Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated December 14, 2023

# Defense Primer: Operations in the Information Environment

## Information as a Joint Function

In 2017, Joint Publication (JP) 1 *Doctrine of the Armed Forces of the United States* was updated to establish information as the seventh joint function of the military, along with command and control, intelligence, fires, movement and maneuver, protection, and sustainment. This designation has necessitated clarification and revisions in some Department of Defense (DOD) doctrine.

## Information Warfare

While there is currently no official United States government (USG) definition of information warfare (IW), DOD doctrine may use the term *information warfare* to describe "the mobilizing of information to attain a competitive advantage and achieve United States (US) policy goals." Some DOD doctrine defines IW not as a strategy but as a subset of OIE conducted during both competition below armed conflict and during warfighting in order to dominate the IE at a specific place and time. The U.S. military contributes to information warfare by deliberately leveraging the inherent informational aspects of activities and by conducting operations in the information environment.

## Operations in the Information Environment

According to the 2022 JP 3-04 *Information in Joint Operations*, Operations in the Information Environment (OIE) involve the integrated employment of multiple information forces to affect drivers of behavior by informing audiences; influencing foreign relevant actors; attacking and exploiting relevant actor information, information networks, and information systems; and protecting friendly information, information networks, and information systems. OIE activities take place within the information environment (IE), defined as "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." Strategic communication, public diplomacy and public and civil affairs, and cyberspace operations may be integrated and employed by information forces. These efforts may take place in and throughout each of the global domains of air, land, sea, space, and cyberspace, and in various forms unrelated to cyberspace, such as dropping pamphlets, cultural exchanges, jamming or broadcasting targeted communications, and foreign aid programs.

All instruments of national power—diplomatic, informational, military, and economic (DIME)—can be projected and employed in the information environment, and by nonmilitary elements of the federal government.

## Strategy for Operations in the Information Environment

The 2022 National Defense Strategy (NDS) places these activities in the context of the "gray zone," coercive actions below the threshold of a military response and across USG areas of responsibility. With an eye toward the NDS, the 2023 Strategy for Operations in the Information Environment aims to improve the DOD's ability to plan, resource, and apply informational power to enable integrated deterrence, campaigning, and building enduring advantages. The NDS describes use of the electromagnetic spectrum across all domains, as well as integration with whole-of-government informational advantages to achieve these strategic goals.

## History of OIE

In 2018, DOD issued a Joint Concept for Operations in the Information Environment. According to this document, the IE comprises and aggregates numerous social, cultural, cognitive, technical, and physical attributes that act upon and affect knowledge, understanding, beliefs, world views, and, ultimately, actions of an individual, group, system, community, or organization. Corresponding DOD policy defined OIE as actions taken to generate, preserve, and apply informational power against a relevant actor in order to increase or protect competitive advantage or combat power potential within all domains of the operating environment. OIE span the competition continuum (cooperation, competition short of armed conflict, and warfighting). This definition of the continuum aligned with the 2018 National Defense Strategy, which emphasized information warfare as competition short of open warfare.

## Information Operations

Past definitions within DOD have conceptualized IO as a purely military activity involving a set of tactics or capabilities. In earlier iterations of DOD JP 3-13, IO consisted of five pillars: computer network operations (CNO), which include computer network attack, computer network defense, and computer network exploitation; psychological operations (PSYOP); electronic warfare (EW); operations security (OPSEC); and military deception (MILDEC). With the advent of U.S. Cyber Command, CNO became cyberspace operations, offensive and defensive with its own doctrine in JP 3-12. In 2010, PSYOP became military information support operations (MISO), to reflect a broader range of activities and the existing Military Information Support Teams consisting of PSYOP personnel deployed at U.S. embassies overseas. JP 3-13.2 replaced the term PSYOP with MISO to "more accurately reflect and convey the nature of planned peacetime or combat operations activities." The name change reportedly caused administrative confusion, and some services reverted to the PSYOP label.

