



PHOENIX CHALLENGE 2002

Intelligence, Information Operations, and Information Assurance

***Mr. Allen Sowder
Deputy Chief of Staff, G-2 IO Team
22 April 2002***

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 22-04-2002		2. REPORT TYPE Briefing		3. DATES COVERED (FROM - TO) xx-xx-2002 to xx-xx-2002	
4. TITLE AND SUBTITLE Phoenix Challenge 2002: Intelligence, Information, Operations, and Information Assurance Unclassified				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Sowder, Allen ;				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME AND ADDRESS USA xxxxxx, xxxxxxxx				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS USA ,				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT APUBLIC RELEASE ,					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT See report.					
15. SUBJECT TERMS IATAC Collection					
16. SECURITY CLASSIFICATION OF:		17. LIMITATION OF ABSTRACT Public Release	18. NUMBER OF PAGES 11	19. NAME OF RESPONSIBLE PERSON Email from Booz, Allen & Hamilton (IATAC), (blank) lfenster@dtic.mil	
a. REPORT Unclassified	b. ABSTRACT Unclassified			c. THIS PAGE Unclassified	19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703767-9007 DSN 427-9007
				Standard Form 298 (Rev. 8-98) Prescribed by ANSI Std Z39.18	

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 074-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE 4/22/2002	3. REPORT TYPE AND DATES COVERED Briefing 4/22/2002	
4. TITLE AND SUBTITLE Phoenix Challenge 2002: Intelligence, Information Operations, and Information Assurance			5. FUNDING NUMBERS	
6. AUTHOR(S) Sowder, Allen				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Department of the Army			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Department of the Army			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; Distribution unlimited			12b. DISTRIBUTION CODE A	
13. ABSTRACT (Maximum 200 Words) This briefing discusses: Policy and Doctrine Foundations, Processes and Players, Understanding the Threat, USA Patriot Act, The Information Dominance Center and Major Challenges. This briefing was given during the Phoenix Challenge Conference and Warfighter Day.				
14. SUBJECT TERMS IATAC Collection, information operations, information assurance			15. NUMBER OF PAGES 10	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT UNLIMITED	



Intelligence, Information Operations, and Information Assurance

AGENDA

**Policy and Doctrine Foundations
Processes and Players
Understanding the Threat
USA PATRIOT ACT
The Information Dominance Center
Major Challenges**



Information Operations Doctrine



JP 3-13 (Information Operations)

Offensive IO

OPSEC

PSYOP

Military Deception

Electronic Warfare

Physical Attack/Destruction

CNA

Defensive IO

Information Assurance

OPSEC

Physical Security

Counterdeception

Counterpropaganda

Counterintelligence

Electronic Warfare

**Public Affairs and Civil Affairs
are related IO Activities**

**Joint and
Army
doctrine are
mutually
supporting**

**Intelligence
supports IO**

FM 3-0 (Operations)

**“Each element may have offensive or
defensive applications.”**

OPSEC

PSYOP

Military Deception

Electronic Warfare

Physical Destruction (Attack)

