

CYBER CHALLENGES TO C4I OPERATIONS

GMU / AFCEA Symposium: Critical Issues in C4I

23 May 2012

Major General George Allen, USMC
Director of Plans and Policy, J5,
USCYBERCOM

The overall classification of this brief is: **UNCLASSIFIED**



IMPORTANCE OF THE CYBER DOMAIN

DECEMBER 1995

16 million Internet users

MARCH 2001

458 million Internet users

DECEMBER 2011

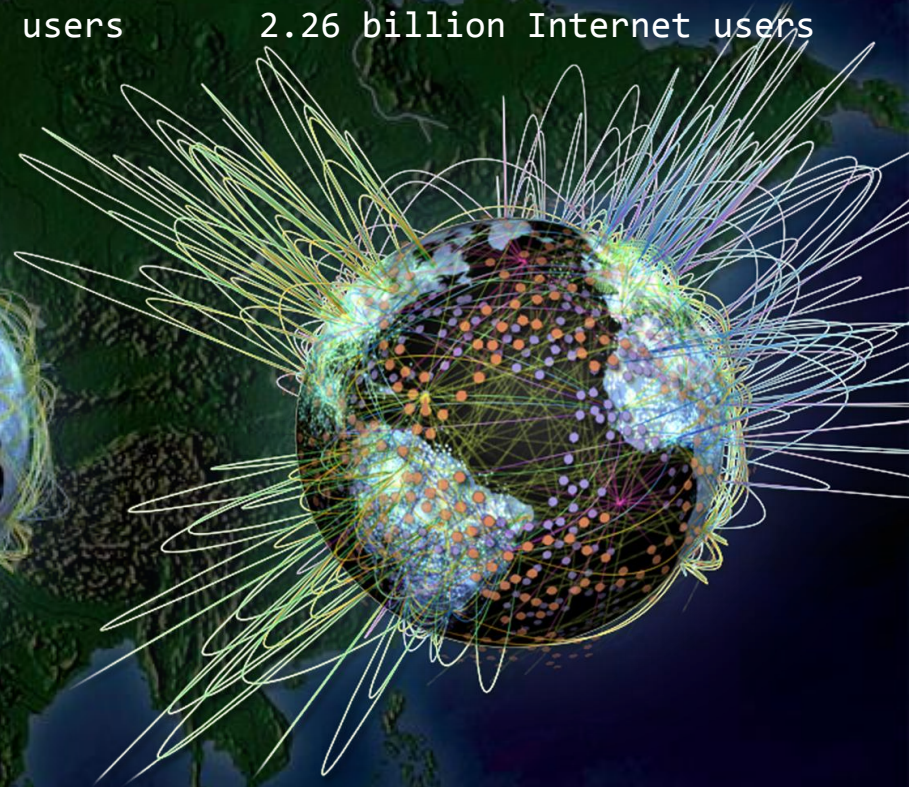
2.26 billion Internet users



Size of the Internet
1 Exabytes



Size of the Internet
16 Exabytes



Size of the Internet
1,000 Exabytes

By 2015, the Number of Internet Hosts Expected to Exceed Human Population

CYBER ENVIRONMENT

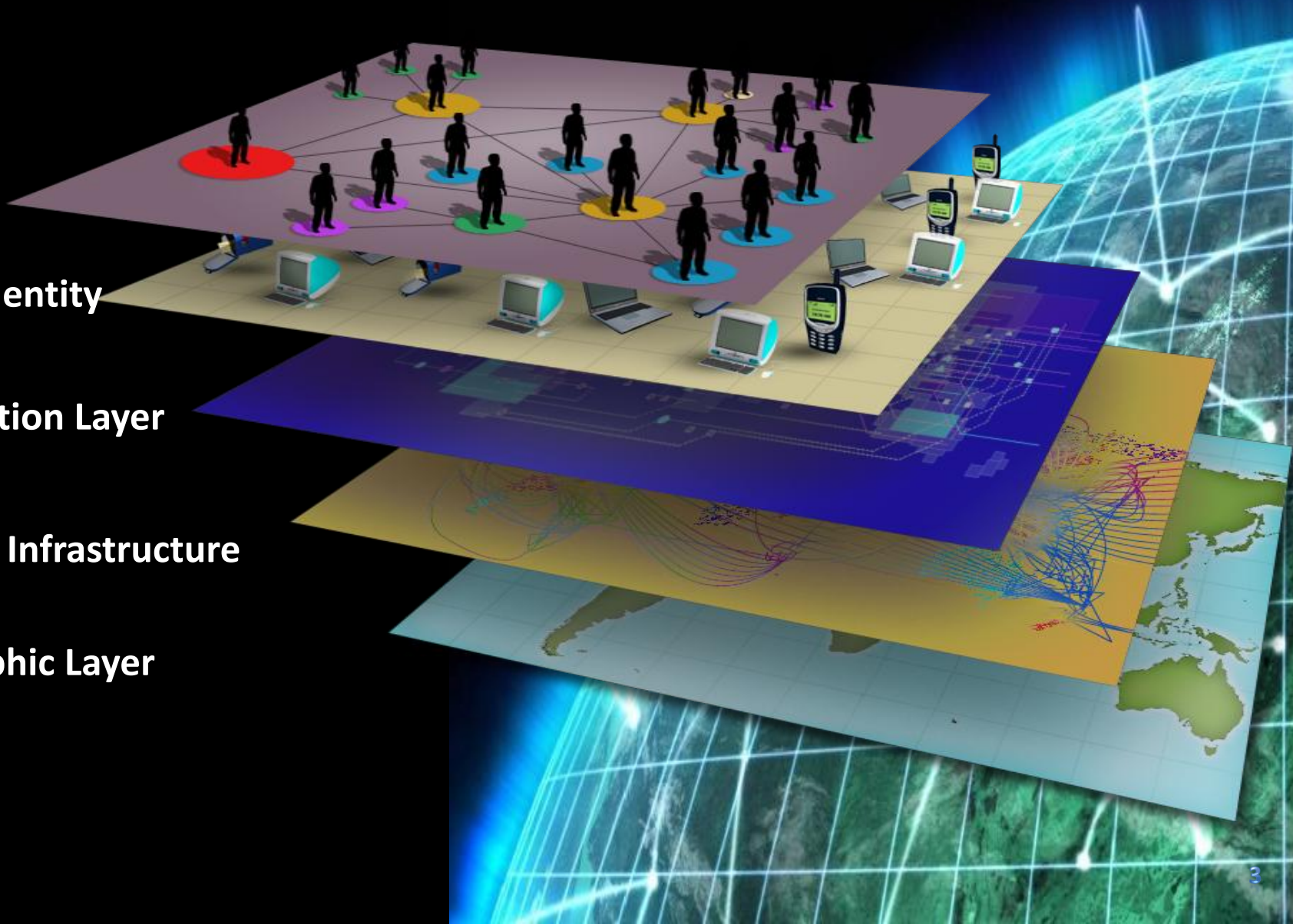
People

Cyber Identity

Information Layer

Physical Infrastructure

Geographic Layer



IMPERATIVES AND CHALLENGES

Imperatives

- Cyber as a **DOMAIN**
- **DYNAMIC** Defense
- Extending Protection to **CIP**
- **COLLECTIVE** Defense
- Leveraging **TECHNOLOGICAL DOMINANCE**

Challenges

- Operationalizing the **CONSTRUCT**
- Building the **FORCE**
- Establishing **AUTHORITIES** Framework
- Developing **DOCTRINE & POLICY**

What is the role of the Military?

The Cyber Threat is Real



The User

THE CYBER TIME BOMB

