FM 3-13 (FM 100-6)

Information Operations: Doctrine, Tactics, Techniques, and Procedures

NOVEMBER 2003

HEADQUARTERS, DEPARTMENT OF THE ARMY

Field Manual
No. 3-13

Headquarters
Department of the Army
Washington, DC, 28 November 2003

Information Operations: Doctrine, Tactics, Techniques, and Procedures

Contents

*This publication supersedes FM 100-6, 27 August 1996.

Preface

Information is an element of combat power. Commanders conduct information operations (IO) to apply it. Focused IO—synchronized with effective information management and intelligence, surveillance, and reconnaissance—enable commanders to gain and maintain information superiority. IO is a prime means for achieving information superiority.

Users of FM 3-13 must be familiar with the military decisionmaking process established in FM 5-0, *Army Planning and Orders Production*; the operations process, established in FM 3-0, *Operations*; and commander's visualization, described in FM 6-0, *Mission Command: Command and Control of Army Forces.*

PURPOSE

As the Army's key integrating manual for IO, this manual prescribes IO doctrine and tactics, techniques, and procedures (TTP). It also establishes doctrine and TTP for the IO elements of operations security and military deception. This manual implements joint IO doctrine established in JP 3-13, *Joint Doctrine for Information Operations*; JP 3-54, *Joint Doctrine for Operations Security*; and JP 3-58, *Joint Doctrine for Military Deception*.

This manual establishes the following as the definition of IO used by Army forces: ***Information operations*** **is the employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to affect or defend information and information systems, and to influence decisionmaking.** This definition supersedes the definition of IO in FM 3-0. It is consistent with joint initiatives.

SCOPE

The publication addresses IO doctrine in Part I and TTP in Part II. Part I also establishes Army operations security (OPSEC) and military deception doctrine.

APPLICABILITY

This publication applies to Army forces from Army service component command (ASCC) to maneuver brigade. It is most applicable to corps and divisions. The primary users of this manual are ASCC, corps, division, and brigade commanders and staff officers—specifically the G-2, G-3, G-7, and staff representatives for military deception, electronic warfare, operations security, fire support, psychological operations, civil affairs, and public affairs. Battalions normally execute higher headquarters IO. In stability operations and support operations, they may be given IO assets. Thus, they need to know their role in brigade and division IO.

TRADOC service schools and branch proponents should use FM 3-13 as a point of departure for integrating IO into branch doctrine and military instruction.

ADMINISTRATIVE INFORMATION

Terms that have joint or Army definitions are identified in both the glossary and the text. The glossary lists most terms used in FM 3-13 that have joint or Army definitions. Terms for which FM 3-13 is the proponent manual (the authority) are indicated with an asterisk in the glossary. Definitions for which FM 3-13 is the proponent manual are printed in boldface in the text. These terms and their definitions will be incorporated into the next revision of FM 1-02. For other definitions in the text, the term is italicized and the number of the proponent manual follows the definition.

The glossary contains referents of acronyms and definitions of terms not defined in JP 1-02 and FM 1-02. It does not list acronyms and abbreviations that are included for clarity only and appear one time, nor those that appear only in a figure and are listed in the legend for that figure. Some common abbreviations and acronyms—for example, the abbreviations for military ranks and publications—are not spelled out; refer to the glossary. Since *ARFOR* is a defined term as well as an acronym, it is not spelled out.

"President" refers to the President and the Secretary of Defense, or their duly deputized alternates and successors.

All references to annexes refer to annexes to operation plans (OPLANs) or operation orders (OPORDs) unless stated otherwise.

Unless stated otherwise, masculine nouns or pronouns do not refer exclusively to men.

Headquarters, US Army Training and Doctrine Command, is the proponent for this publication. The preparing agency is the Combined Arms Doctrine Directorate, US Army Combined Arms Center. Send written comments and recommendations on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to: Commander, US Army Combined Arms Center and Fort Leavenworth, ATTN: ATZL-CD (FM 3-13), 1 Reynolds Road (Building 111), Fort Leavenworth, KS 66027-1352. Send comments and recommendations by e-mail to web-cadd@leavenworth.army.mil. Follow the DA Form 2028 format or submit an electronic DA Form 2028.

Introduction

Information operations (IO) encompass attacking adversary command and control (C2) systems (offensive IO) while protecting friendly C2 systems from adversary disruption (defensive IO). Effective IO combines the effects of offensive and defensive IO to produce information superiority at decisive points.

