Information Assurance Technology newsletter

IATAC is a Department of Defense Sponsored Information Analysis Center. Vol. I, No. 2 • July 1997

DIA SUPPORT TO INFORMATION OPERATIONS

The Defense Intelligence Agency (DIA) has demonstrated its commitment to information warfare by establishing the DIA Information Warfare Support Office. Its mission is:

- To produce integrated all-source intelligence supporting U.S. offensive and defensive Information Operations (IO) plans and operations;
- Identify and analyze the IO threat potential and capabilities of foreign nations, transnational groups, or coalitions; and
- Develop detailed intelligence analysis of:
  - Foreign leadership operations and decisionmaking processes;
  - Information technologies, systems, and networks; and
  - Denial and deception programs.

The Information Warfare Support Office is made up of four divisions: **Special Activities, Intelligence Preparation of the Battlespace, Threat Analysis,** and **Foreign Denial and Deception.**

The **Special Activities Division** serves four principal customers: the Unified Commands, the Services, the Joint Staff, and the intelligence community. For the Unified Commands, the division provides intelligence support to OPLAN/CONPLAN information warfare annex development and provides tailored support to Special Technical Operations planning.

The Special Activities Division also supports the research, development, test and evaluation process of the Services and satisfies information warfare intelligence requirements for the Services.

For the Joint Staff, the division provides political-military assessments; intelligence for contingencies, operations, and deliberate and crisis planning; and tailored, coordinated databases.

For the intelligence community, the Special Activities Division coordinates all-source intelligence for the Special Technical Operations program, interfaces with the collection community, and supports specialized battle damage assessments.

The **Intelligence Preparation of the Battlespace** (IPB) Division provides detailed, all-source, fused intelligence assessments of the operations and decisionmaking processes of the

Continued on page 3

1st Annual Information Assurance Red Team Assessment Workshop Williamsburg, VA on August 13 - 14, 1997

The Defense Information Systems Agency and the Joint Staff (J6K) announce the 1st Annual Information Assurance (IA) Red Team Assessment Workshop to be held August 13 - 14, 1997, at the Fort Magruder Inn (classified sessions at Fort Eustis), Williamsburg, Virginia, under the auspices and sponsorship of the Defense Information Systems Agency and the Joint Staff (J6K) Information Assurance Division.

The workshop is classified **SECRET/ US GOVERNMENT ONLY** and provides an opportunity for participants in IA Red Team Assessments to provide input from their research and experiences and identify what they can provide to mitigate the IA threat.

This Workshop is intended to provide a forum for the discussion, interchange, and debate of accomplishments, discoveries, and issues in the IA area. It is significant because of recent progress made in critical technologies and in the military utilization of these technologies. The Workshop will provide a setting for discussion of the implications of this technology on U.S. government information resources.

To ensure a balanced program for an integrated red team assessment process, the Workshop will consider the various needs of all known customers as well as the capabilities of current and projected models and simulations and analytical methodologies.

For registration information on the Information Assurance Red Team Assessment Workshop, access the IATAC home page at http://www.iatac.dtic.mil on the internet, http://204.36.65.5/index.html on Intelink-S, and http://www.rl.gov./rl/irido/iatac on Intelink or call Alethia Tucker at (703) 902-4664.

contents

IA Definitional Debate 2
Conferences and Symposia 5
Contacting Us.....5

Information Assurance Evolves From Definitional Debate

by Dr. John I. Alger
IATAC Director

When the din of battle subsides, observers, pundits, and especially soldiers focus their attention on lessons learned. The 1991 conflagration in Southwest Asia was no exception in this regard, and the examination of the extremely favorable results achieved by the United States and its United Nations allies brought a new level of intensity to the debate concerning the nature of future war.

To some, a new age beckoned; to others, attention to long established tenets of war, such as "mass," "security," and "surprise," proved their worth. Yet even the iconoclasts recognized that "information" had emerged as the prime, if not decisive, contributor to the allied success. The significance of "information" was derived from the phenomenal advances in the realm of digital technology.

