Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated December 18, 2018

Defense Primer: Information Operations

Information Warfare

While there is currently no official U.S. government 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

Current and past definitions within the DOD have conceptualized IO, as opposed to IW, as a purely military activity involving a set of tactics or capabilities. In DOD Joint Publication 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).

Computer network operations support IO with dissemination assets and the capabilities to deny or degrade and adversary's ability to access, report, process, or disseminate information.

Psychological operations are central to IO. PSYOP has been defined in DOD doctrine as "planned political, economic, military, and ideological activities directed towards foreign countries, organizations, and individuals in order to create emotions, attitudes, understanding, beliefs, and behavior favorable to the achievement of United States and military objectives."

Electronic Warfare represents military action involving the use of electromagnetic and directed energy (e.g., through radio, infrared, or radar) to control the electromagnetic spectrum or to attack the enemy. EW platforms provide a means of disseminating messages and shaping the information environment through the electronic dissemination of products.

Operations Security is a systematic method to identify, control, and protect critical information and analyze friendly actions associated with military operations and other activities. In an IO context, OPSEC is the protection of plans and messages prior to execution through the proper use of information security, information assurance, physical security, and operations security.

Military Deception involves actions that are executed to deliberately mislead adversary military decisionmakers about U.S. military capabilities, intentions, and operations. Unlike PSYOP, which are intended to influence and persuade, MILDEC is intended to deceive.

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 *psychological operations* with *military information support operations* 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.

With the advent of U.S. Cyber Command, CNO became cyberspace operations, offensive and defensive with its own doctrine in JP 3-12.

The Secretary of Defense now 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 shifts the focus from a set of tactics toward the desired effects and how to achieve them. JP 3-13 defines information-related capability 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.

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.

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 includes:

- **The Physical layer:** Command and control systems and associated infrastructure.
- **The Informational layer:** Networks and systems where information is stored.
- **The Cognitive layer:** The minds of people who transmit and respond to information.

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

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.

Who Is Responsible for the "I" in DIME?

Within the U.S. government, 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. 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.

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.

Relevant Statutes

Title 10, U.S. Code, *Armed Forces,* Section 164: Organize and employ commands and forces.

Title 50, U.S. Code, *War and National Defense,* Section 3093: Secure US interests by conducting covert actions.

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

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.