A Nation's Security – A Netcentric Response

Terry Morgan

Director Netcentric Initiatives

Global Government Solutions Group
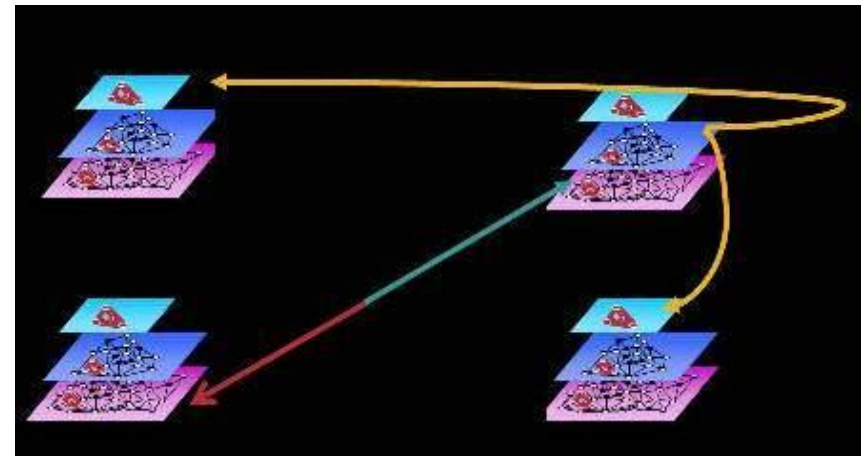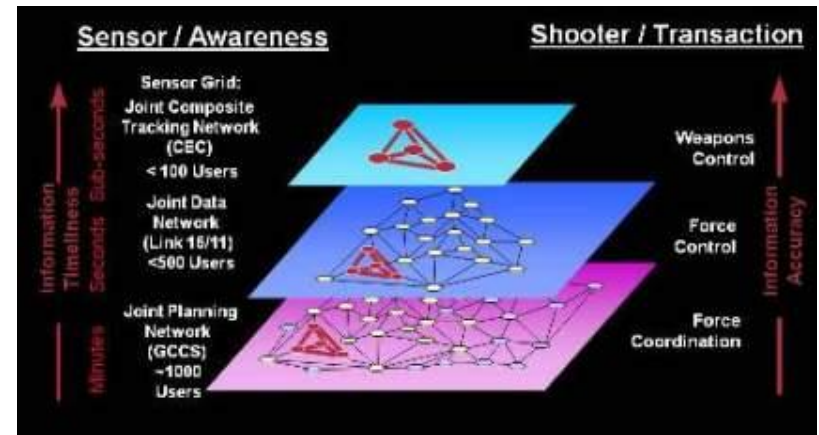
Cisco Expo
2009

Why Cisco?

"I believe we are entering the second phase of the Internet, where the next major market transition will be driven by collaboration, enabled by Web 2.0 technologies. This is the foundation of what we are calling "Cisco 3.0" - **John Chambers, 2007**

"Across broad sectors of the economy, dominant competitors such as Cisco Systems …, Federal Express …, Charles Schwab … Wal-Mart … are successfully employing information-based strategies to create competitive advantage" **NCW Developing & Leveraging Information Superiority 1998**

Agenda

- **Terrain and Situation**
- The Enterprise
- Market Directions
- The Fit

A Nation's Security

- Defense

The Intelligence Community

- Security

The Judiciary

- Public Safety

Interagency Operation Sorbet

The [Australian government](#) ordered the *Pong Su* into harbour; however, the ship attempted to escape into [international waters](#). After a four day chase, known as *Operation Sorbet*, the **Pong Su** was captured after [Australian Army](#) Special Operations Forces stormed the ship in a helicopter landing.
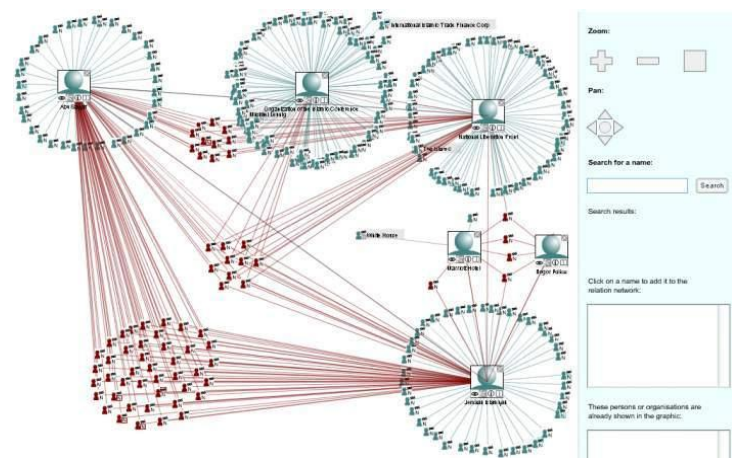

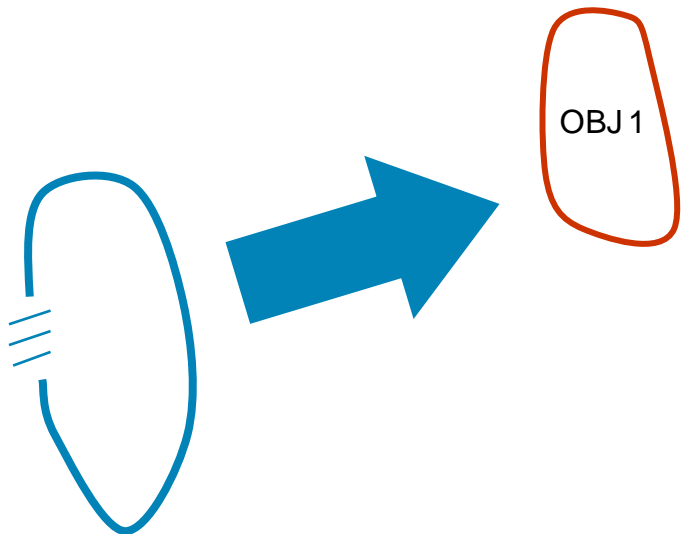Australian Department of Defence photo

Cisco Expo
2009

http://en.wikipedia.org/wiki/Pong_Su_incident

Today's & Tomorrow's Operational Challenges

OBJ 1

Emer Svcs Unavailable

Submarine cable lost

Threat to water supply

Bomb threats in two buildings

Two regional ISPs out of service

Two bridges down

Pipeline disruption

Telephone service outage

Phones jammed

Oil refinery fire

Power outage

- **All information going digital.**

  Accuracy, Fidelity, Storage and Retrieval

  Searching, Analysis, Information Management

- **All devices becoming network nodes.**

  Access, Transmission, Distributed Systems

  Scaling, Fault Tolerance, Management, Flexibility

- *Video, Voice, and Instantaneous information will become more prevalent*

Word of Mouth, Cell, Email Chat, IM ....

Internet and Intranet

Formal staffing, Email

Starfish
(Brafman and Besckstron)
No head - Regenerates

Vs.

Spider
Single Head - Dies

Fred Stein, Mitre C2 Center at NCW 2007, Washington DC

Cisco Expo
2009

Cisco Expo KSA
Feb 09

© 2008 Cisco Systems, Inc. All rights reserv

Indian Defense Trip
Aug 08

© 2006 Cisco Systems, Inc. All rights reserved.

Cisco Public

12

Taliban using Skype phones to dodge MI6

By GLEN OWEN
Last updated at 11:10 PM on 13th September 2008

Comments (0) | Add to My Stories

Taliban fighters targeting British troops in Afghanistan are using the latest 'internet phones' to evade detection by MI6, security sources said last night.

Skype, a popular piece of consumer software that allows free calls to be made over the web, has been adopted by insurgents to communicate with cells strung out across the country.

Unlike traditional mobile calls, which can be monitored by RAF Nimrod spy planes, Skype – the commercial application of a technology called Voice Over Internet Protocol (VOIP) – are heavily encrypted.

How Gadgets Helped Mumbai Attackers

By Noah Shachtman ✉   December 01, 2008 | 9:39:23 AM   Categories: Gadgets And Gear, T Is For Terror

The Mumbai terrorists used an array of commercial technologies -- from Blackberries to GPS navigators to anonymous e-mail accounts -- to pull off their heinous attacks.

For years, terrorists and insurgents around the world have used off-the-shelf hardware and software to stay ahead of bigger, better-funded authorities. In 2007, former U.S. Central Command chief Gen. John Abizaid complained that, with their Radio Shack stockpile of communications gear, "this enemy is better networked than we are." The strikes that killed at least 174 appears to be another example of how wired today's "global guerrillas" can be.

As they approached Mumbai by boat, the terrorists "steered the vessel using GPS equipment," according to the *Daily Mail*. A satellite phone was later found aboard.

Once the coordinated attacks began, the terrorists were on their cell phones constantly. They used BlackBerries "to monitor international reaction to the atrocities, and to check on the police response via the internet," the *Courier Mail* reports.

Modern day sigint and propaganda

- Taliban and al-Qaeda use handheld radios on military frequencies to overload SIGINT platforms with random noise and propaganda
- Openly use military bands to antagonize troops and then use encrypted IP over higher frequency radio channels to communicate
- Supports IP packet service

Los Angeles Times | World

You are here: LAT Home > World News

> World

July 16, 2008

In Colombia, they call him Captain Nemo

Authorities say Enrique Portocarrero was the innovative creator of stealthy submarines called semi-submersibles, used by cocaine traffickers to evade detection.

By Chris Kraul
December 14, 2008

Reporting from Tumaco, Colombia — Squat, bull-necked and sullen-looking, Enrique Portocarrero hardly seems a dashing character out of a Jules Verne science fiction novel.

But law enforcement officers here have dubbed him "Captain Nemo," after the dark genius of "20,000 Leagues Under the Sea." They say the 45-year-old has designed and built as many as 20 fiberglass submarines, strange vessels with the look of sea creatures, for drug traffickers to haul cocaine from this area of southern Colombia to Central America and Mexico.

California | Local
National
World

The Reality
Accelerating Rate of Technology Change

After realizing the potential of the air domain Mitchell, Claire Chennault, and their contemporaries had 20 years to develop the strategy, tactics, and doctrine and "sell" aviation . . .

"Unfortunately, ... **The trends for advances in technology**, often (correctly or incorrectly) related to Moore's Law and derivative theories, **such as the Law of Accelerating Returns** proposed by Ray Kurzweil in his 2001 essay, **dictate that we must move quickly.**

Warfighting in Cyberspace, Keith B. Alexander, JFQ / issue 46, 3d quarter 2007

Ray Kurzweil, "Law of Accelerating Returns," 2001, http://lifeboat.com/ex/law.of.accelerating.returns

Cisco Expo
2009

War will remain primarily a human endeavor. . . .

we will be surprised.

The true test of military effectiveness

. . . the ability of a force to diagnose the conditions it actually confronts and then quickly adapt.

the **JOE** 2008

JOINT OPERATING ENVIRONMENT

2015 Strategic

Challenges and Implications for the Future Joint Force

United States Joint Forces Command
https://us.jfcom.mil/sites/J5/J9/default.aspx

"The illiterate of the 21st century will not be those who cannot read and write, but those who cannot learn, unlearn, and relearn."

