: 1-800-997-8827
E-mail: SMARTbooks@TheLightningPress.com

www.TheLightningPress.com

OPFOR SMARTbook 5 - Irregular & Hybrid Threat (OPFOR5)

Forces, Operations & Tactics

ISBN: 978-1-935886-54-9

Notice of Liability

The information in this SMARTbook and quick reference guide is distributed on an "As Is" basis, without warranty. While every precaution has been taken to ensure the reliability and accuracy of all data and contents, neither the author nor The Lightning Press shall have any liability to any person or entity with respect to liability, loss, or damage caused directly or indirectly by the contents of this book. If there is a discrepancy, refer to the source document. All military references used to compile SMARTbooks are in the public domain and are available to the general public through official public websites and designated as approved for public release with unlimited distribution. The SMARTbooks do not contain ITAR-controlled technical data, classified, or other sensitive material restricted from public release. SMARTbooks are reference books that address general military principles, fundamentals and concepts rather than technical data or equipment operating procedures. "The views presented in this publication are those of the author and do not necessarily represent the views of the Department of Defense or its components."

Photo Credits: Cover - Shutterstock.com, FBI.GOV, Russian Ministry of Defense; others where credited.

Printed and bound in the United States of America.

(OPFOR5) Notes to Reader

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. The term “**hybrid**” has recently been used to capture the seemingly increased complexity of war, the multiplicity of actors involved, and the blurring between traditional categories of conflict.

Irregular forces are armed individuals or groups who are not members of the regular armed forces, police, or other internal security forces. The irregular OPFOR can be part of the hybrid threat (HT). The irregular OPFOR component of the HT can be insurgents, guerrillas, or criminals or any combination thereof. The irregular OPFOR can also include other armed individuals or groups who are not members of a governing authority’s domestic law enforcement organizations or other internal security forces.

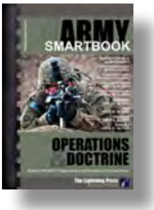
Irregular forces are unregulated and as a result act with no restrictions on violence or targets for violence. Time-honored concepts of “conventional” and “unconventional” war and “traditional” methods versus “adaptive” methods are weapons to a hybrid threat.

Insurgents are armed and/or unarmed individuals or groups who promote an agenda of subversion and violence that seeks to overthrow or force change of a governing authority. A **guerrilla force** is a group of irregular, predominantly indigenous personnel organized along military lines to conduct military and paramilitary operations in enemy-held, hostile, or denied territory.

Terrorism is a tactic. Terrorism can be defined as the use of violence or threat of violence to instill fear and coerce governments or societies. Often motivated by philosophical or other ideological beliefs, objectives are typically political in nature.

Criminal elements exist at every level of society and in every operational environment (OE). Their presence, whatever their level of capabilities, along with a host of **armed and unarmed noncombatants** adds complexity to any operational environment. **Foreign security force (FSF)** threats are not a new phenomenon; however, during recent limited contingency operations, U.S. forces experienced a sharp increase in the number of attacks perpetrated by FSFs.

Insurgents and guerrillas, as part of the irregular OPFOR, may employ adaptive **functional tactics**.



SMARTbooks - DIME is our DOMAIN!

SMARTbooks: Reference Essentials for the Instruments of National Power (D-I-M-E: Diplomatic, Informational, Military, Economic)! Recognized as a “whole of government” doctrinal reference standard by military, national security and government professionals around the world, SMARTbooks comprise a comprehensive professional library.

SMARTbooks can be used as quick reference guides during actual operations, as study guides at education and professional development courses, and as lesson plans and checklists in support of training. Visit **www.TheLightningPress.com**!

The OPFOR SMARTbook Series (Overview)

In today's complicated and uncertain world, it is impossible to predict the exact nature of future conflict that might involve the U.S. Army. So the Army must be ready to meet the challenges of any type of conflict, in all kinds of places, and against all kinds of threats.

In the coming years, the United States and its allies will face an increasingly complex and interconnected global security environment marked by the growing specter of great power competition and conflict, while collective, transnational threats to all nations and actors compete for our attention and finite resources.

Competition and potential conflict between nation-states remains a critical national security threat. Beijing, Moscow, Tehran, and Pyongyang have demonstrated the capability and intent to advance their interests at the expense of the United States and its allies. China increasingly is a near-peer competitor, challenging the United States in multiple arenas—especially economically, militarily, and technologically—and is pushing to change global norms and potentially threatening its neighbors. Russia is pushing back against Washington where it can—locally and globally—employing techniques up to and including the use of force. In Ukraine, we can see the results of Russia's increased willingness to use military threats and force to impose its will on neighbors. Iran will remain a regional menace with broader malign influence activities, and North Korea will expand its WMD capabilities while being a disruptive player on the regional and world stages.

Contemporary Operating Environment

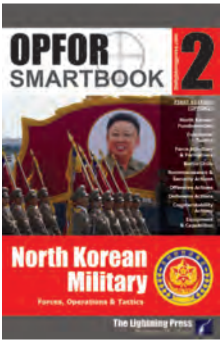
Today's operational environment presents threats to the Army and joint force that are significantly more dangerous in terms of capability and magnitude than those we faced in Iraq and Afghanistan. Major regional powers like Russia, China, Iran, and North Korea are actively seeking to gain strategic positional advantage. The interrelationship of the air, land, maritime, space, and the information environment (including cyberspace) requires a cross-domain understanding of an operational environment.

Opposing Force (OPFOR)

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

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

For more than two thousand years, China has been surrounded by enemies, adversaries, and other competitors. With a force that totals approximately two million personnel in the regular forces, the PLA views protecting Chinese sovereignty and security as a sacred duty. OPFOR1 topics and chapters include the strategic environment (defense & military strategy, strategic & operational environments, territorial disputes), force structure (PLA: Army, Navy, Marine, Air Force, Rocket Force, Strategic Support Force), system warfare, information operations, reconnaissance and security, offensive and defensive actions, antiterrorism and stability actions, and capabilities (maneuver, fire support, air defense, aviation, engineer and chemical defense, network and communications, and special operations forces).



North Korea is one of the most militarized countries in the world and remains a critical security challenge for the United States, our Northeast Asian allies, and the international community. The Kim regime has seen itself as free to take destabilizing actions to advance its political goals, including attacks on South Korea, development of nuclear weapons and ballistic missiles, proliferation of weapons, and worldwide cyberattacks. OPFOR2 topics and chapters include the strategic environment, force structure (KPA: Ground Forces, Navy, Air & Air Defense Force, Strategic Force, Special Operations, Reserve and Paramilitary forces, Internal Security & Intel Services), functional tactics, recon & security, offensive and defensive actions, counterstability actions, electronic intelligence warfare, equipment and capabilities.

It has been nearly thirty years since a holistic explanation of the Soviet-based Opposing Force (OPFOR) was examined in the U.S. Army Field Manual 100-2 series. Recognizing this, OPFOR SMARTbook 3: Red Team Army (Second Edition) re-examines and outlines the doctrinal operational construct and historical foundations of Soviet-era military forces from the FM 100-2 series, which is now out-of-print and largely unavailable. OPFOR3 topics and chapters include RTA overview, offensive and defensive operations, specialized warfare, tactical enabling tasks, small unit drill, urban & regional environments, rear area operations and logistics. *Future editions will be revised and updated to focus centrally on modern Russian forces, operations, tactics and lessons learned in the Ukraine.*

Throughout its 40-year history, the Islamic Republic of Iran has remained implacably opposed to the United States, our presence in the Middle East, and our support to Israel. While attempting to strengthen its deterrence against foreign attack and influence, Tehran has committed itself to becoming the dominant power in the turbulent and strategic Middle East. To achieve its goals, Iran continues to rely on its unconventional warfare elements and asymmetric capabilities—intended to exploit the perceived weaknesses of a superior adversary—to provide deterrence and project power. This combination of lethal conventional capabilities and proxy forces poses a persistent threat. *OPFOR4 SMARTbook is in the early stages of development and will be published at a later date.*

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. Irregular forces are armed individuals or groups who are not members of the regular armed forces, police, or other internal security forces. Irregular forces are unregulated and as a result act with no restrictions on violence or targets for violence. OPFOR5 topics and chapters include irregular and hybrid threat (components, organizations, strategy, operations, tactics), insurgents and guerillas forces, terrorists (motivations, behaviors, organizations, operations and tactics), criminals (characteristics, organizations, activities), noncombatants (armed & unarmed), foreign security forces (FSF) threats, and functional tactics.

(OPFOR5) References

The following primary references were used to compile *OFPOR SMARTbook 4: Irregular & Hybrid Threat (Forces, Operations & Tactics).* All references are open-source, public domain, available to the general public, and/or designated as “approved for public release; distribution is unlimited.” *OPFOR SMARTbook 4: Irregular & Hybrid Threat* does not contain classified or sensitive material restricted from public release.

Army Publications/Field Manuals

TC 7-100, Hybrid Threat, Nov 2010.

TC 7-100.3, Irregular Opposing Forces, Jan 2014.

TC 7-100.4, Hybrid Threat Force Structure Organization Guide, Jun 2015.

FM 3-24, Insurgencies and Countering Insurgencies, May 2014.

FM 3-39, Military Police Operations, Apr 2019.

ATP 3-37.15, Foreign Security Force Threats, Jan 2020.

ATP 3-57.10, Civil Affairs Support to Populace and Resources Control, Aug 2013.

U.S. Army TRADOC G2 Handbook No. 1 (Version 5.0), A Military Guide to Terrorism in the Twenty-First Century, Aug 2007.

Joint Publications

JP 3-0, Joint Operations, w/Chg 1, Oct 2018.

JP 3-07.2, Antiterrorism., Nov 2010.

JP 3-24, Counterinsurgency, April 2018.

JP 3-26, Counterterrorism, Nov 2009.

Other References

Annual Threat Assessment of the U.S. Intelligence Community, Office of the Director of National Intelligence, Feb 2022.

Chivers, C.J. “Turning Tables: U.S. Troops Ambush Taliban with Swift and Lethal Results” The New York Times, April 17, 2009, p. A6.

Connable, Ben; and Libicki, Martin C. How Insurgencies End. Washington, DC: RAND National Defense Research Institute, 2010.

Edwards, Sean J.A. Swarming on the Battlefield: Past, Present, and Future. Washington DC: RAND National Defense Research Institute, 2000.

Hammes, Thomas X. The Sling and The Stone: On War in the 21st Century. St. Paul, MN: Zenith Press, MBI Publishers, 2004.

This publication presents PLA military theory largely as written and prescribed by the PLAA. In most cases this represents a best practice as determined by PLA leadership. Real-world practices of PLA units are largely opaque to outsiders, and they were generally not included as part of the analysis underpinning this document. Moreover, the PLA has not participated in an active conflict in nearly half a century, so real-world applications are minimal. Available information on Chinese military training exercises and the few recent examples of conflict seem to indicate that PLA practices—including those of the PLAA—conform closely to its military theory.

(OPFOR5) Table of Contents

Chap 1 Irregular & Hybrid Threat

Insurgents

Chap 3

Guerillas

Chap 4

Terrorists

Chap 5 Criminal Organizations

Chap 6 Noncombatants (Armed & Unarmed)

Chap 7 Foreign Security Force (FSF) Threats

Chap 8 Functional Tactics

Chap 1

I. Irregular & Hybrid Threat (Overview)

Ref: TC 7-100, Hybrid Threat (Nov '10), chap. 1 and TC 7-100.3, Irregular Opposing Forces (Jan '14), chap. 1.

I. Hybrid Threats

Hybrid threats are innovative, adaptive, globally connected, networked, and embedded in the clutter of local populations. They can possess a wide range of old, adapted and advanced technologies—including the possibility of weapons of mass destruction (WMD). They can operate conventionally and unconventionally, employing adaptive and asymmetric combinations of traditional, irregular, and criminal tactics and using traditional military capabilities in old and new ways. Understanding hybrid threats involves several key concepts, most of which are not actually new.

Hybrid Threat

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

The term "hybrid" has recently been used to capture the seemingly increased complexity of war, the multiplicity of actors involved, and the blurring between traditional categories of conflict. While the existence of innovative adversaries is not new, today's hybrid approaches demand that U.S. forces prepare for a range of conflicts. These may involve nation-state adversaries that employ protracted forms of warfare, possibly using proxy forces to coerce and intimidate, or non-state actors using operational concepts and high-end capabilities traditionally associated with states.

The emergence of hybrid threats heralds a dangerous development in the capabilities of what was labeled a "guerrilla" or "irregular" force in past conflicts. Hybrid threats can combine state-based, conventional military forces—sophisticated weapons, command and control, and combined arms tactics—with attributes usually associated with insurgent and criminal organizations.

Hybrid threats are characterized by the combination of regular and irregular forces. Regular forces are governed by international law, military tradition, and custom. Irregular forces are unregulated and as a result act with no restrictions on violence or targets for violence. The ability to combine and transition between regular and irregular forces and operations to capitalize on perceived vulnerabilities makes hybrid threats particularly effective. To be a hybrid, these forces cooperate in the context of pursuing their own internal objectives.

Threats can challenge U.S. access—directly and indirectly. They can attack U.S. national and political will with very sophisticated information campaigns as well as seek to conduct physical attacks on the U.S. homeland.

See discussion of irregular threat and forces on pp. 1-6 to 1-8 and 1-14 to 1-22.

It is important to note that hybrid threats are not new. History is full of examples of how an adversary has prepared to use his relative perceived strengths against his opponent's perceived weaknesses:

- **1754 to 1763**: regular British and French forces fought each other amidst irregular Colonialists fighting for the British and American Indians fighting for both sides.
- **1814**: Peninsula War ended after the combination of regular and irregular allied forces from Britain, Portugal, and Spain prevented France from controlling the Iberian Peninsula.
- **1954 to 1976**: Viet Cong and People's Army of Vietnam combined irregular and regular forces in fighting the French and U.S. forces. Viet Cong would organize into conventional and unconventional units.
- **2006**: Hezbollah mixed conventional capabilities (such as anti-armor weapons, rockets, and command and control networks) with irregular tactics (including information warfare, non-uniformed combatants, and civilian shielding). The result was a tactical stalemate and strategic setback for Israel.

The U.S. Army will face hybrid threats that simultaneously employ some combination of regular forces, irregular forces, and/or criminal elements, to achieve their objectives. Hybrid threats will use an ever-changing variety of conventional and unconventional organizations, equipment, and tactics to create multiple dilemmas.

Hybrid threats seek to saturate the entire operational environment (OE) with effects that support their course of action and force their opponents to react along multiple lines of operation. A simple military attack may not present enough complexity to stretch resources, degrade intellectual capacity, and restrict freedom of maneuver. Instead, hybrid threats can simultaneously create economic instability, foster lack of trust in existing governance, attack information networks, provide a captivating message consistent with their goals, cause man-made humanitarian crises, and physically endanger opponents. Synchronized and synergistic hybrid threat actions can take place in the information, social, political, infrastructure, economic and military domains.

Opponents of hybrid threats will have difficulty isolating specific challenges. They will be forced to conduct economy of force measures on one or more of several lines of operation. Meanwhile, hybrid threats will continue to shift effort and emphasis to make all choices seem poor ones.

Hybrid threats are networks of people, capabilities, and devices that merge, split, and coalesce in action across all of the operational variables of the OE. Each separate actor and action of a hybrid threat can be defeated if isolated and the proper countermeasure is applied. By creating severe impacts across the total OE, a hybrid threat prevents its opponents from segregating the conflict into easily assailable parts. Often military action will be the least important of a hybrid threat's activities, only coming after exploitation of all the other aspects of the OE has paralyzed its opponent.

Hybrid threats can include criminals and criminal groups used in conjunction with both regular and irregular forces. A picture of this future was provided by the 2008 Russian-Georgian conflict, in which Russia employed the many criminal elements operating in South Ossetia to conduct the cleansing of ethnic Georgians from that region. Additionally, criminal organizations have the potential to provide much-needed funding to operations and facilitate the purchase of equipment. Adversaries will be enabled by WMD and technologies that allow them to be disruptive on a regional and area basis.

Swift tactical success is not essential to victory. The dimension of time favors those fighting the United States. An enemy need not win any engagement or battles; the enemy simply must not lose the war. Wearing down the popular support for U.S.

Hybrid Threats (Historical Perspective)

A hybrid threat is a combination of regular forces, irregular forces, and/or criminal elements unified to achieve mutually benefitting effects. Understanding hybrid threats involves identifying the attributes of this opposing force as well as the principle state and non-state actors within the umbrella of hybrid threat.

It is important to note that hybrid threats are not new. History is full of examples of how adversaries aligned with hybrid forces and used their relative strengths asymmetrically against the opponent's perceived weaknesses. Within the United States history, there are many examples:

- **French & Indian War**. In the mid-18th Century, British and French regular forces fought each other while using irregular colonialist militia and Native American Indians on both sides of the conflict.
- **The American Revolution**. In the late 18th Century, British and American regular forces fought each other while both sides again leveraged private militia, mercenaries, foreign militaries, and Native American Indians.
- **The Indian Wars**. Throughout the 19th Century, American regular forces backed by private militia fought against various tribes of Native American Indian irregular forces.
- **The Philippine Insurrection**. In the early 20th Century, American regular forces fought the regular and irregular forces of the Philippine Islands.
- **The Banana Wars**. In the years between the two world wars, American regular forces fought irregular forces in Central American nations.
- **The Vietnam War**. In the mid-20th Century, American and South Vietnamese regular forces fought against North Vietnamese regular forces, and irregular forces, including militia and foreign militaries.

The U.S. Armed Forces will face hybrid threats that simultaneously employ some combination of regular forces, irregular forces, and/or criminal elements. Hybrid threats will use an ever-changing variety of conventional and unconventional organizations, equipment, and tactics to create multiple dilemmas.

Swift tactical success is not essential to victory. The dimension of time favors those fighting the United States. An enemy need not win any engagement or battles; the enemy simply must not lose the war. Wearing down the popular support for U.S. operations by simply causing a political and military stalemate can be all that is required to claim victory or to change U.S. behavior or policy.

operations by simply causing a political and military stalemate can be all that is required to claim victory or to change U.S. behavior or policy.

The most challenging attribute of our adversaries will be their ability to adapt and transition. Their speed, agility, versatility, and changeability are the keys to success in a fight against a larger, more powerful opponent.

A. Hybrid Adaptation

Adaptation, broadly defined, is the ability to learn and adjust behaviors based on learning. Adaptation is closely linked to one's OE and its variables. Adversaries can approach adaptation from two perspectives: natural and directed.

Natural adaptation occurs as an actor (nation-state or non-state) acquires or refines its ability to apply its political, economic, military or informational power. Natural adaptation may be advanced through—

- Acquisition of technology, key capabilities, or resources (financial and material)
- Effective organization
- Effective use of the information environment or even key regional or global alliances

Directed adaptation refers to adaptation, based specifically on lessons learned, to counter U.S. power and influence. Counters to U.S. actions will be ever changing and likely conducted by a hybrid force. Hybrid threats will offer a mix of capabilities along the spectrum of conflict to counter U.S. military actions. Adversaries will learn from U.S. operations what works and what needs refinement. They will be whatever the U.S. force is not. Like natural adaptation, directed adaptation will inform issues of force design, military strategy, and operational designs.

Success goes to those who master the skills necessary to act, react, and adapt with speed and creativity. Enemies learn quickly and change, often unconstrained by rules or bureaucracy. While this may cause haphazard and incomplete change, it does allow a rapidity that is difficult to counter. Adversaries will continue to be adaptive in terms of using all available sources of power at their disposal.

B. Hybrid Transitions

One of the most dangerous aspects of a hybrid threat is the ability of its components to transition in and out of various forms. Military forces, for example, can remove uniforms and insignia and other indicators of status and blend in with the local population. Insurgent forces might abandon weapons and protest innocence of wrongdoing. Criminals might don the accoutrements of a local police force in order to gain access to a key facility.

Hybrid threats will use the difficulties of positive identification of threat actors as threat actors to their advantage. OEs will be replete with many actors conducting activities counter to U.S. interests but without a clear visual signature as to their status as threats. Indeed, often these actors will be providing signatures similar to friendly or neutral actors.

Time-honored concepts of "conventional" and "unconventional" war and "traditional" methods versus "adaptive" methods are weapons to a hybrid threat. These concepts do not have meaning to a hybrid threat beyond their ability to be used against its opponents. Hybrid threats see war holistically and do not try to break it up into convenient pieces.

Hybrid threat forces will need to perform certain functions in order for them to succeed. Some functions at some points will best be performed by uniformed military forces. At other times or for other reasons, some functions will be best performed by irregular forces. At some points, both types of forces will be acting together. At others, they will shift between the status of regular and irregular. They may also use deception to shift between combatant and noncombatant status. Hybrid threats will present themselves in many ways but always maintain the ability to aggregate at the time and place of their choosing.

Plane Hijackings, 1968 - 2001 (Historical Perspective)

There were 144 plane hijackings worldwide from 1968 through the end of the century. Terrorist organizations saw shock value in targeted violence against innocent civilians as a means of global communication of their cause, as well as pawns for negotiation. Over time the mere hijack of a commercial airline no longer seemed to have the same shock value. To obtain terror impact, violence increased in magnitude and audacity.

- **1968 – El Al Flight 426**: The plane was hijacked by three gunmen of the Popular Front for the Liberation of Palestine (PFLP). After 40 days, all passengers were released unharmed.
- **1970 – Dawson's Field:** Four planes were hijacked the same day by the PFLP. In spite of gunmen blowing up one of the planes, all passengers were released unharmed.
- **1976 – Air France Flight 139**: German revolutionaries and PFLP hijacked the plane and forced it to land at Entebbe Airport, Uganda. Israeli commandos raided the airport. Three hostages were killed, along with one commando and 45 Ugandan militants.
- **1977 – Malaysia Airlines Flight 653:** Unknown hijackers took over the plane and headed for Singapore, but the plane mysteriously crashed, killing all 100 people on board.
- **1985 – TWA Flight 847**: Islamic Jihad gunmen hijacked the plane in Athens and diverted to Beirut. Over a two-week standoff, a US Sailor was killed, but all other passengers were eventually released.
- **1985 – Egyptian Flight 648**: Three gunmen of Abu Nidal Organization (ANO) hijacked the plane in flight from Athens, and a security officer was killed in an exchange of gunfire. Damage to the plane forced a landing at Malta. Egyptian commandos stormed the plane and in the ensuing fight, 56 of the remaining 88 passengers were killed.
- **1986 – Pan Am Flight 73**: Four gunmen of ANO hijacked the plane on the ground in Pakistan, but the pilots escaped. The terrorists then executed an American when their demands for the pilots to return were unmet. Pakistani security forces stormed the plane, and another 19 passengers were killed. Flight attendant Neerja Bhanot helped passengers escape during the gun battle, and lost her life protecting three children.
- **1986 – Iraqi Airways Flight 163**: Four Hezbollah gunmen hijacked the plane enroute to Jordan. Security personnel on board attempted to kill the hijackers, but the gunmen detonated hand grenades in the cabin and cockpit. The plane crashed in Saudi Arabia, killing 63 of the 106 people on board.
- **1996 – Ethiopian Airlines Flight 961**: Three Ethiopian gunmen hijacked the plane and demanded political asylum in Australia. Without enough fuel to make the long trip, the plane crashed near the tourist beach off the Comoros Islands, killing 122 of the 172 people on board.
- **2001 – United Airlines Flights 93 and 175, plus American Airlines Flights 11 and 77**: Nineteen Al-Qaeda terrorists hijacked four planes with crude weapons, killing all 265 passengers and crew on board. Two planes struck the World Trade Center in New York; one plane struck the Pentagon near Washington, DC; the fourth crashed in a field in Pennsylvania. These attacks inflicted a total of 2,977 deaths and more than 6,000 injuries.

II. Irregular Threat

The irregular OPFOR can be part of the Hybrid Threat (HT). The HT can be any combination of two or more of the following components: regular military forces, irregular forces, and/or criminal elements. The irregular OPFOR component of the HT can be insurgents, guerrillas, or criminals or any combination thereof. The irregular OPFOR can also include other armed individuals or groups who are not members of a governing authority's domestic law enforcement organizations or other internal security forces. On occasion, situations may occur where unarmed individuals or groups may be part of the irregular OPFOR and the HT. An example of unarmed individuals aligned with the HT in an active support role is when segments of the population participate in public demonstrations against an enemy of the HT. Possible HT combinations include parts of the irregular OPFOR operating openly with regular military forces, being sponsored directly or indirectly by a state's government, or being supported by non-state organizations.

The irregular OPFOR can be part of the HT, but can also operate independently without any allegiance to or collaboration with other types of forces associated with the HT. Various state and non-state organizations, regular military forces, paramilitary forces, and/or criminal organizations might be operating in the same space and time as the irregular OPFOR but not be part of the irregular OPFOR or the HT. To be a hybrid threat, all these components would have to be "unified to achieve mutually benefitting effects" (ADRP 3-0 and TC 7-100).