CNA

Information Assurance

CND

Physical Security

Counterdeception

Counterpropaganda

Counterintelligence

**Public Affairs and Civil Military
Operations are related activities**

UNCLASSIFIED/HQDA



Intelligence, Information Operations, and Information Assurance

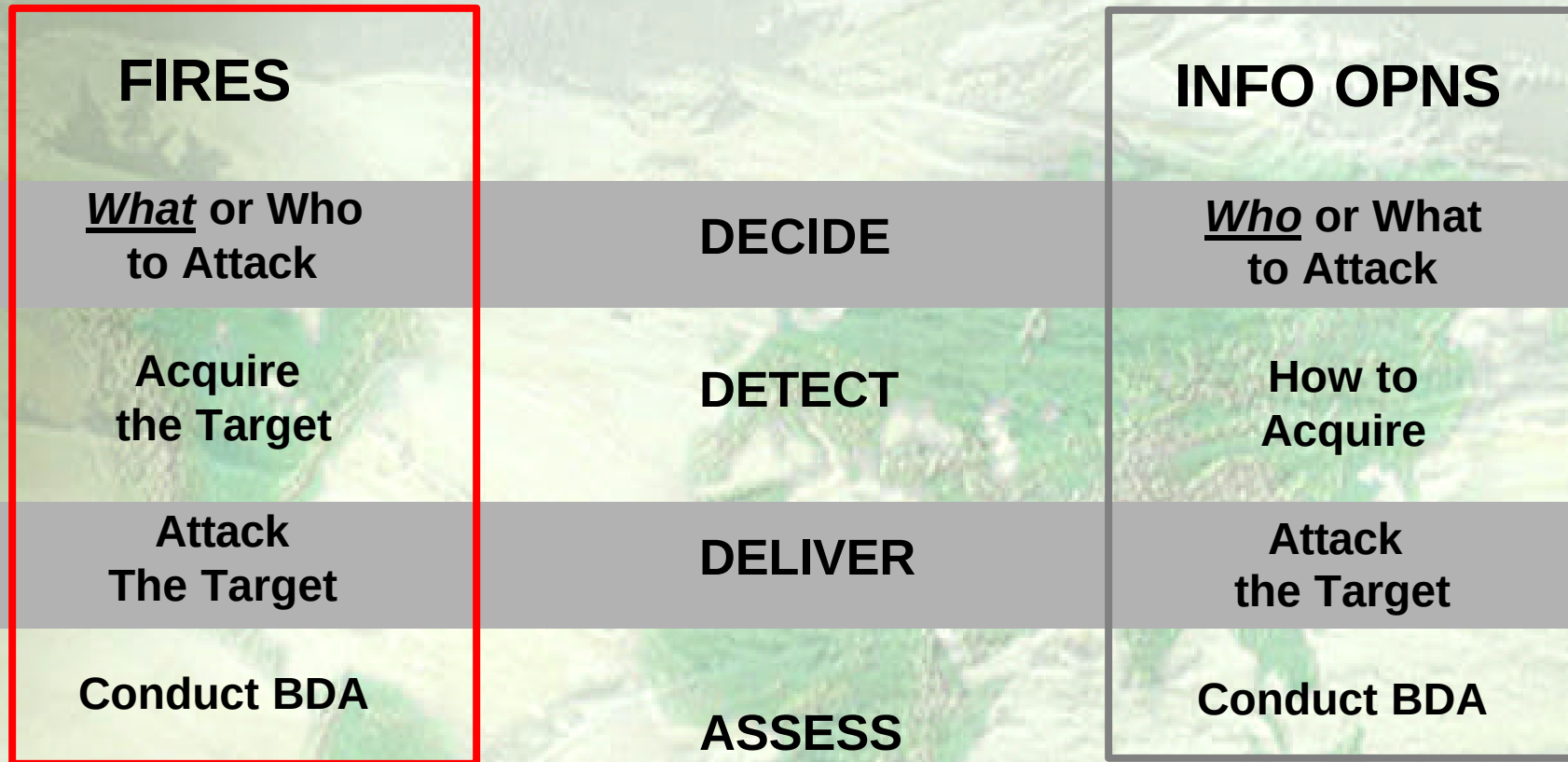
The Army's approach to IO management is built on the IO TRIAD:

- **The G-2 provides the intelligence support and some operational capabilities.**
- **The G-3 is the Army's IO lead, and has OPCON of the Army's full spectrum, IO field deployable force – the Land Information Warfare Activity (LIWA).**
- **The G-6 is the Army's CIO, and provides the foundation of Information Assurance policies.**

The Army's Space and Missile Defense Command provides the Joint interface to USSPACECOM.



Traditional Processes vs. Information Operations Processes



Similar targeting process



Traditional Fires vs. Information Operations Targeting Objectives



Describe the Effects of Target Attack on the Enemy

FIRES		INFO OPERATIONS
Reduce available options or COAs	LIMIT	Minimize influence
Preclude effective combat system cohesion	DISRUPT	Reduce Effectiveness
Alter time of arrival	DELAY	Slow decisionmaking
Tie up critical resources	DIVERT	Redirect resources
Ruin the target's structure	DESTROY	Eliminate influence
Inspect/Assess	DAMAGE	Often Subjective

Similar objectives

UNCLASSIFIED/HQDA



Understanding the Threats' Tactics



“... 99% of Computer Attack is Access.”

LTG Minihan, DIRNSA March 1998

Relationship between a probe, or an intrusion and a computer network attack (CNA) is often one key-stroke ... Without access there can be no external CNA.

Access and exploitation are required even in absence of attack.

At least 88% of all intrusions to Army networks in CY 00 came from the exploitation of KNOWN vulnerabilities.

- **How we might conduct CNA is a clue to how “they” might conduct CNA. There is tremendous value from Red Teaming.**
- **Must view “probes” as Intelligence Preparation of the Battlespace, and a precursor to CNA. We must be able to detect, and recognize the activity; this is attack sensing and warning.**
- **Effective computer network defense requires cooperation between the network operators, end users, CNA Forces and intelligence assets.**

UNCLASSIFIED/HQDA



USA PATRIOT ACT of 2001 Helps



The Act does not erode Constitutional protections, it does not minimize E.O. 12333, but it does insert “technology neutral” language to help in the war on international terrorism.

