

INFORMATION OPERATIONS—HOW MEANINGFUL IS IO DOCTRINE?

Amanda J. Brosnan

Abstract. It has been claimed that, for the most part, meaningful IO doctrine is non-existent. This paper explores that claim focusing on US IO doctrine. First, internal issues relating to doctrine architecture are examined. Possible uses of IO contained in the doctrine are broad, but can be viewed as going some way to incorporate the potential of IO into the relatively static environment of doctrine. Doctrinal IO components include a variety of activities that influence the information domain, and these too are generalised enough to accommodate development in IO. However, staff structures and processes on which current US IO doctrine is based are ill-suited to IO. In addition, the doctrine fails to adequately deal with vulnerabilities derived from connectivity between the DII and deployed force networks, and an over-emphasis on the role of IT in IO introduces weaknesses into IO doctrine. Secondly, external issues are addressed. Legal problems associated with the conduct of IO compromise the meaningfulness of IO doctrine, as do problems encountered when conducting IO in multinational environments. Also, the lack of adequate national IO policy adversely affects both the conduct of IO and the ability to protect military IO vulnerabilities. Overall, although current US IO doctrine contains much that is useful, the points of weakness are fundamental and do indeed significantly degrade the overall meaningfulness of IO doctrine as it stands today.

INTRODUCTION

At the beginning of the Twenty First Century it seems safe to say that IO is not simply the latest military fad, but rather is a concept that has come of age at one of those crossroads of history where intent and capability coincide. Information has always been an essential element in military victories and defeats, but only in the Information Age have we acquired the capabilities to better harness the potential benefits and minimise the potential risks of using information as a weapon to influence the mind and decision-making ability of an opponent.

The process by which the concept of IO is embraced by military forces is, of course, the development of military doctrine—the set of fundamental principles that a military force uses to guide actions in support of national objectives. Military IO doctrine seeks to take the principles of IO and translate them into guidelines for the conduct of IO.

In a paper assessing the effectiveness of IW in Kosovo, Frederic H. Levien comments that: “Much of the most exciting technology of IW is still in its infancy and, for the most part, meaningful doctrine is non-existent.” [1] A thought-provoking assertion. The aim of this paper is to assess just how meaningful current IO doctrine is by examining a number of issues pertinent to the on-going development of military IO. These issues will be classified as either internal or external, with internal issues being those directly related to IO doctrine architecture, while external issues are matters which affect how meaningful IO doctrine is in practice.

Before proceeding, the scope of the paper should be defined. Although many states have developed or are developing IO doctrine, the United States military has led the way in both doctrine development and implementation. For that reason it is US IO doctrine that is the focus of this paper. [2]

INTERNAL ISSUES

IO Uses and Components

In US doctrinal terms, IO are a tool a commander can use to dominate the information environment and thereby influence an adversary’s decision making and ability to act. Together with information management, and supporting activities such

as Civil Military Affairs, Public Affairs and intelligence, IO are conducted to achieve the overarching goal of information superiority (IS), defined as:

“The ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary’s ability to do the same. It is a window of opportunity created by focused efforts that allows the actions or beliefs of the adversary commander to be influenced in support of decisive operations.” [3]

US doctrine allows for the use of IO across the range of military operations—from military operations other than war (MOOTW) through to conflict and war—and across the spectrum of conflict—from peace, through escalation and conflict, to cessation of conflict. Doctrine also accommodates the use of IO at all levels of war, from strategic, through operational, to tactical. Further, offensive IO (IO-O) may be conducted as a stand-alone operation, as the main effort of an operation, as a supporting effort (force multiplier) within a conventional campaign, or as a phase of an operation. [4]

Is this meaningful, or is the doctrine simply having a bet all possible ways? The answer to this question brings us back to IO theorist Martin Libicki’s analogy of a blind man and an elephant—the blind man may think he is touching many quite separate and different animals when in fact all parts belong to one large whole. [5] IO encompasses age-old pursuits such as psychological operations and deception, more recent activities such as command and control warfare (C2W), and quite recent activity of cyberwarfare. It has many different parts and many possible uses, and the beast is still evolving. Military doctrine lags behind evolutionary trends and, once formulated, is slow to change. So, the broad descriptions of how doctrine envisions IO being used in a military environment could be viewed as an attempt to incorporate the potential of IO into the relatively static environment of doctrine.

Can the same be said for the activities doctrine groups under the IO umbrella? Within US doctrine, IO-O activities include PSYOPS, EW, deception, destruction, OPSEC and computer network attack. Activities included in defensive IO (IO-D) doctrine are EW, physical security, counterdeception, counterpropaganda, counterintelligence and OPSEC. Is this list meaningful? Yes, because what all these components