A. Capabilities and Intent

The irregular OPFOR is adaptive, flexible, and agile. It can quickly change its composition to optimize organizational capabilities and use those capabilities against known or perceived vulnerabilities of an enemy. The irregular OPFOR takes prudent risks when an expectation exists for successful attack on an enemy. However, it may also make significant practical sacrifices in individuals and materiel in order to achieve a major psychological impact on an enemy. An example of such deliberate sacrifice is a number of nearly simultaneous, small unit or direct action cell assaults on targets that result in the deaths of all attackers, but receive sensational media coverage to a global audience.

The intent of the irregular OPFOR is to acquire a range of capabilities and use them at selected times and locations in order to achieve desired effects. It can use those capabilities against an enemy. However, the irregular OPFOR can also use functional tactics and/or terrorism to manipulate a population and dissuade support to an enemy's military forces and/or other institutions. When necessary, it will use acts of violence to gain influence and develop willing or coerced cooperation. Concurrently, it will use indirect means to progressively degrade an enemy's physical power and infrastructure, and to psychologically influence the political, social, economic, military, and information variables of an OE. The irregular OPFOR will attempt to exploit its familiarity with the physical environment and its ability to blend into the local populace. The time variable normally favors the irregular OPFOR. The activities of the irregular OPFOR are constant over a long period of time, but may change in pace, tempo, and speed. The timing of actions will sometimes appear random when the actual mode of the irregular OPFOR and its activities are deliberate decisions as part of a long-term campaign or strategy.

One of the most significant capabilities of the irregular OPFOR is the ability to manipulate and/or ignore the restrictions and sanctions that apply to regulated military forces, law enforcement agencies, and internal security forces belonging to a sovereign state. International protocols and conventions, national statutes and law, and moral codes that guide behavioral norms and social interactions can limit the enemy's use of weapon systems and other capabilities that overmatch irregular OPFOR capabilities. The irregular OPFOR can make exceptions by complying with these codes of conduct when that is advantageous for its information warfare campaign. However, it can easily abandon those standards when they no longer provide operational value. When regular military forces of a state incorporate clandestine use of the irregular OPFOR, the state can often plausibly deny responsibility for actions conducted by irregular forces.

Although violent actions by any individual organization or combination intend to receive immediate notoriety, the irregular OPFOR complements violent actions with methodical, long-term psychological warfare. The overarching agenda of the irregular OPFOR can include but is not limited to the following issues:

- Expand support and/or control within an area or region.
- Deter opposition to its objectives within a relevant population.
- Obtain popular recognition and support of its objectives by designated segments of a population.
- Marginalize the governance and/or extraregional influence of an adversary.
- Attract an international or global audience and/or external sources of influence to support irregular OPFOR aims.

The irregular OPFOR seeks to gain the approval and support of at least certain elements of a relevant population in order to obtain active or passive assistance. The methods by which it acquires such influence are complex in any OE. Normally, it must communicate a compelling narrative of legitimacy that is accepted by the population. This credential of legitimacy may require a gradual process of convincing the relevant population that the irregular OPFOR is an acceptable means to achieve desired social, religious, or political effects. However, the irregular OPFOR may confer authority on itself without regard to the population's goals.

An enemy of the irregular OPFOR may maintain that the OPFOR concept of legitimacy is corrupt and illicit. The irregular OPFOR may declare that its actions are justifiable under existing conditions, and attempt to degrade the legitimacy of a governing authority. Over time, the irregular OPFOR seeks to obtain recognition of its legitimacy by a willing populace and official recognition from external states and/or organizations in order to accomplish its long-term goals. Once its authority is recognized, the irregular OPFOR seeks to maintain the legitimacy of its cause, its leadership role, and its actions.

Sometimes external recognition and support is not as important to the irregular OPFOR as is establishing a geographic enclave from which to plan, prepare, and conduct its activities and influence. The irregular OPFOR conducts direct and indirect actions that are adaptive and persistent. This form of conflict incorporates irregular forces typically categorized as insurgents or guerrillas, and includes selective actions coordinated with criminal organizations. Particular actions can be purposely conducted as acts of terrorism, or can employ more military-like tactics. All of these actions are described in terms of the common functional framework described in the 7-100 series of FMs and TCs.

B. Complexity and Collaboration

The irregular OPFOR may be part of a complex array of irregular and regular OPFOR organizations, units, or individuals with various coordinated and/or disparate single-agenda aims. A particular geographic, political, cyberspace, or ideological environment may lead to alliances or affiliations that are dynamic and constantly changing. Discrete incidents may not seem to be part of an overall plan. However, detailed analysis of the irregular OPFOR actions and associated political, social, economic, information, and other events normally reveals a vision supporting a long-range aim.

In particular conditions and circumstances, irregular OPFOR actions can include support from regular military forces and/or special-purpose forces (SPF) from a state or states. Internal security forces and/or law enforcement organizations that have been infiltrated by the irregular OPFOR can also support irregular OPFOR actions within an area or region. The collaboration among organizations, units, and/or individuals of a relevant population may be based on coercion, contractual agreement, and/or temporary or long-term common goals and objectives.

Possible rationales for irregular OPFOR collaboration with other organizations or individuals in an OE can include—

- Spotlight grievances for resolution.
- Establish influence over a relevant segment of a population.
- Develop acceptance and legitimacy of irregular OPFOR programs and actions.
- Achieve OPFOR objectives without alienating critical segments of indigenous and/or extraregional populations.
- Cultivate active or passive supporters.

Irregular OPFOR objectives may promote solutions to grievances in the context of a particular population. The irregular OPFOR may prefer to use indirect approaches such as subterfuge, deception, and nonlethal action to achieve its objectives. However, it is committed to violent action, when necessary, in order to compel an enemy and/or an opposing form of governance to submit to its intentions. Some irregular OPFOR organizations such as affiliated criminal gangs exist for their own commercial profit and power, and are not interested in the quality of life and/or civil security of a relevant population that they influence or coerce. Other forms of the irregular OPFOR can be rogue individuals with single-issue agendas who are willing to use criminal activity and/or terrorism in order to achieve their objective.

C. Adaptability

The irregular OPFOR is constantly adapting its capabilities in an agile and flexible manner to achieve its objectives. These capabilities include improvements in organization, equipment, and tactics. The irregular OPFOR can readily task-organize for a particular action. It tailors actions to support a compelling agenda that resonates with a relevant population for active and/or passive support. It makes adjustments when it gains or loses affiliated support or experiences degradation due to recent actions.

Irregular OPFOR actions are conducted as a continuum. Any pause in its operations is part of a coherent campaign of persistent conflict. A long-term perspective guides near- and mid-term actions to marshal capabilities for future actions. While one form of action may appear stalled, another form of action is likely underway against an enemy weakness. Protracted actions can change quickly if the irregular OPFOR observes unexpected enemy vulnerabilities.

The irregular OPFOR's ability to quickly transition also gives it the agility and flexibility to—

- Command, control, and/or influence various activities.
- Task-organize its forces.
- Deceive and surprise.
- Disperse and concentrate.
- Retain freedom of movement.
- Apply physical and psychological techniques in order to create anxiety in an enemy.

This agility and flexibility is critical to how effectively the irregular OPFOR adapts its patterns of operations to maintain the initiative over an enemy. The irregular OPFOR perseveres in adversity by its ability to adapt.

II. Irregular & Hybrid Threat Components

Ref: TC 7-100, Hybrid Threat (Nov '10), chap. 2.

Through formal structure and informal agreement, military and state paramilitary forces can work in concert to varying degrees with insurgent, guerrilla, and criminal groups towards common ends. Typically, the common goal is the removal of U.S. and coalition forces from their area of operations. The goals of hybrid threat forces may or may not coincide with those of other actors in the same geographic area.

Hybrid Threat Components

I

Threats and Other Actors

A. Nation-State Actors
B. Non-State Actors
C. Regular Military Forces
D. Irregular Forces

II

Enemy Combatants

A. Combatants

- **Enemy Combatant**
- **Lawful Enemy Combatant**
- **Unlawful Enemy Combatant**

B. Paramilitary Forces *(Irregular Forces)*

- **Paramilitary**
- **Insurgent**
- **Guerrilla**
- **Terrorist**
- **Mercenary**
- **Criminal Organizations**

*****

Weapons of Mass Destruction (WMD)

Ref: TC 7-100, Hybrid Threat (Nov '10), chap. 2.

II. Enemy Combatants & Paramilitary Forces

Ref: TC 7-100, Hybrid Threat (Nov '10), pp. 2-3 to 2-7.

A. Combatants

The DOD defines an enemy combatant as "in general, a person engaged in hostilities against the United States or its coalition partners during an armed conflict" (JP 1-02 from DODD 2311.01E). Other essential terms are lawful enemy combatant and unlawful enemy combatant.

Enemy Combatant

In general, a person engaged in hostilities against the United States or its coalition partners during an armed conflict. The term enemy combatant includes both "lawful enemy combatants" and "unlawful enemy combatants." (DODD 2310.01E)

Lawful Enemy Combatant

Lawful enemy combatants, who are entitled to protections under the Geneva Conventions, include members of the regular armed forces of a State party to the conflict; militia, volunteer corps, and organized resistance movements belonging to a State party to the conflict, which are under responsible command, wear a fixed distinctive sign recognizable at a distance, carry their arms openly, and abide by the laws of war; and members of regular armed forces who profess allegiance to a government or an authority not recognized by the detaining power. (DODD 2310.01E)

Unlawful Enemy Combatant

Unlawful enemy combatants are persons not entitled to combat immunity, who engage in acts against the United States or its coalition partners in violation of the laws and customs of war during an armed conflict. … [The] term unlawful enemy combatant is defined to include, but is not limited to, an individual who is or was part of or supporting … forces that are engaged in hostilities against the United States or its coalition partners. (DODD 2310.01E)

B. Paramilitary

Combatants can be casually and incorrectly categorized without appropriate attention to what a particular term defines as the purpose, intent, or character of an enemy combatant. Several terms that can easily be misused include paramilitary forces, insurgents, guerrillas, terrorists, militia, and mercenaries. The discussion below provides DOD definitions of the first four terms.

Paramilitary

Paramilitary forces are "forces or groups distinct from the regular armed forces of any country, but resembling them in organization, equipment, training, or mission" (JP 3-24). Thus, there are various types of non-state paramilitary forces, such as insurgents, guerrillas, terrorist groups, and mercenaries. However, there are also nation-state paramilitary forces such as internal security forces, border guards, and police, which are specifically not a part of the regular armed forces of the country.

Note. The term militia has acquired many definitions based on the situational context. This context may be the culture; historical traditions such as which group of people have familial, social, theological, or political power; and the external or self-descriptions such forces use in media affairs or propaganda. A generic definition of a militia can parallel the definition of a paramilitary force. However, a nation-state can also have militia that are considered an extension of its armed forces.

Insurgent *(See chap. 2.)*

An insurgency is “the organized use of subversion and violence by a group or movement that seeks to overthrow or force change of a governing authority” (JP 3-24). Insurgent organizations have no regular table of organization and equipment structure. The mission, environment, geographic factors, and many other variables determine the configuration and composition of each insurgent organization and its subordinate cells. A higher insurgent organization can include organizations at regional, provincial, district, national, or transnational levels. Higher insurgent organizations can contain a mix of local insurgent and guerrilla organizations. Each of these organizations provides differing capabilities.

Guerrilla *(See chap. 3.)*

A guerrilla is “a combat participant in guerrilla warfare” (JP 1-02). Guerrilla warfare is “military and paramilitary operations conducted in enemy-held or hostile territory by irregular, predominantly indigenous forces” (JP 3-05.1). A prime characteristic of guerrilla operations is to attack points of enemy weakness and in conditions developed or selected by the guerrilla force. Deception and mobility are critical to achieving surprise and avoiding engagements unless the tactical opportunity weighs heavily in the favor of the guerrilla. At the tactical level, attacks are planned and conducted as sudden, violent, decentralized actions. Principles of rapid dispersion and rapid concentration facilitate these types of operation.

Terrorist *(See chap. 4.)*

A terrorist is “an individual who commits an act or acts of violence or threatens violence in pursuit of political, religious, or ideological objectives” (JP 3-07.2). A terrorist group is “any number of terrorists who assemble together, have a unifying relationship, or are organized for the purpose of committing an act or acts of violence or threatens violence in pursuit of their political, religious, or ideological objectives” (JP 3-07.2). Categorizing terrorist groups by their affiliation with governments or supporting organizations can provide insight in terrorist intent and capability. Terrorist groups can align as state-directed, state-sponsored, or non-state supported organizations. In some cases, the state itself can be a terrorist regime.

Mercenary

Mercenaries are armed individuals who use conflict as a professional trade and service for private gain. Those who fall within that definition are not considered combatants. However, those who take direct part in hostilities can be considered unlawful enemy combatants. The term mercenary applies to those acting individually and in formed units. Soldiers serving officially in foreign armed forces are not mercenaries. Loan service personnel sent to help train the soldiers of other countries as part of an official training agreement between sovereign governments are not mercenaries even if they take a direct part in hostilities.

Criminal Organizations *(See chap. 5.)*

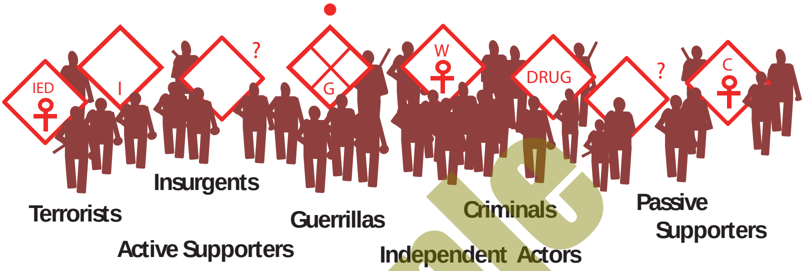
There is no part of the world that is criminal-free. Therefore, there will always be criminal elements present in any OE. The only question is whether those criminal organizations will find it in their interests to become part of a hybrid threat and to perform some of the functions required to achieve common goals and objectives.

Criminal organizations are normally independent of nation-state control. However, large-scale criminal organizations often extend beyond national boundaries to operate regionally or worldwide and include a political influence component. Individual criminals or small gangs do not normally have the capability to adversely affect legitimate political, military, and judicial organizations. However, large-scale criminal organizations can challenge governmental authority with capabilities and characteristics similar to a paramilitary force.

III. Irregular Forces

Irregular forces are armed individuals or groups who are not members of the regular armed forces, police, or other internal security forces (JP 3-24). The distinction of being armed as an individual or group can include a wide range of people who can be categorized correctly or incorrectly as irregular forces. Excluding members of regular armed forces, police, or internal security forces from being considered irregular forces may appear to add some clarity. However, such exclusion is inappropriate when a soldier of a regular armed force, policeman, or internal security force member is concurrently operating in support of insurgent, guerrilla, or criminal activities.

Irregular forces can be insurgent, guerrilla, or criminal organizations or any combination thereof. Any of those forces can be affiliated with mercenaries, corrupt governing authority officials, compromised commercial and public entities, active or covert supporters, and willing or coerced members of a populace. Independent actors can also act on agendas separate from those of irregular forces.



Ref: TC 7-100.3 (Jan '14), fig. I-1. Irregular force actors.

Closely related to the subject of irregular forces is irregular warfare. JP 1 defines irregular warfare as "a violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s). Irregular warfare favors indirect and asymmetric approaches, though it may employ the full range of military and other capacities, in order to erode an adversary's power, influence, and will." The definition spotlights a dilemma of conflict in and among a population. It also indicates that the non-state actors characterized as irregular forces may operate in other than military or even military-like (paramilitary) capacities.

Blurring of Categories

Although three basic types of forces can be part of the irregular OPFOR, the distinctions among insurgents, guerrillas, and criminals are sometimes blurred. That is because they may have more in common than they have that is different. From the viewpoint of the existing government authority, for instance, the activities of all three types are illegal, that is, criminal. Not just criminals but also insurgents and guerrillas can engage in criminal activities. Some insurgent organizations can include guerrilla units (developed from within or affiliated) and some guerrilla units may be part of an insurgency. In advanced phases of an insurgency, guerrilla units may begin to look and act more like regular military units.

There are three general tactics available to the irregular OPFOR—

- Military-like functional tactics.
- Criminal activity.
- Terrorism.

At any given time, the irregular OPFOR could use any of these means. The differences among these three can become blurred.

See following pages (pp. 1-16 to 1-18) for a comparison & contrast of insurgent, guerrilla, and criminal organizations.

Comparison & Contrast of Insurgents, Guerrillas, and Criminals

Ref: TC 7-100.3, Irregular Opposing Forces (Jan '14), table pp. 1-16 to 1-18.

Within the irregular OPFOR, guerrilla units, insurgent organizations, and criminal organizations have various capabilities and limitations. Table 1-1 compares and contrasts the basic three types of forces in order to highlight their similarities and their differences.

Characteristic	Insurgent Organization	Guerrilla Unit	Criminal Organization
Leadership	Network is typical, but can include hierarchical sub-organizations; leaders may be located distant from the geographic area of conflict; political or ideological mentors or council advisors and/or counsel senior leaders. Title for personnel in command is usually "leader." Some leaders may use a religious, historical, or honorific title.	Hierarchical with military-like chain of command and control or support systems; leaders predominantly indigenous; political advisors may accompany guerrilla units in actions. Leader titles are military in nature such as battalion and/or company commander, platoon leader, section leader, team leader, hunter-killer group leader.	Hierarchical structure or network dependent on origin of organization; even in small criminal organizations, leaders may be located distant from the geographic area of conflict; political or ideological mentors or council advise and/or counsel senior leaders. Leader titles can be traditional or historical terms, or simple authority terms.
Motivation	Insurgency movement with a political and/or ideological agenda. Can also be social identity or religion.	Social identity, religion, or politics. Can be military component to an insurgency; or can be independent of an insurgency with a specified agenda.	Intention to profit fiscally through control of a process, commodity, and/or area; social identity as a power broker in a designated geographic, economic, or social environment.
Organization	Cellular-network model; can be hierarchical for designated capabilities or functions; can include paramilitary capability for a primarily political-oriented organization; can be affiliated with other irregular OPFOR and/or regular military forces.	Military unit model with echelons of command and control; can include land, sea, and air capabilities; can be affiliated with other irregular OPFOR and/or regular military forces; more likely that other irregular OPFOR components to be closely integrated with regular military forces.	Hierarchical structure or network dependent on origin of organization; general categories of gangs, large-scale syndicates, and transnational organizations; organizations can be based on family, ethnic, commodity, or specialized purpose. Can infiltrate or become affiliated with insurgent, guerrilla, or regular military forces.
Objectives	Concessions from and/or defeat of a political opponent; ultimately, overthrow an enemy governing authority and replace governance with insurgent movement leadership; seek legitimacy as movement.	Military mission success within a campaign in support of unit goals and desired end state; can be an independent and specified guerrilla unit agenda; can be the military capability in insurgent organization.	Profit from activities and coercion; expand organizational influence within an area, regional, or transnational scope; preserve control of specified commodities, geographic areas, and/or services; avoid contact with governing authority.
Internal Support	Active and passive support in local and larger area population; can have legitimate social-economic-political activities to mobilize civil support.	Active and passive support by segments of a local area population for military-type capabilities; can expand support to regional area population.	Active and passive support in local and larger area population; can use coercion to influence legitimate social-economic-political activities or individual support.
External Support	Regional safe havens; Diaspora systems to promote insurgent movement in regional and/or international communities; can receive cooperation or assistance from regular forces, SPF, or state activities opposing the governing authority.	Regional safe havens; can receive cooperation or assistance from regular military, SPF, or state activities opposing the governing authority in the area of guerrilla operations.	Cooperative affiliations among gangs, large-scale syndicates, and/or transnational organizations can provide designated support and services; co-opted governing authority offices may also assist.
Activity Patterns	Local, regional, provincial, and/or district activities with intention of obtaining support of relevant population; can be social, economic, diplomatic, political, and military activities.	Military-like functional tactics as norm; can expand tactical actions into a military campaign focused in a geographic area.	Local, regional, and/or transnational activities; random or systematic activity to sustain influence; specialized expertise can be part of functional business model of larger commercial enterprises.

III. Hybrid Threat Organizations

Ref: TC 7-100, Hybrid Threat (Nov '10), chap. 6.

The Hybrid Threat (HT) tailors its organizations to the required missions and functions. It determines the functions that must be performed in order to successfully accomplish its goals. Then it builds teams and organizations to execute those functions without regard to traditional military hierarchy, the law of war, or rules of engagement.

Hybrid Threat Organizations

I **Military Organizations**

II **Insurgent Organizations**

III **Guerrilla Organizations**

IV **Criminal Organizations**

***** **Hybrid Relationships**

Ref: TC 7-100, Hybrid Threat (Nov '10), chap. 6.

Task-Organizing

The HT will task-organize forces in a fashion that matches its available resources to its goals. Task organizations will often include more than purely military formations. The HT's regular military and irregular components are tailored forces depending on training requirements. FM 7-100.4 provides a baseline of organizational size, equipment, and weapons. Its organizational directories provide a very detailed listing of personnel and equipment. For some training requirements, the opposing force (OPFOR) order of battle (OB) might not need to include personnel numbers. Trainers and exercise planners can extract the appropriate pages from the organizational directories and tailor them by eliminating the detail they do not need and adding the necessary units from other pages to develop the required task organization.

For more detail on organizations, refer to FM 7-100.4, which introduces baseline organizational structures of a flexible, thinking, and adaptive OPFOR.

The baseline organizations presented in the organizational directories of FM 7-100.4 are intended to be tailored and task-organized in a manner that is appropriate for the training objectives. Depending on the training requirement, the OPFOR may be a

A. Elements of INFOWAR (IO*)

Ref: TC 7-100, Hybrid Threat (Nov '10), p. 3-6.

*Editor's note: At the time of release (Nov '10), TC 7-100 used the term "INFOWAR" which is outdated. The current correct doctrinal term in use is "Information Operations (IO). **Information Operations (IO)** is the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own (JP 3-13). See facing page for further discussion in U.S. doctrine.*

Electronic Warfare (EW)

Measures conducted to control or deny the enemy's use of the electromagnetic spectrum, while ensuring its use by the HT.

Deception

Measures designed to mislead the enemy by manipulation, distortion, or falsification of information to induce him to act in a manner prejudicial to his interests.

Physical Destruction

Measures to destroy critical components of the enemy's information infrastructure.

Protection and Security Measures

Measures to protect the HT's information infrastructure and to deny protected information to other actors.

Perception Management

Measures aimed at creating a perception of truth that best suits HT objectives. Perception management uses a combination of true, false, and misleading information targeted at the local populace and/or external actors. This element is crucial to successful strategic INFOWAR. The HT is continuously looking for ways to sway international opinion in its favor or impact critical foreign strategic decisionmakers.

Information Attack (IA)

Measures focused on the intentional disruption of digital information in a manner that supports a comprehensive strategic INFOWAR campaign. IAs focus exclusively on the manipulation or degradation of the information moving throughout the information environment. Unlike computer warfare attacks that target the information systems, IAs target the information itself.

Computer Warfare

Measures ranging from unauthorized access (hacking) of information systems for intelligence collection purposes to the insertion of destructive viruses and deceptive information into enemy computer systems. Such attacks focus on the denial of service and/or disruption or manipulation of the infrastructure's integrity. Strategic INFOWAR typically targets critical nodes or hubs, rather than targeting the entire network or infrastructure.

The seven elements of INFOWAR (information operations) do not exist in isolation from one another and are not mutually exclusive. The overlapping of functions, means, and targets makes it necessary that they all be integrated into a single INFOWAR plan. However, effective execution of strategic INFOWAR does not necessary involve the use of all elements concurrently. In some cases, one element may be all that is required to successfully execute a strategic INFOWAR action or a supporting action at the operational or tactical level. The use of each element or a combination of elements is determined by the overall situation and specific strategic goals.*

Information Operations (IO)

Ref: JP 3-0, Joint Operations, w/Chg 1 (Oct ‘18), pp. III-17 to III-22.

All military activities produce **information**. Informational aspects are the features and details of military activities observers interpret and use to assign meaning and gain understanding. Those aspects affect the perceptions and attitudes that drive behavior and decision making. The JFC leverages informational aspects of military activities to gain an advantage; failing to leverage those aspects may cede this advantage to others. Leveraging the informational aspects of military activities ultimately affects strategic outcomes.

The **information function** encompasses the management and application of information and its deliberate integration with other joint functions to change or maintain perceptions, attitudes, and other elements that drive desired behaviors and to support human and automated decision making.

The **instruments of national power** (diplomatic, informational, military, and economic) provide leaders in the US with the means and ways of dealing with crises around the world. Employing these means in the information environment requires the ability to securely transmit, receive, store, and process information in near real time. The nation’s state and non-state adversaries are equally aware of the significance of this new technology, and will use information-related capabilities (IRCs) to gain advantages in the information environment, just as they would use more traditional military technologies to gain advantages in other operational environments. As the strategic environment continues to change, so does information operations (IO).

Regardless of its mission, the joint force considers the likely impact of all operations on **relevant actor** perceptions, attitudes, and other drivers of behavior. The JFC then plans and conducts every operation in ways that **create desired effects** that include maintaining or inducing relevant actor behaviors. These ways may include the timing, duration, scope, scale, and even visibility of an operation; the deliberately planned presence, posture, or profile of assigned or attached forces in an area; the use of signature management in deception operations; the conduct of activities and operations to similarly impact behavioral drivers; and the **employment of specialized capabilities** -- e.g., key-leader engagements (KLE), cyberspace operations (CO), military information support operations (MISO), electronic warfare (EW), and civil affairs (CA) -- to reinforce the JFC’s efforts.