Policy and doctrinal guidance have attempted to keep pace with the spiral of information technology advances, but agreement on even the most fundamental definitions has provided a challenge within the Department of Defense (DoD). This article traces the evolution of that definitional debate through the five-plus years since the end of the Gulf War, calls attention to the role of information in the deterrence and prosecution of future war, and hopefully promotes a better understanding of the evolving definitions themselves.

The recognition of the elevated role of information in deterrence and in war was manifested in a revision of the Department of Defense Directive 3600.1, which appeared under the title, *Information Warfare,* in December 1992.

Following the DoD lead on information war, the Office of the Joint Chiefs of Staff undertook the writing of a complementary publication on new concepts of war demonstrated in the Gulf. The result of the Joint Staff effort was the publication of "Chairman of the Joint Chiefs of Staff Memorandum of Policy Number 30" (MOP 30), in March 1993. It took the title, *Command and Control Warfare.*

MOP 30 defined the relationship between "command and control warfare (C^2W)" and "information warfare (IW)" by stating explicitly: "C^2W is the military strategy that implements Information Warfare on the battlefield and integrates physical destruction." Implicit in this definition is the recognition that information warfare also occurs "off the battlefield" and that it can be void of "physical destruction."

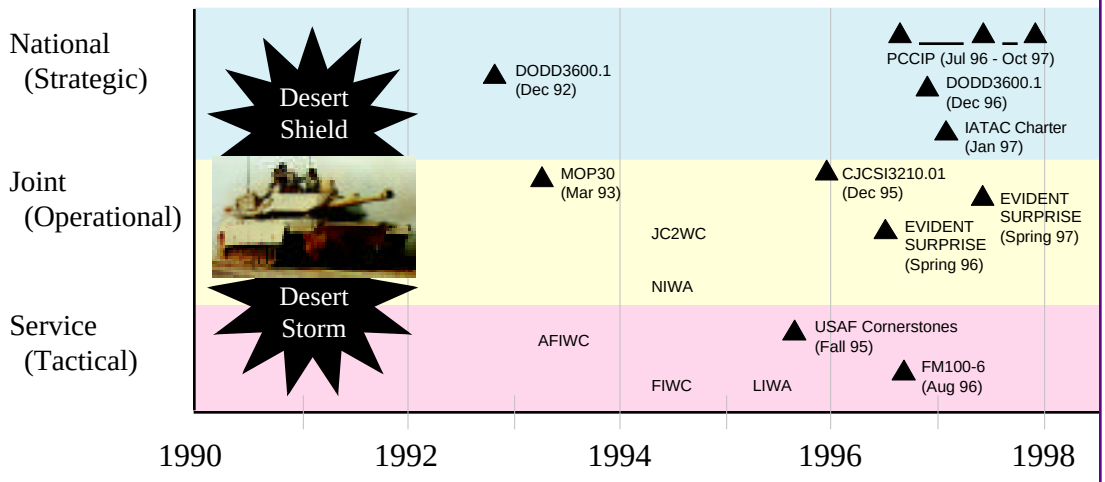
In addition to defining the relationship between C^2W and IW, MOP 30 also stated that C^2W encompassed the "integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW) and physical destruction, mutually supported by intelligence." Widely known as the five pillars of C^2W, these elements did not, however, address the role of computers and networks in future warfare.

To better address the role of information and information systems in future war, the US Air Force transitioned its Electronic Warfare Center at Kelly AFB, San Antonio, TX, to an organization with a much broader perspective. The new center is called the Air Force Information Warfare Center, and focuses on both the role of information in future war and the need for information assurance. One year later, under the auspices of the Chairman of the Joint Chiefs of Staff, the Joint Electronic Warfare Center, also at Kelly AFB, became the Joint Command and Control Warfare Center. Its focus is on information support to the Commanders-in-Chief of the Unified Commands. Further attention to the primacy of information in future war was evidenced at the National Defense University where the School of Information Warfare and Strategy opened its doors to the first of two 10-month pilot programs in information warfare in August 1994.