IO brings together several previously separate functions as IO elements and related activities. IO elements include the IO core capabilities, specified supporting capabilities, and related activities discussed in chapter 1. It also allows commanders to use all of them both offensively and defensively, as they deem appropriate. The assistant chief of staff (ACOS) G-7 has the coordinating staff responsibility for coordinating IO elements and related activities. This enables the G-7 to shape the information environment to friendly advantage and protect commanders and friendly C2 systems from adversary IO.

Commanders do not conduct IO simply for the sake of doing IO. Effective IO is an integrated effort that synchronizes the effects of IO elements/related activities to accomplish specific objectives designated by the commander. It is the means commanders use to mass the effects of the information element of combat power.

Offensive IO destroy, degrade, disrupt, deny, deceive, exploit, and influence adversary decisionmakers and others who can affect the success of friendly operations. Offensive IO also target the information and information systems (INFOSYS) used in adversary decisionmaking processes.

Defensive IO protect and defend friendly information, C2 systems, and INFOSYS. Effective defensive IO assure friendly commanders an accurate common operational picture (COP) based not only on a military perspective, but also on nonmilitary factors that may affect the situation. An accurate COP is essential to achieving situational understanding. (See FM 6-0.) Most IO elements may be used either offensively or defensively. Effective IO requires integrating IO related activities—such as, public affairs and civil military operations—into IO as well.

The goal of IO is to gain and maintain information superiority, a condition that allows commanders to seize, retain, and exploit the initiative. It facilitates more effective decisionmaking and faster execution. IO involve constant efforts to deny adversaries the ability to detect and respond to friendly operations, while simultaneously retaining and enhancing friendly force freedom of action. When expeditiously exploited, IO provide a potent advantage that facilitates rapid military success with minimal casualties. Effective IO and information management allow commanders to take advantage of opportunities, while denying adversary commanders the information needed to make timely and accurate decisions or leading them to make decisions favorable to friendly forces.

Army forces routinely employed the elements of IO separately in past conflicts. Psychological operations, operations security, military deception, physical destruction, and electronic warfare were viable tools of Army commanders during World War II. The Gulf War demonstrated the benefit of employing these elements

together and synchronizing them with ground operations. Capitalizing on this knowledge, the Joint Staff produced a series of doctrinal publications that culminated in October 1998 with JP 3-13, *Joint Doctrine for Information Operations*.

Today, Army IO doctrine and tactics, techniques, and procedures (TTP) adapt joint IO doctrine to achieve information superiority at decisive points during full spectrum operations. Because adversaries have asymmetric abilities to counter finite friendly IO capabilities, the probability of maintaining information superiority over long periods is unlikely. Therefore, commanders execute IO to gain information superiority at times and places where it supports their intent and concept of operations.

Technological advancements in automated INFOSYS and communications have allowed commanders to see the battlefield as actions unfold, closer to near real-time than ever before, and to rapidly pass information across their areas of operations. Combined, IO and advanced INFOSYS and communications continue to shorten the time required for staff processes. This compresses the decision cycle and increases operational tempo, the rate of military action. Commanders now have opportunities to achieve decisive results early in an operation, reducing casualties and conserving resources.

Advancements in automated INFOSYS and communications carry with them vulnerabilities commanders need to recognize and offset. Clearly, a force dependent on technology offers adversaries new opportunities to degrade its effectiveness. Army forces face significant vulnerabilities due to their dependence on information technology. Army communications and technologies are becoming more and more dependent on commercial backbones and commercial off-the-shelf products and systems that are also readily available to potential adversaries. This situation makes defensive IO an essential aspect of all operations.

PART ONE

Information Operations Doctrine

Commanders conduct (plan, prepare, execute, and assess) information operations (IO) to apply the information element of combat power. Combined with information management and intelligence, surveillance, and reconnaissance operations, effective IO results in gaining and maintaining information superiority. Information superiority creates conditions that allow commanders to shape the operational environment and enhance the effects of all elements of combat power. IO has two categories, offensive IO and defensive IO. Commanders conduct IO by synchronizing IO elements and related activities, each of which may be used either offensively or defensively. Army IO doctrine supports joint IO doctrine, supplementing it where necessary to meet the conditions of land operations. Part One discusses the doctrinal concepts that underlie IO and the capabilities of, contributions made by, and links among the IO elements and related activities. It also establishes doctrine for two IO elements: operations security and military deception.

Chapter 1

Design of Army Information Operations

Information operations (IO) bring together several previously separate functions as IO elements and related activities. To provide unity of effort, IO is placed under a special staff officer, the assistant chief of staff G-7.

CONTENTS