Section 217 defines a **computer trespasser** as “a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy...”

This Section authorizes a computer system owner to consent to the interception of computer intruders’ communications without a court order, so long as the government conduct is part of a lawfully authorized investigation.

Other important Sections include 203, 206, 207, 224, 504, and 905.



INFORMATION DOMINANCE CENTER

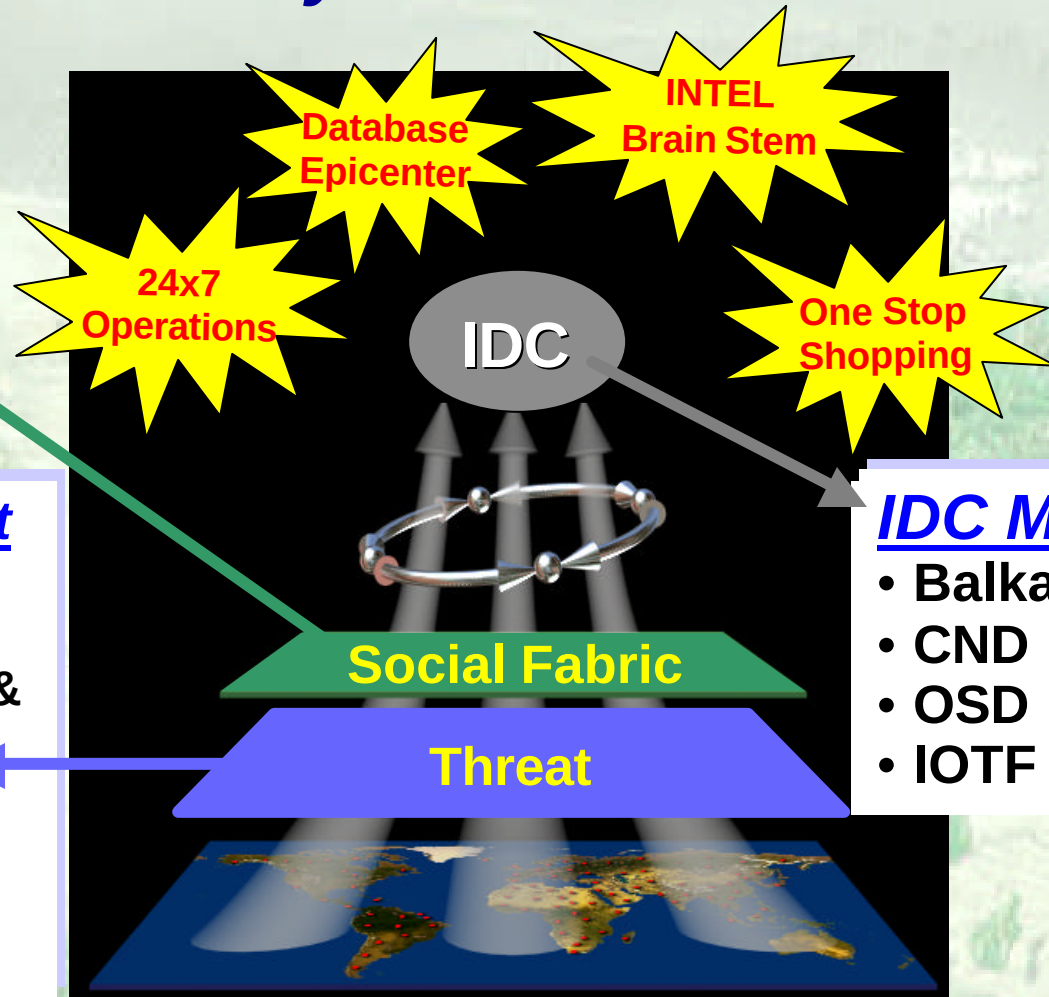
The Army's TOC for IO

Social Fabric

- Mugs
- Thugs
- Wackos

Asymmetric Threat

- Complex & Changing
- Adaptive, Cunning & Learning
- Asynchronous
- Commercial Technology Levels Playing Field



IDC Mission

- Balkans
- CND
- OSD
- IOTF



The Major Challenges

- ❖ **Definition and implementations : Legal/Regulatory policies**
- ❖ **Robust, fault tolerant technologies with built-in security features, configuration management**
- ❖ **Intelligence support to IO:
More, Faster, New Areas (subjects, and locations),
languages (human, and technical)**
- ❖ **IO education and training challenges**
- ❖ **Skill identifiers and optimal force mix; enlisted, warrant, and officer**
- ❖ **Personnel turnover**
- ❖ **IO funding issues – Nothing is more complex, or critical**