Following the lead of the Air Force

Continued on page 3

Toward Information Assurance



and the Joint Staff, the Navy and the Army were quick to establish organizations to support the new concepts of deterrence and warfighting. The Navy established the Naval Information Warfare Activity at Fort Meade, MD, and the Fleet Information Warfare Center at Norfolk, VA, with detachments at San Diego, CA, Honolulu, HI, and Chesapeake, VA. The Land Information Warfare Activity was established by the Army at Fort Belvoir, VA. Information assurance is a critical element in each of these organizations.

As each organization pursued concepts and definitions suited to its mission, each was also involved in the definitional debate within the Department of Defense. By 1994, it was widely recognized that the concepts of information warfare were not well served by the definition of information warfare that appeared in the December 1992 DoD directive. Not surprisingly, each of the principal organizations involved in the concepts of information warfare tailored definitions consistent with and appropriate to its own culture, missions, and doctrine.

Insights into the concepts of each of the major organizations involved in information warfare are clearly seen in the publications of those organizations. The first major organization to promote widely the concept of information warfare was the US Air Force. In the fall of 1995, General Fogleman, the Air Force Chief of Staff, and Secretary Widnall, Secretary of the Air Force, signed the Foreword to a pamphlet entitled, *Cornerstones of Information Warfare.* The pamphlet defined information warfare as: "any action to deny, exploit, corrupt, or destroy the enemy's information and its function; protecting ourselves against those actions; and exploiting our own military information functions." The pamphlet also detailed six elements of information war. Four were fully consistent with the elements of command and control warfare presented in MOP 30. These were: psychological operations, military deception, physical destruction, and electronic warfare. Where MOP 30 had focused on OPSEC as an element, *Cornerstones* focused on "security measures," which was defined as OPSEC, COMSEC (communications security), and COMPUSEC (computer security). The sixth element of information warfare from the Air Force perspective was "information attack," which was defined as "directly corrupting information without visibly changing the physical

Continued on page 4

DIA SUPPORT TO INFORMATION OPERATIONS

Continued from page 1

national leadership in potential adversary countries to support information operations planning and operations.

The division also develops methodologies for assessing the influence of cultural, psychological, and other human factors on leadership operations and decisionmaking. To support IO targeting, the division produces detailed communications and information system templates of potential adversary countries. Finally, the division provides consultative support to IO operational planners and creates new products and display formats for providing the most useful access to required intelligence.

The **Threat Analysis Division** detects, identifies and assesses IO capabilities of nations, groups, coalitions, and individuals that threaten the U.S. defense and national information infrastructures. Through all-source intelligence products, the division assists in force protection and defensive IO operations. The division also supports the design and implementation of a defense intelligence warning system for IO attacks, and supports Department of Defense Information Assurance activities.

The Threat Analysis Division also supports the Defense Information Infrastructure, or DII, by producing:

- IO national intelligence estimates,
- System threat assessment reports,
- Country-specific IO threat assessments,
- Information on foreign IO technologies and tools,
- An Electronic Warfare Integrated Reprogramming Data Base, and
- Information on threats to components of the DII.

The **Foreign Denial and Deception Division** of the Information Warfare Support Office detects and analyzes foreign denial and deception directed against U.S. intelligence, national security policy and military strategy, and strategic and conventional targeting, weapons acquisition, military operations, IO, and strategic arms control monitoring. The division detects, identifies, characterizes and monitors foreign underground and enigma facilities and produces all-source intelligence products to support U.S. policy, plans, operations, and acquisitions. Other areas of interest to the Foreign Denial and Deception Division include:

- Foreign denial and deception programs,
- Deception technologies and equipment,
- Foreign perception management,
- Military industrial concealment, and
- Underground facilities and enigmas.

