PHOENIX CHALLENGE 2002

Intelligence, Information Operations, and Information Assurance

Mr. Allen Sowder
Deputy Chief of Staff, G-2 IO Team
22 April 2002
Phoenix Challenge 2002: Intelligence, Information, Operations, and Information Assurance

Title and Subtitle

Sowder, Allen

Author(s)

USA

Performing Organization Name and Address

USA

Sponsoring/Monitoring Agency Name and Address

Performing Organization Report Number

DISTRIBUTION/AVAILABILITY STATEMENT

PUBLIC RELEASE

Abstract

See report.

Subject Terms

IATAC Collection

Security Classification of:

Unclassified

Unclassified

Unclassified

Report

Abstract

THIS PAGE

19. NAME OF RESPONSIBLE PERSON

Email from Booz, Allen & Hamilton (IATAC), blank

19b. TELEPHONE NUMBER

International Area Code

Area Code Telephone Number

703767-9007

DSN

427-9007

16. SECURITY CLASSIFICATION OF:

a. REPORT

Unclassified

b. ABSTRACT

Unclassified

c. THIS PAGE

Unclassified

17. LIMITATION OF ABSTRACT

Public Release

18. NUMBER OF PAGES

11
### Phoenix Challenge 2002: Intelligence, Information Operations, and Information Assurance

**Synopsis**

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.

**Subject Terms**

IATAC Collection, information operations, information assurance

**DISTRIBUTION / AVAILABILITY STATEMENT**

Approved for public release; Distribution unlimited

**NUMBER OF PAGES**

10

**Security Classification**

- Report: UNCLASSIFIED
- This Page: UNCLASSIFIED
- Abstract: UNCLASSIFIED
- Unlimited

---

**Author(s):** Sowder, Allen

**Performing Organization Name(s) and Address(es):** Department of the Army
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)**

<table>
<thead>
<tr>
<th>Offensive IO</th>
<th>Defensive IO</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPSEC</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>PSYOP</td>
<td>OPSEC</td>
</tr>
<tr>
<td>Military Deception</td>
<td>Physical Security</td>
</tr>
<tr>
<td>Electronic Warfare</td>
<td>Counterdeception</td>
</tr>
<tr>
<td>Physical Attack/Destruction</td>
<td>Counterintelligence</td>
</tr>
<tr>
<td>CNA</td>
<td>Electronic Warfare</td>
</tr>
</tbody>
</table>

**Joint and Army doctrine are mutually supporting**

**Intelligence supports IO**

**FM 3-0 (Operations)**

“Each element may have offensive or defensive applications.”

<table>
<thead>
<tr>
<th>OPSEC</th>
<th>PSYOP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Military Deception</td>
<td>Electronic Warfare</td>
</tr>
<tr>
<td>Physical Destruction (Attack)</td>
<td>CNA</td>
</tr>
<tr>
<td>Information Assurance</td>
<td>CND</td>
</tr>
<tr>
<td>Physical Security</td>
<td>Counterdeception</td>
</tr>
<tr>
<td>Counterpropaganda</td>
<td>Counterintelligence</td>
</tr>
</tbody>
</table>

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

**Public Affairs and Civil Affairs are related IO Activities**
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.
<table>
<thead>
<tr>
<th><strong>FIRES</strong></th>
<th><strong>INFO OPNS</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What</strong> or <strong>Who</strong> to Attack</td>
<td><strong>Who</strong> or What to Attack</td>
</tr>
<tr>
<td>Acquire the Target</td>
<td>How to Acquire</td>
</tr>
<tr>
<td>Attack The Target</td>
<td>Attack the Target</td>
</tr>
<tr>
<td>Conduct BDA</td>
<td>Conduct BDA</td>
</tr>
</tbody>
</table>

**Similar targeting process**
**Traditional Fires vs. Information Operations**

**Targeting Objectives**

*Describe the Effects of Target Attack on the Enemy*

<table>
<thead>
<tr>
<th>Traditional Fires</th>
<th>INFO OPERATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fires</strong></td>
<td><strong>Info Operations</strong></td>
</tr>
<tr>
<td>Reduce available options or COAs</td>
<td>LIMIT Minimize influence</td>
</tr>
<tr>
<td>Preclude effective combat system cohesion</td>
<td>DISRUPT Reduce Effectiveness</td>
</tr>
<tr>
<td>Alter time of arrival</td>
<td>DELAY Slow decisionmaking</td>
</tr>
<tr>
<td>Tie up critical resources</td>
<td>DIVERT Redirect resources</td>
</tr>
<tr>
<td>Ruin the target’s structure</td>
<td>DESTROY Eliminate influence</td>
</tr>
<tr>
<td>Inspect/Assess</td>
<td>DAMAGE Often Subjective</td>
</tr>
</tbody>
</table>

**Similar objectives**

UNCLASSIFIED/HQDA 6
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.
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.
**Social Fabric**
- Mugs
- Thugs
- Wackos

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

**IDC Mission**
- Balkans
- CND
- OSD
- IOTF

**INFORMATION DOMINANCE CENTER**
The Army’s TOC for IO

INTEL Brain Stem
Database Epicenter
24x7 Operations
One Stop Shopping

Social Fabric
Threat
IDC

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