THREAT EFFECTS

2011 Estimated Costs

- Annual cost of IP theft to US companies: **\$250 Billion**
- Symantec estimate of costs due to global cyber crime: **\$388 Billion**
- Amount McAfee estimates was spent globally on remediation: **\$1 Trillion**



2011 Suspected Victims

- Defense Industry: **97**
- Government Organizations: **98**
- Universities & Institutes: **576**
- Non-Defense Advanced Tech Sector: **1230**
- CNE Infrastructure: **4381**

THE EVOLUTION OF CYBERCOM



2002

USSTRATCOM assumes Cyber mission

2003

DIRNSA dual-hatted as Deputy CDR, Net Attack Planning and Integration

2004

JTF-GNO established, DIRDISA dual-hatted as Commander

2005

JFCC-NW established, DIRNSA dual-hatted as Commander

2008

OCT 2008: OBY

NOV 2008: GNO OPCON to NW

2009

JFCC NW & JTF-GNO combine to form USCYBERCOM staff

2010

Activation of U.S. Cyber Command

MISSION AND CAPABILITIES

USCYBERCOM Mission: *USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.*

DoD Global Information Grid Operations (DGO)

- Employment of manual and automated methods to preserve and sustain the availability, confidentiality, integrity and non-repudiation of military information networks