Alvin Toffler
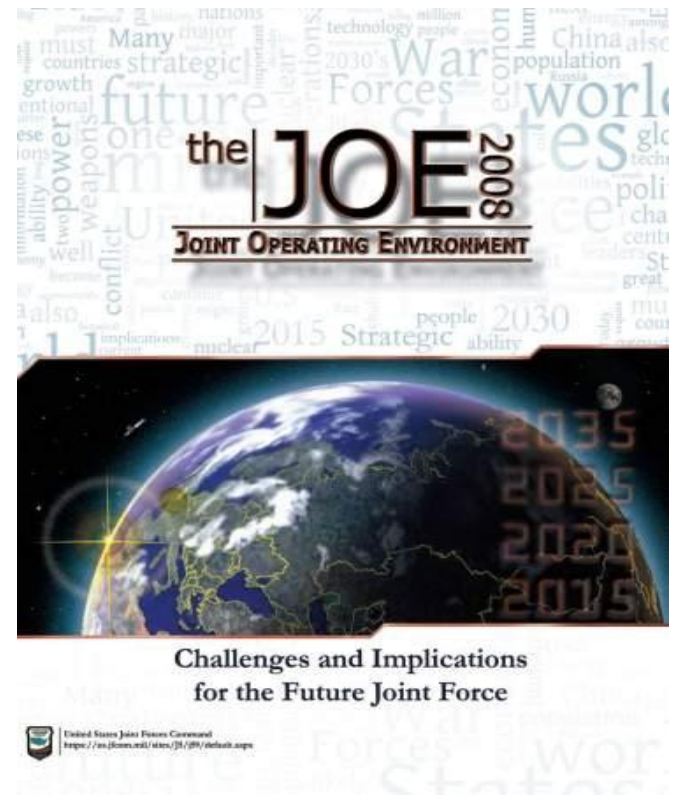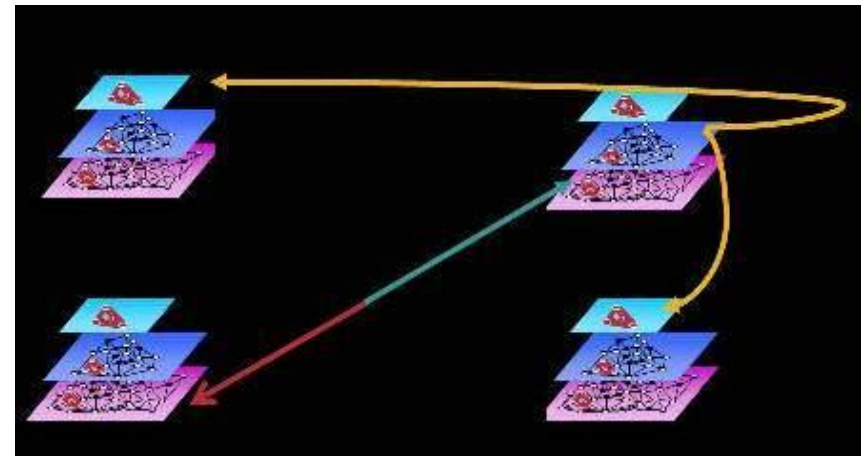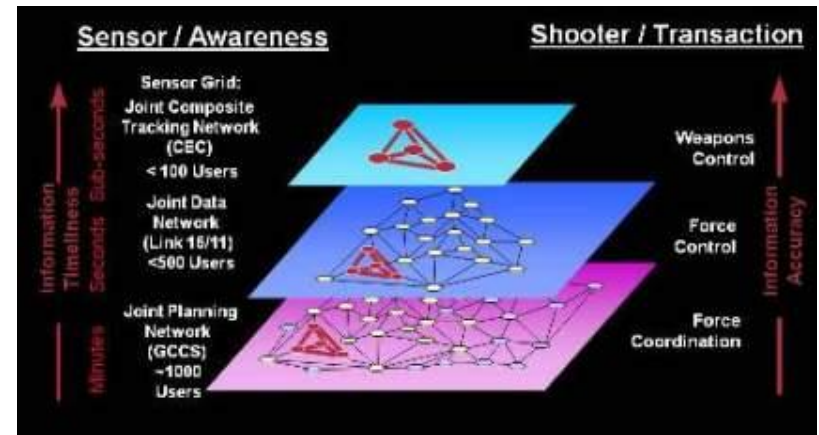
Agenda

- Terrain and Situation
- The Enterprise
- Market Directions
- The Fit

Unity of Command or Unity of Effort?

- **Municipal** -- Bases, Camps & Port Facilities

- **Multi-national industrial** -- Procurement, warehousing & transportation of supplies

- **Training, Doctrine and Education** -- Basic and Advanced Technical and Professional Education

- **Telecommunications and Service Provider** -- nationwide and global voice and data connectivity

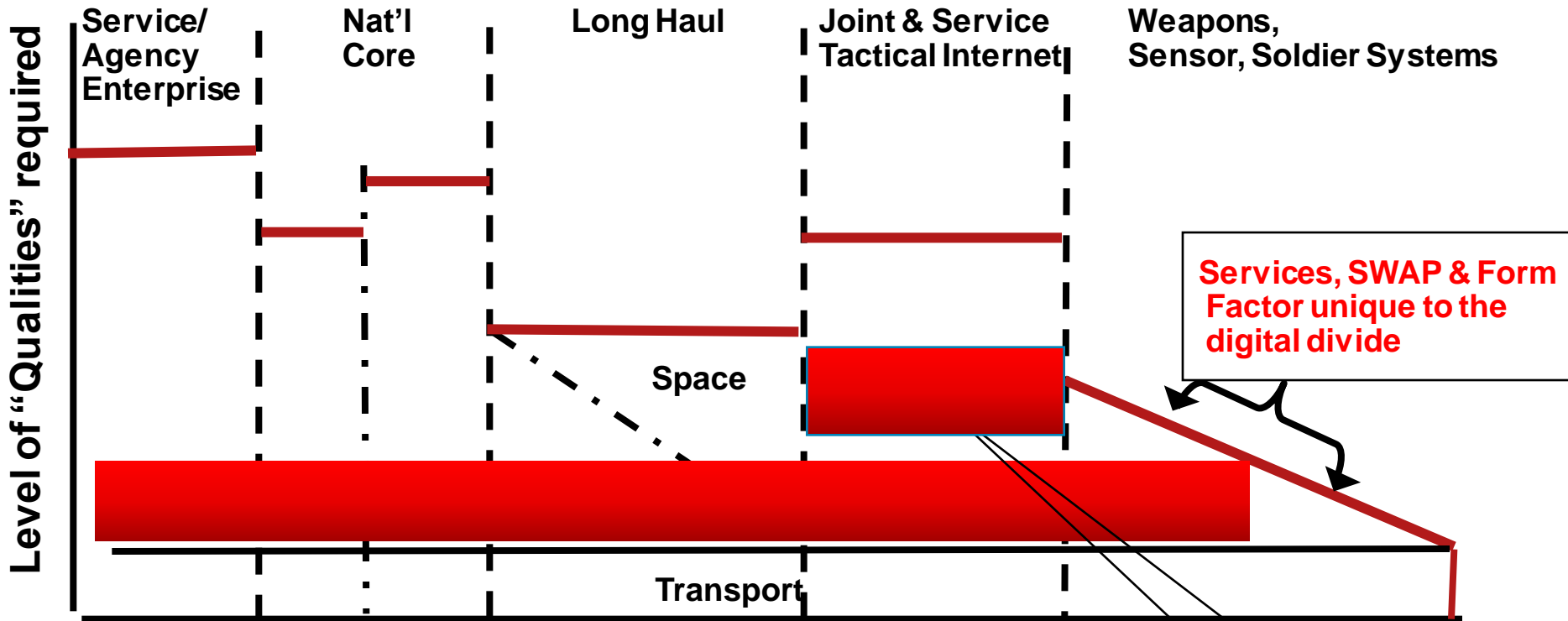- **War Fighting**

    C4ISTAR

    Weapons, Soldier and Sensor Systems

The Defense Enterprise
Connect the Front lines to Rear-most Soldier

Level of "Qualities" required

Service/ Agency Enterprise	Nat'l Core	Long Haul	Joint & Service Tactical Internet	Weapons, Sensor, Soldier Systems

Space

Transport

Services, SWAP & Form Factor unique to the digital divide

**FLOT**

SWAP & Form Factors for Transportability

A set of end-to-end "services" that meet the needs of the war fighter & can be "serviced by the enterprise"

Cisco Expo
2009

Network … NNEC, NEC, NBD, NBO

- **The power of NCO is derived from the effective linking or networking of knowledgeable entities that are geographically and/or hierarchically dispersed through the most effective information technologies**
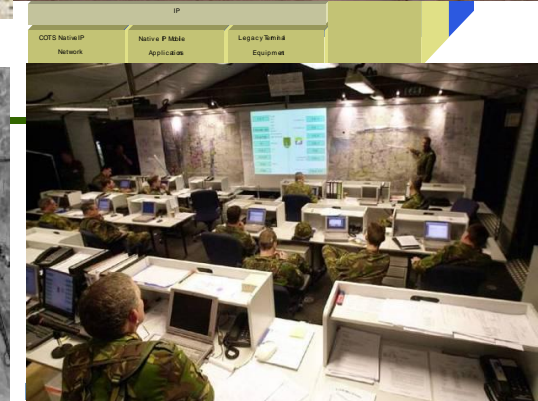
Rich Information as a Principle of War

Maneuver, mass, surprise, firepower, and logistics … have been the coins of the military realm.

Networked capabilities give defense the capability to maneuver information to develop the appropriate mass for
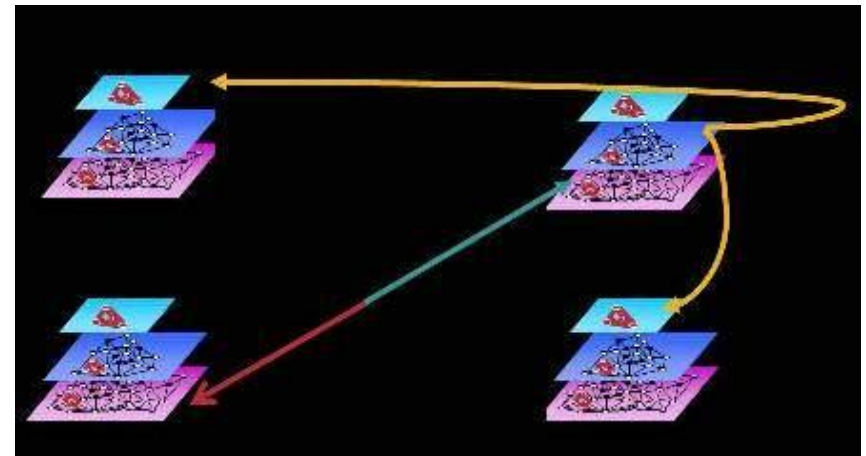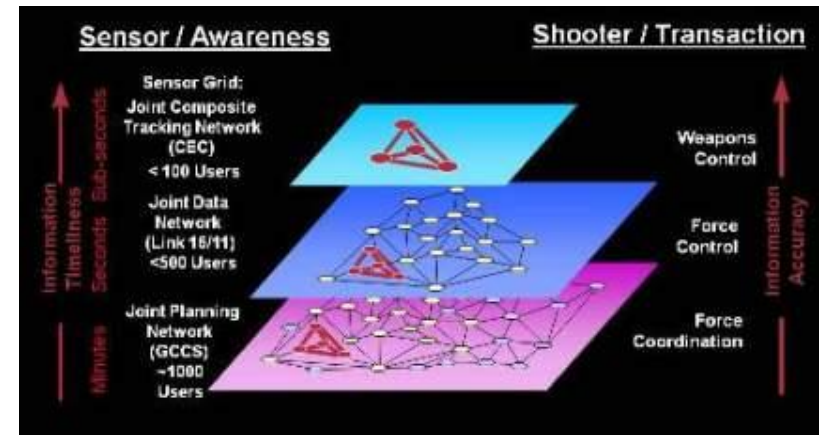
Staff collaboration,

