Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated January 14, 2020

Defense Primer: Information Operations

Information Warfare

While there is currently no official U.S. government (USG) definition of information warfare (IW), practitioners typically conceptualize it as *a strategy for the use and management of information to pursue a competitive advantage, including both offensive and defensive operations.* Strategy can be defined as the process of planning to achieve objectives and goals in the national interest. Operations link strategic objectives with tactics, techniques, and procedures. For IW strategy, that link is information operations (IO).

Information Operations

Past definitions within the DOD have conceptualized IO as a purely military activity involving a set of tactics or capabilities. In DOD Joint Publication (JP) 3-13 and the IO Roadmap, 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. Joint Publication 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 the services are beginning to revert to the PSYOP label.

The Secretary of Defense characterizes 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 defines 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.

Strategic communication, public diplomacy and public and civil affairs, and cyberspace operations may be considered supporting capabilities. 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. Military Information Support Operations are one of Special Operations Forces' (SOF's) core activities, but IO is not the exclusive purview of SOF.

All of these activities take place within the information environment, which is the aggregate of individuals, organizations, and systems that collect, disseminate, or act on information. This consists of three dimensions: *the physical dimension*, where information overlaps with the physical world; the *information dimension*, where information is collected, processed, stored, disseminated, displayed, and protected, including both the content and the flow of information between nodes; and *the cognitive dimension*, where human decisionmaking takes place based upon how information is perceived. 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.

Types of Information

In common parlance, the term "disinformation campaign" is often used interchangeably with information 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 IO include the following:

Propaganda: This means 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: This is 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.

Cyber-Enabled Information Operations

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 IO is conducted in cyberspace, leading many to associate IO with cybersecurity. Within DOD, however, IO and cyberspace operations are distinct doctrinal activities.

Cyberspace operations can be used to achieve strategic information warfare goals; an offensive cyberattack, for example, may be used to create psychological effects in a target population. A foreign country may use cyberattacks to influence decisionmaking and change behaviors, for example the DPRK-attributed cyberattacks on Sony in late 2014. Cyber operations may be conducted for other information operations purposes, such as to disable or deny access to an adversary's lines of communication or to demonstrate ability as a deterrent. IO 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 information 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 creates a stovepipe effect that hinders coordination of these closely related capabilities. As such, some services such as the Army and Air Force are reorganizing assets from Cyber Commands into Information Warfare Commands. The Marine Corps has created a Deputy Commandant for Information in order to oversee Operations in the Information Environment, to include cyberspace operations.

Information as a Joint Function

In 2017, 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 C2, intelligence, fires, movement and maneuver, protection, and sustainment. This designation has necessitated clarification and revisions in some DOD doctrine.

Operations in the Information Environment

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. The IE also includes technical systems and their use of data. The IE directly affects and transcends all operating environments.

New DOD policy would define Operations in the Information Environment (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 would align with the 2018 National Defense Strategy, which emphasizes information warfare as competition short of open warfare. IW is defined 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. IO would be defined not as a set of capabilities but as the staff function that synchronizes IRCs for the Commander to conduct OIE. Superseded by the Information Joint Function, IO may in the future considered a legacy term by the DOD.

Who Is Responsible for the "I" in DIME?

Within the USG, much of the current information operations 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 IW/IO relate to this so-called military propaganda ban. P.L. 115-232 tasked the State Department's Global Engagement Center (GEC) to "direct, USG 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, who is the lead.

Information Operations 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. A similar question is whether a cyberattack that falls below the threshold of damage and destruction that a kinetic event would impart could be considered an armed attack under international law. 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.

Other Resources

DOD. Joint Publication 3-13, *Information Operations*, November 27, 2012.

DOD. Defense Directive 3600.01, *Information Operations*, May 2, 2013.

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

IF10771

Disclaimer