Inform activities involve the release of accurate information to domestic and international audiences to put joint operations in context; facilitate informed perceptions about military operations; and counter adversarial misinformation, disinformation, and propaganda. Inform activities help to assure the trust and confidence of the US population, allies, and partners and to deter and dissuade adversaries and enemies.

The joint force **attacks and exploits information, information networks, and systems** to affect the ability of relevant actors to leverage information in support of their own objectives. This includes the manipulation, modification, or destruction of information or disruption of the flow of information for the purpose of gaining a position of military advantage. This also includes targeting the credibility of information.

Refer to INFO1: The Information Operations & Capabilities SMARTbook (Guide to Information Operations & the IRCs). INFO1 chapters and topics include information operations (IO defined and described), information in joint operations (joint IO), information-related capabilities (PA, CA, MILDEC, MISO, OPSEC, CO, EW, Space, STO), information planning (information environment analysis, IPB, MDMP, JPP), information preparation, information execution (IO working group, IO weighted efforts and enabling activities, intel support), fires & targeting, and information assessment.

B. The Strategic Dimension

Because of its significance to the overall achievement of the HT's strategy, INFOWAR at the strategic level receives special attention. Strategic INFOWAR is the synergistic effort of the HT to control or manipulate information events, be they diplomatic, political, economic, or military in nature. Specifically, the HT defines strategic INFOWAR as any attack (digital, physical, or cognitive) against the information base of an adversary nation's critical infrastructures.

The ultimate goal of strategic INFOWAR is strategic disruption and damage to the overall strength of an opponent. This disruption also focuses on the shaping of foreign decisionmakers' actions to support the HT's strategic objectives and goals. Perception management activities are critical to strategic INFOWAR. The HT attempts to use all forms of persuasion and global media to win the "battle of the story."

Strategic INFOWAR can undermine an extraregional power's traditional advantage of geographic sanctuary from strategic attack. Strategic INFOWAR is not confined to a simple zone of territory, but can extend globally to encompass attacks on an opponent's homeland or the homelands of various military coalition members.

In addition to using all its own assets, the HT will seek third-party actors or outside resources to support its overall information strategy. The HT facilitates these shadow networks as necessary and continuously cultivates and maintains them during peacetime.

III. Strategic Preclusion

Strategic preclusion seeks to completely deter extraregional involvement or severely limit its scope and intensity. The HT would attempt to achieve strategic preclusion in order to reduce the influence of the extraregional power or to improve its own regional or international standing. It would employ all its instruments of power to preclude direct involvement by the extraregional power. Actions can take many forms and often contain several lines of operation working simultaneously.

The primary target of strategic preclusion is the extraregional power's national will. First, the HT would conduct diplomatic-political and perception management activities aimed at influencing regional, transnational, and world opinion. For example, the HT might use a disinformation campaign to discredit the legitimacy of diplomatic or economic sanctions imposed upon it. The extraregional power's economy and military would be secondary targets, with both practical and symbolic goals. This might include using global markets and international financial systems to disrupt the economy of the extraregional power, or conducting physical and information attacks against critical economic centers. Similarly, the military could be attacked indirectly by disrupting its power projection, mobilization, and training capacity. Preclusive actions are likely to increase in intensity and scope as the extraregional power moves closer to military action. If strategic preclusion fails, the HT will turn to operational methods that attempt to limit the scope of extraregional involvement or cause it to terminate quickly.

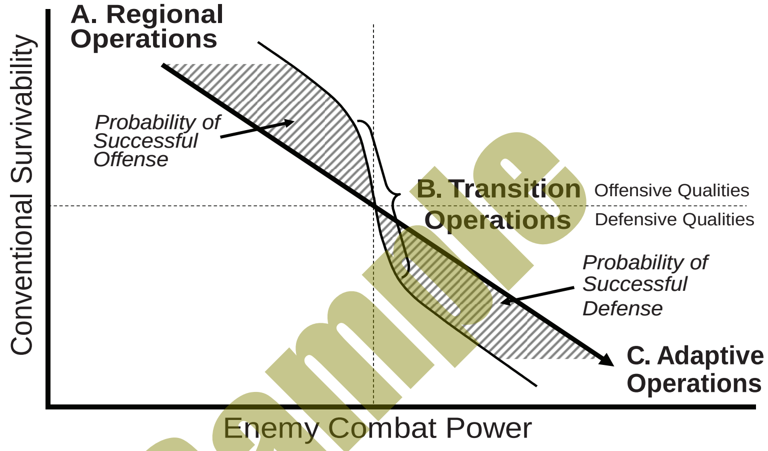
V. Irregular & Hybrid Threat Operations

Ref: TC 7-100, Hybrid Threat (Nov '10), chap. 4.

I. Operational Designs

The HT employs three basic operational designs:

Operational Designs



A **Regional Operations**

B **Transition Operations**

C **Adaptive Operations**

Ref: TC 7-100, Hybrid Threat (Nov '10), fig. 3-1. Strategic operations and other courses of action.

Each of these operational designs is the aggregation of the effects of tactical, operational, and strategic actions, in conjunction with the other three instruments of power, that contribute to the accomplishment of strategic goals. The type(s) of operations the HT employs at a given time will depend on the types of threats and opportunities present and other conditions in the operational environment (OE). Figure 4-1 above illustrates the HT's basic conceptual framework for the three operational designs.

A. Regional Operations

Against opponents from within its region, the HT may conduct "regional operations" with a relatively high probability of success in primarily offensive actions. HT offensive operations are characterized by using all available HT components to saturate the OE with actions designed to disaggregate an opponent's capability, capacity, and will to resist. These actions will not be limited to attacks on military and security forces, but will affect the entire OE. The opponent will be in a fight for survival across many of the variables of the OE: political, military, economic, social, information, and infrastructure.

HT offensive operations seek to—

- Destabilize control
- Channel actions of populations
- Degrade key infrastructure
- Restrict freedom of maneuver
- Collapse economic relationships
- Retain initiative

These operations paralyze those elements of power the opponent possesses that might interfere with the HT's goals.

The HT may constantly shift which components and sets of components act to affect each variable. For example, regular forces may attack economic targets while criminal elements simultaneously act against an enemy military base or unit in one action, and then in the next action their roles may be reversed. In another example, information warfare (INFOWAR) assets may attack a national news broadcast one day, a military command and control (C2) network the next day, and a religious gathering a day later. In addition to military, economic, and information aspects of the OE, HT operations may include covert and overt political movements to discredit incumbent governments and serve as a catalyst to influence popular opinion for change. The synergy of these actions creates challenges for opponents of the HT in that it is difficult to pinpoint and isolate specific challenges.

The HT may possess an overmatch in some or all elements of power against regional opponents. It is able to employ that power in an operational design focused on offensive action. A weaker regional neighbor may not actually represent a threat, but rather an opportunity that the HT can exploit. To seize territory or otherwise expand its influence in the region, the HT must destroy a regional enemy's will and capability to continue the fight. It will attempt to achieve strategic decision or achieve specific regional goals as rapidly as possible, in order to preclude regional alliances or outside intervention.

During regional operations, the HT relies on its continuing strategic operations to preclude or control outside intervention. It tries to keep foreign perceptions of its actions during a regional conflict below the threshold that will invite in extraregional forces. The HT wants to achieve its objectives in the regional conflict, but has to be careful how it does so. It works to prevent development of international consensus for intervention and to create doubt among possible participants. Still, at the very outset of regional operations, it lays plans and positions forces to conduct access-limitation operations in the event of outside intervention.

B. Transition Operations

Transition operations serve as a pivotal point between regional and adaptive operations. The transition may go in either direction. The fact that the HT begins transition operations does not necessarily mean that it must complete the transition from regional to adaptive operations (or vice versa). As conditions allow or dictate, the

Principles

Ref: TC 7-100.3, Irregular Opposing Forces (Jan '14), pp. 1-7 to 1-10.

Initiative

Initiative is the ability of the irregular OPFOR to retain a freedom of action in its plans and operations. Initiative enables the irregular OPFOR to force an enemy to react to its actions. Success often goes to the side that conducts itself more actively and resolutely. Irregular OPFOR leaders encourage initiative to make and implement bold decisions in order to establish or change the terms of the irregular conflict in favor of the irregular OPFOR. Subordinates are expected to take advantage of new developments immediately. They seek to overcome a position of relative inferiority while operating within a senior OPFOR leader's intentions. Initiative exploits an enemy's restrictive rules of engagement or political restrictions.

Deception

Deception is the ability to deliberately convey a false and/or distorted picture of the situation to an enemy leader that is targeted for deception. Deceptive information causes an enemy leader to believe he has accurate situational awareness and understanding. Irregular OPFOR leaders plan and direct deception that helps them accomplish their objective, but does not hamper other concurrent OPFOR actions. Feints and demonstrations are examples of deception. Other elements of INFOWAR attempt to optimize the effects of deception in tactics and techniques. Various irregular OPFOR capabilities and actions can lead to a compelling yet inaccurate analysis by the enemy leader.

Surprise

Surprise is the ability of the irregular OPFOR to take advantage of an enemy vulnerability in a manner for which an enemy is unprepared or unable to effectively counter. Irregular OPFOR action is normally swift and fleeting and may employ unexpected means. The irregular OPFOR attempts to shape a setting so that an enemy is not expecting the action or create conditions that an enemy is not prepared to confront. The irregular OPFOR achieves surprise through deception activities in conjunction with protection and security measures and/or other elements of INFOWAR. Surprise can be achieved by means such as the following:

- Changing tactics, techniques, or the intensity of actions against an enemy.
- Employing commercial or industrial materiel as a weapon in unexpected ways.
- Presenting public indications of compromise or cessation of armed conflict.

Protection

Protection is the ability to preserve irregular OPFOR effectiveness of its organizational assets and capabilities. These assets and capabilities include OPFOR personnel, equipment, weapon systems, operations, information, facilities, and/or infrastructure. Protection involves a continuous, integrated series and/or group of measures that sustain the ability for the irregular OPFOR to plan, prepare, and conduct successful actions. Protection and security measures are a key element in INFOWAR (see appendix A). The irregular OPFOR normally operates with a minimal or unidentifiable signature within a relevant population in order to avoid being a lucrative target. Protection complements the use of a safe haven, when required, to refit or reconstitute irregular OPFOR combat power. An example of protection is an irregular OPFOR guerrilla unit exfiltrating from a raid in hostile territory to a secure location in a neighboring state. This unofficial support by a state near the area of OPFOR actions provides security and protection to the guerrilla unit while it recruits and trains replacements due to casualties incurred in the raid.

Mobility

Mobility is the ability to sustain irregular OPFOR freedom of movement within areas controlled or occupied by the enemy. The irregular OPFOR seeks to create an advantage over the enemy regarding knowledge and use of geographic terrain and populations in order to position, reposition, and/or prepare for and conduct effective actions. A high degree of mobility enables the irregular OPFOR to use available combat power with maximum effect at a decisive time and place. For example, the irregular OPFOR can blend into a population with similar clothing and daily habits in order to maintain anonymity while transiting an area or region. This type of mobility can allow the timely supply of weapons and materiel, fiscal resources, and/or manpower for designated actions in an area or region.

Adaptability

Adaptability is the ability of the irregular OPFOR to use initiative and creative thinking in order to set particular conditions and take advantage of the resulting opportunities. Irregular OPFOR leaders recognize emergent developments that change existing conditions, and apply initiative that causes the enemy to react at a disadvantage to the actions of the irregular OPFOR. Simple tactics and techniques can be adapted for use against an enemy's sophisticated technology and weapon systems. For example, a system of couriers can negate the intrusive ability of electronic monitoring devices to detect and locate the financial transaction networks of a local insurgent organization that were formerly conducted with cellular telephones. Conversely, the irregular OPFOR can adapt to sophisticated techniques such as encrypting and hiding information within harmless appearing communiqués such as electronic files, images, and documents transiting the Internet.

Concentration

Concentration is the ability of the irregular OPFOR to mass the capabilities of combat power in time and space, in order to achieve a desired effect. Concentration of effort allows the irregular OPFOR to create and dominate a condition for a specific amount of time. When the irregular OPFOR concentrates rapidly or gradually from dispersed locations to conduct a particular action, a normal subsequent action is to quickly disperse in order to avoid an effective enemy response against the massed OPFOR. An example of concentration is the coordination to quickly mass irregular OPFOR insurgent cells, and use a swarming technique in a raid to overwhelm a designated target at an isolated combat outpost. Once insurgents have seized the objective and secured or destroyed designated weapons, equipment, and documents, the cells quickly disperse into the countryside or urban areas in order to avoid capture or death.

Perseverance

Perseverance demonstrates the will of the irregular OPFOR to persist in long-term commitment to fight an enemy until it accomplishes its goals and objective. Protracted and persistent operations are the norm of the irregular OPFOR. Actions may be subtle and can be part of a gradual series of actions toward achieving a task. Dramatic individual actions are often used to establish or sustain notoriety for the irregular OPFOR, but rarely achieve a decisive effect. Periodic setbacks in irregular OPFOR missions are anticipated and rationalized with effective INFOWAR announcements to sustain a moral dominance of the irregular OPFOR over an enemy. INFOWAR techniques can also convince a relevant population to sustain support of the irregular OPFOR even though its actions may require an extended period of time before the population eventually benefits. The irregular OPFOR may attempt to achieve its objectives within a specified timetable and announced milestones; however, the objectives may take decades or generations to achieve.

II. Operational Variables (PMESII-PT)

The irregular OPFOR is part of the military variable, which explores the military and/or paramilitary capabilities of all relevant actors (enemy, friendly, and neutral) in a given OE. However, irregular OPFOR actions can affect or be affected by all the operational variables: political, military, economic, social, information, infrastructure, physical environment, and time (PMESII-PT) and their subvariables. The impacts may be robust, moderate, or relatively insignificant. The interaction of the operational variables and subvariables establishes conditions for various levels of irregular OPFOR capabilities and limitations. The dynamic interaction and effects by the irregular OPFOR on operational variables are a physical and psychological combat multiplier for the OPFOR. The following paragraphs discuss the impacts of the irregular OPFOR on each of the operational variables. They also provide examples of how the actions of one variable can directly or indirectly impact on other variables and affect the capabilities and influence of the irregular OPFOR.

P - Political

The centers of responsibility and power at various levels of governance can be an objective for irregular OPFOR subversion or violent action. The irregular OPFOR may target for willing or coerced support of its aims—

- Constituted authorities at local, provincial, and/or state levels.
- Tribal leaders and/or clan chiefs.
- Religious leaders and councils.
- Influential political organizations.

The irregular OPFOR may want to institute its own political goals for the perceived benefit of a relevant population, or to create chaos within a governing authority in order create a protected geographic enclave within a sovereign state. In either case, influence over a relevant population is essential. Given enough electoral support in a relevant population, the irregular OPFOR may be able to win formal political recognition at varied levels of a governing authority that it opposes.

Conditions of the political variable would very likely interact with social and economic conditions of an OE. The political aim of the irregular OPFOR could have a genuine intent to provide a voice in politics to an under-represented relevant population, or be self-serving in order to obtain control of political institutions for its own commercial profit. It may start as the former and transition into the latter. An example of this transition could be if the irregular OPFOR emerged from an indigenous population of rural farmers and tenants with grievances against absentee landowners and corporate businesses. However, over time, the irregular OPFOR might shift its focus to commercial profit in racketeering and the production, and distribution of illegal drugs to a transnational market.

M - Military

The irregular OPFOR can infiltrate regular military and/or paramilitary forces of an enemy governing authority. It can collect intelligence on military unit strengths and weaknesses, unit leader preferences and biases, and/or readiness of weapons, support, and materiel. Covert actions by irregular OPFOR members can undermine the effectiveness of enemy units by—

- Raising doubts about the validity of enemy unit missions.
- Subverting leader and subordinate allegiances.
- Questioning the general treatment of military and/or paramilitary members by the governing authority.

With military training, weapons and equipment stolen or purchased by the irregular OPFOR can be used more effectively to improve its armed capabilities. In some cases, the irregular OPFOR may attempt to transition highly trained irregular forces into a more formalized paramilitary or security force in order to demonstrate its ability.

An example of interaction of military and information variables could be a media campaign directed at a local, regional, and transnational audience, in which the irregular OPFOR uses the symbols and appearance commonly associated with military power and influence. The irregular OPFOR could use progressive success in establishing and protecting a geographic safe haven with a declaration of sovereignty. Announcements to a global information network could display senior irregular OPFOR leaders in military uniform and attire, speaking publicly with official banners or flags, and maps or images of territory declared as independent. A focused defense of the safe haven, assisted by an extensive and supportive diaspora could achieve irregular OPFOR objectives unless challenged by an enemy governing authority.

E - Economic

The economic effectiveness and prosperity of a governing authority can be marginalized with black market activities coordinated by the irregular OPFOR. Criminal activities can include smuggling, theft, and/or piracy of marketable goods. Insurgent or guerrilla actions can include disrupting the flow of commerce throughout the economic chain of production, distribution, and consumption by the general populace. The irregular OPFOR, in some instances, can become the illicit commercial broker for what transactions occur in an economic sector. Front companies and/or organizations can launder resources and money into legitimate enterprises in support of irregular OPFOR objectives.

An example of interaction between economic, infrastructure, and information variables could be when the irregular OPFOR can deliver a satisfactory level of livelihood, health care, and commercial advancement for a relevant population. The population may have been denied access to such expectations by transnational corporations and a governing authority that extract natural resources from the region for their own profit and exclusive use. The grievance of this economic poverty can result in irregular OPFOR actions such as sabotage of pipelines, disruption of refining facilities, kidnapping of corporate officials, and/or random acts of murder. The irregular OPFOR can use a media campaign aligned with the economic grievances of the relevant population to emphasize the validity of OPFOR offensive actions. For example, it could call attention to the presence of significant private security contractors of transnational corporations and regular military forces of a governing authority conducting business security actions and military operations for their own financial gain.

S - Social

Cultural, religious, and ethnic differences can be stress points within a population that the irregular OPFOR can incite with real or false claims to further fracture a society and its social institutions. Unsettled grievances based on traditional values and customs can range from dissatisfaction to violent demonstrations against issues such as human rights, educational opportunities, and/or social mobility. The irregular OPFOR can nurture the support of particular social and religious leaders of a community that align themselves with OPFOR initiatives. Civic improvement associations and social welfare projects administered by the irregular OPFOR focused on a relevant population can be part of a comprehensive social unity program.

An example of interaction of the social and information variables could be the compelling influence that a cleric or advisory council of clerics can have on a relevant population. Religious leaders may have traditional authority in a culture that recognizes such an overarching authority, Based on that perceived authority, the directives and prohibitions of that cleric or council can direct popular support of the irregular OPFOR or civil disobedience to a governing political authority.

An example of interaction among variables could be the impact of a governing authority's land reforms that adversely affect the immediate prosperity of a local or regional population. This could include a directed destruction of one type of farming crop on limited usable terrain, and a replacement crop that does not provide the same economic value to the farmer or local distributor. This situation can be part of INFOWAR, with the irregular OPFOR promoting a story of how the governing authority it to blame for these negative impacts.

T - Time

Time can be a combat multiplier for the irregular OPFOR when the cultural perception of time accepts a protracted conflict. During such a protracted conflict, the irregular OPFOR can use violent actions, INFOWAR, diplomatic discussions, economic pressures, and progressive representations of value-added for a relevant population. Timing and duration of activities, events, or conditions, as well as how the timing and duration are perceived by various actors in the OE, can prevent or delay governing authority activities in favor of irregular OPFOR aims.

The irregular OPFOR seeks to chose the time and place for engaging the enemy. Timing can be the most significant aspect of determining when to tactically execute a decision to delay, deceive, fix, and/or block. Timeliness of information and intelligence is another key aspect that the irregular OPFOR uses to its own advantage. In order to affect enemy pace, tempo, and/or speed of action and reaction, the irregular OPFOR may plant false information at a particular time and ensure that an enemy obtains it. The prudent use of time is often combined with characteristics of a physical environment to create opportunities in support of near-, mid-, and/or long-term objectives.

III. Tactical Concepts

Initiative and mobility characterize tactics the HT would use while establishing and preserving bases in which to train, self-sustain, prepare for future missions, and evolve organizational capability. Concurrently, collective tactical actions can have strategic consequences of denying an enemy a secure area or making it politically untenable to remain. Actions are aimed at keeping an enemy physically and psychologically stressed from constant harassment and disruption when a distinct defeat or destruction of an enemy is not practical.

Tactical Concepts

A Synergy of Regular and Irregular Forces

B Info Warfare as a Key Weapon System

C Complex Battle Positions

D Systems Warfare

E Adapting by Function

I. Insurgents (Overview)

Ref: TC 7-100.3, Irregular Opposing Forces (Jan '14), chap. 2; JP 3-24, Counterinsurgency (Nov '13), chap. II & III and FM 3-24, Insurgencies and Countering Insurgencies (May '14), chap. 4.

Insurgents

Insurgents are armed and/or unarmed individuals or groups who promote an agenda of subversion and violence that seeks to overthrow or force change of a governing authority. They can transition between subversion and violence dependent on specific conditions. Both types of action intend to disrupt a governing authority. They gradually undermine the confidence of a relevant population in a governing authority's ability to provide and justly administer civil law, order, and stability. Insurgents can achieve their aims without violence, but this is not the norm.

I. Nature of Insurgency

Insurgency is the organized use of subversion and violence to seize, nullify, or challenge political control of a region. The conflict often begins long before it is recognized, allowing the insurgency to spread and develop a covert organization within the HN until it reveals its presence through overt subversive acts and violence. Recent operations indicate that insurgencies in the 21st century often may attract transnational terrorists in addition to covert or overt external support. Also, the increasing influence of commercial, informational, financial, political, and ideological links between previously disparate parts of the world has created new dynamics that further shape insurgencies and other irregular forms of conflict. The interaction of these dynamics with local politics makes modern insurgencies distinct and complex challenges for HNs, multinational partners, and the USG, especially when using the military instrument of national power.

The objective of insurgency is to gain political control of a population or a geographic area, including its resources. Unlike traditional warfare, nonmilitary, nonlethal means are often the more effective elements, with military forces still fulfilling a major security requirement and playing a larger enabling role in creating nonlethal effects to attain USG and HN objectives. Political power is the central issue in insurgencies, and insurgencies are designed to weaken government control and legitimacy while increasing insurgent control and influence, especially with the relevant populations. Insurgencies are typically protracted conflicts of 10 to 20 years and add to long-term regional instability that is normally contrary to US national interests. Insurgencies often end through a negotiated settlement involving political reform by the incumbent HN government.

Insurgent groups adopt an irregular approach because they initially lack the resources required to directly confront the incumbent government in traditional warfare. In some cases an irregular approach may also suit the geographic terrain and/or sociopolitical context of the OE. By adopting an irregular approach, insurgencies avoid decisive battles in which the incumbent government can apply its superior combat power. This allows the insurgent to exploit the terrain and population as cover and concealment for their operations. Insurgents typically begin and organize in a covert if not clandestine manner.

A. Insurgency Lines of Effort

Ref: TC 7-100.3, Irregular Opposing Forces (Jan '14), pp. 2-2 to 2-3.

Scope

Insurgent organizations normally conduct irregular conflict within or near the sovereign territory of a state in order to overthrow or force change in that state's governing authority. Some insurgent activities— such as influencing public opinion and acquiring resources—can occur outside of the geographic area that is the focus of the insurgency.

An insurgent organization may begin or remain at the local level. A local insurgent organization may exist at small city, town, village, parish, community, or neighborhood level. It may expand and/or combine with other local organizations. Cities with a large population or covering a large area may be considered regions and may include several low-level insurgent organizations. A higher insurgent organization may exist at regional, provincial, district, national, or transnational level. Higher insurgent organizations usually contain a mix of local insurgent and guerrilla organizations. The higher insurgent organization can apply both types of forces with a wider scope of impact. The OE and the specific goals determine the size and composition of each insurgent organization and the scope of its activities.

See pp. 2-30 to 2-36 on Higher Insurgent Organizations and Lower Insurgent Organizations, below, for more detail.

An insurgency is fundamentally a political movement. The expectation of a long-term conflict requires plans for and use of physical and psychological force. Civic actions develop, expand, and marshal the support of a relevant population for the insurgency's agenda. A comprehensive plan of action typically incorporates three main lines of effort:

- Political influence.
- Direct action violence and terrorism.
- Civic interaction and support.

Political Influence

The political element provides the overarching command and control (C2) of the insurgent organization. The political leadership plans and directs the strategy and actions to divide or weaken the governing authority they oppose. Information warfare (INFOWAR) activities foster dissatisfaction of the relevant population with the governing authority and show the insurgency as an opportunity for change. The insurgency degrades the confidence of the population in the governing authority. At the same time, the political element is preparing and/or implementing its own administrative and governance capabilities that provide solutions to the population's grievances.