Timely and informed decisions by the commander

and precise and efficient actions by the warrior

Agenda

- Terrain and Situation
- The Enterprise
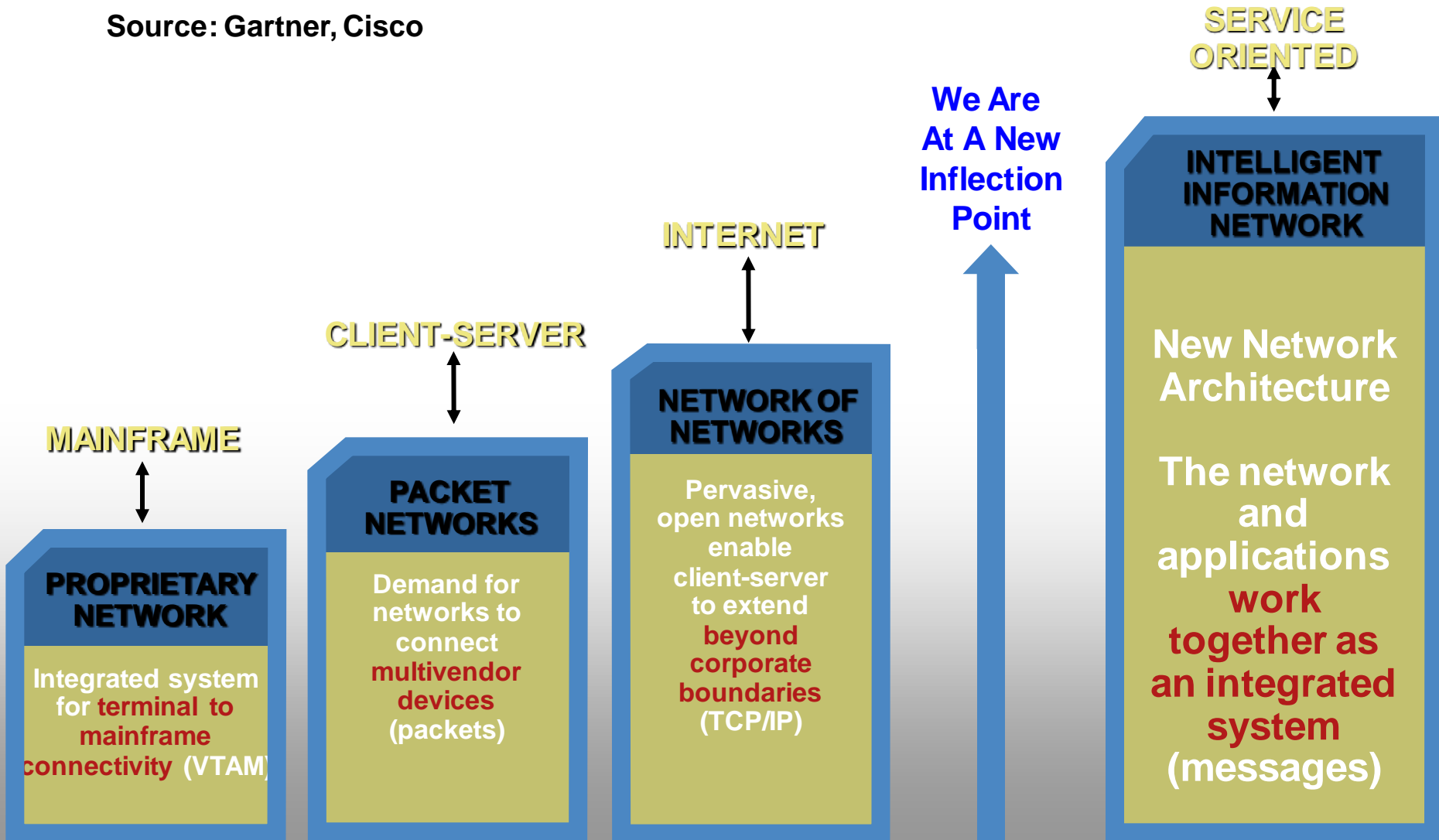- **Market Directions**
- The Fit
- The Plan

▪ **Municipal**

▪ **Multi-national industrial**

▪ **Training, Doctrine and Education**

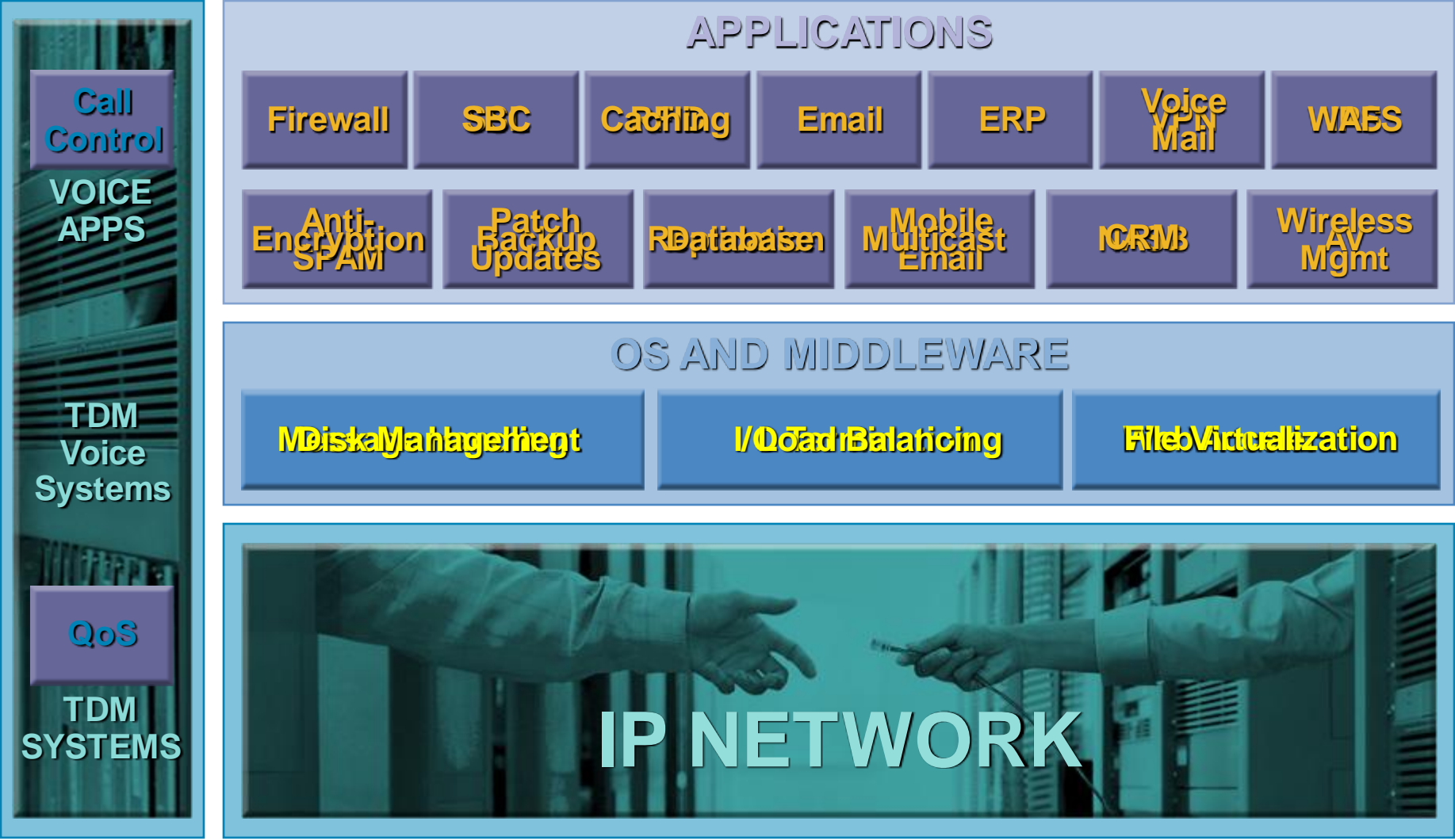▪ **Telecommunications & Service Provider**

▪ **War Fighting**

Cisco Publicl

The Technology Future – Industry Inflection Points Historically Drive New Architectures

Source: Gartner, Cisco

SERVICE ORIENTED

We Are At A New Inflection Point

INTELLIGENT INFORMATION NETWORK

New Network Architecture

The network and applications **work together as an integrated system (messages)**

INTERNET

NETWORK OF NETWORKS

Pervasive, open networks enable client-server to extend **beyond corporate boundaries (TCP/IP)**

CLIENT-SERVER

PACKET NETWORKS

Demand for networks to connect **multivendor devices (packets)**

MAINFRAME

PROPRIETARY NETWORK

Integrated system for **terminal to mainframe connectivity (VTAM)**

Intelligence Migration Is Part of a Natural Evolution

Left panel (vertical):

Call Control

VOICE APPS

TDM Voice Systems

QoS

TDM SYSTEMS

APPLICATIONS

Firewall	SBC	Caching / WAN	Email	ERP	Voice Mail / VPN	WAAS / IPS
Anti-Encryption / SPAM	Patch Backup Updates	RADIUS / Database	Mobile Multicast / Email	CRM / IMB	Wireless AV Mgmt

OS AND MIDDLEWARE

Disk Management / Mirror Arrangement	I/O and Balancing / Load Balancing	File Virtualization / Web Virtualization

IP NETWORK

Service Convergence for IPTV/Video

Unparalleled Network Linkages for Better User Experience

APPLICATION LAYER

PRESENCE-BASED

WEB

MOBILE

IP CONTACT

SERVICE LAYER

Service Exchange

Registration

Open Framework for Enabling 'Triple Play on the Move' (Data, Voice, Video, Mobility)

