



January 5, 2024

# Defense Primer: What Is Irregular Warfare?

## Introduction

United States military doctrine distinguishes between two types of warfare: traditional warfare and irregular warfare. In Department of Defense (DOD) Joint Publication (JP) 1 *Doctrine for the Armed Forces of the United States*, traditional warfare is characterized as “a violent struggle for domination between nation-states or coalitions and alliances of nation-states.” The publication further states that “traditional warfare typically involves force-on-force military operations in which adversaries employ a variety of conventional forces and special operations forces (SOF) against each other in all physical domains as well as the information environment (IE).” According to JP 3-04 *Information in Joint Operations*, the IE is “the aggregate of social, cultural, linguistic, psychological, technical, and physical factors that affect how humans and automated systems derive meaning from, act upon, and are impacted by information, including the individuals, organizations, and systems that collect, process, disseminate, or use information.”

In DOD Directive 3000.07 and in other DOD doctrine, irregular warfare (IW) is characterized as “a violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s).” These actors may use nontraditional methods such as guerrilla warfare, terrorism, sabotage, subversion, criminal activities, and insurgency in their efforts to control the target population. In IW, a less powerful adversary seeks to disrupt or negate the military capabilities and advantages of a more powerful military force, which usually serves that nation’s established government. Because of its emphasis on influencing populations, actions to control the IE, to include actions in cyberspace, play a prominent role in IW.

## Missions of Irregular Warfare

IW includes, among other activities, the specific missions of unconventional warfare (UW), stabilization, foreign internal defense (FID), counterterrorism (CT), and counterinsurgency (COIN).

**Unconventional Warfare.** DOD Directive 3000.07 *Irregular Warfare* and P.L. 114-92 Section 1097, National Defense Authorization Act (NDAA) for FY2016 define UW as “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 is a core component of IW.

**Stabilization.** Stability operations involve a range of activities, from responding to natural disasters to repairing critical infrastructure and strengthening indigenous institutions to provide security, essential services, justice

and economic opportunity. Stability operations may be an interagency effort.

**Foreign Internal Defense.** DOD JP 3-22 *Foreign Internal Defense* characterizes FID as “participation by civilian agencies and military forces of a government or international organizations in any of the programs and activities undertaken by a host nation government to free and protect its society from subversion, lawlessness, insurgency, terrorism, and other threats to its security.”

**Counterterrorism.** The DOD Dictionary of Military and Associated Terms defines CT as “activities and operations taken to neutralize terrorists and their organizations and networks to render them incapable of using violence to instill fear and coerce governments or societies to achieve their goals.” They are distinct from counterinsurgency and stability operations as well as from security cooperation.

**Counterinsurgency.** In JP 3-24, COIN are “comprehensive civilian and military efforts designed to simultaneously defeat and contain insurgency and address its root causes.”

## Operations in Irregular Warfare

Related activities such as military information support operations (MISO) or psychological operations, cyberspace operations, countering threat networks, counter-threat finance, civil-military operations, and security cooperation also shape the information environment and other population-focused arenas of competition and conflict.

**Military Information Support Operations.** Also known as psychological operations, MISO are “planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator’s objectives.” (JP3-13.2)

**Cyberspace Operations.** In JP 3-12, cyberspace operations are “the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.” They include offensive measures intended to project power in and through cyberspace, and defensive measures to protect and preserve the ability to use one’s own cyberspace capabilities.

**Countering Threat Networks.** JP 3-25 describes countering threat networks as “the aggregation of activities across the DOD and United States Government departments and agencies that identifies and neutralizes, degrades, disrupts, or defeats designated threat networks.”

**Counter-Threat Finance.** JP 3-05 *Special Operations* defines counter threat finance as “activities conducted to deny, disrupt, destroy, or defeat the generation, storage, movement, and use of assets to fund activities that support an adversary’s ability to negatively affect United States interests.”

**Civil-Military Operations.** According to JP 3-57 *Civil-Military Operations*, civil-military operations are “activities of a commander performed by designated military forces that establish, maintain, influence, or exploit relations between military forces and indigenous populations and institutions by directly supporting the achievement of objectives relating to the reestablishment or maintenance of stability within a region or host nation.”

