Net-Centricity and Global NetOps

COL Carl W. Hunt, Ph.D.
J9, Director of Technology and Analysis
15 March 2006
Net-Centricity

Net-Centric Operations & Warfare (NCOW) is...

...the application of Net-Centricity to the activities of the Department of Defense, both day to day business and warfighting.

Net-Centric Operational Environment (NCOE)...

...provides the Joint Force with pervasive knowledge through the full integration of 3 critical components: Knowledge Management (KM), Network Management (NM) and Information Assurance (IA).”

Net-Centric Warfare (NCW) is...

... an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters. In short, the application of Net-Centricity to warfighting is “Net-Centric Warfare.”

NCOW is the approach to operations and warfare by which DoD will achieve the goals and objectives of Joint Vision 2020.
Transforming to Net-Centricity

- Transformational Satellite Communications
- Presidential Communications
- Joint Tactical Radios
- High Bandwidth Network Backbone
- Joint Command and Control & Coalition Info Sharing
- Net-Centric Enterprise Services
- Combat Support Enterprise Computing
Globally interconnected end-to-end infrastructure supporting war-fighters, policy makers, and business processes.

DoD CIO Memo, 22 Sep 1999

UNCLASSIFIED
The Threat: Growing; Sophisticated; and Organized

Most activity was from moderately skilled individuals
• Hackers, Script kiddies
• Criminals
• Individual unfocused efforts

February 2003 – Present
Shift to a series of intrusion focused sets by skilled and organized actors (possibly nation state sponsored)
• Titan Series Sets
• Organized crime, BotNets

“Recent exploits have reduced operational capabilities on our networks. Failure to secure our networks will weaken our warfighting ability and potentially put lives at risk.”

DEPSECDEF Aug 04
Global NetOps Defined

“We must change the paradigm in which we talk and think about the network; we must ‘fight’ rather than ‘manage’ the network and operators must see themselves as engaged at all times, ensuring the health and operation of this critical weapons system.”

~ Secretary of Defense Donald Rumsfeld

“NetOps is the operational construct that the Commander, US Strategic Command (CDRUSSTRATCOM) will use to operate and defend the Global Information Grid (GIG)”

~ USSTRATCOM, Joint CONOPS for GIG NetOps
15 Aug 2005

It is the mission that executes every day, worldwide, 24x7x365
NetOps – The Construct

NetOps is end-to-end across all GIG assets, in support of all Operational Environments

NetOps is the Operational Construct for operating and securing the GIG in support of Network Centric Operations and Warfare

Key Attributes
- Operational Commander in Charge
- Organizational Structure Established
- TTPs Defined, Established
- Integrates Net Management & Defense
- Shared Situational Awareness

“The source of flexibility is the synergy of the core competencies of the individual Services, integrated into the joint team.” Joint Vision 2020
A Changing Operational Environment

NetOps & JTF-GNO are important
- Transformational Communications
- Increasing Complexity
- Increasing Threats to the GIG
- Unclear C2, Roles and Responsibilities for Operating & Defending the GIG

“... Single-most transforming thing in our force will not be a Weapon System, but a set of interconnections…”

Secretary of Defense, Donald Rumsfeld, August 2001
Assigned Component Forces

- OPCON of NOSCs/NOCs
- TACON of CERTs/CIRTs

“Commanders working with Commanders”
NetOps Mission and Relationships

Allied Partnerships

Department of Homeland Security
National Cyber Security Division (US CERT)

National Cyber Response Coordination Group

Nat'l Comm Sys (Watch) Nat'l Coord Center

Law Enforcement/Counter Intelligence Center

Intelligence Community
- CIA
- NSA
- DIA

Federal Law Enforcement
- FBI
- DCIOs
- DSS

Private Sector
Information Sharing & Analysis Centers
- Telecommunications
- Banking & Finance
- Transportation
- Info Technology
- Carnegie Mellon Univ.

Joint Staff

Combatant Commands

DOD CC/S/A CND Forces

DISA Engineering Acquisition Software Dev
Questions?
Back-Up Slides
Cyber Crime – Threat to the GIG

- 26 Year-old Venezuelan, Rafael Nunez-Aponte, aka “RaFa” pleaded guilty to hacking DOD computers
- Time served 7 months, deported in Dec 05

- 20 Year-old American, Jeanson James Ancheta, aka “syzt3m” indicted by DOJ
- 17-count indictment, alleges he controlled 1000’s of computers remotely
- Pleased guilty to 4 felonies - Jan 06, awaiting sentence

Indictments the result of groundbreaking inter-agency analysis
**DOD Defense-in-Depth Strategy**

- **Basic Defenses**
  - Host Intrusion Detection
  - Block high risk applications
  - Traffic Filtering
  - Anti-Virus/Spyware
  - Patch Management
  - User awareness

- **Moderate Defenses**
  - Firewall management
  - Password changes
  - Configuration mgt.
  - Automated scanning
  - Network IDS
  - Risk management

- **Advanced Security**
  - Policy based
  - Configuration control
  - Account auditing
  - Disciplined growth
  - Baseline management
  - Analysis tools
  - Security Scanner

- **Sophisticated Global Security**
  - Command involvement
  - Standard response procedures
  - Shared Situational Awareness
  - Password Policy Enforcement
  - CAC/PKI
  - Accountability
  - Limited internet connections

---

**Hacker**

**Nation-state effort**

**Sophisticated Hacker**

**Intermediate Hacker**

**Basic Hacker**

**Internet**

**Aggressive CND Measures: No silver bullets!!!**