Direct Action Violence and Terrorism

Insurgent cellular organization provides an adaptable function-based capability. Direct action cells reside primarily in local insurgent organizations and usually conduct small-scale and focused violent acts at the tactical level of conflict. (Direct action cells are described in detail later in this chapter.) Actions can range from one-person tasks to multiple cells tailored temporarily for specific operations. Subversion and selective or random violence are planned acts to incite frustration and overreaction by a governing authority. The government reaction can anger the relevant population and further undermine its allegiance or passive support to the governing authority. If an insurgency advances to the

IV. Countering Insurgencies - COIN (Military Operational Considerations)

Within the context of operating in a given HN, there are several operations, programs, and activities that may be conducted as a part of or simultaneously with **COIN**, including negotiation and diplomacy, SC (FID, SFA, and SA), unconventional warfare (UW), CT, counterguerrilla operations, stability operations, and PO. Each may be conducted simultaneously with or independently of the others but each would likely require overlapping operational areas within the HN. Additionally, each may have different root causes and objectives, but would become part of the overarching COIN operation/campaign. Other key operations related to COIN are CMO, IO, MISO, maritime security operations (MSO), and counterdrug operations.

A. Negotiation and Diplomacy

Negotiation and diplomacy is a way to influence an insurgency. The counterinsurgent must convince the HN government and subordinate elements, such as the ministry of defense or ministry of the interior to remove the root causes of the instability; some of these root causes may be caused by or aggravated by ministerial policies themselves. At the strategic and operational levels it could be working with the HN senior military leadership to assist them in evaluating the root causes of the insurgency. In other situations, the ministerial level official or general officer (being advised) may be able to influence other governmental organizations that could be a root cause of the insurgency. At the tactical level this could be a key leader engagement. These engagements can be used to shape and influence foreign leaders at the strategic, operational, and tactical levels, and may also be directed toward specific groups such as religious leaders, academic leaders, and tribal leaders (e.g., to solidify trust and confidence in US forces).

B. Security Cooperation (SC)

SC involves all DOD interactions with foreign defense establishments to build defense relationships that promote specific US security interests, develop allied and friendly military capabilities for self-defense and multinational operations, and provide US forces with peacetime and contingency access to an HN. These activities help the US and HN gain credibility and help the HN build legitimacy. These efforts can help minimize the effects of or prevent insurgencies and thwart their regeneration.

- **Security Assistance (SA).** SA is a group of SC programs funded by DOS to be administered by DOD/Defense Security Cooperation Agency.
- **Foreign Internal Defense (FID)**. FID is the participation by civilian and military agencies of a government in any of the action programs taken by another government or other designated organization to free and protect its society from subversion, **lawlessness, insurgency, terrorism, and other threats to its security.**
- **Security Force Assistance (SFA).** SFA encompasses joint force activities conducted within unified action to train, advise, assist, and equip foreign security forces in support of a partner nation's efforts to generate, employ, and sustain local, HN, or regional security forces and their supporting institutions.

C. Unconventional Warfare (UW)

UW consists of whole-of-government activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerrilla force in a denied area. UW can support COIN operations by giving the JFC and/or the GCC an additional option for curtailing support to an ongoing insurgency. For example, if a neighboring state to the one in which a COIN operation is being waged has proven to be a major source of insurgent resources, personnel, and support, the JFC may recommend UW operations inside that insurgent-supporting state in order to modify that nation's counterproductive behavior or even remove its government altogether. While SOF play a major role in the execution of UW operations and posses specific tactical UW competencies, the JFC must ensure operational and strategic synchronization of COIN and UW activities.

D. Counterterrorism (CT)

Terrorism has evolved as a preferred tactic for ideological extremists around the world, directly or indirectly affecting millions of people. Terrorists use many forms of unlawful violence or threats of violence to instill fear and coerce governments or societies to further a variety of political, social, criminal, economic, and religious ideologies. Terrorists threaten the national power, sovereignty, and interests of the United States and our allies. Terrorists organize and operate in a number of ways. Some operate within transnational networks, others operate as small independent groups, and others operate alone.

E. Counterguerrilla Operations

Counterguerrilla operations are operations and activities conducted by armed forces, paramilitary forces, or nonmilitary agencies against guerrillas. Counterguerrilla operations are essential supporting efforts, or a subset of COIN operations focused on the insurgents' military forces.

F. Stability Operations

Stability operations refer to various military missions, tasks, and activities conducted outside the US in coordination with other instruments of national power to maintain or reestablish a safe and secure environment and provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief. Stability operations are consequently fundamental to COIN. Stability operations address the root causes of insurgency as well as drivers of conflict and are therefore essential to long-term success. US military forces should be prepared to lead the activities necessary to accomplish these tasks when indigenous civil, other USG departments and agencies, multinational, or international capacity does not exist or is not yet capable of assuming responsibility.

G. Peace Operations (PO)

For the Armed Forces of the United States, PO are crisis response and limited contingency operations involving all instruments of national power and international efforts and military missions to contain conflict, restore the peace, and shape the environment to support reconciliation and rebuilding and to facilitate the transition to legitimate governance. PO include peacekeeping operations, peace enforcement operations (PEO), peace building post-conflict actions, peacemaking processes, and conflict prevention. PO may be conducted under the sponsorship of the UN, another IGO, within a multinational force, or unilaterally.

H. Related Operations

The complex nature of COIN often requires many types of operations to effectively shape the OE and set the conditions to reach the desired end state. For example, all or part of unsuccessful PEO can transition to COIN as the situation devolves and becomes more unstable. COIN and PEO can also occur simultaneously if some parties have agreed to peace while one or more use insurgency to reach their goals.

Refer to TAA2: Military Engagement, Security Cooperation & Stability SMARTbook (Foreign Train, Advise, & Assist). Topics include the Range of Military Operations (JP 3-0), Security Cooperation & Security Assistance (Train, Advise, & Assist), Stability Operations (ADRP 3-07), Peace Operations (JP 3-07.3), Counterinsurgency Operations (JP & FM 3-24), Civil-Military Operations (JP 3-57), Multinational Operations (JP 3-16), Interorganizational Cooperation (JP 3-08), and more.

Chap 2

II. Insurgency Threat Characteristics

Ref: FM 3-24, Insurgencies and Countering Insurgencies (May '14), chap. 5.

Threat characteristics involve the composition, disposition, activities, and tactics of an insurgency. The composition of an insurgency is covered under the eighth dynamic, organizational and operational patterns. Tactics for an insurgency include political activities, criminal actions, and military tactics. Counterinsurgents consider how these threat characteristics create strengths and weaknesses for an insurgency.

I. Disposition and Activities

The disposition is the geographic location of insurgent elements and the way they are deployed, employed, or located. The dispositions of an insurgency are partially determined by an operational environment and the operational variables. For example, if an insurgency has connections to a black market, some of its dispositions will normally be to protect that market. Terrain will also affect the dispositions of an insurgency. Commanders and staffs must understand an operational environment to understand an insurgency's dispositions.

Insurgent Actions

A Political Activities

B Population Control

C Military Tactics (including terrorist activities and conventional tactics)

D Support Activities

Insurgents who rely solely on violence to achieve their political goals are probably ineffective. Instead, effective insurgents conduct a wide range of activities to achieve their goals. Many of these activities are not enemy or terrain oriented, but political. Insurgents use a range of activities supporting both military and political actions.

A. Political Activities

Insurgents may use political activities to achieve their goals and enhance their cause's legitimacy. An insurgency's actions can come from inside the government's political system or can be used to communicate a message to the population. Political actions that happen within a government normally happen in a democracy or a semidemocracy. In these systems, an insurgency and related political parties can have some political power through elections. This gives groups the ability to launch official investigations and a platform to question government actions. This was a technique used by the Irish Republican Army and Sinn Fein.

Political and Military Components

Ref: JP 3-24, Counterinsurgency (Nov '13), pp. II-15 to II-17.

Insurgent structure may be generally broken down into two wings: political and military. Insurgent sociocultural factors, approaches, and resources tend to drive its organization, and most insurgencies. Figure II-2 depicts them in any activities that these two wings may perform, from exploiting root causes to overt guerrilla operations. Progression up the diagram does not have to be linear; insurgencies can perform many of these activities at any time, in any order or combination.

Political Wing

Insurgencies will have some form of political wing, although some may only require an emerging political wing. The political wing is primarily concerned with undermining the legitimacy of the HN government and its allies while building up support for the insurgency. This may be accomplished by participation of members of the political wing in legitimate elections and political processes in order to infiltrate the government and undermine it from within. The political wing of the insurgency builds credibility and legitimacy for the insurgency within the population and potentially with the international community. The political wing may downplay insurgent violence and subversion, some to the point of outright deception.

Shadow Government

An insurgency and its political wing may become strong enough to not only challenge the HN government, but it may act as an alternative government. It may provide some or all of the functions or services of a government, for example food distribution, health care, security, and education. Normally the shadow government will attempt to satisfy grievances in local areas first. They may attempt to transfer blame for any residual issues to foreign presence or the HN government in order to facilitate popular support.

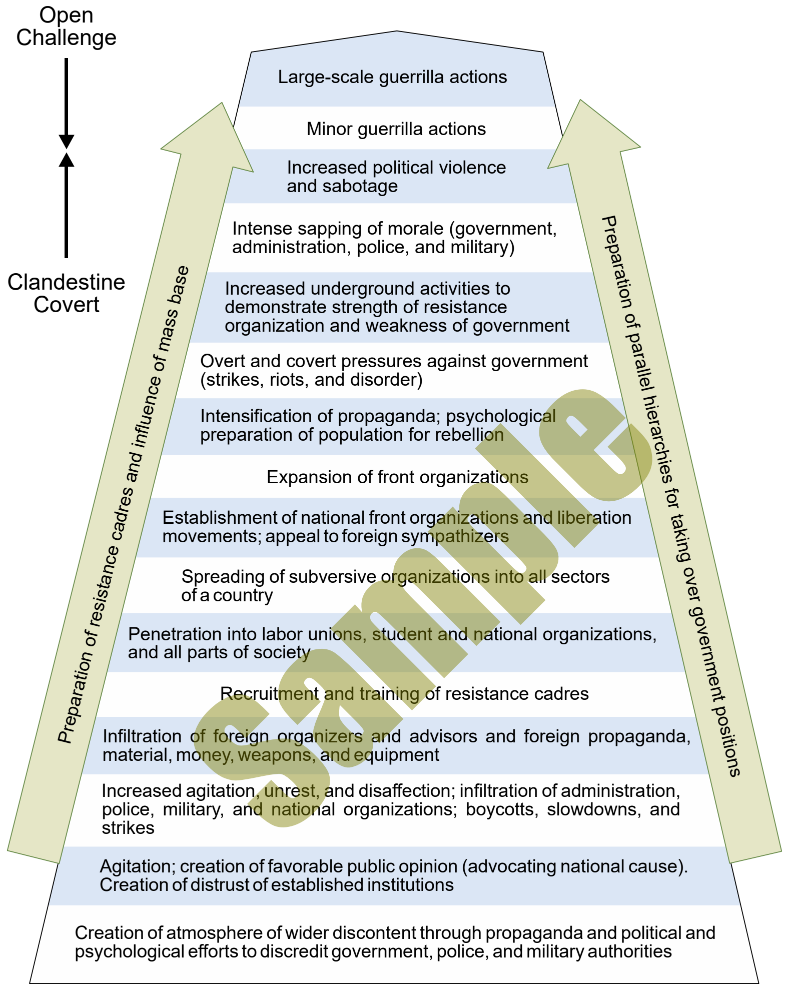
Supportive Parties

While not part of the insurgency, an existing legal political party may come to support the insurgency or may form a legal political party that supports the insurgency. These legal political parties may become the insurgents' conduit for diplomacy and political reconciliation. In some cases, the political party may consist of former insurgent strategic leaders and cadre. Efforts should be made to open and maintain these avenues for reconciliation.

Military Wing

The military wing of the insurgency conducts violent criminal activities and ultimately some forms of combat operations. Most insurgencies may initially have few combatants; however, military-focused insurgencies will focus on this wing and build their guerrilla force (military) capability and capacity over time and may execute overt operations and go back into hiding to survive. As the insurgency grows in relative strength, however, its military wing will likely form a larger guerrilla force and may be able to operate continuously in an overt fashion. Guerrilla forces usually start with paramilitary operations, but advanced insurgencies may transition to more traditionally planned and organized military operations. Thus, if security is ineffective or the insurgency has grown powerful relative to the HN government, the military elements may exist openly. If the state maintains a continuous and effective security presence, some part of the military wing will likely maintain a secret existence.

Insurgent Actions: Political and Military



Open Challenge

Clandestine Covert

Large-scale guerrilla actions

Minor guerrilla actions

Increased political violence and sabotage

Intense sapping of morale (government, administration, police, and military)

Increased underground activities to demonstrate strength of resistance organization and weakness of government

Overt and covert pressures against government (strikes, riots, and disorder)

Intensification of propaganda; psychological preparation of population for rebellion

Expansion of front organizations

Establishment of national front organizations and liberation movements; appeal to foreign sympathizers

Spreading of subversive organizations into all sectors of a country

Penetration into labor unions, student and national organizations, and all parts of society

Recruitment and training of resistance cadres

Infiltration of foreign organizers and advisors and foreign propaganda, material, money, weapons, and equipment

Increased agitation, unrest, and disaffection; infiltration of administration, police, military, and national organizations; boycotts, slowdowns, and strikes

Agitation; creation of favorable public opinion (advocating national cause). Creation of distrust of established institutions

Creation of atmosphere of wider discontent through propaganda and political and psychological efforts to discredit government, police, and military authorities

Preparation of resistance cadres and influence of mass base

Preparation of parallel hierarchies for taking over government positions

Ref: JP 3-24, Counterinsurgency, fig II-2, p. II-16.

IV. Local Insurgent Organizations

The term local insurgent organization applies to any insurgent organization below regional, provincial, or district level. This includes small cities, towns, villages, parishes, communities, neighborhoods, and/or rural environments. (Large cities are equivalent to regions and may contain several local insurgent organizations.) Activities remain focused on a local relevant population.

Differences between a local insurgent organization and a higher insurgent organization are as follows:

- Direct actions cells are present within a local insurgent organization. Their multifunctional and/or specific functional capabilities may be enhanced or limited based on availability of resources and technical expertise in or transiting the local OE. These direct actions are planned for immediate and/or near-term effects related to the local insurgent organization's area of influence.
- Guerrilla units might not be subordinate to the local insurgent organization. However, temporary affiliations between local insurgents and guerrillas are possible for specified missions coordinated by a higher insurgent organization. Direct action personnel may use, fight alongside of, or assist affiliated forces, and guerrillas to achieve their common goals or for any other agenda. Guerrilla units may operate in a local insurgent organization's area of influence and have no connection to the local insurgent organization or a higher insurgent organization.

Criminals can affiliate with a local insurgent organization or a higher insurgent organization as a matter of convenience and remain cooperative only as long as criminal organization aims are being achieved. The local insurgent organization retains a long-term vision of its political agenda, whereas cooperation by a criminal organization is usually related to localized commercial profit and/or organizational influence in a local environment. This usually equates to criminals controlling or facilitating materiel and commodity exchanges. The criminal is not motivated by a political agenda.

The local insurgent organization uses functional tactics (see chapter 7) and terrorism (see chapter 6) as the primary means to achieve its goals. Terrorism instills fear and anxiety that coerces and degrades the resolve of an enemy governing authority and selected people in a relevant population.

Relation to Other Insurgent Organizations

The local insurgent organization is the basic level of insurgent organization. Local insurgent organizations are not always subordinate to a regional, national, or transnational insurgent organization. They may be completely autonomous and independent of a larger insurgent movement and not be associated with it in any way. In other cases, they can be either subordinate to or loosely affiliated with such a larger organization. They may operate under the guidance of a larger insurgent organization even is no command relationship exists. In some cases a local insurgent organization may provide only financial support and general guidance to its direct action and supporting cells *(see figure 2-4).*

Cells of a local insurgent organization may be forced to provide for themselves in several areas. A typical example of this is a smaller direct action cell separated from the parent insurgent organization by distance, population, or ability to communicate securely. They may not have access to the expertise or products such as IEDs provided by the technical support cell and must improvise IEDs by themselves.

Any relationship to a higher organization or among independent local insurgent organizations may be dependent upon only a single shared or similar goal. These relationships are generally fluctuating and may be fleeting, mission dependent, event-or agenda-oriented, mutually coordinated, and/or coerced for a specific temporary purpose. There may be loose coordination of certain actions, after which the organizations revert back to their independent modes.

Guerillas

Ref: TC 7-100.3, Irregular Opposing Forces (Jan '14), chap. 3.

Guerilla

A guerrilla force is a group of irregular, predominantly indigenous personnel organized along military lines to conduct military and paramilitary operations in enemy-held, hostile, or denied territory (JP 3-05). Thus, guerrilla units are an irregular force, but structured similar to regular military forces. They resemble military forces in their command and control (C2) and can use military-like tactics and techniques. Guerrillas normally operate in areas occupied by an enemy or where a hostile actor threatens their intended purpose and objectives. Therefore, guerrilla units adapt to circumstances and available resources in order to sustain or improve their combat power. Guerrillas do not necessarily comply with international law or conventions on the conduct of armed conflict between and among declared belligerents.

I. Scope and Duration of Operations

The area of operations (AOR) for guerrilla units may be quite large in relation to the size of the force. The reason for this is that a large number of small guerrilla units can be widely dispersed. Guerrilla operations may occur as independent squad or team actions. In other cases, operations could involve a guerrilla brigade and/or independent units at battalion, company, and platoon levels. A guerrilla unit can be an independent paramilitary organization and/or a military-like component of an insurgency. Guerrilla actions focus on the tactical level of conflict and its operational impacts. Guerrilla units can operate at various levels of local, regional, or international reach. In some cases, transnational affiliations can provide significant support to guerrilla operations.

Guerrilla forces are adaptive, flexible, and agile in quickly changing their composition to optimize organizational capabilities against known or perceived vulnerabilities of an enemy. Guerrillas exploit familiarity with their physical environment and the ability to blend into the local populace. Small guerrilla units have great mobility and ability to move throughout enemy-occupied areas.

Guerrillas seek to gain small psychological victories. These victories do not need to be significant in terms of material damage to the enemy. These tactical victories only need to show that a small guerrilla force can defeat [at least parts of] a much larger enemy force.

Guerrilla forces take prudent risks when an expectation exists for successful attack on an enemy, but may also make significant practical sacrifices in individuals and materiel in order to achieve a major psychological impact on an enemy. Guerrillas also apply information warfare (INFOWAR) capabilities to weaken or exhaust enemy resolve.

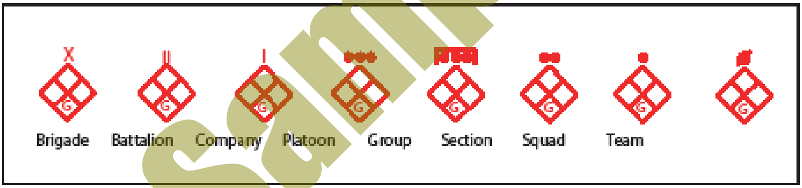
Ultimately, the resolve of guerrilla leaders and members of guerrilla organizations determines how long to continue guerrilla operations. Time is a key factor that guerrilla forces use as a combat multiplier in a long-term commitment to degrade and eventually defeat the will of an enemy. The goal is not necessarily to defeat enemy forces but to outlast them. This long-term struggle includes a full range of actions that range from espionage and media manipulation to more violent actions such as sabotage, assassination, bombing, ambushes, and raids. Guerrillas can use acts of terrorism to achieve either selective or random psychological stress and physical damage or destruction. Actions are typically quick and violent, followed by rapid dispersal of assembled guerrilla forces.

II. Guerilla Organizations

Ref: TC 7-100.3, Irregular Opposing Forces (Jan ‘14), pp. 3-7 to 3-27.

Guerrillas use a military-like organizational structure for C2 and conduct of operations. For example, the basic building block of a guerrilla organization may be a squad consisting of two fire teams. Such squads are the basis for building guerrilla platoons, companies, battalions, and brigades. However, guerrilla commanders can task-organize these units for specific actions. Even prior to specific actions, whole guerrilla companies may already be restructured (task-organized) as hunter-killer (HK) companies, made up HK groups, HK sections and HK teams. When a guerrilla battalion consists predominantly of HK companies, it may be called a guerrilla HK battalion. When a guerrilla brigade consists predominantly of HK battalions (or conceivably of multiple separate HK companies), it may be called a guerrilla HK brigade.

Guerrilla organizations may be as large as several brigades or as small as a platoon and/or independent HK teams. Often a brigade-size guerrilla force may not be appropriate for a particular mission or area AOR. It may be too large, and a task-organized guerrilla battalion may be sufficient. An example task-organized battalion might have four or five HK companies, organic battalion units, a weapons battery (with a composite of mortar, rocket launcher, and antitank platoons) from brigade, and possibly intelligence and INFOWAR augmentations.



TC 7-100.3, fig. 3-1. Guerrilla organization symbols: brigade to team level.

The hierarchy of military-like terms for guerrilla units (from the bottom up) is as follows:

- Team or HK team.
- Squad or HK section.
- Platoon or HK group.
- Company or HK company.
- Battalion (or HK battalion).
- Brigade (or HK brigade).

Note. Some guerrilla organizations may have honorific titles that do not reflect their true nature or size. For example, a guerrilla force that is actually of no more than battalion size may call itself a “brigade,” a “corps,” or an “army.” A guerrilla organization may also refer to itself as a “militia.” This is a loose usage of the term militia, which generally refers to citizens trained as soldiers (as opposed to professional soldiers), but applies more specifically to a state-sponsored militia that is part of the state’s armed forces but subject to call only in emergency. To avoid confusion, the TC 7-100 series uses militia only in the latter sense.

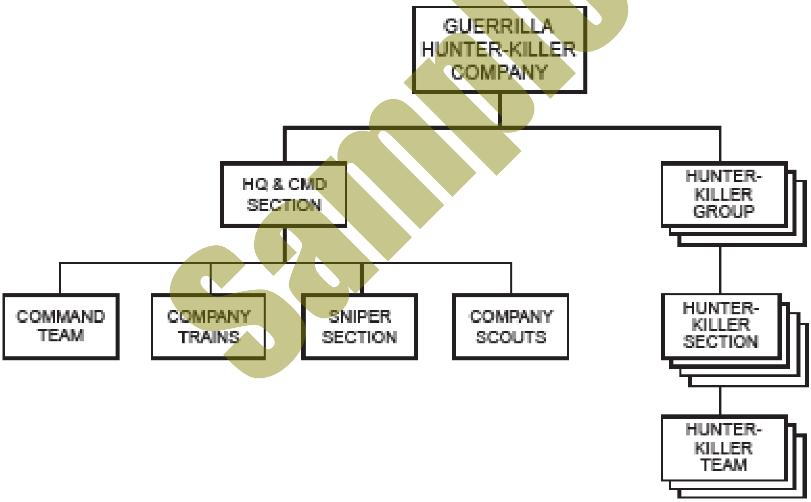
I. Guerrilla Hunter-Killer (HK) Company

Ref: TC 7-100.3, Irregular Opposing Forces (Jan '14), pp. 3-25 to 3-27.

The guerrilla company can be augmented and restructured into a guerrilla hunter-killer (HK) company made up of numerous small HK teams. Those teams are typically organized into HK sections and the sections into HK groups. The HK team structure is ideal for dispersed combat such as fighting in urban areas and can provide similar capabilities in rural terrain when cover and concealment and channelized avenues favor the guerrilla. Tailored HK units are usually a company-level configuration; however, complete battalions and brigades can be organized for combat as HK units.

An HK company is based on the personnel and equipment originally found in a guerrilla company. However, the HK company may have additional equipment due to the dispersed nature of HK team employment. For example, it typically would have additional antitank disposable launchers and flame weapons. It may also have three additional 60-mm mortars, possibly dispersed to one team in each HK group. These additional weapons do not necessarily require additional personnel.

The guerrilla company task-organized as an HK company typically consists of a headquarters and command section and three HK groups. Typically, each HK group has four HK sections, and each HK section has three HK teams. Figure 3-6 shows an example of such a company.



Ref: TC 7-100.3 (Jan '14), fig. 3-6. Guerrilla hunter-killer company (example).

An HK company structured as in figure 3-6 can contain a total of 36 HK teams. If the two sniper teams and the company scouts in the headquarters and command section are counted, the HK company can have a total of 39 HK teams.

Note. When a guerrilla platoon is task-organized into an HK group, its machinegun section ceases to exist as a separate unit. Its personnel and equipment are distributed among HK sections and teams. Likewise, when a guerrilla company is restructured into an HK company, the weapons platoon typically ceases to exist as a separate unit. Its weapons are then redistributed among various parts of the HK company.