In conclusion, DIA products address the full spectrum of information operations activities. DIA provides integration of intelligence and operations for the warfighter, Defense HUMINT Service information warfare support, information systems support, and a robust open source intelligence program. Since the range of potential contingencies in which the United States is likely to become involved covers the spectrum of conflict, IO support will remain a priority DIA mission area well into the future.

Information Assurance Evolves From Definitional Debate

Continued from page 3

entity in which it resides." Thus, the Air Force elevated the elements of command and control warfare to elements of information warfare. The Air Force also added "information attack" to the taxonomy of IW. These Air Force contributions were indicative of the Air Force's focus on technology and its impact on traditional Air Force missions.

Following the publication of the Air Force's *Cornerstones*, the Chairman of the Joint Chiefs of Staff (CJCS) published CJCS Instruction 3210.01, *Joint Information Warfare Policy.* Its IW definition was identical with the then-current definition in the working draft of DoD Directive 3600.1: "Actions taken to achieve information superiority by affecting adversary information, information-based processes, and information systems while defending one's own information, information-based processes, and information systems." The instruction also discussed the elements of information warfare and spoke of them in terms consistent with MOP 30 and *Cornerstones.*

The third major doctrinal publication to appear, while the revision of DoD Directive 3600.1 was in progress, was the Army's Field Manual 100-6, *Information Operations.* The Army recognized "that IW as defined by DoD was more narrowly focused on the impact of information during actual conflict, [and chose] to take a somewhat broader approach to the impact of information on ground operations and adopted the term information operations." The Army took this view to recognize "that information issues permeate the full range of military operations (beyond just the traditional context of warfare) from peace through global war."

The definition of information operations offered by the Army differed significantly from other official definitions. Army IO was defined as, "Continuous military operations within the MIE [military information environment] that enable, enhance, and protect the friendly force's ability to collect, process, and act on information to achieve an advantage across the full range of military operations; IO include interacting with the GIE [global information environment] and exploiting or denying an adversary's information and decision capabilities." The Army accepted the five C^2W elements as a part of IO and added that civil and public affairs were also fully integral to Army IO. Again, the Service's culture established the perspective given to the key definitions and taxonomy of information terms.

While the publication of key information terms occurred at the Joint Staff level and in the Services, the staffing of the overarching term from a DoD perspective continued for more than two years. The Joint Staff, Air Force, and Army each proposed its own culturally driven terms and definitions. When the new DoD Directive 3600.1 was signed on 9 December 1996, it took the title, *Information Operations,* which hence became the DoD overarching term pertinent to the role of information in warfare. The directive defined Information Operations simply as "Actions taken to affect adversary information and information systems while defending one's own information and information systems." In its discussion of the components of IO, the directive included the elements of C^2W from MOP 30, the idea of computer network attack suggested in the Air Force's *Cornerstones,* and the contributions of public affairs and civil affairs as set forth by the Army in FM 100-6. Thus the new DoD Directive had evolved to incorporate the seminal ideas of the Services and other key players in the information arena. It also defined Information Assurance (IA) as: "IO that protect and defend information and information systems. . . ." and stated that IA activities should be vigorously pursued.

While the key influencing factors in the evolution of the present DoD definition of information operations cited above focused on the Air Force, Joint Staff, and Army, the role of the Navy, Marine Corps, and especially the intelligence community should not be overlooked. The Navy has incorporated the concepts of information operations into their day-to-day fleet activities. The Marines have written about command and control which subsumes information concepts, and similarly the intelligence community has contributed immensely to the process of definition.

From the 1992 DoD Directive on information warfare through each of the publications discussed in this article, the idea of protecting information has been an integral part of every examination of information concepts. The primacy of protecting and defending information has been evident, and today, it is well incorporated into the DoD Directive on Information Operations and in Service publications.

As information operations evolved to accept elements of the earlier definitions of information warfare, so information assurance evolved as the term of choice for defensive IW or command and control protection. The concepts of "protect and defend" are very much in evidence in the DoD Directive 3600.1 definition of information assurance: "Information Operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities."