OPERATIONAL LAYER

NETWORK LAYER

Customer Element

Access/ Aggregation

Intelligent Edge

Multiservice Core

Transport

Open Platform for Service Differentiation Through Innovation

Beyond just IPTV to IP Rich Media in Connected Home

INTELLIGENT NETWORKING

Cisco Expo 2009

Service Exchange Framework
Multimedia Service Control for Wireline / Wireless Convergence
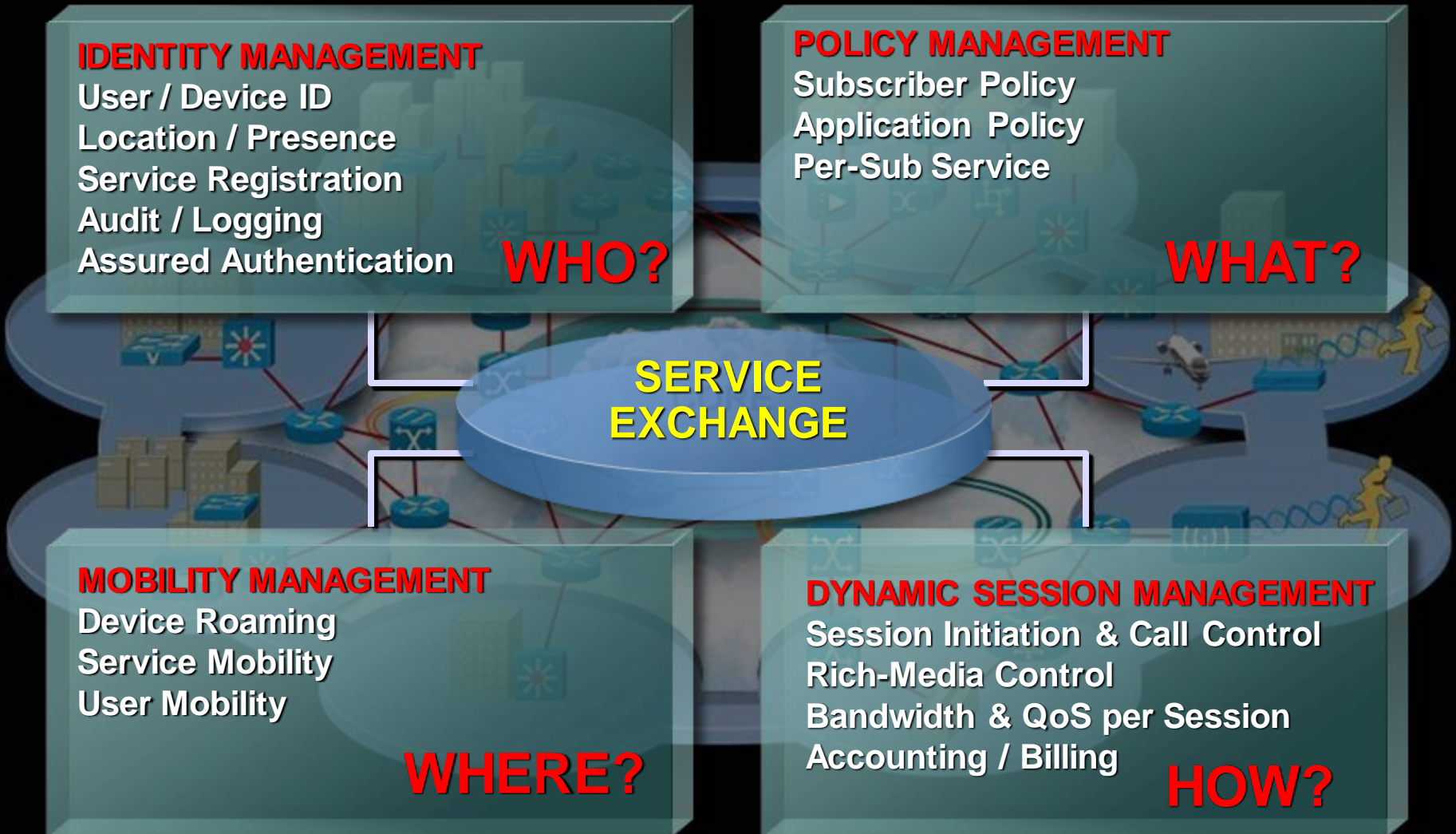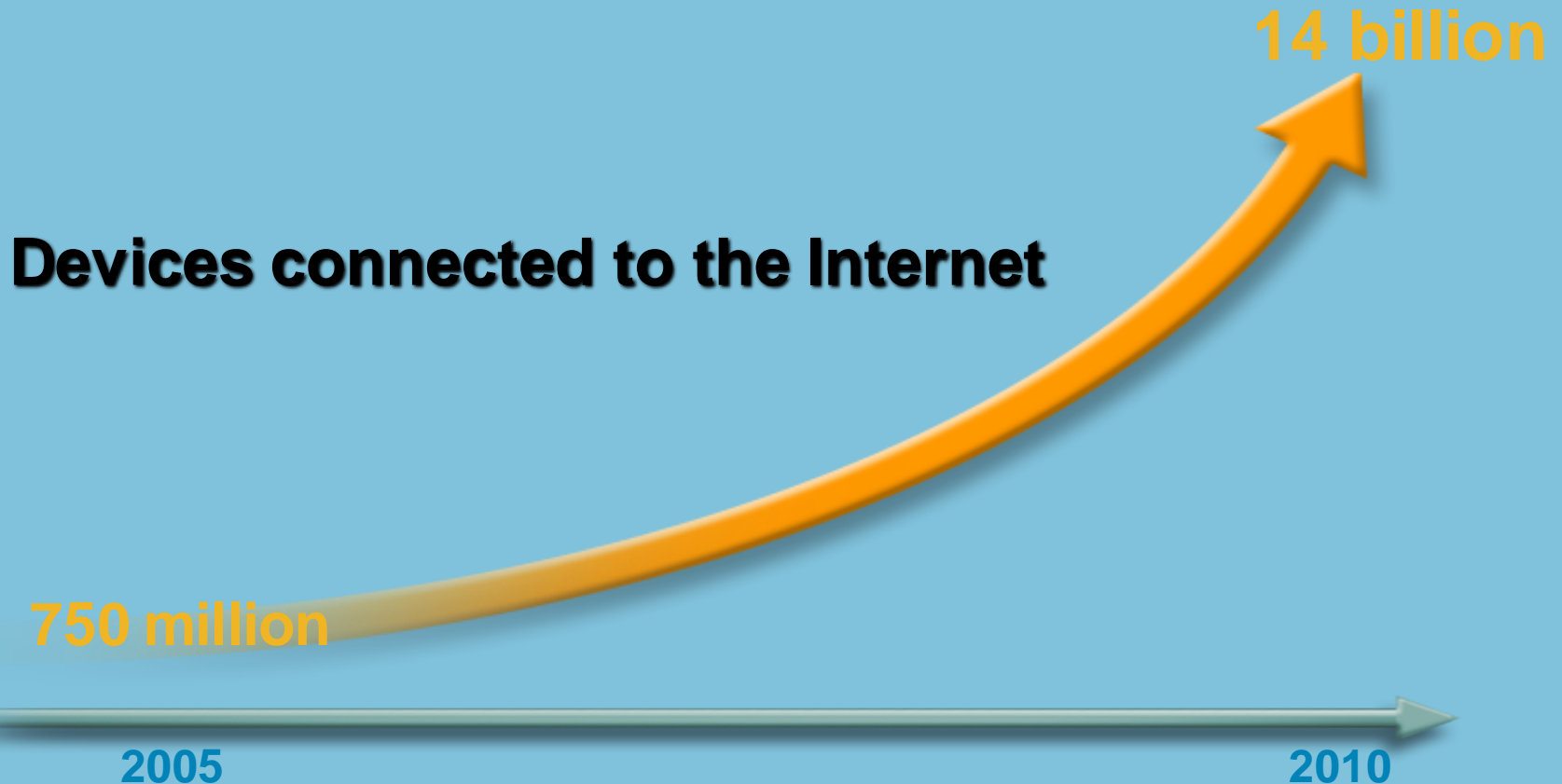
IDENTITY MANAGEMENT
User / Device ID
Location / Presence
Service Registration
Audit / Logging
Assured Authentication **WHO?**

POLICY MANAGEMENT
Subscriber Policy
Application Policy
Per-Sub Service **WHAT?**

SERVICE EXCHANGE

MOBILITY MANAGEMENT
Device Roaming
Service Mobility
User Mobility **WHERE?**

DYNAMIC SESSION MANAGEMENT
Session Initiation & Call Control
Rich-Media Control
Bandwidth & QoS per Session
Accounting / Billing **HOW?**

Security

Network as the Platform

- Location-Based Services
- Access Control
- Video Training
- Campus Transportation Monitoring
- Digital Signage
- First-Responder Monitoring
- Unified Communications
- Radio Interoperability
- Conferencing and Collaboration
- Visitor Management
- Video Surveillance
- Building System Monitoring
- Sensors
- Intrusion Detection

IP Network

Cisco Open Platform for Safety and Security

Security Management
Recording, Monitoring, and Policy-Based Administration

Access Controls
Physical and Info System access control

Correlation
Physical and info security event correlation

Connectivity
Wired or Wireless Any-to-Any

Network Platform

Self Defending Network
Enabling connected systems to identify and prevent threats

Communications Interoperability
How to Deliver "Right Information, Right Time, Right Format to the Right Person"

Convergence
Physical and Info Security policy based control, enforcement and auditing

Cisco Expo
2009

Internet Router in Space (IRIS)

The Challenge

- The US government requires mobile, flexible and dynamic connectivity

- Government partners need to globally share information throughout all phases of joint, combined and coalition operations in austere environments

An Elegant Solution

- Everything over IP: voice, data and video capability

- Funded by Information Technology commercial partners

- Supports from disadvantaged users to strategic HQ

- Service based model: only pay for what you use

IRIS

1

2

3

C Band

Ku Band-1

Ku Band-2

From band to band, AOR to AOR or multi-address with the ease of IP addressing

Types of Mobility

Node or
moves, r

Nodes or networks interconnect
opportunistically; no dependence
on any node or reach-back to fixed
infrastructure

ork stays connected
on, using predefined
, Mobile IP)