- **Headquarters and Command Section.** The headquarters and command section of an HK company typically comprises the command team, company trains, a

Chap 4

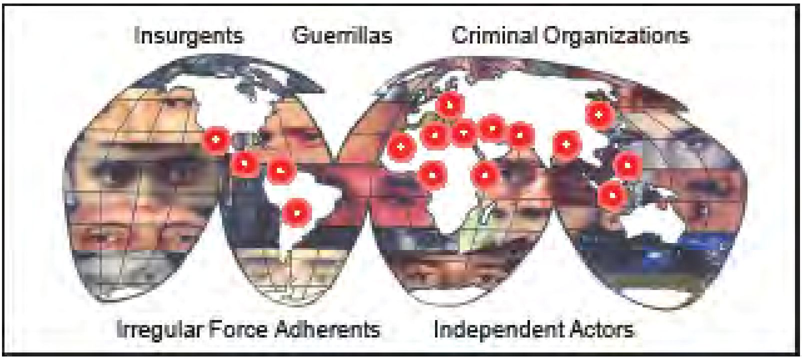
I. Terrorists (Overview/Introduction)

Ref: TC 7-100.3, Irregular Opposing Forces (Jan '14), chap. 6 and JP 3-26, Counterterrorism (Nov '09), chap 2 and JP 3-26 (2014), chap. 1.

Terrorism is a tactic. This chapter presents an overview of conditions that are a composite of real-world capabilities and limitations that may be present in a complex operational environment that includes terrorism. Acts of terrorism demonstrate an intention to cause significant psychological and/or physical effects on a relevant population through the use or threat of violence. Terrorism strategies are typically a long-term commitment to degrade the resilience of an enemy in order to obtain concessions from an enemy with whom terrorists are in conflict. International conventions and/or law of war protocols on armed conflict are often not a constraint on terrorists. Whether acts of terrorism are deliberate, apparently random, and/or purposely haphazard, the physical, symbolic, and/or psychological effects can diminish the confidence of a relevant population for its key leaders and governing institutions. Social and political pressure, internal and/or external to a relevant population and governing authority, is frequently exploited by terrorists with near real-time media coverage in the global information environment. The local, regional, international, and/or transnational attention on acts of terrorism by state and/or non-state actors can often isolate an enemy from its relevant population and foster support of organizations, units, or individuals who feel compelled to use terror to achieve their objectives. The themes and messages promoted by terrorists can accent anxiety, demoralize the resolve of a relevant population and its leaders, and eventually defeat an enemy.

I. Terrorism

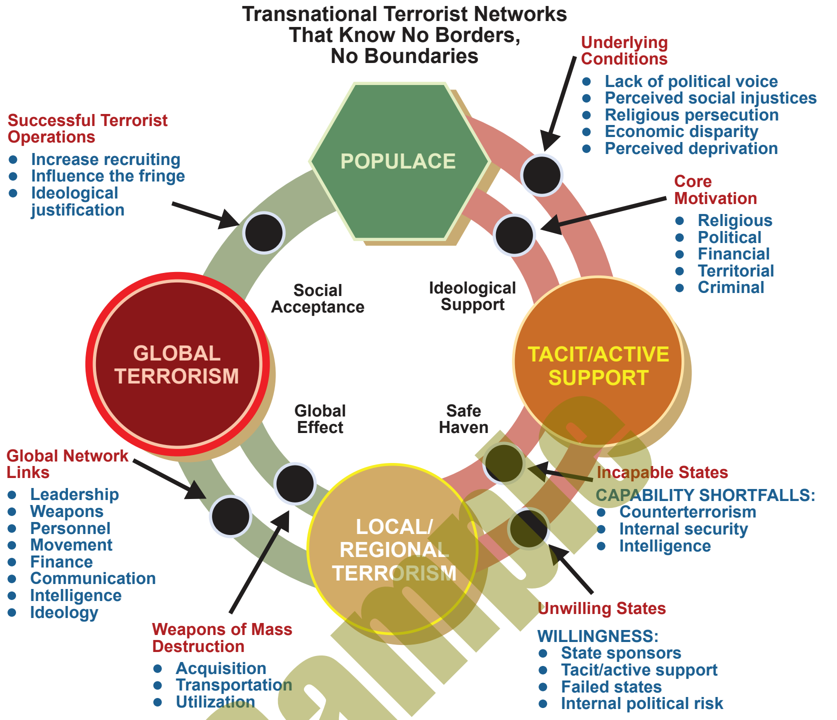
Terrorism can be defined as the use of violence or threat of violence to instill fear and coerce governments or societies. Often motivated by philosophical or other ideological beliefs, objectives are typically political in nature. The pursuit of goals and conduct labeled as terrorism by some actors in complex operational environments (OE) can be considered fully justifiable by other actors. The spectrum of actors in an OE can range political, public, and/or commercial institutions, other institutions appearing legitimate but disguising an illicit agenda, and/or organizations and individuals who openly declare intent to use terror as a matter of policy and practice. Irregular forces typically use terrorism.



Ref: TC 7-100.3 (Jan '14), fig. 6-1. Terrorism actors in complex operational environments.

III. Terrorism Threat Model

Ref: JP 3-26, Counterterrorism (Nov '09), fig. III-2, p. III-8.



This representative model from JP 3-26 (2009) shows how violent extremist organizations (VEOs) can use terrorism as a circle that operates around four critical components:

- **A populace** from which extremists have the potential to draw support
- **Tacit and/or active support** given to the extremist by some of the sympathetic populace
- **Local/regional terrorism** as a result of states unwilling or incapable of countering violent extremists
- **Global terrorism** that results from global networks built upon popular support and the inability of states to control local and regional extremist networks

The cycle is completed when successful terrorist operations (at the global or local/regional level) reinforce their ideological justification, and influence that portion of the populace that is susceptible to the extremist ideology.

IV. Forms of Terrorism

Ref: JP 3-26, Counterterrorism (Nov '09), chap 2.

Terrorism is one of the oldest forms of human conflict. Before societies organized to wage war against each other, individuals and small bands engaged in terror tactics to achieve limited goals–to overthrow existing leaders, toward off potential rivals, or to frighten opposing groups from lands they wished to claim for themselves.

Forms of terrorism threats range from non-state transnational networks with global reach capability such as Al-Qaeda, terrorist cells affiliated with regional or international aims, or individual self-radicalized and unaffiliated terrorists with single issue agendas. Terrorists exist as a foreign and domestic threat of the United States in the U.S. Homeland and in United States presence throughout the world.

Although the means and ends have evolved throughout history, the central elements of terrorism–fear, panic, violence, and disruption–have changed little through time. As the world enters the 21st Century, terrorism remains a vexing problem–an anachronistic fixture of human relations as paradoxically human and inhuman in the third Millennium as it was before the dawn of recorded history.

A. State-Sponsored Terrorism

Some nations and states often resort to violence to influence segments of their population, or rely on coercive aspects of state institutions. National governments can become involved in terrorism or utilize terror to accomplish the objectives of governments or individual rulers. Most often, terrorism is equated with non-state actors or groups that are not responsible to a sovereign government. However, internal security forces can use terror to aid in repressing dissent, and intelligence or military organizations can perform acts of terror designed to further a state's policy or diplomatic efforts abroad.

Refer to CTS1, pp. 1-25 to 1-30 for further discussion.

B. International Terrorism

International terrorism involves violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or any state, or that would be a criminal violation if committed within the jurisdiction of the United States or any state. These acts appear to be intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of a government by assassination or kidnapping. International terrorist acts occur outside the United States or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

Refer to CTS1, pp. 1-31 to 1-74 for further discussion.

C. Domestic Terrorism

Domestic terrorism is the unlawful use, or threatened use, of force or violence by a group or individual based and operating entirely within the United States or Puerto Rico without foreign direction committed against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof in furtherance of political or social objectives.

Refer to CTS1, pp. 1-75 to 1-84 for further discussion.

Refer to CTS1: The Counterterrorism, WMD & Hybrid Threat SMARTbook for further discussion. CTS1 topics and chapters include: the terrorist threat (characteristics, goals & objectives, organization, state-sponsored, international, and domestic), hybrid and future threats, forms of terrorism (tactics, techniques, & procedures), counterterrorism, critical infrastructure, protection planning and preparation, countering WMD, and consequence management (all hazards response).

II. Terrorist Behavior, Characteristics, Motivations

Ref: JP 3-26, Counterterrorism (Nov '09), pp. II-4 to II-8, and U.S. Army TRADOC G2 Handbook No. 1 (Version 5.0), A Military Guide to Terrorism in the Twenty-First Century (Aug '07), chap. 2.

The following discussion provides an insight into terrorist behaviors at both the individual and group levels, examines the impact of group goals and motivations on terrorist planning and operations, and provides observations of general terrorist characteristics. Goals and objectives of terrorist organizations differ throughout the world and range from regional single-issue terrorists to the aims of transnational radicalism and terrorism.

(FBI.GOV)

Terrorism is primarily a psychological act that communicates through violence or the threat of violence. Common motivational categories include separatism, ethnocentrism, nationalism, and revolution. Ideological categories can be framed by political, religious, or social purpose.

Domestic or indigenous terrorists are "home-grown," that is, they can be native born or naturalized citizens of a nation. They operate normally within and against their own country of residence. International or transnational terrorists can be visualized as operating primarily between two nations and their geographic region. International groups may operate in multiple countries, but retain a regional geographic focus for their activities. Terrorism is becoming more violent as terrorist organizations realize the value of notoriety due to spectacular attacks and the mass media exploitation that results.

I. Terrorist Behavior

Terrorism is a rationally selected tactic usually employed in the pursuit of ideological aims. However, some individuals or small violent organizations that employ terrorist means may not always be concerned with particular causes or an avowed ideology. These terrorists may be motivated purely by a desire to commit violent acts. From a psychological behavioral perspective, terrorism may fulfill a compelling need and this form of terrorism treats avowed ideology and political causes as after the fact justification. Another behavioral perspective is one based on rational choice. Terrorism is a tactic selected after rational consideration of the costs and benefits in order to achieve an objective.

A. Individual Terrorist Behaviors

Utopian View

Some terrorists have utopian goals regardless of their aims. This utopianism expresses itself forcefully as an extreme degree of impatience with the “status quo” of the rest of the world that validates the terrorists’ extreme methods. This view commonly perceives a crisis too urgent to be solved other than by the most extreme methods. Alternately, the perception is of a system too corrupt or ineffective to see or adopt the “solution” the terrorist espouses. This sense of desperate impatience with opposition is central to the terrorist world view. This is true of both the secular and religiously motivated terrorist, although with slightly different perspectives as to how to impose their solutions. There is also a significant impractical element associated with this utopian mind-set. Although their goals often involve the transformation of society or a significant reordering of the status quo, individual terrorists, even philosophical or intellectual leaders, are often vague or uncaring as to what the future order of things will look like or how their ideas will be implemented. Change, and the destructive method by which change is brought about, may be much more important than the end result.

Interaction with Others

Terrorists interact within their groups at both the member and leadership levels. Individuals forming or joining groups normally adopt the “leader principle” which amounts to unquestioning submission to the group’s authority figure. This explains the prevalence of individual leaders with great charisma in many terrorist organizations. Such leaders can demand tremendous sacrifices from subordinates. This type of obedience can cause internal dissension when a leader is at odds with the group or factions arise in the organization. Another adaptation of the individual is accepting an “in-group” (us against the world) mentality. This results in a presumption of automatic morality on the part of the other members of the group, and purity of their cause and goals. Thus, violence is necessary and morally justified and the use of violence becomes a defining characteristic.

Dehumanization of Nonmembers

There is a dehumanization of all “out-group” individuals. This dehumanization permits violence to be directed indiscriminately at any target outside the group. Dehumanization also removes some of the stigma regarding the killing of innocents. Another aspect is that by making the oppressed people an abstract concept, it permits the individual terrorist to claim to act on their behalf.

Lifestyle Attractions

A terrorist may choose violence as a lifestyle. It can provide emotional, physical, perceived religious, and sometimes social rewards. Emotionally, the intense sense of belonging generated by membership in an illegal group can be satisfying. Physical rewards can include such things as money, authority, and adventure. This lure often can subvert other motives. Social rewards may be a perceived increase in social status or power.

II. Terrorist Characteristics

Ref: JP 3-26, Counterterrorism (Nov '09), pp. II-7 to II-8 (chap 2).

Singular personality profiles of terrorists do not exist. In general, terrorists often feel alienated from society, have a perceived grievance, or regard themselves as victims of an injustice. The following provides some general characteristics:

Status

Contrary to a belief that terrorism is a product of poverty and despair, terrorists most commonly originate from middle class backgrounds, with some coming from extreme wealth and privilege. While guerilla fighters and gang members often come from poor and disadvantaged backgrounds, and may adopt terrorism as a tactic, terrorist groups that specifically organize as such generally come from middle and upper social and economic strata. The leadership may use less educated and socially dispossessed people to conduct acts of terrorism. Even within terrorist groups that espouse the virtues of "the people" or "the proletariat," leadership consists of those of middle class backgrounds.

Education and Intellect

In general, terrorists, especially their leaders, are usually of average or better intelligence and have been exposed to advanced education. Very few terrorists are uneducated or illiterate. Some leaders of larger terrorist organizations may have minimal education, but that is not the norm. Terrorist groups increasingly are recruiting members with expertise in areas such as communications, computer programming, engineering, finance, and the sciences. Among terrorists that have had exposure to higher learning, many are not highly intellectual and are frequently dropouts or possess poor academic records. However, this is subject to the norms of the society from which they originate. Societies where religious fundamentalism is prevalent, the focus of advanced studies may have been in religion or theology.

Age

Terrorists tend to be young. Leadership, support, and training cadres can range into the 40- to 50-year-old age groups, but most operational members of terrorist organizations are in the 20- to 35-year-old age group. The amount of practical experience and training that contributes to making an effective operative is not usually present in individuals younger than the early 20s. Individuals in their teens have been employed as soldiers in guerilla groups, but terrorist organizations tend to not accept extremely young members, although they will use them as nonoperational supporters. Groups that utilize suicide operations often employ very young individuals as suicide assets, but they likely are not actual members of the organization and are simply coerced or exploited into an operational role.

Gender

The terrorists' gender is predominately male, but not exclusively male, even in groups that are rigorously Islamic. Females in these groups are used to support operations or assist in intelligence gathering. Some fundamentalist Islamic groups, however, may use females in the actual conduct of terrorist operations. In groups where religious constraints do not affect women's roles, female membership may be high and leadership roles within the group are not uncommon. Female suicide bombers have been employed with a growing frequency.

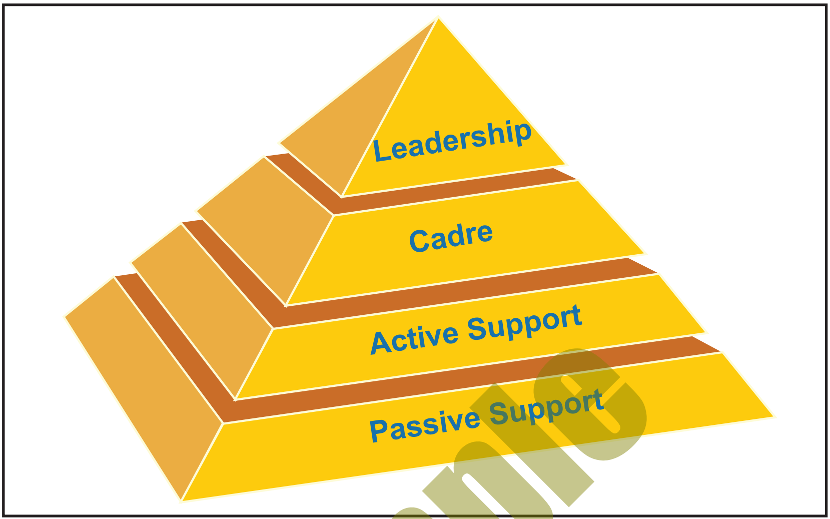
Appearance

Terrorists are often unremarkable in individual characteristics and attempts to "profile" likely terrorist groups' members may not be productive. They may not appear out of the ordinary and are capable of normal social behavior and appearance. Over the long term, elements of fanatical behavior or ruthlessness may become evident, but they are typically not immediately obvious to casual observation.

Terrorist Levels of Commitment

Ref: JP 3-26, Counterterrorism (Nov '09), chap. 2, pp. 2-8 to 2-10 (fig. 2-1, p. 2-9).

Typically, there are four different levels of commitment within a terrorist organization: passive supporters, active supporters, cadre, and leadership.



Leaders

Leaders provide direction and policy; approve goals and objectives; and provide overarching guidance for operations. Usually leaders rise from within the ranks of any given organization, or create their own organization, and are ruthless, driven, and very operationally oriented in order to accomplish their objectives.

Cadre

Cadre is the nucleus of "active" members, the zealots, who comprise the core of a terrorist organization. This echelon plans and conducts not only operations, but also manages areas of intelligence, finance, logistics, IO, and communications. Mid-level cadres tend to be trainers and technicians such as bomb makers, financiers, and surveillance experts. Low-level cadres are the bombers and foot soldiers for other types of attacks.

Active Supporters

Active supporters participate in the political, fund-raising, and information activities of the group. Acting as an ally or tacit partner, they may also conduct initial intelligence and surveillance activities, and provide safe houses, financial contributions, medical assistance, and transportation assistance for cadre members. Usually, they are fully aware of their relationship to the terrorist group but do not commit violent acts.

Passive Supporters

Passive supporters are typically individuals or groups that are sympathetic to the announced goals and intentions of the terrorist organization or its ideology, but are not committed enough to take action. Passive supporters may interact with a front group that hides the overt connection to the terrorist group, or passive supporters may intermingle with active supporters without being aware of what their actual relationship is to the organization. Sometimes fear of reprisal from terrorists compels passive support. Sympathizers can be useful for political activities, fund-raising, and unwitting or coerced assistance in intelligence gathering or other nonviolent activities.

Basic Network Concepts

Ref: JP 3-26, Counterterrorism (Nov '09), chap. 2, pp. 2-12 to 2-13.

Terrorists are now increasingly part of a far broader but indistinct system of networks than previously experienced. Groups based on religious or single-issue motives lack a specific political or nationalistic agenda and therefore have less need for a hierarchical structure to coordinate their actions. Instead, they can depend on loose affiliation with like-minded groups or individuals from a variety of locations. General goals and targets are announced, and individuals or cells are expected to use flexibility and initiative to conduct the necessary actions.

Tactical Concepts

A **Chain Network**

B **Hub or Star and Wheel Network**

C **All-Channel Network**

A network structure may be a variation of several basic nodal concepts, a node being an individual, a cell, another networked organization, or even a hierarchical organization. A terrorist network may consist of parts of other organizations (even governments), which are acting in ways that can be exploited to achieve the network's organizational goals. The effectiveness of a networked organization is dependent on several things.

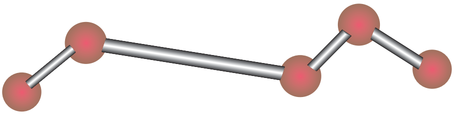
- Network effectiveness requires a unifying idea, concern, goal, or ideology. Without that unifier, networks can take actions or pursue objectives that are counterproductive, and independent nodes may not develop the necessary synergism for success of the network.
- Networks can distribute the responsibility for operations while providing redundancies for key functions. The various cells need not contact or coordinate with other cells except for those essential to a particular operation or function. The avoidance of unnecessary coordination or command approval for action provides deniability to the leadership and enhances operations security.
- Networks need not be dependent on the latest information technology to be effective. The organizational structure and the flow of information inside the organization (i.e., their information management plan) are the defining aspects of networks. While information technology can make networks more effective, low-technology means such as couriers and landline telephones can enable networks to operate effectively.
- Changes in terrorist leadership, whether through generational transition or as a response to enhanced security operations, may signal significant adjustments to terrorist group organizational priorities and its means of conducting terrorism

Basic Types of Networks

There are three basic types of network structures, depending on the ways in which elements (nodes) are linked to other elements of the structure: the chain, hub (or star and wheel), and all-channel. A terrorist group may also employ a hybrid structure that combines elements of more than one network type. For example, a transnational terrorist organization might use chain networks for its money laundering activities, tied to a hub network handling financial matters, tied, in turn, to an all channel leadership network to direct the use of the funds into the operational activities of a hub network conducting pre-targeting surveillance and reconnaissance. Organizational structure that may appear very complex during initial assessments of terrorist groups may be more understandable when viewed in the context of chain, hub variants, or all channel networks.

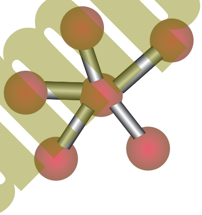
Chain

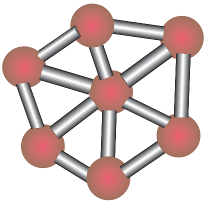
Each node links to the node next in sequence and communication between the nodes is by passing information along the line. This organization is typical among networks that have a common function such as smuggling goods and people or laundering money.



Hub or Star and Wheel

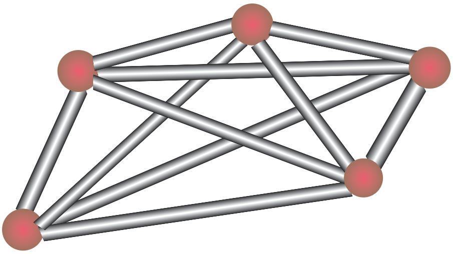
Outer nodes communicate with one central node, which may not be the leader or decision maker for the network. A variation of the hub is a wheel design where the outer nodes communicate with one or two other outer nodes in addition to the hub. A wheel configuration is common for a financial or economic network.





All-Channel

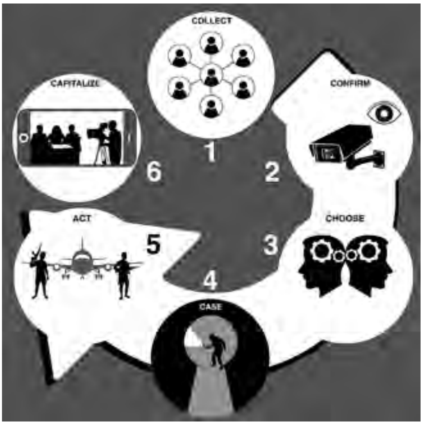
All nodes are connected to each other. The network is organizationally "flat," meaning there is no hierarchical command structure above it. Command and control is distributed within the network. This is communication intensive and can be a security problem if the linkages can be identified or reconstructed. However, the lack of an identifiable "head" confounds the targeting and disrupting efforts normally effective against hierarchies.



VIII. Plan & Action Cycle

Ref: TC 7-100.3, Irregular Opposing Forces (Jan '14), pp. 6-3 to 6-7.

Criminal and terrorist organizations, indeed most hybrid threat actors, predicate their plan and action (P&A) cycle on functions. Function can be defined as a task or role natural to an individual for specified outcome. That is, hybrid threats task individual or unit capabilities toward intended outcomes for each tactical mission.



There is no universal model for the P&A cycle, but hybrid threats tend to mimic the success of crime cartels. The criminal P&A cycle has been elaborated upon by Hollywood movies since Scarface (1932) up to more recent films such as the Ocean's Eleven (2001) series blockbusters. Moreover, the criminal P&A cycle has been the subject of scholarly studies in justice since the 1960s. A trending pattern of the criminal P&A cycle can be discerned.

Criminals do not move randomly through their environment. On the contrary, target selection, planning, and action templates produce clear spatial patterns. Commission of a criminal or terrorist act is the end result of a multistage decision process that seeks out and identifies, within the general environment, a target. The target can be defined as an asset or victim positioned in time and space.

1. Collect

Criminals and terrorists collect intelligence through direct observation or associated networks to conduct a broad target analysis. These groups use cues from the environment, or a network of informants and collaborators, to locate and identify multiple targets. Each target is assessed for its suitability and feasibility towards achieving expressed operational or strategic objectives.

2. Confirm

Criminals and terrorists confirm intelligence on identified targets through surveillance. Additionally, they will confirm the availability of tactical assets brought to bear for each target. The target generates many signals or cues about its physical, spatial, cultural, legal, and psychological characteristics. How will the breach be achieved? Is an "insider" available, or can the security forces or police be bribed? Can the direct action unit obtain uniforms to mimic employees?

I. Criminal Characteristics & Motivations

Ref: TC 7-100.3, Irregular Opposing Forces (Jan '14), chap. 4.

Criminal elements exist at every level of society and in every operational environment (OE). Their presence, whatever their level of capabilities, adds to the complexity of any OE. They may be intertwined with irregular forces and possibly with regular military and/or paramilitary forces of a nation-state. However, they may also pursue their criminal activities independent of such other actors.

I. Characteristics

Some individuals, groups, and activities are criminal or illegal only because they violate laws established by a recognized governing authority. Others may violate moral or ethical standards of a given society or of the international community.

Note. In some OEs, the threat is more criminal than military or paramilitary in nature. Insurgents, guerrillas, or other armed groups often use or mimic established criminal enterprises and practices to move contraband, raise funds, or otherwise further their goals and objectives.

Criminal activity is a category of violence that is enmeshed in the daily life of most people in both urban and rural areas. However, criminal activity thrives in areas where there is instability and lack of government control or law enforcement. The actions of insurgents and guerrillas further erode stability and effective governance, creating more opportunities for criminal pursuits. Sometimes, given those opportunities, insurgent or guerrillas themselves turn to crime—either to sustain themselves or for personal profit. It may be difficult to distinguish crime from ethnic feuds, ideological and theological extremism, or other elements of a culture that incite insurgency or guerrilla warfare.