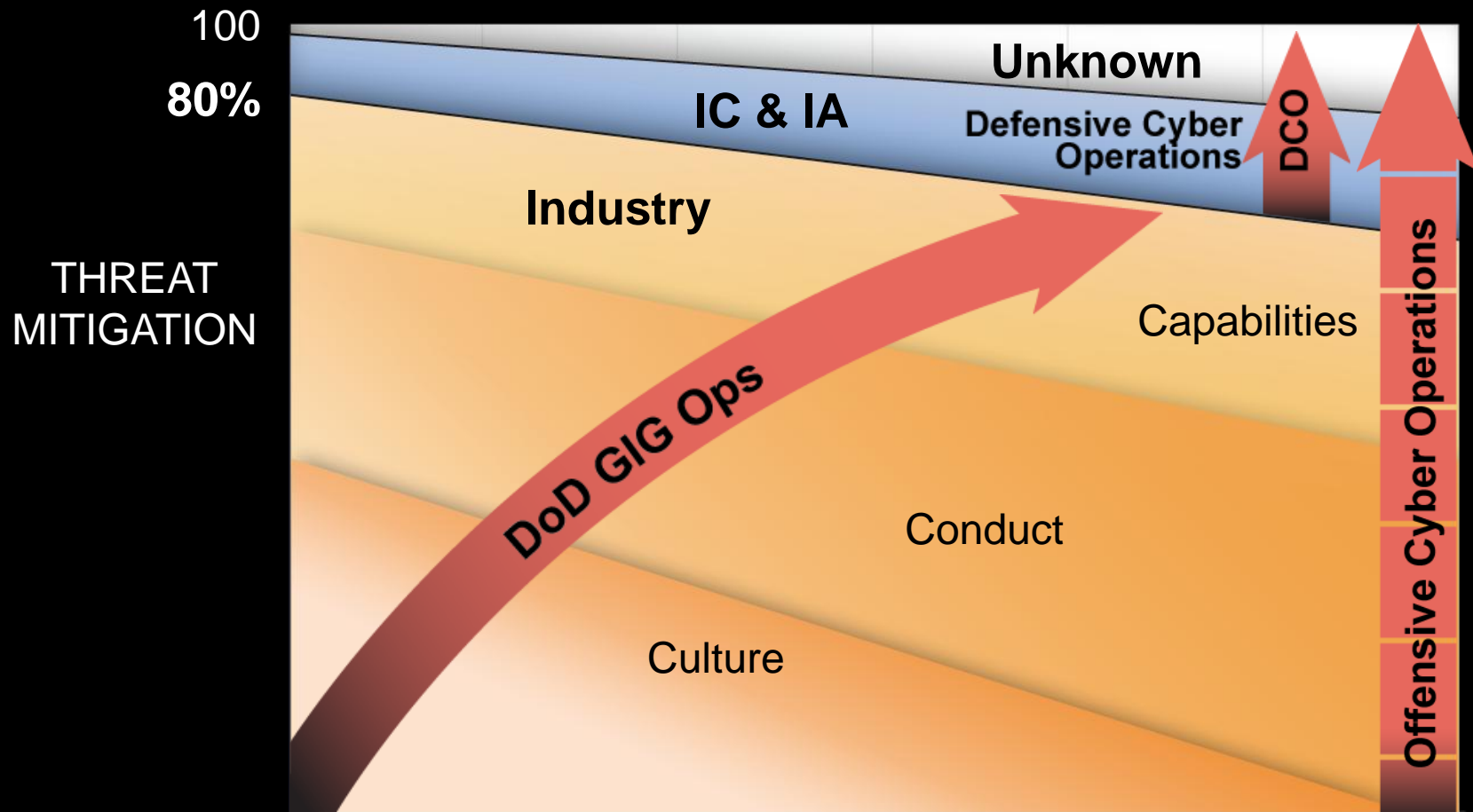
Defensive Cyber Operations (DCO)

- Synchronized real-time capability to discover, detect, analyze and mitigate threats and vulnerabilities, and outmaneuver adversaries, in order to defend Cyberspace and enable freedom of action

Offensive Cyber Operations (OCO)

- Employment of full spectrum cyberspace operations to support COCOM operational requirements and the defense of DoD information networks