Headquarters

Headquarters

Headquarters
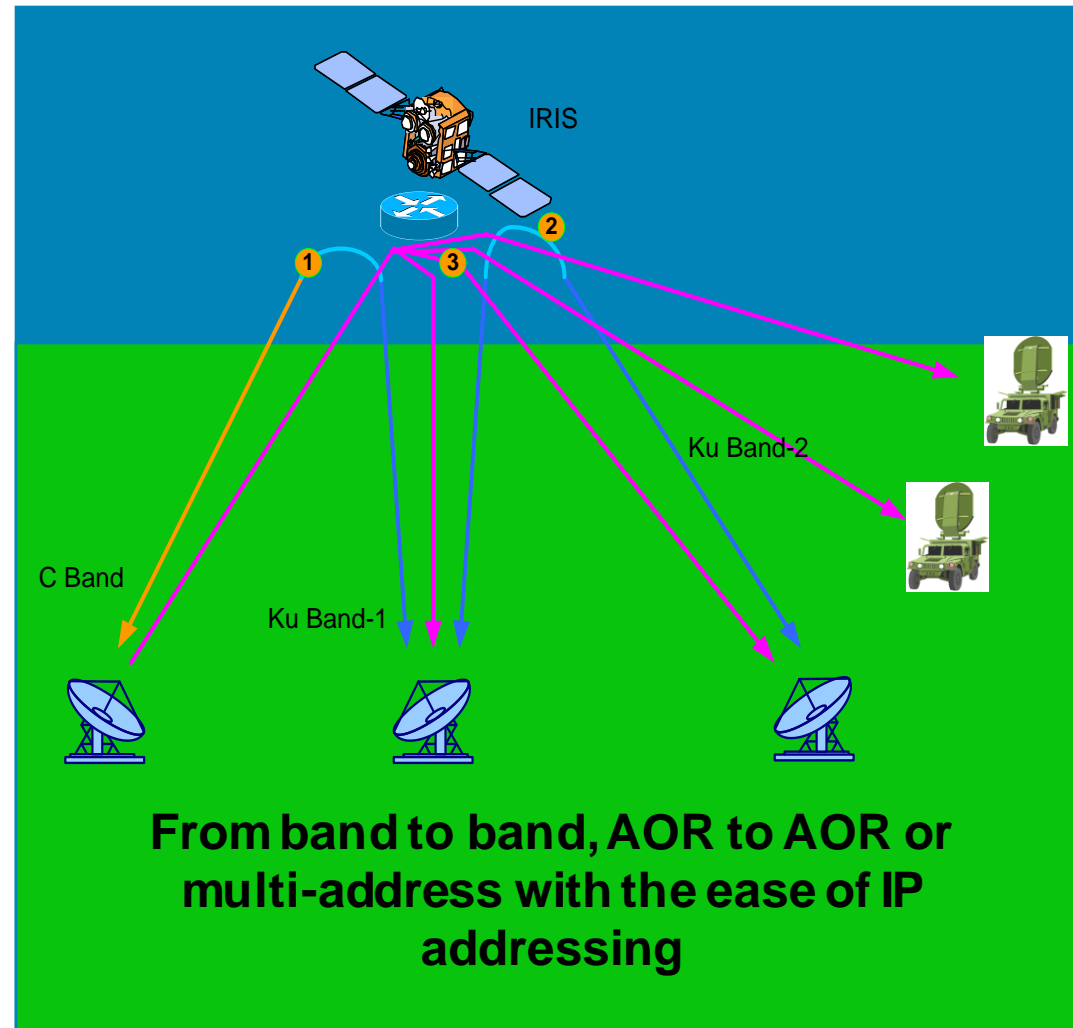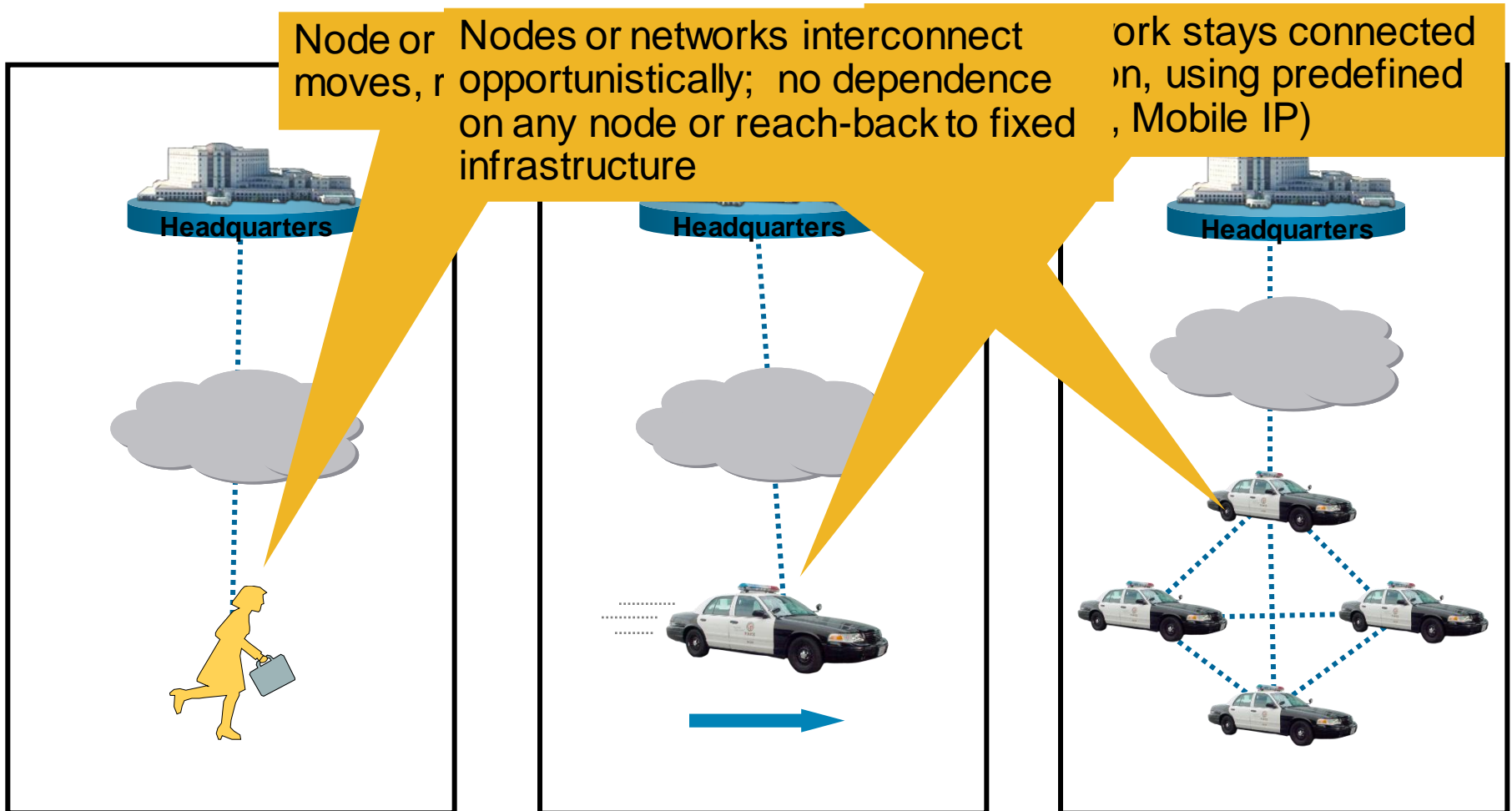
Radio-Aware Routing

- **Optimizes IP routing over radio networks**
- **Immediately recognizes and adapts to network changes**
- **Easily routes between line-of-sight and non-line-of-sight links**
- **Based on Cisco-authored IETF draft RFC 4938**
- **Draft updated by Cisco in support of L3 implementation for CDL (RFC 4938bis)**

Agenda

- Terrain and Situation
- The Enterprise
- Market Directions
- The Fit
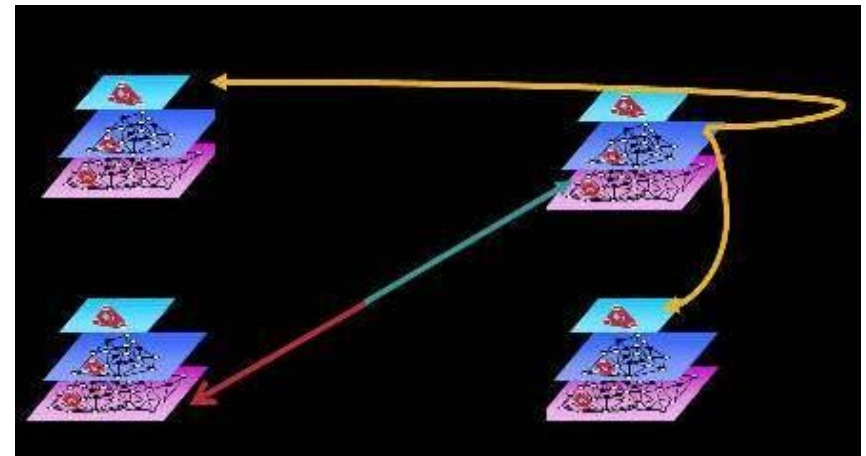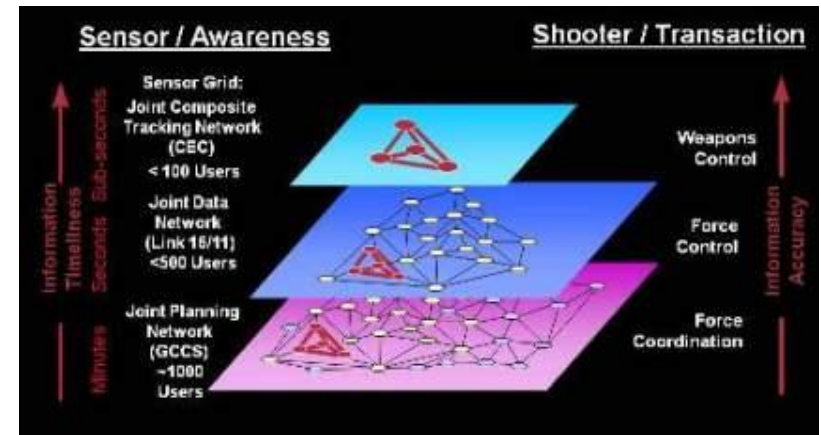
Core vs. Context – Teaming to Leveraging Skill Sets and Knowledge

Core is the COTS capability delivered by the IT vendors. These solutions are the starting point and for many customers are sufficient.

Applications
Services
Network
Connectivity
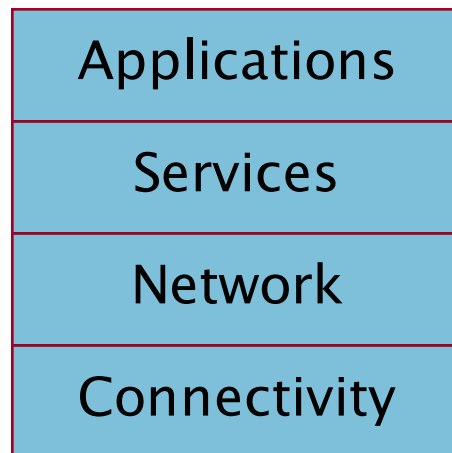
SECURITY

Core vs. Context – Teaming to Leveraging Skill Sets and Knowledge

Context are the specific capabilities required by the customer's Business problems and Domain requirements (e.g. ruggedized & environmentally protected). The customer, his integration partners and Cisco team, especially Advanced Services, to identify and accommodate the domain specific requirements.