Governing authorities often characterize insurgents and guerrillas as "bandits." The reason for this is that their activities in opposing the governing authority and sustaining themselves are illegal (from the government perspective). Acts of subversion may be against the law (that is, criminal) even if not violent.

II. Scope of Operations

Criminal organizations are normally independent of nation-state control. Large-scale organizations often extend beyond national boundaries to operate regionally or worldwide. Large-scale organizations may have the capability to adversely affect legitimate political, military, and judicial organizations. However, individual criminals or small-scale criminal organizations (gangs) typically do not. Still, any criminal organization can affect such government organizations and/or military operations by becoming affiliated with the irregular OPFOR or with military forces of another nation-state.

Unless a criminal organization is in league with government officials, it must operate in ungoverned or poorly governed areas. Otherwise, the governing authority would interfere with the criminal activity. In today's world, the ungoverned area may be virtual—in the Internet and cyberspace. Criminal organizations can draw on virtual sanctuaries such as websites, chat rooms, and blogs.

Criminal organizations desire a space where they can conduct their activities unconstrained by a government. They may seek to create or maintain a region where there is no governmental control or only governmental control that they can co-opt.

Such an area allows them sufficient latitude to operate and discourage rival criminal enterprises. From this base area, they can generate more and more violence and instability over wider sections of the political map.

Some criminal organizations can generate instability and insecurity within a state or across borders. They can become partners with insurgents in order to further their criminal ends. A criminal organization takes on the characteristics of an insurgency when it uses subversion and violence to negate law enforcement efforts. Some criminal organizations may seek to co-opt political power through corruption and intimidation. The more they seek freedom of action, the more they inhibit state sovereignty. A criminal organization may create its own form of "government" by providing protection and enforcing its will on the populace. If it can challenge the governing authority's control beyond the local level of government, it in effect becomes an insurgency unto itself, although its ends are materially focused rather than ideological.

III. Relations with Other Organizations and Actors

Criminal organizations may have some type of relationship with guerrilla and/or insurgent organizations or other actors, based on similar or shared goals and/or interests. The nature of the shared goal or interest determines the tenure and type of relationship and the degree of affiliation. Any affiliation depends on the needs of the criminal organization at a particular time. To criminals, any cooperation with other actors is viewed through the lens of profitability. They may actually oppose other actors whose activities degrade their criminal enterprises.

Note. Criminals and criminal organizations, both armed and unarmed, may be considered noncombatants as long as they are neutral. However, they may be considered as combatants if they become affiliated with regular military or irregular forces. In the latter case, they can be considered part of the irregular OPFOR.

Irregular Forces

By mutual agreement, or when their interests coincide, criminal organizations may become affiliated with insurgents and/or guerrillas controlling and operating in the same area. Such allies can provide security and protection against government forces or other common enemies. They can also provide support to the criminal organization's activities. In exchange, the criminal organization may provide financial assistance, advanced technologies, or weapons.

Mutual interests of criminals, insurgents, and/or guerrillas can include preventing extraregional or local government forces from interfering in their respective spheres. The amount of mutual protection depends on the size and sophistication of each organization and its level of influence on the government or the local population.

On behalf of a criminal organization, insurgents or guerrillas can conduct—

- Diversionary actions.
- Reconnaissance and early warning.
- Money laundering.
- Smuggling.
- Transportation.
- Civic actions.

Criminal organizations may not be part of an insurgency. However, their activities—such as theft, hijackings, kidnappings, and smuggling—can further undermine the governing authority. Insurgent organizations often link themselves to criminal networks to obtain funding and logistics support. In some cases, insurgent networks and criminal networks become indistinguishable. Many insurgent organizations are

Transnational Organized Crime (DNI Worldwide Threat Assessment 2022)

Ref: Office of the Director of National Intelligence, Annual Threat Assessment of the US Intelligence Community (Feb '22), pp. 23-24.

Global transnational criminal organizations (TCOs) pose a direct threat to the United States through human trafficking, the production and trafficking of lethal illicit drugs, cyber crime, and financial crimes and money laundering schemes eroding the integrity of the international financial system. Cyber criminals, in addition to phishing and other online fraud schemes, are also increasing their ransomware attacks. TCO activities also indirectly threaten U.S. national security by compounding and aggravating corruption, violence, and challenges to governance that undermine the rule of law in partner nations, spurring violence, driving atrocities, and contributing to migration.

- Human trafficking, including sex trafficking and forced labor, is not only a violation of human rights and freedoms but a threat to U.S. national security and economic development and is enabled by corrupt actors and networks that fuel the growth of transnational organized crime.

Foreign Illicit Drugs. Illicit drug trafficking by TCOs, particularly synthetic drugs, endangers the health and safety of millions of U.S. citizens and imposes as much as one trillion dollars in direct and indirect economic losses. The threat from illicit drugs is at historic levels, with more than 100,000 American drug-overdose deaths for the first time annually, driven mainly by a robust supply of synthetic opioids from Mexican TCOs.

- Mexican TCOs are the dominant producers and suppliers of illicit drugs for the U.S. market. They produce fentanyl, heroin, methamphetamine, and marijuana in Mexico, and obtain cocaine from South America to smuggle into the United States. Mexican TCOs probably will seek to continue expanding their capacity to produce finished fentanyl.
- Since 2019, Mexican TCOs have shifted from importing finished fentanyl from China to synthesizing fentanyl from precursor chemicals, primarily also from China, partly because of China's fentanyl class controls. Mexican TCOs are able to circumvent international controls on precursor chemicals by changing analogues and methodologies for synthetizing and producing synthetics.
- Turf battles among Mexican TCOs vying for drug routes and territory have resulted in steady, high homicide rates since 2018 that are four times the rate of homicides in the U.S.

Money Laundering and Financial Crimes. TCOs exploit the U.S. financial, services, and manufacturing sectors by conducting complex money laundering and fraud schemes.

- TCOs generate hundreds of billions of dollars of revenue by trafficking illicit drugs and other goods and people; conducting extortion and racketeering that targets U.S. persons; producing and selling counterfeit and stolen goods in U.S. markets; and running financial fraud schemes.

Cyber Crime. Transnational cyber criminals are increasing the number, scale, and sophistication of ransomware attacks, fueling a virtual ecosystem that threatens to cause greater disruptions of critical services worldwide. These criminals are driven by the promise of large profits, reliable safe havens from which to operate, and a decreasing technical barrier to entry for new actors.

- Many major transnational cybercrime groups have diversified business models that engage in direct wire-transfer fraud from victims, or use other forms of extortion alongside or in place of ransomware. In 2020, business-e-mail compromise, identity theft, spoofing, and other extortion schemes ranked among the top five most costly cybercriminal schemes.

U.S. Government entities, businesses, and other organizations face a diverse range of ransomware threats. Attackers are innovating their targeting strategies to focus on victims whose business operations lack resilience or whose consumer base cannot sustain service disruptions, driving ransomware payouts up.

Most criminal networks are loosely structured and function primarily because each participant is pursuing his own interests. Such a network is not necessarily a formally structured, hierarchical organization with one individual controlling and running the operation. Rather, it may be a loose-knit, intricate web of individuals or groups selected for their particular skills. Even when there are strong vertical links, there can still be a great deal of autonomy among the numerous small gangs that make up the network.

These criminal networks use violence as a means to create and protect their market as well as marginalize and control their competition. They seek to control or weaken state security institutions. They often begin to dominate community life within large areas of a nation-state. Criminal groups at this level may begin to develop overtly political agendas to improve their market share.

Criminal networks that control local or regional markets may have ties to and frequently do business with criminal organizations in other regions or other countries. They do so when they need wider networks of customers, fences, money-laundering expertise, access to technologies, and other essentials for an effective criminal venture.

Some criminal networks may develop into larger criminal networks or into transnational criminal organizations. In some cases, a smaller network may simply grow into a larger organization. In other cases, several networks may willingly join to form a larger organization. In still other cases, smaller organizations may be forced (by coercion or by circumstances) to become part of a larger organization.

III. Transnational Criminal Organizations

Some criminal organizations develop into sophisticated transnational criminal organizations. These organizations may have ambitious economic and political agendas. They often begin to fill the power vacuum in ungoverned or poorly governed regions within a nation-state and to challenge government control of other regions. This provides the transnational organization with security and freedom of movement to pursue its criminal enterprises. In some cases, the organization becomes a de facto insurgency with ends focused on the material rather than ideological goals. Actions can include any or all of the items listed under "Criminal Activities" later in this chapter—such as drug and arms trafficking, money laundering, and terrorism. Transnational criminal organizations develop their own transit routes for illegal shipments and develop their own access to contraband.

Transnational criminal organizations take advantage of increased opportunities for profit and power that are found internationally. Globalization is not limited to legal trade and commerce. Criminals in various countries can cooperate in criminal ventures that take place across several countries. The increasing ease and effectiveness of global communications plays a significant role in arranging criminal ventures and in laundering the proceeds.

For example, smuggling is a big business that requires international organization. Illegal substances or legal goods less expensive elsewhere are smuggled across state boundaries. (Drugs are the most lucrative of smuggled items.) A significant part of the profits may go to suppliers and associates in other countries, and profits may be laundered using international financial systems.

Also contributing to the international nature of crime is the increased movement of people across borders. Businesses, both legitimate and illegitimate, benefit from expanding global travel. Another aspect is movement of people forced from their homes by war or political persecution. Others move in order to seek the opportunity to build a better life for themselves and their families. The vast majority of these people are not criminals. However, the size of the movement provides perfect cover for those who are connected to transnational criminal organizations. Some migrants avoid formal channels and pay smugglers to get them into another country.

See p. 5-3 "Transnational Organized Crime" from the Office of the Director of National Intelligence, Annual Threat Assessment (Feb '22).

III. Criminal Activities

Ref: TC 7-100.3, Irregular Opposing Forces (Jan '14), pp. 4-8 to 4-17.

Criminals use many and varied tactics and techniques. Some of these methods overlap with one another. The activities typically include an objective to make fiscal profit and/or achieve influence.

Criminal Activities

- **Security**
- **Theft**
- **Fraud**
- **Racketeering**
- **Gambling**
- **Prostitution**
- **Extortion**
- **Bribery**
- **Arson**
- **Hijacking**
- **Kidnapping**
- **Hostage Taking**
- **Murder**
- **Assassination**
- **Maiming**
- **Smuggling**
- **Money Laundering**
- **Civic Actions**
- **Information Warfare**
- **Trafficking**
- **Cyber Crime**
- **Terrorism**

A. Security

Security is crucial for criminal organizations. They may use the highest degree of sophistication available to conduct intelligence collection and counterintelligence activities. These activities are a priority and can be well funded. Intelligence sources may extend to high levels within government and law-enforcement agencies. The local populace may willingly provide ample intelligence collection, counterintelligence, and security support. Intelligence and security can also be the result of bribery, extortion, or coercion.

Most members of criminal organizations are capable of protecting themselves and their assets. Typically, they carry small-caliber weapons, such as handguns, pistols, rifles, and shotguns. They are lightly armed out of necessity or convenience, not for lack of resources. When greater force of arms is necessary to control people, protect vital resources, or obtain information, these organizations typically have members who can use heavier arms, such as machineguns and assault weapons. Large criminal organizations may hire PSCs to conduct surveillance, provide personal security for leaders, or guard key facilities.

B. Theft

Theft is the taking of another person's property without that person's permission or consent with the intent to deprive the rightful owner of it. Thus, theft is an overarching term that covers various crimes against property such as burglary, embezzlement, larceny, looting, robbery, and fraud. (See also identity theft and intellectual property theft, both under Cyber Crime.)

Chap 6

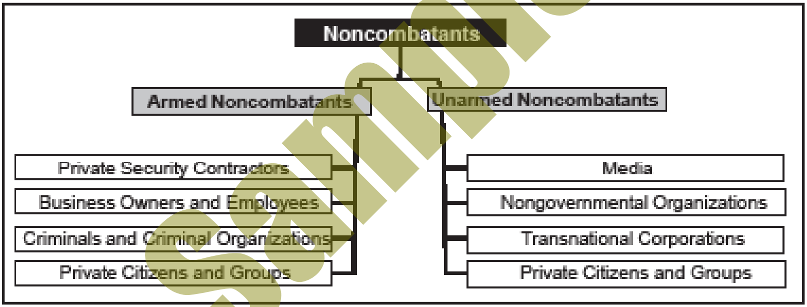
I. Noncombatants (Overview)

Ref: TC 7-100.3, Irregular Opposing Forces (Jan '14), chap. 5.

A host of noncombatants add complexity to any operational environment (OE). The irregular OPFOR attempts to manipulate these noncombatants in ways that support its goals and objectives. Many noncombatants are completely innocent of any involvement with the irregular OPFOR. However, the irregular OPFOR will seek the advantage of operating within a relevant population of noncombatants whose allegiance and/or support it can sway in its favor. This can include clandestine yet willing active support (as combatants), as well as coerced support, support through passive or sympathetic measures, and/or unknowing or unwitting support by noncombatants.

I. General Characteristics

Noncombatants are persons not actively participating in combat or actively supporting of any of the forces involved in combat. They can be either armed or unarmed. Figure 5-1 shows examples of these two basic types of noncombatants that can be manipulated by the irregular OPFOR. These examples are not all-inclusive, and some of the example entities can be either armed or unarmed.


Noncombatants
Armed Noncombatants
Unarmed Noncombatants
Private Security Contractors
Business Owners and Employees
Criminals and Criminal Organizations
Private Citizens and Groups
Media
Nongovernmental Organizations
Transnational Corporations
Private Citizens and Groups

Ref: TC 7-100.3 (Jan '14), fig. 5-1. Armed and unarmed noncombatants (examples).

Note. From a U.S. viewpoint, the status of noncombatants is typically friendly, neutral, or unknown. Conversely, the noncombatants would view U.S. and/or local governing authority forces as friendly or neutral in regard to themselves. For the sake of consistency throughout the chapters of this TC, however, this chapter occasionally refers to the governing authority and associated U.S. or coalition forces as "enemy," referring to the enemy of the irregular OPFOR.

Aside from military and paramilitary forces, the civilian population of a nation or region is often the single most important aspect of an OE. This situation can be further complicated by the presence of other noncombatants who are not indigenous to the country or region.

II. Relation to the Irregular OPFOR

The irregular OPFOR recognizes that noncombatants living and/or working in an area of conflict can be a significant source of—

- Intelligence collection.
- Reconnaissance and surveillance.
- Technical skills.
- General logistics support.

II. Armed Noncombatants

Ref: TC 7-100.3, Irregular Opposing Forces (Jan ‘14), pp. 5-3 to 5-7.

In any OE, there are likely to be nonmilitary personnel who are armed but are not part of an organized paramilitary or military structure. Nonetheless, such people may be disgruntled and hostile to the governing authority or forces that support it. Armed noncombatants may represent a large portion of the undecided citizens in a population. Some of these nonaffiliated people may possess small arms legally to protect their families, homes, and/or businesses. Some may use weapons as part of their occupation (such as hunters, security guards, or local police). Some may be minor criminals who use their weapons for activities such as theft or extortion. Given the fact that they are already armed, it would be easy for such noncombatants to become combatants. Any number of reasons, including prejudices and grievances, can cause them to choose sides or change sides. They may switch allegiances repeatedly as circumstances evolve.

Some armed noncombatant entities can be completely legitimate enterprises. However, some activities can be criminal under the guise of legitimate business. The irregular OPFOR can embed operatives in legitimate commercial enterprises or criminal activities to obtain information and/or capabilities not otherwise available to it. Actions of such operatives can include sabotage of selected commodities and/or services. They may also co-opt capabilities of a governing authority infrastructure and civil enterprises to support irregular OPFOR operations.

Examples of armed noncombatants commonly operating in an OE are—

- Private security contractor (PSC) organizations.
- Local business owners and employees.
- Private citizens and private groups authorized to carry and use weapons.
- Criminals and/or organizations with labels such as cartels, gangs.
- Ad hoc local “militia” or neighborhood watch programs.

I. Private Security Contractors (PSCs)

Private security contractors (PSCs) are commercial business enterprises that provide security and related services on a contractual basis. PSCs are employed to prevent, detect, and counter intrusions or theft; protect property and people; enforce rules and regulations; and conduct investigations. They may also be used to neutralize any real or perceived threat. PSCs can act as an adjunct to other security measures and provide advisors, instructors, and support and services personnel for a state’s military, paramilitary, and police forces. They may also be employed by private individuals and businesses (including transnational corporations).

PSCs may be legitimate, well-respected corporations providing contract advisors and employees as part of a military nation-building program funded by a foreign government. A PSC that provides services on a contract basis outside its country of origin also falls into the category of a transnational corporation. Other PSCs may be domestic firms that supply contract guard forces. In its simplest form, a PSC might be a local citizen organization that performs actions on a short-term contractual basis.

See following pages (pp. 6-4 to 6-5) for an overview and discussion of PSC functions.

A. Private Security Contractor Functions

Ref: TC 7-100.3, Irregular Opposing Forces (Jan '14), pp. 5-6 to 5-7.

Most functions of a PSC involve protecting personnel, facilities, or activities. Such security functions normally require armed contractors. However, PSCs can also perform other, security-related functions that do not require armed personnel.

Armed Functions

Functions typically requiring armed personnel can include—

- Personal security details to protect a person or group of people.
- Guard protection of static sites (such as housing areas, building sites, government complexes, and businesses—both legal and illegal).
- Transport security support to convoys and special materiel shipments.
- Security escorts.
- Cash transport.
- Covert operations.
- Surveillance.
- Intelligence services.
- Advising and/or training of indigenous or extraregional security forces.
- Operations and administration within governing authority prisons and/or detention facilities.

Unarmed Functions

Functions typically not requiring armed personnel include—

- Unarmed security functions when presence is deemed an appropriate deterrent.
- Air surveillance.
- Psychological warfare.
- Intelligence support (including information collection and threat analysis).
- Operational coordination (such as command and control, management, and communications).
- Personnel and budget vetting.
- Hostage negotiation services.
- Risk advisory services.
- Weapons procurement.
- Weapons destruction.
- Transportation support.

Advantages and Disadvantages

PSCs provide key capabilities and can often be hired quickly and deployed faster than a military force with similar skill sets. This flexibility allows governmental or commercial organizations to adapt quickly to a rapidly changing OE. Employing a PSC can keep military forces available to conduct traditional or specialized military missions.

Evolution of private sector military-like services by corporations can be a very influential factor in international and regional diplomacy. Although coalition operations may appear in need of services from PSC, governmental authorities and private citizen groups can be concerned on the level of PSC transparency and accountability when high-profile incidents occur that involve PSCs.

V. Dislocated-Civilian Operations

Ref: ATP 3-57.10, Civil Affairs Support to Populace and Resources Control (Aug '13).

The term dislocated civilian, or DC, refers to several categories of civilians, such as a displaced person, an evacuee, an internally displaced person, a migrant, a refugee, or a stateless person. Legal and political considerations define these categories. DCs are removed from or leave their homes or places of habitual residence for reasons such as fear of persecution or to avoid the effects of armed conflict, situations of generalized violence, violations of human rights, natural or man-made disasters, or economic privation. Categories of DCs include—

- **Displaced person**. A broad term used to refer to internally and externally displaced persons collectively (JP 3-29, Foreign Humanitarian Assistance).
- **Refugee**. A person who owing to a well-founded fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group or political opinion, is outside the country of his or her nationality and is unable or, owing to such fear, is unwilling to avail himself or herself of the protection of that country (JP 3-29).
- **Evacuee**. A civilian removed from a place of residence by military direction for reasons of personal security or the requirements of the military situation (JP 3-57, Civil-Military Operations).
- **Stateless person**. A person who is not considered as a national by any state under the operation of its law (JP 3-29).
- **War victim.** A classification created during the Vietnam era to describe civilians suffering injuries, loss of a family member, or damage to or destruction of their homes because of war. War victims may be eligible for a claim against the United States under the Foreign Claims Act.
- **Internally displaced persons**. Any person who has been forced or obliged to flee or to leave their home or places of habitual residence, in particular as a result of or in order to avoid the effects of armed conflict, situations of generalized violence, violations of human rights or natural or manmade disasters, and who have not crossed an internationally recognized state border (JP 3-29).
- **Migrant**. A person who (1) belongs to a normally migratory culture who may cross national boundaries, or (2) has fled his or her native country for economic reasons rather than fear of political or ethnic persecution (JP 3-29).
- **Returnee**. A displaced person who has returned voluntarily to his or her former place of residence (JP 3-29).
- **Resettled person**. A refugee or an internally displaced person wishing to return somewhere other than his or her previous home or land within the country or area of original displacement (JP 3-29).

DC operations (also commonly referred to as resettlement operations) pertain to those actions required to move civilians out of harm's way or to safeguard a displaced population in the aftermath of a disaster. The disaster may be natural, as in a flood or an earthquake, or man-made, as in combat operations, social or political strife, or a hazardous material emergency, such as a chemical, biological, or radiological spill. DC operations may occur across the range of military operations or be the focus of a limited contingency operation, such as FHA.

Typically, the UN or other IGOs and NGOs build and administer DC camps, if needed, and provide basic assistance and services to the affected population. However, when the U.S. military is requested to provide support, DC support missions may include camp organization (basic construction and administration); provision of care (food, supplies, medical treatment, and protection); and placement (movement or relocation to other countries, camps, and locations).

III. Unarmed Noncombatants

Ref: TC 7-100.3, Irregular Opposing Forces (Jan '14), pp. 5-7 to 5-16.

Other actors in an OE include unarmed noncombatants. These nonmilitary actors may be neutral or potential side-changers in a conflict involving the irregular OPFOR. Their choice to take sides depends on their perception of who is causing a grievance for them. It also depends on whether they think their interests are best served by supporting the governing authority. Given the right conditions, they may decide to purposely support hostilities against a governing authority that is the enemy of the irregular OPFOR. Even if they do not take up arms, such active support or participation moves them into the category of unarmed combatants. (See the section on Unarmed Combatants at the end of this chapter.)

Some of the more prominent types of unarmed noncombatants are—

- Media personnel.
- Nongovernmental organizations (NGOs).
- Transnational corporations and their employees.
- Private citizens and groups.

However, unarmed noncombatants may also include internally displaced persons, refugees, and transients. They can also include foreign government and diplomatic personnel present in the area of conflict.

I. Media Personnel

An area of conflict attracts a multitude of media personnel. This includes local, national, and international journalists, reporters, and associated support personnel. They may be independent actors or affiliated with a particular news organization.

Capabilities and Vulnerabilities

The media can be a credible source of current information for multiple actors in an OE. News cycles demand timely information and near-simultaneous reporting on current events. The irregular OPFOR recognizes the value of media coverage of significant incidents. This coverage can draw attention to irregular OPFOR successes or highlight failures or missteps by its enemies. The irregular OPFOR can exploit media coverage to attack the will and resolve of—

- Its enemies' regular military and internal security forces.
- The governing authority.
- A relevant population.

Media coverage of operations can dramatically affect international relations and strategic interaction.

The irregular OPFOR may closely observe media personnel. This surveillance can identify character flaws or weaknesses of personnel the irregular OPFOR can co-opt to the advantage of its INFOWAR activities. Although media personnel may seek to remain objective and report accurately, they can be coerced or persuaded to promote an irregular OPFOR perspective. The irregular OPFOR uses threats, extortion, and/or physical violence to minimize media coverage that is counter to its interests. Some media representatives who support irregular OPFOR motives may purposely distort information to support irregular OPFOR objectives.

The balancing effect of multiple reporting sources tends to reduce the impact of any one source with overt bias. The irregular OPFOR recognizes that democracies with freedom of the press and widespread access to media and other information systems can be less susceptible to INFOWAR. However, the international public and foreign governments are still susceptible to how the irregular OPFOR presents its agenda to a global audience.

Exploiting Media Access

The pervasive presence of the media provides access to information that might not otherwise be available to the irregular OPFOR. The irregular OPFOR can use the physical access allowed to media representatives to enhance its intelligence collection, information analysis, and consequent actions. Some members of the irregular OPFOR or individuals who support them may be able to pass themselves off as independent reporters or embed themselves in a media team under the guise of functional media expertise. Media credentials can be easily counterfeited. The embedding may take place with or without the knowledge of a sponsoring media organization. This may enable them to access plans and monitor operations of the governing authority or regular military forces with which the irregular OPFOR is in conflict.

Relationship to OPFOR Public Relations

Like media affairs, OPFOR public relations involve focused efforts to understand and engage key audiences of a relevant population. Their purpose is to create, strengthen, or preserve conditions favorable for the advancement of OPFOR interests, policies, and objectives. They accomplish this through the use of coordinated programs, plans, themes, messages, and products synchronized with all regular OPFOR and irregular OPFOR actions.

Public relations are part of the perception management element of INFOWAR. In an expanding INFOWAR campaign, the irregular OPFOR seeks partners within the specific OPFOR AOR and regional and/or global supporters. When external states provide overt and/or covert support, the irregular OPFOR provides appropriate public relations guidance on how to portray or hide such support.