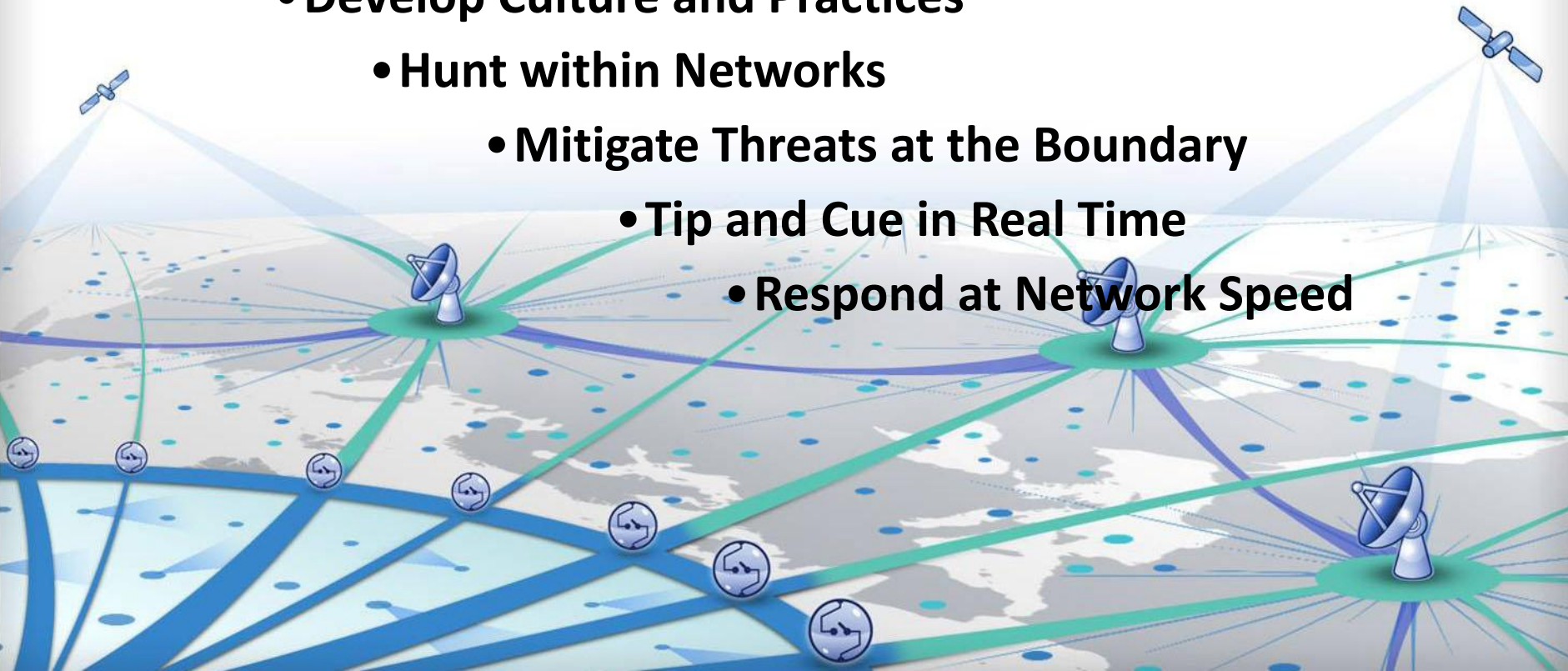
CHANGING THE DYNAMICS



Culture, Conduct, Capability, Capacity

ACTIVE DEFENSE

- Build Defensible Systems
 - Develop Culture and Practices
 - Hunt within Networks
 - Mitigate Threats at the Boundary
 - Tip and Cue in Real Time
 - Respond at Network Speed



PARTNERSHIPS: TEAM CYBER & INTERNATIONAL ENGAGEMENTS



Network Vulnerabilities Are Not Solely a US Problem

- Shared Situational Awareness
- Agile Tipping and Cueing
- Integrated Defensive & Offensive Capabilities
- Synchronized Command & Control



A FINAL THOUGHT

The cyber environment will evolve rapidly, and only the most innovative and agile institutions and users will be able to consistently guard their own data and make the most of new opportunities.

Technical
Convergence

Social
Convergence

Military
Convergence

Future Reality: Convergence

WHAT DOES THIS MEAN FOR THE USCYBERCOM?

As more and more data **converges to a single network** (gov, mil & com), and as the means to analyze it becomes widespread:

Everyone
will compete

Not just large
organizations

But **individuals**
and **groups**

On the ability to
make sense of
vast amounts of
data

Armed with powerful technology from the cloud, nation states, organizations, and even individuals may actually **compete** with the US by achieving effects through **cyberspace**

Ensure Partnership Between Preserving Liberty & Providing Security



QUESTIONS?