Cisco Expo
2009

| COI Applications |
| Applications |

| COI Services |
| Services |

| COI Networking |
| Network |

| COI Connectivity |
| Connectivity |

DEFENCE SECUITY
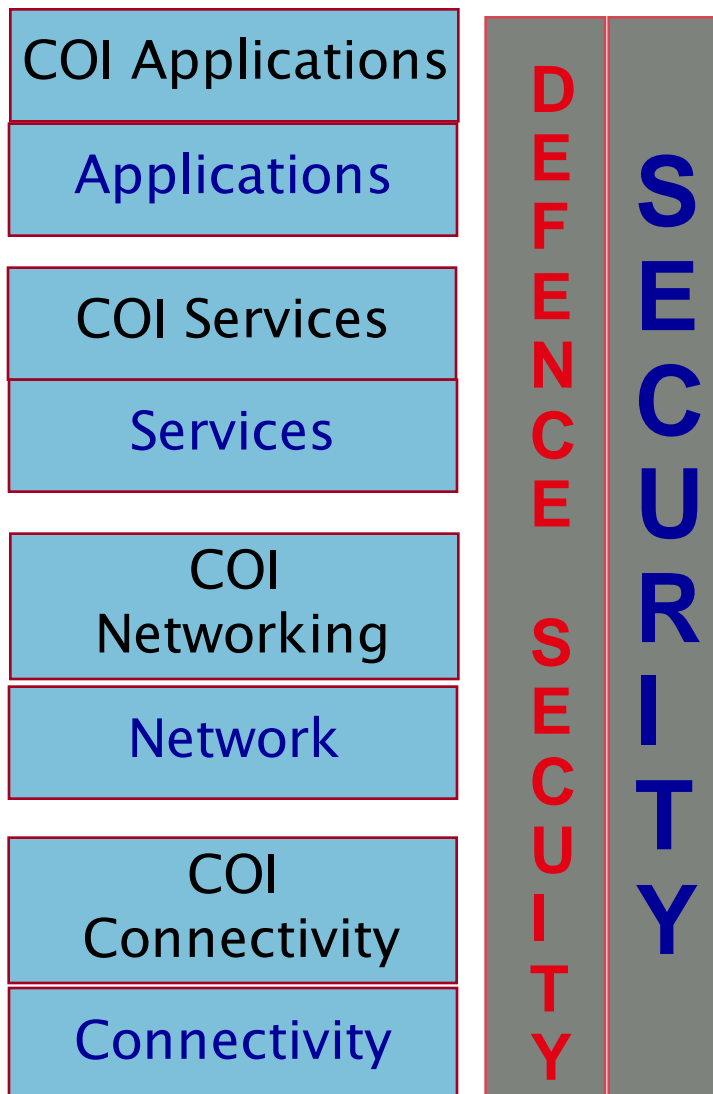
SECURITY

Netcentric . . .

Operational art is the ability to envision the actions required to achieve a strategic *end state*
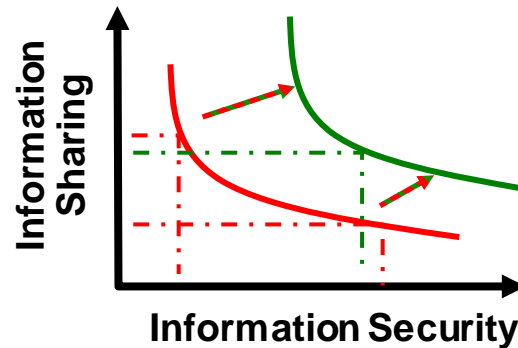
Netcentric = The <u>Acceptable Intersection</u> of Information Sharing & Information Security

"t"ask - "m"ission

capabilities   Desired End State

"T"ask - "M"ission

The Reality . . .
    The Speed of Information

Loose Organizations Very Agile
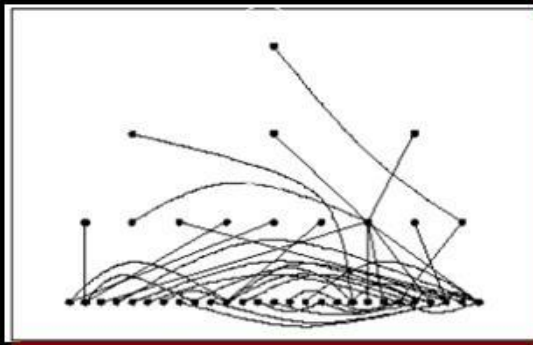
Data / Information
WEB

Larger - Formal Less Flexible
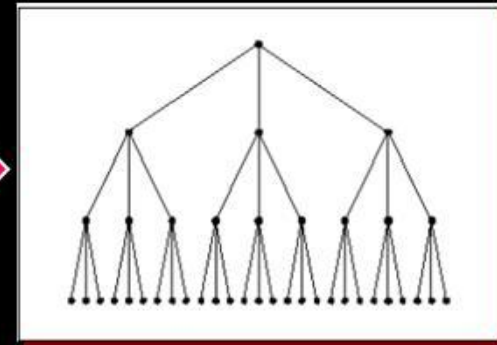
Word of Mouth, Cell, Email Chat, IM ....

Internet and Intranet

Formal staffing, Email

Starfish
(Brafman and Besckstron)
No head - Regenerates

Vs.

Spider
Single Head - Dies

Fred Stein, Mitre C2 Center at NCW 2007, Washington DC

Indian Defense Trip
Aug 08

© 2006 Cisco Systems, Inc. All rights reserved.   Cisco Public

12

It Starts with Connectivity, but …
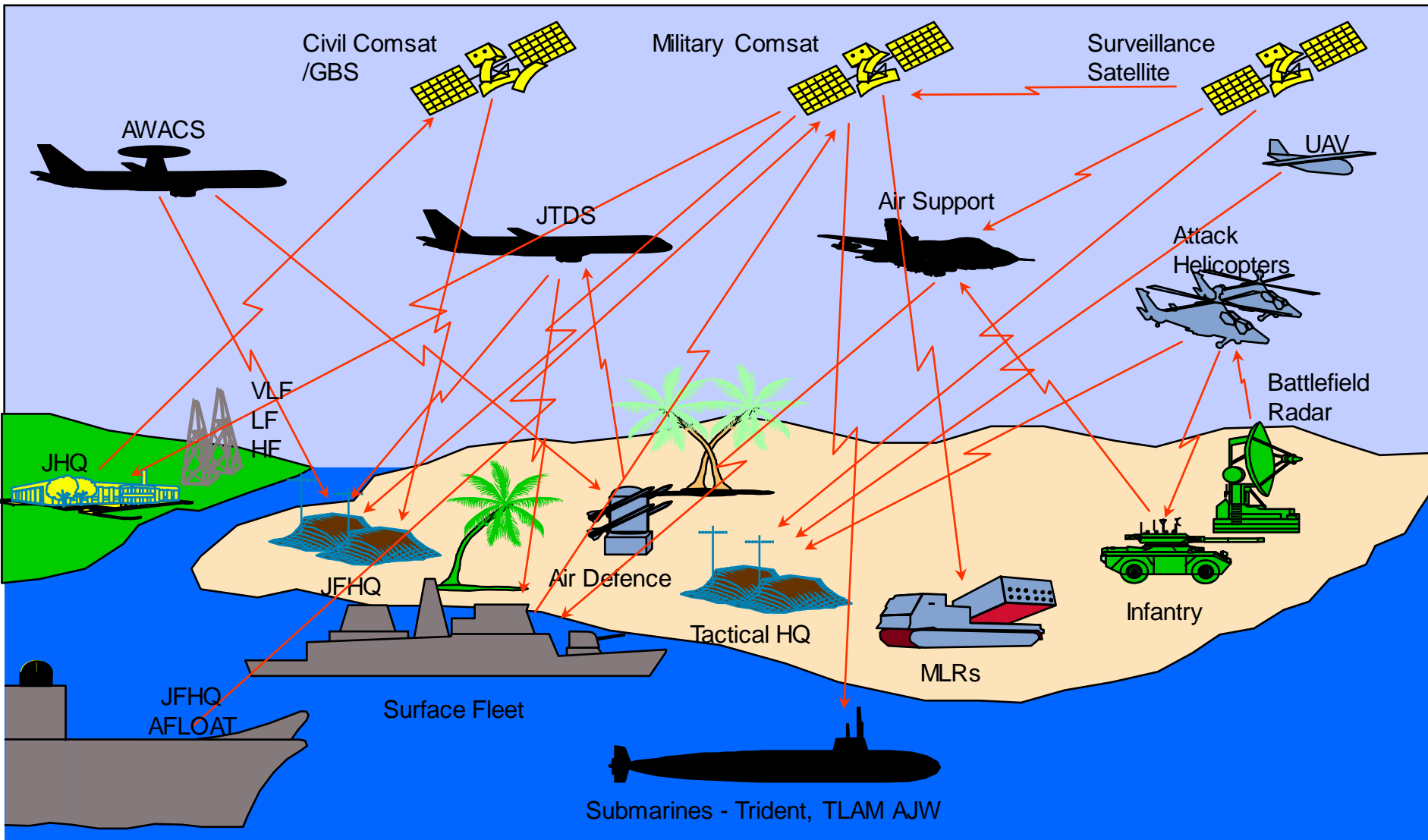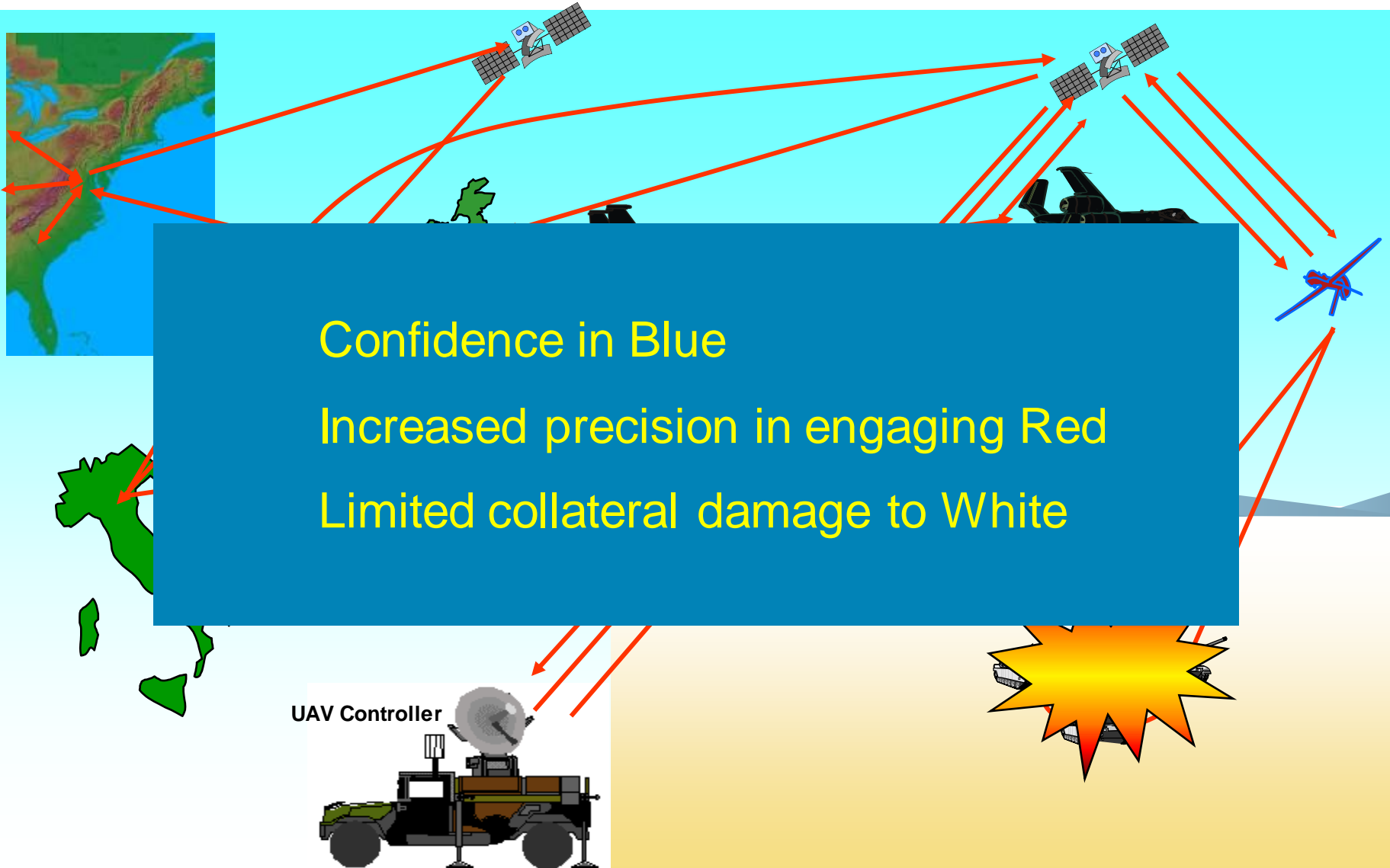
Network Enhanced Operations
It is Doable NOW -- IP-enabled AWACS

One year later ….