A significant audience external to an irregular OPFOR AOR can be the diaspora of a relevant population. INFOWAR and public opinion are critical to obtaining diaspora support and keeping the struggle of guerrillas and/or insurgents in the spotlight of globalized media.

II. Nongovernmental Organizations (NGO)

A nongovernmental organization (NGO) is a private, self-governing, not-for-profit organization dedicated to alleviating human suffering; promoting education, health care, economic development, environmental protection, human rights; supporting conflict resolution; and/or encouraging establishment of democratic institutions and civil society (JP 3-08). NGOs are likely to be present in any OE.

A. Variety of Types

The global community of NGOs includes a wide variety of organizations that are independent, diverse, and flexible. They differ greatly in size, resources, capabilities, expertise, experience, and missions. An NGO may be local, national, or transnational. It may employ thousands of individuals or just a handful. It may have a large management structure or no formal structure at all. It may be a large organization with a huge budget and decades of global experience in developmental and humanitarian relief or a newly created small organization dedicated to a particular emergency or disaster. NGOs are involved in such diverse activities as education, technical projects, relief activities, refugee assistance, public policy, development programs, human rights, and conflict resolution.

Chap 7

I. Foreign Security Force (FSF) Threats

Ref: ATP 3-37.15, Foreign Security Force Threats (Jan '20), chap. 1.

The foreign security force (FSF) threat is not a new phenomenon; however, during recent limited contingency operations, U.S. forces experienced a sharp increase in the number of attacks perpetrated by FSFs. This chapter introduces the FSF threat by exploring its context, causation, and methods. It also facilitates shared understanding and dialogue by defining relevant terms. Armed with this knowledge, Soldiers and leaders will be better positioned to properly implement the threat prevention and defeat techniques described in subsequent chapters.

I. Foreign Security Force Threat Characteristics

A FSF threat is the potential for violence posed by FSFs working with, or granted access to, U.S. Service members, civilians, or contractors. An FSF threat attack is a violent act perpetrated against a U.S. Service member, civilian, or contractor by a FSF member or members who have access to U.S. Service members, civilians, or contractors. Foreign security forces are those forces, including, but not limited to military, paramilitary, police, and intelligence forces; border police, coast guard, and customs officials; and prison guards and correctional personnel, that provide security for a host nation and its relevant population or support a regional security organization's mission (FM 3-22). FSFs may belong to the host-nation government, belong with a paramilitary organization, or consist of a third party's contribution to a multinational operation. When operating in an expeditionary, multi-partner environment, the potential for a violent attack by FSFs increases significantly since they operate alongside U.S. Service members and civilians. This threat has proven particularly challenging during protracted limited contingency operations in which U.S. forces work with FSFs to stabilize a fragile state by advising and assisting its security or police forces.

Often referred to as green-on-blue violence or an inside the wire attack, FSF attacks are characterized by speed, surprise, shock, opportunity, and violence. The attacks often occur quickly and without warning intending to shock both local security forces and a wider audience through their brazen nature. The opportunity for these attacks exists once FSFs have access to U.S. forces or facilities and can operate closely with them.

Whether successful or not, FSF attacks seek to directly kill or injure U.S. Service members or civilians. These attacks can take many forms such as assassinations, mass shootings, suicide bombings, and vehicle-borne improvised explosive device (also called VBIED) attacks. Often notable for their brazen and irrational nature, attackers show little regard for their own safety or the threat of capture.

An attacker often has intended victims and will seek them out during an attack. However, attackers will also accept targets of opportunity and will likely continue the attack after finding intended victims. As such, an attacker will often continue attacking throughout buildings or compounds until stopped by U.S. forces, FSFs, or suicide.

FSF attacks generally target U.S. forces during periods of perceived security. Attackers often intend to use the element of surprise to exploit vulnerable Soldiers and maximize lethality. Attacks often occur at locations where U.S. Service members believe they are safe and have little reason to expect an enemy attack. Potential locations for FSF attacks include U.S. or FSF bases, host-nation government build-

II. FSF Threat Prevention & Response

Ref: ATP 3-37.15, Foreign Security Force Threats (Jan '20), chap. 2.

The FSF threat prevention and response framework consists of five functions: prevent, deter, defeat, exploit, and recover. Prevention and deterrence occur continuously, whereas the defeat, exploit, and recover functions occur once a threat evolves into an attack. Each function includes several components that, when applied in concert, better position the unit to prevent and respond to an FSF threat.

FSF Threat Prevention & Response Framework

I **Prevent**

II **Deter**

III **Defeat**

IV **Exploit**

V **Recover**

Prevention and deterrence are complementary functions that occur throughout operations. Prevention consists of the internal processes and behaviors employed by units to increase threat awareness and reduce the likelihood of an attack. Deterrence includes the active measures employed by a unit to discourage a potential attacker from acting and, should an attack occur, to reduce the consequences of the attack. Distinguishing between the two is a matter of perspective. Prevention should be understood from a unit or Soldier perspective; it consists of the behaviors, TTP, and practices designed to preclude an attack by inhibiting the emergence of a threat. Deterrence is best understood from an attacker's perspective. What practices will make FSF threats believe their attack will fail? This internal and external construct enables a comprehensive approach to threat prevention.

Conversely, the defeat, exploit, and recover functions occur sequentially. Defeat consists of the immediate response procedures executed to neutralize an attack and restore local security. The exploit function is transitional and consists of actions to collect information about the attack, consolidate lessons learned, and share this information with other units. Effective Soldiers apply lessons learned to prevent, deter, and defeat future threats. Exploitation and recovery may occur simultaneously; however, they serve different purposes. The recover function consists of the steps taken to regain trust and cohesion with the partnered FSF, resume pre-attack operations, and manage the wider consequences of an attack.

FSF Threats

Jordanian Soldier Kills Three U.S. Soldiers

In November 2016, three U.S. Soldiers were shot and killed by a Jordanian soldier as their vehicle approached the entry control point at the King Faisal Airbase in southern Jordan. The Soldiers were returning to the base in a four-vehicle convoy after completing a training mission as part of the U.S. effort to defeat the Islamic State in Iraq and Syria. The attacker, Marik al-Tuwayha, claimed he believed the convoy presented a threat; however, in video footage recovered from the scene he is seen reloading his weapon after the Americans identified themselves as friendly. Although his motive was unclear, al-Tuwayha was found guilty of voluntary manslaughter, violating military orders, and insulting the dignity and reputation of the Jordanian armed forces. In July 2017 he received a life sentence.

This incident is an important reminder that foreign security force (FSF) threats are not limited to counterinsurgency or stability operations and can occur anytime U.S. forces partner closely with FSFs. This includes during operations to shape or prevent, where an enemy may exploit the perceived lack of an active threat to surprise U.S. forces.

III. Causation

The Army uses six categories to classify FSF attacks: personal, ideological, reactionary, criminal, enemy, and general. These categories assist in understanding the motives behind FSF attacks and can aid in detecting a potential threat. The categories are not mutually exclusive, and an attack can often be classified in two or more categories at once. For example, an FSF member may have a dispute with a U.S. Service member (personal) while simultaneously beginning to sympathize with an extremist organization and its cause (ideological). There are many reasons why FSFs may decide to attack; however, they are usually motivated by a trigger that falls into one of the categories listed below.

Causation

A **Personal**

B **Ideological**

C **Reactionary**

D **Criminal**

E **Enemy**

F **General**

II. FSF Threat Training Program

Ref: ATP 3-37.15, Foreign Security Force Threats (Jan '20), chap. 3.

This chapter provides guidance for incorporating FSF threat prevention and response techniques into unit training programs. The techniques offered can be incorporated into unit training before or during a deployment requiring close cooperation with FSFs.

I. Training to Prevent

Commanders are responsible for ensuring units conduct FSF threat prevention training. FSF threat prevention training includes personnel selection and cultural awareness training.

A. Personnel Selection

Training to prevent the FSF threat begins with assessing and selecting appropriate personnel to partner with FSFs. Many FSF attacks stem from personal disputes, cultural animosity, or disagreements between FSF and U.S. Service members. Because of this, Soldiers who work closely with FSFs should be mature, possess strong interpersonal communications skills, have high emotional intelligence, and demonstrate patience when working with peers and teammates. Soldiers working alongside FSFs need to possess conflict resolution skills and the cultural adaptability to operate in a multi-partner environment. Culturally adaptable Soldiers demonstrate awareness, interaction, skillful rapport-building, respectfulness, self-reflection, and self-control.

B. Cultural Awareness Training

Training to prevent includes cultural awareness training. Cultural misunderstandings may result in grievances that, if combined with other tensions, can lead to an attack. Commanders can mitigate these tensions by conducting cultural awareness and sensitivity training before and during deployment.

II. Training to Deter

Units train to deter an FSF attack by developing and rehearsing TTP, SOPs, and battle drills that make the unit difficult to attack and demonstrate to a potential attacker the unlikelihood of carrying out a successful attack. Training to deter promotes a culture of vigilance and discipline within the unit and ensures Soldiers can identify and mitigate a threat before the unit is compromised. As such, this training reinforces the Soldier's ability to detect and respond to a threat without ceding initiative to the enemy. Training to deter consists of detection, escalation of force, and biometric toolkit training.

A. Detection

The threat of detection is a strong deterrent; attackers may be unwilling to follow through with an attack if they believe it will be unsuccessful or costly. Training to detect consists of instructing Soldiers on the environmental, physiological, and behavioral indicators of an FSF threat and then challenging them to identify, communicate, and rapidly react to those indicators in accordance with the unit's TTP, SOPs, and battle drills.

Training to identify potential threat indicators is an important step in detecting FSF threats. Incorporating indicators into live training environments enhances Soldiers' abilities to identify an FSF threat. Effective leaders brief role players on these indicators and include role players in exercises conducted at combat training centers and mobilization training centers prior to deployment.

Training to detect includes detecting counterfeit credentials. Leaders train Soldiers to recognize FSF badging and access credentials, so Soldiers can quickly recognize inauthentic or unauthorized badges. Trained Soldiers can identify FSF uniforms and ranks as well as render the proper customs and courtesies due senior ranking FSF members.

B. Escalation of Force

Although all Soldiers generally receive escalation of force training, because of their requirement to continually assess, identify, and defeat potential threats, this skill is especially important for Soldiers performing duties on a security force or as guardian angels. Escalation of force measures provide Soldiers with an actionable framework for discerning and neutralizing a threat. Generally, once a perceived threat is identified, Soldiers employ escalation of force measures that progress from audible and visual warnings, through less-than-lethal force to lethal force until the threat is neutralized. Escalation of force training consists of classroom instruction and situational training exercises that require Soldiers to identify and react to threats in accordance with the prescribed escalation of force measures. During escalation of force training, trainers vary the threat so that Soldiers are required to both progress through each of the steps and, at times, escalate rapidly through the steps to address a significant threat. Units conduct escalation of force training before and during deployments and often include it in pre-mission briefs and rehearsals. Table 3-1 presents a basic threat detection and neutralization framework that can be used in conjunction with escalation of force measures to stop a threat. However, commanders ensure Soldiers are trained on the rules for the use of force and escalation of force measures applicable to the theater in which they operate.

Threat Detection and Neutralization

Step	*Action*
Identify the threat.	Visually scan foreign security forces (FSFs) looking for concealed weapons, odd mannerisms, and demeanor. Start with the hands and move up and down the body. Scan for bulky protrusions or odd shapes concealed under clothing.
Stop the threat.	If a threat is detected, begin with a verbal warning and then use escalation of force to stop their movement and gain time and space.
Disarm and search the threat.	If possible, have other FSFs disarm and search the suspected individual for concealed weapons or explosives. United States forces should observe this search and provide armed overwatch to ensure thoroughness and security.
Verify identity.	Trusted FSF leadership verify the suspected individual's identity. Verify security badges for authenticity and authorization to access the facility.
Communicate.	Disseminate updates about the security situation to the patrol and request additional support if necessary.
Neutralize the threat.	If the suspected individual refuses to comply with commands, act decisively to neutralize the threat. In accordance with rules for the use of force, the law of land warfare, and the rules of engagement, apply the lowest level of force necessary to stop the threat.

Ref: OPF4, (Jan '21), table 3-1. Threat detection and neutralization.

To properly conduct escalation of force, Soldiers are trained and proficient with common host-nation and FSF key words and phrases. Commanders can use interpreters, HNSF, and FSFs to assist in teaching and rehearsing common words and phrases necessary for Soldiers to conduct basic escalation of force.

C. Biometric Toolkit Training

When leaders train Soldiers to detect, they include training on biometric toolkits and devices. Soldiers use these devices in theater to enroll and screen enemy fighters, FSFs, and local contractors in threat databases.

II. Types of Offensive Action

Ref: TC 7-100.3, Irregular Opposing Forces (Jan '14), pp. 7-3 to 7-24.

Insurgents and guerrillas can employ some of the types of offensive action also used by smaller tactical units of the regular OPFOR. Such actions can include—

- Ambush.
- Assault.
- Raid.
- Reconnaissance attack (guerrillas only).

Insurgent cells typically do not have sufficient combat power to conduct a reconnaissance attack.

Irregular OPFOR leaders and commanders select the offensive action best suited to accomplishing their mission. Insurgent cells and small guerrilla units typically execute one combat mission at a time. Therefore, it would be rare for such a cell or unit to employ more than one type of offensive action simultaneously. However, irregular OPFOR organizations are dynamic and adapt very quickly to the situation. An offensive action may have to make use of whatever cell(s) or unit(s) can take advantage of a window of opportunity.

I. Ambush

An ambush is a surprise attack from a concealed position against a moving or temporarily halted target. In an ambush, the actions of the enemy determine the time, and the irregular OPFOR leader decides on the location. Similar to purposes used by regular military OPFOR, the irregular OPFOR can conduct ambushes to—

- Destroy or capture enemy elements, personnel, and/or designated very important persons.
- Secure supplies.
- Demoralize enemy military forces and officials of a governing authority.
- Delay introduction of international and/or enemy coalition assistance to a governing authority.
- Block enemy movements and/or logistics support.
- Canalize or restrict enemy movement.

The irregular OPFOR can use an ambush as a primary psychological tool in its information warfare (INFOWAR) activities. The psychological effects of ambushes can be enhanced by—

- Conducting recurring ambushes at known areas and/or points where enemy forces must travel.
- Changing the tempo or the number of ambushes to appear unpredictable.
- Attacking targets that were previously considered safe or had not been attacked.
- Using weapons with range capabilities previously not used in an area of conflict.
- Increasing weapons and/or demolitions effects against particular targets.

A common tactic is to conduct an ambush as a means to set up ambush(es) of enemy forces that respond to the original ambush. Multiple and nearly simultaneous ambushes can be conducted along likely avenues of approach to the area of the initial ambush. Ambushes may also target enemy medical treatment and evacuation assets, when irregular OPFOR commanders or leaders decide to not comply with international conventions and law of war norms that regular military forces use. The destruction of means to evacuate and treat wounded can instill a sense of tentativeness in enemy soldiers because they realize that, should they become wounded or injured, medical help may not be forthcoming.

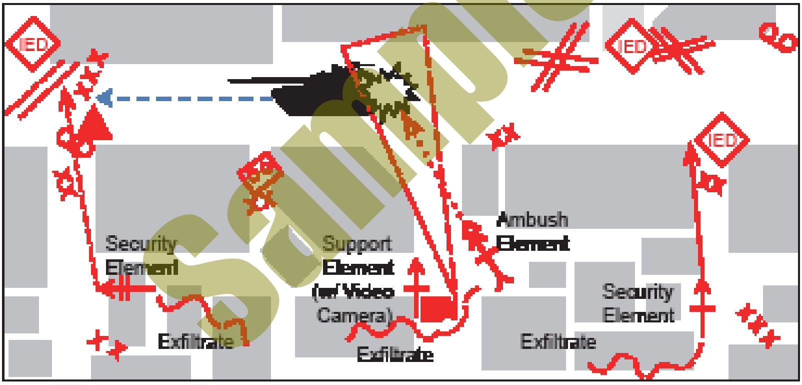
Attacking known points of enemy weakness is a fundamental planning consideration for the irregular OPFOR. Correspondingly, the irregular OPFOR avoids enemy strength.

Surprise and overwhelming massed firepower at a specific place and time provides an expectation of tactical success for the irregular OPFOR. Factors that complement tactical surprise and massed firepower are—

- Detailed plans and rehearsals.
- Selection of ambush positions.
- Rapid and violent conduct of the ambush.
- Disciplined withdrawal of irregular OPFOR elements from the ambush site.

A. Functional Organization for an Ambush

An ambush force is typically organized into three elements: the ambush element, security element, and support element. There may be more than one of each element.



Ref: TC 7-100.3 (Jan '14), fig. 7-1. Insurgent ambush (example).

Ambush Element(s)

The ambush element has the mission of attacking and destroying enemy elements in kill zone(s). Other tasks may include capturing personnel and/or recovering supplies and equipment.

Security Element(s)

The security element has a mission to provide early warning to irregular OPFOR elements of any enemy presence that might disrupt the ambush. Another task can be to protect the ambush element from becoming decisively engaged by enemy forces before, during, or after the ambush.

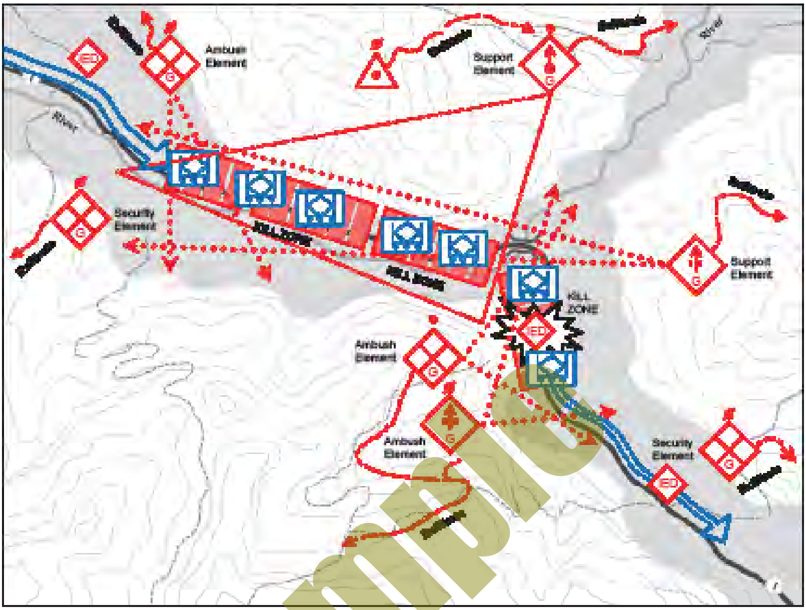
Support Element(s)

The support element can include direct and/or indirect fires and provides general support to improve success of the ambush. The insurgent leader or guerrilla commander typically commands and controls the ambush from the support element. However, he will position himself where he can best command and control.

B. Executing an Ambush

There are three types of ambushes based on the desired mission effects -- annihilation, harassment, or containment. The irregular OPFOR conduct ambushes with a particular purpose that often supports a larger tactical action.

See following pages (pp. 8-8 to 8-9) for further discussion of the three types.



Ref: TC 7-100.3 (Jan '14), fig. 7-1. 7-2. Guerrilla ambush (example).

C. Command and Control of an Ambush

The commander or leader of the ambush force normally positions himself with the support element and designates a subordinate leader to move and maneuver with the ambush element. However, the ambush force commander or leader locates himself where he can best command and control the ambush.

Urban and rural complex terrain provides several tactical advantages to irregular OPFOR ambush, security, and support elements. Operating among indigenous citizens in an urban area or other complex terrain can be used to—

- Observe enemy forces along known canalized routes or areas of reconnaissance and/or avenues of approach or directions of attack.
- Provide for easily camouflaged irregular OPFOR reconnaissance and surveillance activities.
- Provide covered and/or concealed irregular OPFOR routes into and out of the ambush kill zone area.
- Improve irregular OPFOR ambush, security, and support positions with cover, concealment, and camouflage of the natural and manmade tactical environment.
- Encourage deception activities in a relevant civilian population against enemy forces and a governing authority.
- Encourage techniques that employ overlapping direct fires from multiple directions into a designated kill zone.

Types of Ambushes

Ref: TC 7-100.3, Irregular Opposing Forces (Jan '14), pp. 7-6 to 7-7.

There are three types of ambushes based on the desired mission effects--annihilation, harassment, or containment. The irregular OPFOR conduct ambushes with a particular purpose that often supports a larger tactical action.

Annihilation Ambush

The purpose of an annihilation ambush is to destroy an enemy force within a designated kill zone. In addition to massed direct fires, the irregular OPFOR often increases the lethality of a kill zone with indirect fires, manmade obstacles, mines, and/or improvised explosive devices (IEDs) to halt, contain, and kill the enemy force in the kill zone

Note. For guerrilla forces, annihilation ambushes in complex terrain, including urban environments, often involve task-organized hunter-killer (HK) teams.

Irregular OPFOR commanders and leaders may be willing to accept decisive engagement with the enemy in this type of ambush. An annihilation ambush typically emphasizes tactical tasks to—

- Block.
- Contain.
- Destroy.

The ambush and support elements normally remain in their fighting positions until the enemy in the kill zone is rendered combat ineffective. The intent is to destroy enemy personnel and equipment within the kill zone with concentrated firepower.

Once the enemy is destroyed, the ambush element can secure the kill zone and eliminate any remaining enemy in the kill zone. The support element provides overwatch protection to the ambush element when the ambush element is directed to search the destroyed enemy force and equipment for information and/or intelligence. Weapons and materiel can be seized by the ambush element for future irregular OPFOR tactical actions. 7-25. The security element remains in fighting positions to ensure early warning, isolate a kill zone, and prevent any enemy from escaping the kill zone. Once the ambush element clears the kill zone, the ambush force withdraws from the ambush area. The ambush element withdraws first and is followed by the support element. The security element is the last element to depart the kill zone area and delays or blocks any rapid response of enemy forces that attempt to pursue irregular OPFOR elements as they depart the kill zone area. Depending on the size of the ambush force, the elements typically reassemble at a predetermined location and time at a safe house or safe haven.

Note. An irregular OPFOR ambush could employ security elements to provide early warning and/or isolate a series of kill zones on a known convoy route of the enemy. Restrictive natural terrain and manmade features are reinforced with IEDs to disrupt and contain an enemy force in the kill zones. A simple ambush technique is to employ a decoy IED that is observable on an enemy force route. Once enemy forces halt to investigate the potential of an IED detonation, the ambush force initiates the actual ambush with the simultaneous detonation of IEDs directed into the kill zone where enemy soldiers and vehicles are expected to halt. Lead and trail vehicles are initially the primary targets for massed direct fires and destruction. When they are destroyed, the ambush and support elements shift direct and indirect fires from both ends of the enemy column toward the center of the contained enemy forces. The enemy convoy is destroyed with massed overlapping direct and indirect fires. Ambush elements and designated support elements exfiltrate from the area while security elements provide rear security and an all-arms air defense capability against any enemy response forces. On order, security elements also exfiltrate from the ambush site and rendezvous with other guerilla elements at a safe haven.

and logistics support. Other opportunities may arise when insurgents or guerrillas in armed conflict capture or acquire sophisticated air defense weapons. In either case, clandestine state or non-state agents and/or technicians can provide technical support to ensure the effective use of the weapon systems. Examples of state-of-the-art air defense systems include shoulder-fired MANPADS and/or other air defense missiles with detection and tracking systems mounted on wheeled or tracked vehicles.

Engineer-Like Capabilities

Mobility and countermobility support often depends on insurgents or guerrillas with specialized skills and expertise from their civilian occupations or previous military experience. Guerrilla units include sappers, who are not engineers but can perform some engineer-like functions. Covert or overt assistance may also be provided from external sources such as SPF of another state.

Logistics

Logistics are prepared as caches or supported from safe houses and havens as part of detailed planning and rehearsals. The ambush force typically moves from a secured location with everything it needs to complete the mission. In those rare situations that require a multi-day hide prior to executing the ambush, the ambush force will have to move with its own extra life support. Resupply of the ambush force would significantly increase the chances of its detection and defeat its purpose.

INFOWAR

INFOWAR activities can support ambushes by concealing the intended action through deception and information protection. An INFOWAR campaign may use successful ambushes to demonstrate the progressive failure of an enemy force and/or governing authority. INFOWAR support of an ambush can temporarily and psychologically isolate the enemy force.

See pp. 1-32 to 1-33 for additional discussion (information operations).

II. Assault

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

A. Functional Organization for an Assault

The insurgent cell(s) or guerrilla unit(s) conducting an assault constitute an assault force. The assault force typically is organized into three types of elements:

- Assault element.
- Security element.
- Support element.

There may be more than one of each of these types of element.