**Security Cooperation.** JP 3-20 *Security Cooperation* counts security cooperation as “DOD interactions with foreign security establishments to build relationships that promote specific United States security interests, develop allied and partner military and security capabilities for self-defense and multinational operations, and provide United States forces with peacetime and contingency access to allies and partners.”

### Asymmetric Warfare and IW

While there appears to be no single government definition, asymmetric warfare is often characterized in national security literature as a type of war between opposing forces that have divergent military power, strategy, or tactics. It often involves the use of unconventional weapons and tactics, such as those associated with guerrilla warfare and terrorism. Asymmetric warfare is a form of irregular warfare. Because of its association with and similarities to irregular warfare, the terms are sometimes used interchangeably.

### Irregular Forces

According to Hague conditions outlined in Article 4(A)(2) of the 1949 Third Geneva Convention, a country or state’s armed forces or regular forces are those that are (1) “commanded by a person responsible for his subordinates”; (2) “hav[e] a fixed distinctive sign recognizable at a distance”; (3) “carry arms openly”; and (4) “conduct their operations in accordance with the laws and customs of war.” Any force that does not meet these four conditions can be considered an irregular force. Simply put, irregular forces, also known as irregular military, are armed forces that employ irregular tactics. Existing outside of the conventional military, irregular forces include—but are not limited to—partisan and resistance fighters in opposition to occupying conventional military forces.

### Special Operations Command

The United States Special Operations Command (USSOCOM) organizes, trains, and equips special operations forces (SOF) for special operations core activities and other such activities as may be specified by the President and/or the Secretary of Defense. These core activities reflect the collective capabilities of all joint special operations forces rather than those of any one military service or unit. Activities or actions requiring unique modes of employment, tactical techniques,

equipment, and training often conducted in hostile, denied, or politically sensitive environments. Many of the IW component activities listed are coordinated and conducted by USSOCOM and SOF. For example, unconventional warfare is led by special operations forces.

Conventional forces also play a role in IW. The Irregular Warfare Annex of the 2018 National Defense Strategy (NDS), released by DOD in 2020, set a goal of maintaining an IW core competency throughout the entire Joint Force, not just the Special Operations Command. Additionally, USSOCOM engages with partners, allies, and interagency components to fulfill its mission. For instance, the U.S. Department of State’s Global Engagement Center (GEC) works with USSOCOM as part of its mission to counter foreign propaganda and disinformation. Within the federal government, the GEC is the lead for these activities.

### Irregular Warfare in the National Security Strategy

The IW Annex of the 2018 NDS outlined the principles of IW as a core competency of the DOD. The IW Annex notes that China, Russia, and Iran are willing practitioners of campaigns of disinformation, deception, sabotage, and economic coercion, as well as proxy, guerrilla, and covert operations, and calls for a revised understanding of IW to account for its role in great power competition. The 2022 NDS contains some mentions of irregular warfare, particularly in the context of competitor’s gray zone activities, referring to the so-called gray zone between peace and wartime.

### Irregular Warfare in the National Defense Authorization Act

Section 1202 of the National Defense Authorization Act (NDAA) for FY2018 provided that the Secretary of Defense may, with the concurrence of the relevant Chief of Mission, expend up to \$10,000,000 during each of fiscal years 2018 through 2020 to provide support to foreign forces, irregular forces, groups, or individuals engaged in supporting or facilitating ongoing and authorized irregular warfare operations by United States Special Operations Forces. The NDAA for FY2022 amended Section 1202 to extend it through FY2025, while requiring a report on the IW strategy called for in the IW annex of the 2018 NDS. The NDAA for FY2024 codified the support provision and raised the expenditure to up to \$20,000,000 per fiscal year. Issues for Congress include whether to limit or expand IW funding, and redefining IW terminology.

#### CRS Resources

CRS Report R45142, *Information Warfare: Issues for Congress*, by Catherine A. Theohary.

CRS In Focus IF10771, *Defense Primer: Operations in the Information Environment*, by Catherine A. Theohary.

CRS In Focus IF10537, *Defense Primer: Cyberspace Operations*, by Catherine A. Theohary.

**Catherine A. Theohary**, Specialist in National Security Policy, Cyber and Information Operations

## Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.