The Secretary of Defense later characterized IO in JP 3-13 as *"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."* This definition shifted the focus from a set of tactics toward the desired effects and how to achieve them. JP 3-13 defined information-related capability (IRC) as a tool, technique, or activity employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions. *JP 3-04 supersedes JP 3-13, and legacy terms such as IO and IRC are to be removed from the Dictionary of Military and Associated Terms.*

## Types of Information in OIE

In common parlance, the term *disinformation campaign* is often used interchangeably with *information operations* and/or *psychological operations*. However, disinformation or deception is only one of the informational tools that comprise an IW strategy; factual information can also be used to achieve strategic goals and in some cases more effectively than deceptive means. Different categories of information that may be used in OIE include the following:

**Propaganda.** The propagation of an idea or narrative that is intended to influence, similar to psychological or influence operations. It can be misleading but true, and may include stolen information. A government communicating its intent, policies, and values through speeches, press releases, and other public affairs can be considered propaganda.

**Misinformation.** The spreading of unintentionally false information. Examples include internet trolls who spread unfounded conspiracy theories or web hoaxes through social media, believing them to be true.

**Disinformation.** Unlike misinformation, disinformation is intentionally false. Examples include planting false news stories in the media and tampering with private and/or classified communications before their widespread release.

## Cyberspace and OIE

Cyberspace presents a force multiplier for IW activities. Social media and botnets can amplify a message or narrative, using all three elements of information to foment discord and confusion in a target audience. Much of today's IW is conducted in cyberspace, leading to associations with cybersecurity. Cyberspace operations can be used to achieve strategic IW goals; an offensive cyberattack, for example, may be used to create psychological effects in a target population. A foreign country may likewise use cyberattacks to influence decisionmaking and change behaviors. Cyberspace operations may be conducted for IW purposes, such as to disable or deny access to an adversary's lines of communication or to demonstrate ability as a deterrent. These operations may be overt, such as a government's production and dissemination of materials intended to convey democratic values. In this case, the government sponsorship of such activity is known. Covert operations are those in which government sponsorship is denied if exposed. The anonymity afforded by cyberspace presents an ideal battlespace to conduct covert operations.

In JP 3-12, DOD defines cyberspace as "the global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." Some have criticized this as lacking the cognitive, human element that the internet represents, which in turn could adversely affect how the military organizes, trains, and equips for IO in cyberspace. Additionally, there are concerns that the split between IO and cyberspace operations in doctrine and organization created a stovepipe effect that hinders coordination of these closely related forces. As such, some services such as the Army and Air Force are reorganizing assets from Cyber Commands into Information Warfare Commands. The Marine Corps created a Deputy Commandant for Information in order to oversee Operations in the Information Environment, to include cyberspace operations.

## Who Is Responsible for the "I" in DIME?

Within the USG, much of the current information doctrine and capability resides with the military. Many consider DOD to be relatively well funded, leading some to posit that the epicenter for all IW activities should be the Pentagon. Some fear that military leadership of the IW sphere represents the militarization of cyberspace, or the weaponization of information. In addition, the military may not possess the best tools to successfully lead information efforts across the USG. Title 10 U.S.C. 2241 prohibits DOD from domestic "publicity or propaganda," although the terms are undefined. It is unclear how OIE relate to this so-called military propaganda ban. P.L. 115-232 tasked the State Department's Global Engagement Center (GEC) to "direct, lead, synchronize, integrate, and coordinate efforts of the Federal Government to recognize, understand, expose, and counter foreign state and foreign non-state propaganda and disinformation efforts." P.L. 116-92 created a Principal Information Operations Advisor within DOD to coordinate and deconflict its operations with the GEC.

## OIE as an Act of War?

Some have questioned whether tampering with, interfering with, or otherwise influencing a sovereign nation's democratic processes in an IW campaign is an act of war that could trigger a military response, and not necessarily in cyberspace. U.S. policy suggests that these types of operations fall below the threshold of armed conflict.

### CRS Reports

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

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

**IF10771**

## Disclaimer