Assault Element

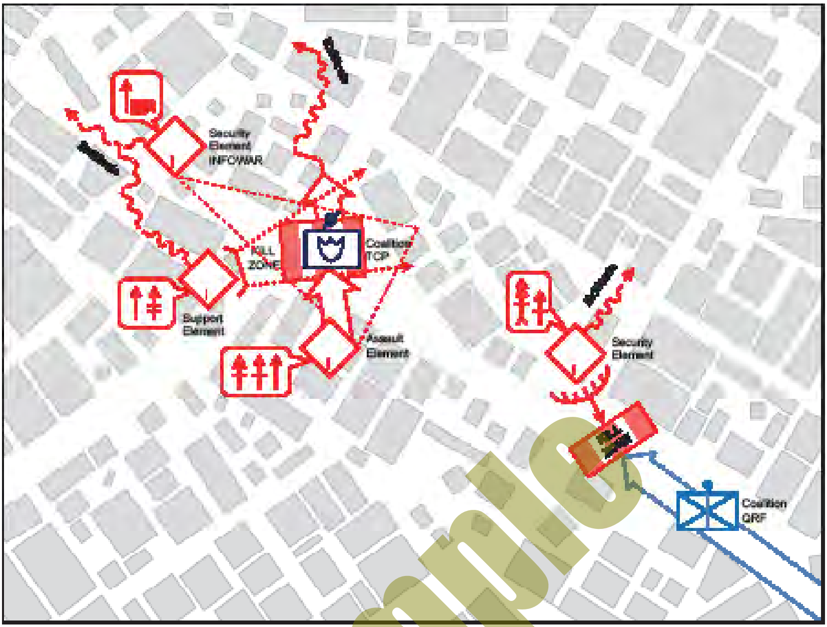
The assault element is the action element. It maneuvers to and seizes the enemy position, destroying any forces there.

Security Element

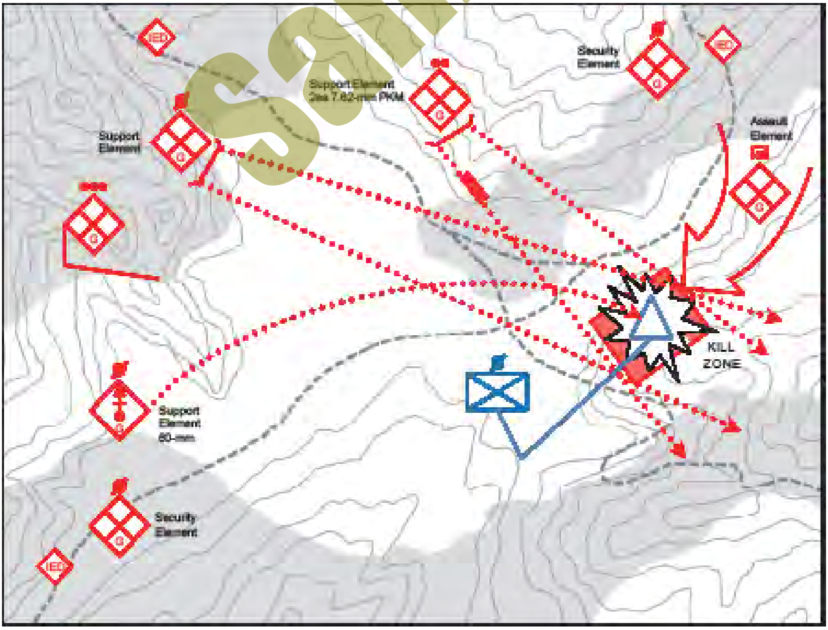
The security element provides early warning of approaching enemy forces and prevents them from reinforcing the assaulted enemy unit. Security elements often make use of terrain choke points, obstacles, ambushes, and other techniques to

Examples of Assaults

Ref: TC 7-100.3, Irregular Opposing Forces (Jan '14), pp. 7-10 to 7-11.



Ref: TC 7-100.3 (Jan '14), fig. 7-3. ***Insurgent*** *assault (example)*



Ref: TC 7-100.3 (Jan '14), fig. 7-4. ***Guerrilla*** *assault (example)*

III. Types of Defensive Action

Ref: TC 7-100.3, Irregular Opposing Forces (Jan '14), pp. 7-24 to 7-36.

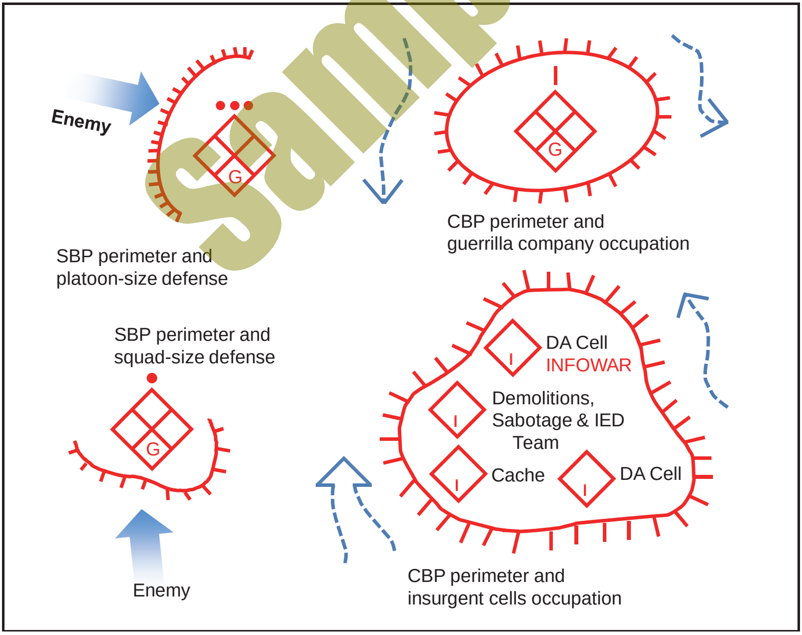
Insurgents and guerrillas can employ some of the types of defensive action also used by smaller tactical units of the regular OPFOR. Such actions can include—

- Defense of a simple battle position.
- Defense of a complex battle position.

Irregular OPFOR leaders and commanders select the defensive action best suited to accomplishing their mission, given the conditions under which they assume a defensive posture. Some parts of an insurgent or guerrilla organization may conduct defensive actions while other parts of the same organization are on the offense.

Battle Position (BP)

A battle position (BP) normally is a defensive location oriented on a likely enemy avenue of approach. However, the irregular OPFOR may select defensive locations to avoid contact with an enemy but provide for defense if discovered. When irregular OPFOR leaders determine that they will operate in a defensive posture, defensive positions will be either a simple battle position (SBP) or complex battle position (CBP). The mission and specific circumstances will influence the type of BP to establish and occupy. Figure 7-8 shows examples of symbols for SBPs and CBPs.



Ref: TC 7-100.3 (Jan '14), fig. 7-8. Simple and complex battle positions. Note. Sometimes graphics show a relatively large unit, such as a guerrilla battalion or brigade, inside a symbol for a CBP. This actually means that such a unit's subordinates occupy a series of CBPs within that area.

Simple Battle Position (SBP)

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 fortification and C3D measures as time allows. Defenses are improved upon continuously until the SBP is abandoned.

Complex Battle Position (CBP)

A complex battle position (CBP) is a defensive location designed to employ a combination of complex terrain, C3D, and engineer-like capabilities to protect the cells or units 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:

- Not on or along an enemy avenue of approach.
- Limited avenues of approach toward and/or in vicinity of a CBP.
- Observation of any existing avenues of approach.
- Defensive posture with an integrated 360-degree perimeter.
- Countermobility and mobility efforts prioritizing C3D measures of the CBP location.
- Substantial logistics caches.
- Sanctuary.

I. Defense of a Simple Battle Position (SBP)

Construction of an SBP places special attention on the camouflage, concealment, and cover of fighting positions in urban and rural terrain. The irregular OPFOR normally expects significant enemy reconnaissance, intelligence, surveillance, and target acquisition (RISTA) capabilities and recognizes that sophisticated RISTA capabilities may be supporting the enemy. An effective counter to such levels of sophisticated technology and systems may be to embed the SBP within a relevant population in an urban and/or rural environment, or physically use rural and/or urban terrain to mask the presence of SBPs. Examples include the use manmade underground shelters, tunnels, natural shelters such as caves, and/or village or city dwellings. An SBP or group of SBPs establishes kill zone(s) on likely enemy avenues of approach.

Deceptive techniques can include the façade of being commercial or private equipment, vehicles, work places, and/or public institutions and public gathering places such as houses of worship, hospitals, and civic centers with regular intermingling of the relevant population. Insurgents usually wear the clothing of the local population and often keep weapons, munitions, and materiel in caches that are easily retrievable in the vicinity of the SBP. The same may be true of guerrillas. However, guerrillas may transition to recognizable paramilitary uniforms.

The irregular OPFOR commander or leader makes prudent risk assessments when establishing SBPs. He evaluates the desirability and/or requirement to invest substantial time, effort, and materiel on an SBP. He weighs this against the expectation that he must defeat an enemy that can typically mass combat power quickly against an SBP.

Once the commander or leader decides to defend an SBP, he focuses his available combat power on one or more kill zones. The irregular OPFOR plans and rehearses all actions necessary to prevent enemy penetration of an SBP and/or what an SBP or group of SBPs is protecting, and also considers measures to defeat an enemy penetration of an SBP if it occurs.

The commander or leader considers what criteria he will use to direct a withdrawal and/or withdrawal under pressure from an SBP or group of SBPs. Unless directed to retain a specific SBP by a higher level, the commander or leader responsible for an SBP recognizes that he is committed to a long-term struggle and that preserving combat power for a future engagement may be the appropriate decision. However, some insurgents or guerrillas may have a self-determined commitment or directed mission to fight until killed or captured in a particular SBP.

A. Functional Organization for Defending an SBP

The commander or leader defends an SBP with cells or units that are organized as functional elements. Typical functional designations are—

- Disruption element.
- Main defense element.
- Reserve element.
- Support element.
- Deception element.

There may be more than one of each type. The name of an element describes its function within the defensive action.

Disruption Element(s)

Insurgents or guerrillas assigned to a disruption element have a mission of identifying enemy reconnaissance efforts and reporting the location, disposition, and composition of approaching enemy forces. When disruption elements have the capability to target and attack designated subsystems of an enemy force, they conduct disruption actions as part of a comprehensive defense plan of the higher commander or leader.

Disruption activities may include direct and indirect fires, remote-controlled or command-detonated IEDs and/or other execution of obstacles to slow, channel, contain, or block an enemy force. The normal intention of a disruption element is to not become decisively engaged by the enemy. However, a commander or leader can direct decisive engagement if the action is necessary to preserve the combat power of other critical capabilities in the irregular OPFOR organization.

Tactical tasks typical of a disruption element include—

- Ambush.
- Attack by fire.
- Delay.
- Disrupt.

The irregular OPFOR will typically not assign a small cell or unit a fixing task when an expectation of “fix” is to deny movement of any part of an enemy force. A more probable task for the irregular OPFOR in an SBP is “delay” with an expectation to slow the momentum of an enemy advance and cause significant damage to the enemy force without becoming decisively engaged.

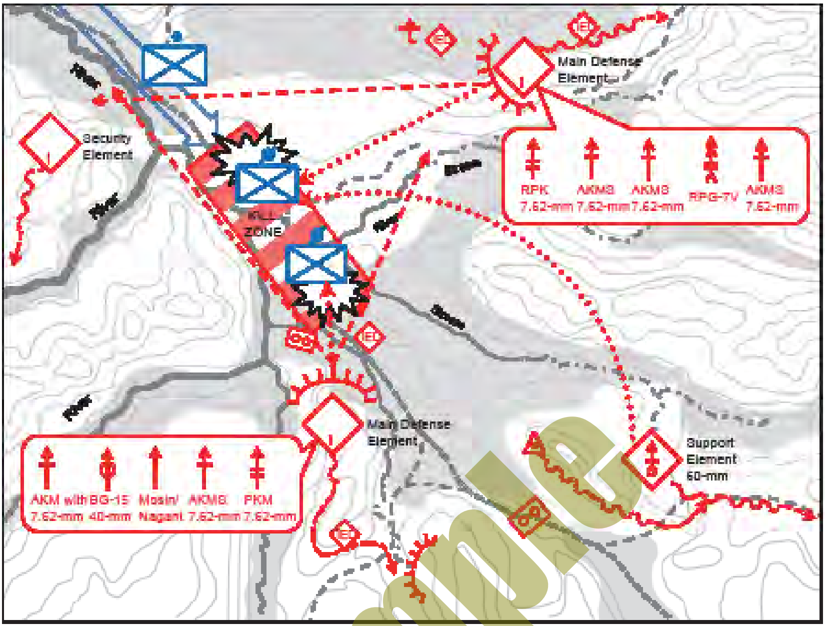
A disruption element for an SBP can be as small as one or two insurgents or guerrillas with assault rifles, light and/or medium machineguns, grenade launchers, IEDs, and/or ATGLs. Typically, it is no larger than eight to 12 such personnel.

Main Defense Element(s)

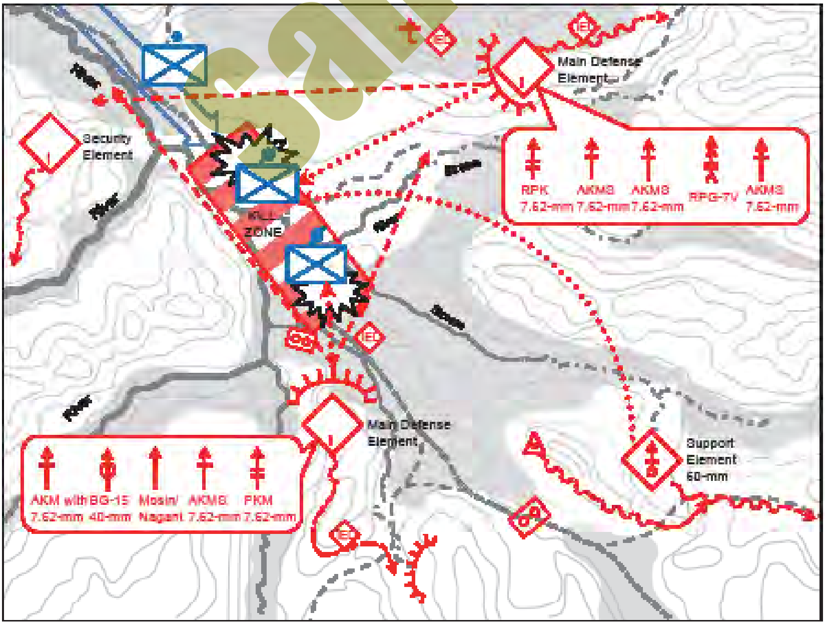
The main defense element of an SBP is responsible for defeating an attacking force. Insurgents or guerrillas in a main defense element are prepared to use fires and maneuver to defeat the penetration or seizure of their SBP or other SBPs. Main defense elements focus the combat power of available weapon systems into designated kill zones to defeat or destroy an enemy force.

Examples of an SBP Defense

Ref: TC 7-100.3, Irregular Opposing Forces (Jan '14), pp. 7-28 to 7-29.



*Ref: TC 7-100.3 (Jan '14), fig. 7-9. **Insurgent** defense of a SBP (example).*



*Ref: TC 7-100.3 (Jan '14), fig. 7-10. **Guerrilla** defense of a SBP (example).*

IV. Tactical Enabling Operations

Ref: ADP 3-90, Offense and Defense (Jul '19), ADRP 3-90, Offense & Defense (Aug '12) and FM 3-90-2 Reconnaissance, Security and Tactical Enabling Tasks (Mar '13).

Enabling Operations

Commanders conduct enabling operations as shaping or supporting efforts during decisive action, but they are not primarily offensive, defensive, and stability operations, or defense support of civil authorities tasks. Tactical enabling tasks include tasks such as:

- Reconnaissance
- Security
- Troop movement
- Relief in place
- Passage of lines
- Encirclement operations
- Urban operations

IGF in Enabling Operations

Ref: Kulikov, The Tactics of Insurgent Groups in the Republic of Chechnya; and Jalali & Grau, The Other Side of the Mountain, chap 6.

IGF enabling operations are based from the dispersed defense. Because the defense is dispersed in networks of neighborhood safe houses, villages across the countryside, and sanctuaries along porous borders or vast interiors, it is already well positioned to conduct enabling operations and support all facets of IGF activities. On the following pages we shall focus on discussing those enabling operations that support direct action operations.

Enabling operations apply to all elements of decisive action. The enabling operations discussed in ADP 3-90 include reconnaissance, security, troop movement, relief in place, and passage of lines. Other publications discuss other enabling operations. For example, FM 3-13 discusses information operations, ATP 3-90.4 discusses mobility operations, and ATP 3-90.8 discusses countermobility operations. Commanders direct enabling operations to support the conduct of the offensive, defensive, and stability operations and defense support of civil authorities tasks. Enabling operations are usually conducted by commanders as part of their shaping operations or supporting efforts.

Refer to SUTS3: The Small Unit Tactics SMARTbook, 3rd Ed. Chapters and topics include tactical fundamentals, the offense; the defense; train, advise, and assist (stability, peace & counterinsurgency ops); tactical enabling tasks (security, reconnaissance, relief in place, passage of lines, encirclement, and troop movement); special purpose attacks (ambush, raid, etc.); urban and regional environments (urban, fortified areas, desert, cold, mountain, & jungle operations); patrols & patrolling.

V. Battle Drills, TTPs & Equipment

Ref: Suholessky, Spetsnaz GRU in Afghanistan; Kulikov, The Tactics of Insurgent Groups in the Republic of Chechnya; and Chivers, Turning Tables.

I. Vehicle Mounted

Ref: Kulikov, The Tactics of Insurgent Groups in the Republic of Chechnya; and Suholessky, Spetsnaz GRU in Afghanistan, pp. 89-90.

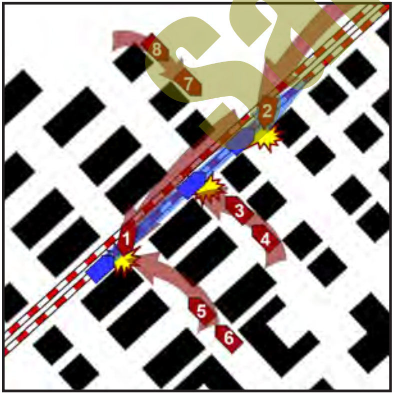
IGF units employ vehicles in direct action for surveillance, rolling ambush, and raids. When used for surveillance, vehicles are rarely modified. Instead IGF prefer that surveillance vehicles remain inconspicuous to blend with routine civilian traffic.

However, for ambush platforms and raids, IGF vehicles are often modified to fit specific weapon systems. When available some vehicles may be fitted with limited ballistic armor plating, stripped for ambulatory uses, or rigged with IED/EFP.

There is no single drill for IGF vehicle ambush or raid. IGF vehicle convoys typically comprise just two vehicles in trail, but often include three or more vehicle convoys. This complicates enemy targeting protocol and systems, but requires sophisticated planning.

Rolling Ambush

The emergent tactic of mobile, rolling ambush involves the two leading IGF vehicles disabling and blocking key enemy vehicles caught within the kill zone – typically at the front and rear of an enemy convoy or checkpoint. Trailing IGF vehicles then move against enemy caught in the kill zone and conduct attack-by-fire from the flanks of their vehicles.



Rolling Ambush: IGF lead vehicles (#1 & #2) halt the enemy at the front and rear of the convoy – either from a frontal or rear attack in the designated kill zone. Additional IGF vehicles converge on the kill zone from multiple angles of attack. This is a complexly coordinated, highly mobile form of ambush.

Just as any other ambush that plans to close with the enemy and overwhelm them, the rolling ambush must significantly outnumber the enemy force it targets in the kill zone.

(OPFOR5) Index

dept of defense
air force
navy
marines
interagency
army
coast guard
joint staff
multinational

SMARTbooks

INTELLECTUAL FUEL FOR THE MILITARY

MILITARY REFERENCE: SERVICE-SPECIFIC

Recognized as a "whole of government" doctrinal reference standard by military professionals around the world, SMARTbooks comprise a comprehensive professional library.

MILITARY REFERENCE: MULTI-SERVICE & SPECIALTY

SMARTbooks can be used as quick reference guides during operations, as study guides at professional development courses, and as checklists in support of training.

JOINT STRATEGIC, INTERAGENCY, & NATIONAL SECURITY

The 21st century presents a global environment characterized by regional instability, failed states, weapons proliferation, global terrorism and unconventional threats.

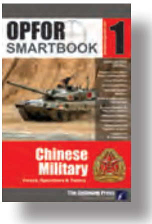
JFODS5-1 SMARTBOOK
JOINT FORCES Operations & Doctrine
Joint/Interagency SMARTBOOK 1
joint strategic & operational PLANNING
Joint/Interagency SMARTBOOK 2
interagency PLANNING & PROCESS
INFO1 SMARTBOOK
IO information OPERATIONS & CAPABILITIES
CYBER1 SMARTBOOK
Cyberspace Operations & Electronic Warfare

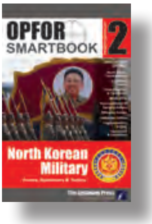
The Lightning Press is a **service-disabled, veteran-owned small business,** DOD-approved vendor and federally registered — to include the SAM, WAWF, FBO, and FEDPAY.

RECOGNIZED AS THE DOCTRINAL REFERENCE STANDARD BY MILITARY PROFESSIONALS AROUND THE WORLD.

THREAT, OPFOR, REGIONAL & CULTURAL

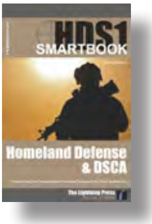
In today's complicated and uncertain world, the military must be ready to meet the challenges of any type of conflict, in all kinds of places, and against all kinds of threats.

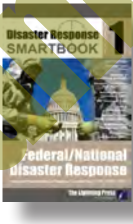




HOMELAND DEFENSE, DSCA, & DISASTER RESPONSE

Disaster can strike anytime, anywhere. It takes many forms—a hurricane, an earthquake, a tornado, a flood, a fire, a hazardous spill, or an act of terrorism.




Disaster Response SMARTBOOK 1
Federal/National Disaster Response

DIGITAL SMARTBOOKS (eBooks)

In addition to paperback, SMARTbooks are also available in digital (eBook) format. Our digital SMARTbooks are for use with Adobe Digital Editions and can be used on up to **six computers and six devices**, with free software available for **85+ devices and platforms—including PC/MAC, iPad and iPhone, Android tablets and smartphones, Nook, and more**! Digital SMARTbooks are also available for the **Kindle Fire** (using Bluefire Reader for Android).

Download FREE samples and SAVE 15% everyday at:

www.TheLightningPress.com

Purchase/Order

www.TheLightningPress.com

SMARTsavings on SMARTbooks! Save big when you order our titles together in a SMARTset bundle. It's the most popular & least expensive way to buy, and a great way to build your professional library. If you need a quote or have special requests, please contact us by one of the methods below!

View, download FREE samples and purchase online:

www.TheLightningPress.com

Order SECURE Online

Web: www.TheLightningPress.com

Email: SMARTbooks@TheLightningPress.com

24-hour Order & Customer Service Line

Place your order (or leave a voicemail)
at 1-800-997-8827

Phone Orders, Customer Service & Quotes

Live customer service and phone orders available
Mon - Fri 0900-1800 EST at (863) 409-8084

Mail, Check & Money Order

2227 Arrowhead Blvd., Lakeland, FL 33813

Government/Unit/Bulk Sales

The Lightning Press is a **service-disabled, veteran-owned small business**, DOD-approved vendor and federally registered—to include the SAM, WAWF, FBO, and FEDPAY.

We accept and process both **Government Purchase Cards** (GCPC/GPC) and **Purchase Orders** (PO/PR&Cs).

Keep your SMARTbook up-to-date with the latest doctrine! In addition to revisions, we publish incremental "**SMARTupdates**" when feasible to update changes in doctrine or new publications. These SMARTupdates are printed/produced in a format that allow the reader to insert the change pages into the original GBC-bound book by simply opening the comb-binding and replacing affected pages. Learn more and sign-up at: **www.thelightningpress.com/smartupdates/**

5

thelightningpress.com

[OPFOR5]

Irregular & Hybrid Threat

Forces, Operations & Tactics

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.

Irregular forces are armed individuals or groups who are not members of the regular armed forces, police, or other internal security forces. Irregular forces are unregulated and as a result act with no restrictions on violence or targets for violence. Time-honored concepts of "conventional" and "unconventional" war and "traditional" methods versus "adaptive" methods are weapons to a hybrid threat.

Insurgents are armed and/or unarmed individuals or groups who promote an agenda of subversion and violence that seeks to overthrow or force change of a governing authority.

A **guerrilla force** is a group of irregular, predominantly indigenous personnel organized along military lines to conduct military and paramilitary operations in enemy-held, hostile, or denied territory.

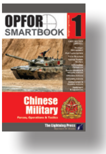
Terrorism is a tactic. Terrorism can be defined as the use of violence or threat of violence to instill fear and coerce governments or societies. Often motivated by philosophical or other ideological beliefs, objectives are typically political in nature.

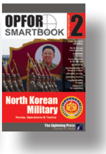
Criminal elements exist at every level of society and in every operational environment (OE). Their presence, whatever their level of capabilities, along with a host of armed and unarmed **noncombatants** adds complexity to any operational environment.

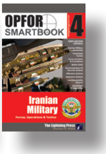
DIME is our DOMAIN!

SMARTbooks: Reference Essentials for the Instruments of National Power

Part of our "Military Reference" Series







ISBN 9781935886549
90000 >
9 781935 886549

www.TheLightningPress.com