Conferences & Symposia

IIBW9xxx: Intermediate Information Operations/Warfare (IBW)

5 days, Secret Clearance required, O-4 through O-6 and equivalents.
School of Information Warfare and Strategy
National Defense University, Fort McNair, DC
IBW9801 17-21 Nov 97
IBW9802 12-16 Jan 98
IBW9803 9-13 Mar 98
IBW9804 13-17 Jul 98
IBW9901 19-23 Oct 98
POC: Dr. Fred Giessler, 202-685-2209

SIW9xx: Senior Information Warfare (SIW)

2 days, TS/SCI required, O-7, equivalents and above.
O-6s accepted on waiver
School of Information Warfare and Strategy
National Defense University, Fort McNair, DC
SIW9801 5-6 Nov 97
SIW9802 12-13 Feb 98
POC: Dr. Fred Giessler, 202-685-2209

Introduction to Information Operations

5 days, TS/SCI Clearance required, O-3 through O-6 and equivalents.
Joint Military Intelligence Training Center, Bolling AFB, DC
20-24 Oct 1997
2-6 Feb 1998
4-8 May 1998
POC: Mr. Doug Dearth, 703-780-2584 – e-mail: dhdearth@aol.com

Information Assurance Red Team Assessment Workshop by DISA and the Joint Staff (J6K)

13-14 August 97
SECRET/US GOVERNMENT ONLY
Fort Magruder Inn, Williamsburg, VA
POC: 703-902-4664
(See article on page 1.)

infoWARcon '97, "Safeguarding Your Information from Your Competitors" by the National Computer Security Association and Winn Schwartau, Infowar.com

11-12 September 97
Sheraton Premier, Tysons Corner, VA
POC: 1-800-488-4595, ext 3226

"National Information Systems Security Conference" by the National Computer Security Center at the National Security Agency and the National Institute of Standards and Technology

7-10 October 97 with Pre-Conference Workshops on 6 October
Baltimore Convention Center, Baltimore, MD
POC: 301-975-2775

Information Assurance Technology Newsletter, Vol. 1 No. 2

This second issue of the Information Assurance Technology Newsletter focuses on the evolution of concepts and definitions pertinent to information assurance. The newsletter also features an overview of the central role that the Defense Intelligence Agency and the Defense Information Systems Agency play in important information operations issues.

IATAC, a DoD-Sponsored Information Analysis Center (IAC), is administratively managed by the Defense Technical Information Center (DTIC) under the DoD IAC Program. Inquiries about IATAC capabilities, products, and services, or comments regarding this publication may be addressed to:

Dr. John I. Alger
Director, IATAC
2560 Huntington Avenue
Alexandria, VA 22303-1403

Contacting Us

Telephone: (703) 329-7337
Facsimile: (703) 329-7197
STU-III: (703) 329-3940
STU-III Facsimile: (703) 329-7106
e-mail: iatac@dtic.mil
www: http://www.iatac.dtic.mil
Intelink-S: http://204.36.65.5/index.html
Intelink: http://www.rl.gov./rl/irido/iatac

Distribution & Information

U.S. Distribution Only.

❑ CHANGE ME (as noted below) ❑ ADD ME

❑ SEND IATAC TECHNICAL AREA TASK INFO (Government only)

Name_____

Title _____

Company/Organization _____

Address _____

_____

City/State/Zip_____

Phone _____ Fax _____

DSN_____ E-mail _____

ORGANIZATION: ❑ USA ❑ USN ❑ USAF ❑ USMC ❑ OSD ❑ Contractor

Your Input Is Welcome...

The Information Assurance Technology Newsletter welcomes input from our readers. To submit photographs, related articles, notices, feature programs or ideas for future issues, please use the address, fax or e-mail as noted.

CLIP & SEND TO:

Information Assurance Technology Analysis Center
2560 Huntington Avenue,
Alexandria, VA 22303-1410

FAX (703) 329-7197

E-mail: iatac@dtic.mil

Information Assurance Technology newsletter