> ***Today, I was in a briefing where AWACS (group) briefed IP-enabling of Block 30/35 planes. The timeline was no longer 2012 or 2015 but 2006 through 2008. We are in the process of***

The IP-enabled AWACS flew in JEFX06 MainEx (April 27- 29 2006).

http://www.military-information-Technology.com/article.cfm?DocID=1494

" the capability to see the Common Operations Picture (COP), jabber chat, weather maps from the Joint Weather Information Services, Web-enabled Execution Monitor Console for mission execution, mail and Web browsing."

TTNT - **Optimized for fast moving tactical A/C and highly interconnected LOS networks**

+
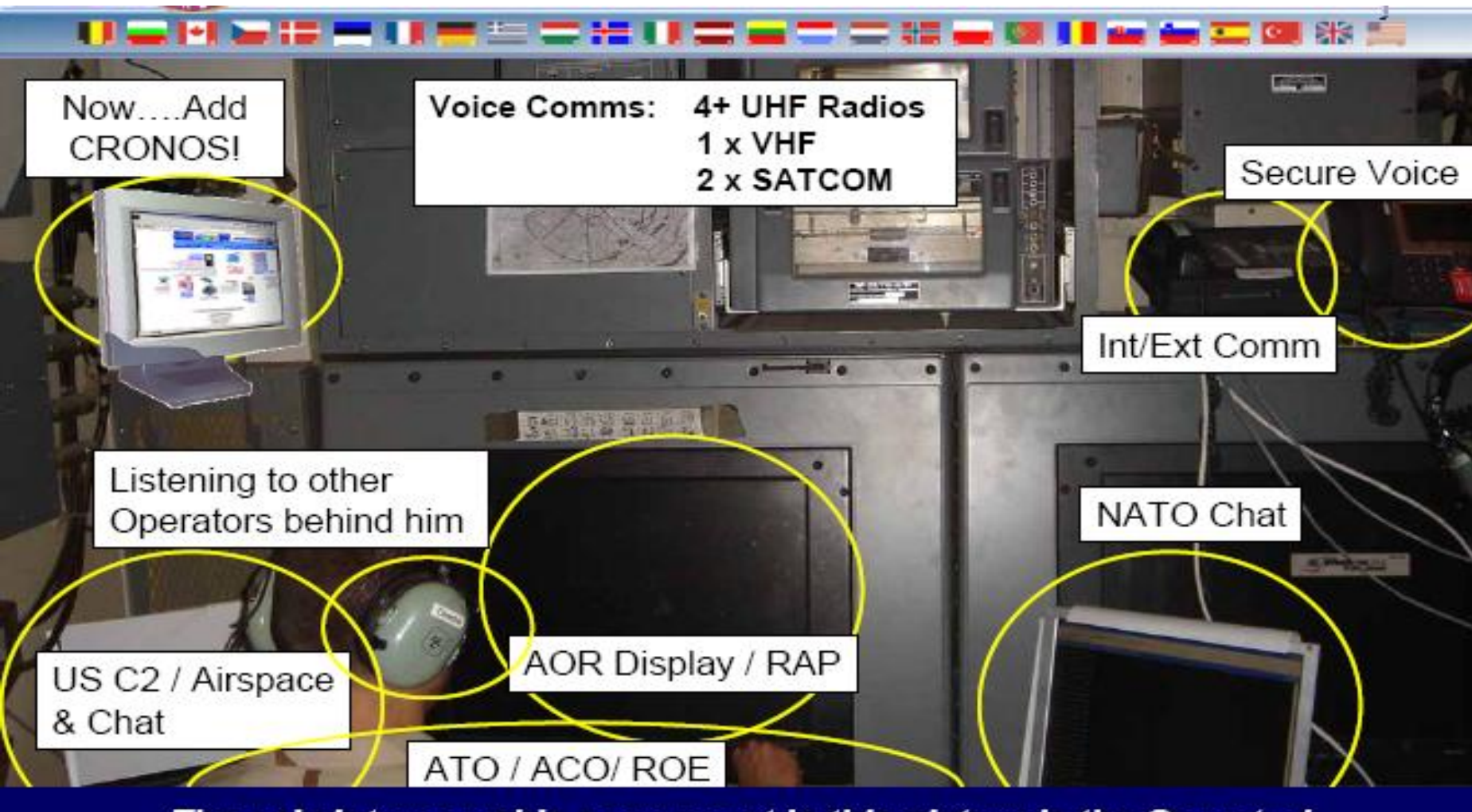**ISR**

AWACS In the Network
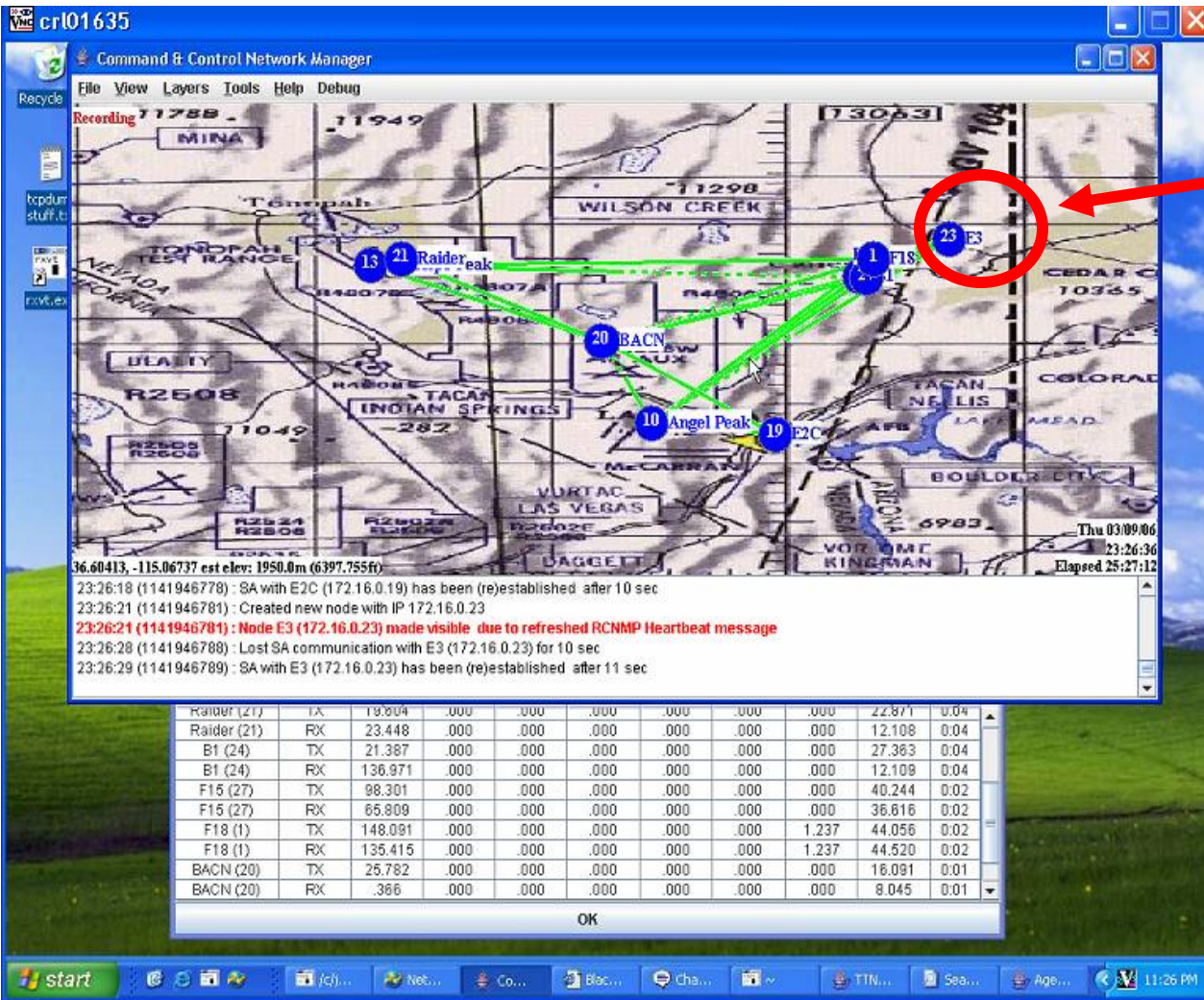
- **AWACS (#23) shows up for the first time ever in an IP-based network with other aircraft and the ground**

Applications Demonstrated
- Airborne web services
  - Blue and Red force tracks which originated from the Cursor on target server on coalition net and the Army's FCS
- Email
- Netmeeting
- Common Operational Picture (C2PC)
- Primary AWACS Display

What Do We Need?
A C2 System with the Ability to

Now....Add CRONOS!

Voice Comms: 4+ UHF Radios
1 x VHF
2 x SATCOM

Secure Voice

Int/Ext Comm

Listening to other Operators behind him

NATO Chat

US C2 / Airspace & Chat

AOR Display / RAP

ATO / ACO/ ROE

However, we need simplification

Voice, Web, Chat, Blue Force Tracking . . . Right Service for the Right Requirement

Joint Time Sensitive Targets

Chat is enduring, I don't have to stop what I'm doing when a chat message arrives, I get a tone, take a quick look and then do what has priority – with voice radio I have to stop and listen. US Marine LCpl
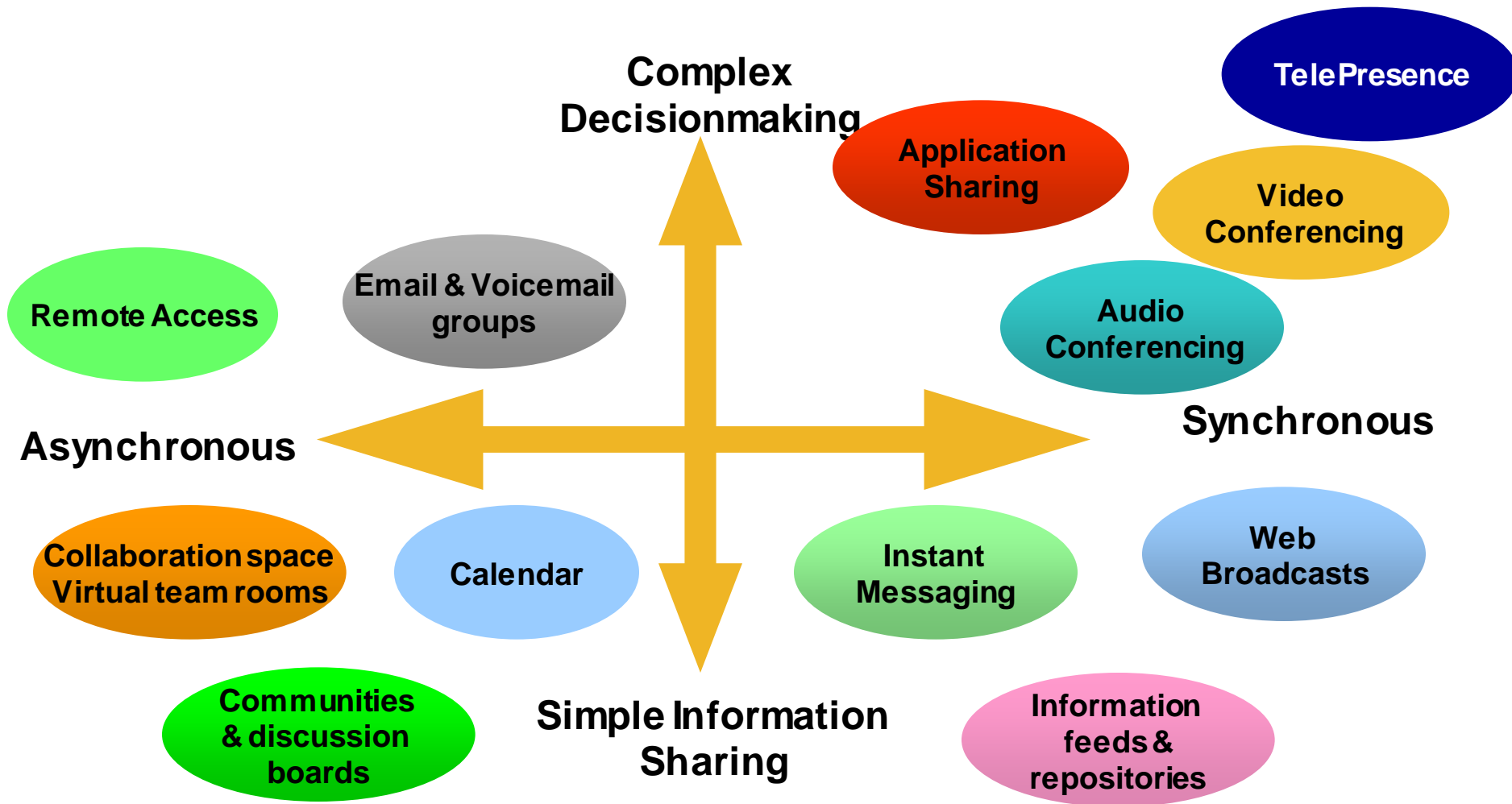
- **VoIP – clear secure voice conferencing, hands-free speaker, critical enabler of the process**
- **Chat – huge enabler of info sharing in real time**
- **Email**
- **Other ISR products and systems feeding the process**

Duct Tape

#C6F_Targeting

<DINO_real> All FRUs continue with maint with the exception of BRI and TOL...BRI/TOL report current status....we will still keep alert shooters on short tether to meet any tasking.
<TOL_OOD> DINO: rg brk currently aligning missles tubes 1,2,3,4
<DINO_FC1> TOL: Up and ready
<TOL_OOD> DINO: aligning missiles tubes 1,2,3,4
TF69_ASWO says:
<AA_STK1> BRI; ALIGN 1 3-C PLACE MISSILE IN RELOAD POOL.
<BRI-THAWK> AA: rgr Align 1 3-C Place in reload pool
<TOL_OOD> Dino: line A: 0317.
<TOL_OOD> DINO: Line A:0317 R01
<BOI_OOD> Dino: line A R01: 0318.
TF69_ASWO says:
<TOL_OOD> DINO: Line B: aff
<TOL_OOD> DINO: Line B: aff ownship all others in progress Line C: no Line E: 0322 P14S/P13N Line F: 0340
<TOL_OOD> DINO: revised Line B: aff all
<CUTLASS> anyone have it, that can turn it around

Collaboration Tools For Different Process Needs

Complex Decisionmaking

TelePresence

Application Sharing

Video Conferencing

Remote Access

Email & Voicemail groups

Audio Conferencing

Asynchronous

Synchronous

Collaboration space Virtual team rooms

Calendar

Instant Messaging

Web Broadcasts

Communities & discussion boards

Simple Information Sharing

Information feeds & repositories

Messages: the Net Centric "Currency"
Evolution to Application Oriented Networking

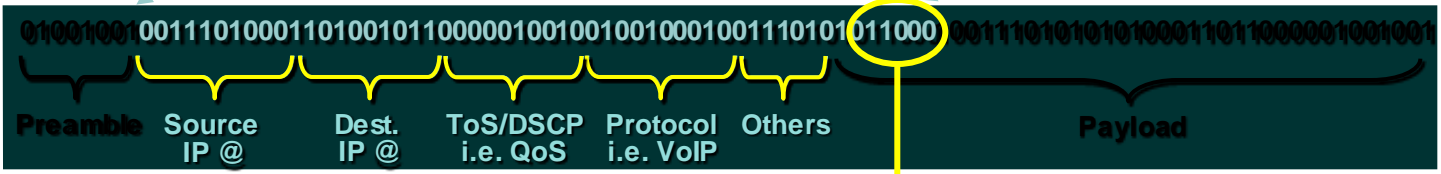| TODAY		FUTURE
Packet-level routing	→	Message routing, e.g. XML
Network protocol decisions	→	Application protocol decisions
Packet-level security	→	Message-level security
Static caching	→	Content-based caching
Protocol translation	→	Message transformation

Fueled by Emerging XML and Web Services Standards

Purposed Information Becomes Multi-purposed

Simple Forwarding Paradigm with Optimized Performance…

| Preamble | Source IP @ | Destination IP @ | Others | Payload |
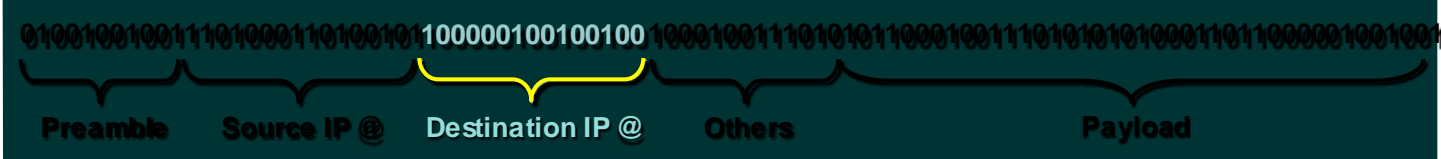
Intelligent Forwarding Paradigm, Optimized for Service Creation

| Preamble | Source IP @ | Dest. IP @ | ToS/DSCP i.e. QoS | Protocol i.e. VoIP | Others | Payload |

e.g., HTTP/NBAR

Deep Payload Inspection

Payload
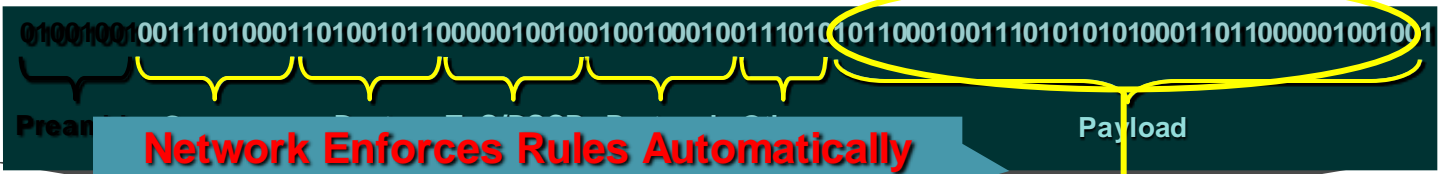
Network Enforces Rules Automatically and Transparently According to Business Policy

Aggregating Message-Level Information

Applying Policies and Security

Fire Mission

**BN 3
Chg 7 GB
He/VT**

Cisco Expo
2009

Battlefield Communications is Changing

- Demands High Datarate Tactical Environment
  - Network Core ➜ Comm Data Link (CDL), IP in Space
  - Network Edge ➜ Ad Hoc Mobility & RF Communications
  - Network Access ➜ Disruption Tolerant Networking solutions (TBD)
  - Critical Services ➜ Secure Unified Communication for Collaboration

--- always connected, always mobile – confront uncertainty with agility…..

The Security Environment is Changing

- Collaboration is No Longer Optional – Comprehensive Approach

  Joint Operations: Army, Navy, Air Force, Marines, Interagency

  Coalition Operations: Terrorism, Peace Keeping Operations, Humanitarian Relief

  Security Operations: Terrorism, Borders, Interagency, Non-Traditional Partners

- Enterprise to Tactical ➜ Voice, Video and Data: Fixed and On the Move

- Across the Boundaries: Ground, Sea, Air, Space and Agency

  Horizontal and Vertical Integration
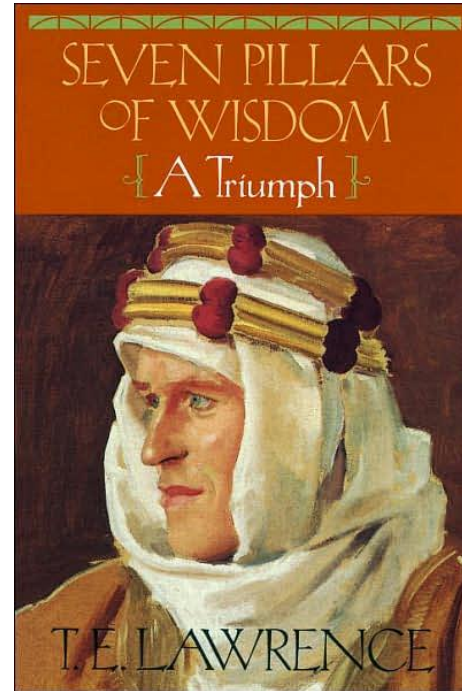
- Agility, Flexibility, Resilience, and Security
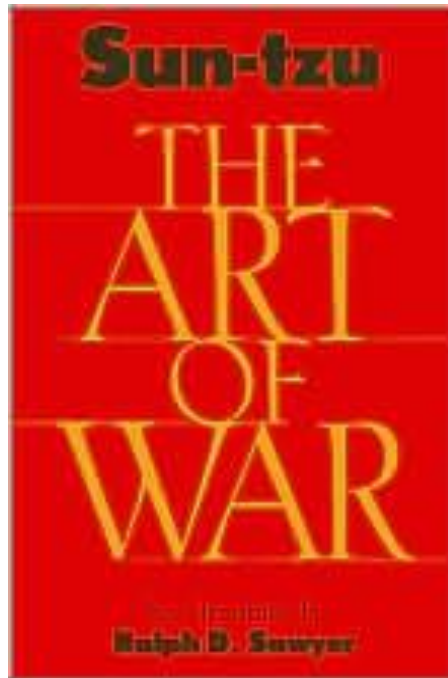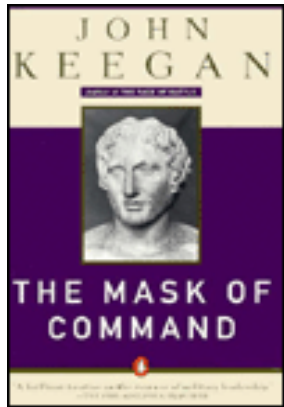

Always connected, always mobile, access to voice, video and data everywhere with Assurance

Net Centric

The Human Network …

**is found throughout
the literature of our profession**