Cyberspace Operations

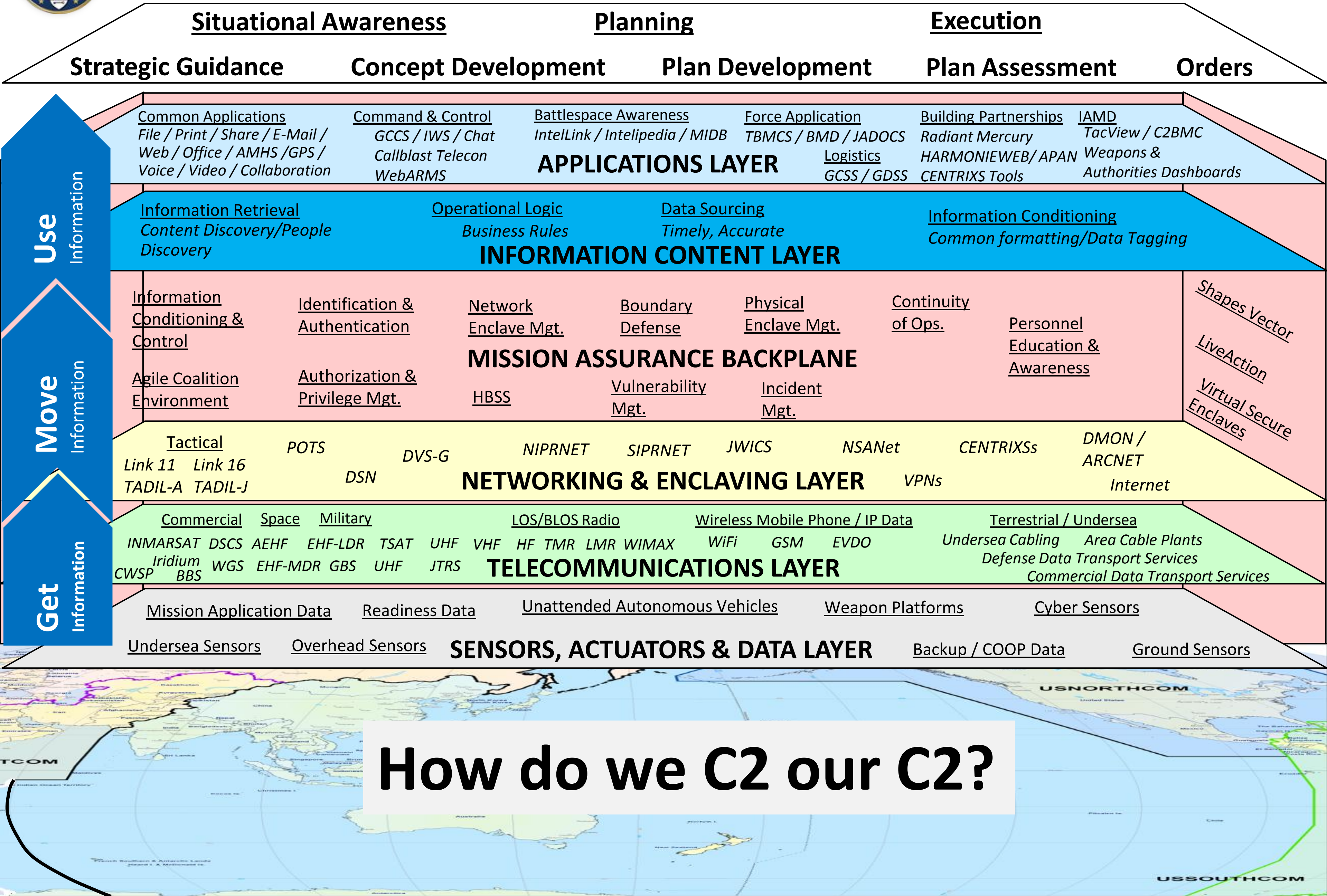
Prepared for the 18th International Command and Control Research and Technology Symposium

Major General Brett T. Williams
Director of Operations (J3), USCYBERCOM

The overall classification of this briefing is: **UNCLASSIFIED//FOR OFFICIAL USE ONLY**

**Classified By: btwill3
Derived From: USCYBERCOM SCG
Dated: 20111011
AND
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20280102**

Operational C2 Architecture



Situational Awareness Planning Execution

Strategic Guidance Concept Development Plan Development Plan Assessment Orders

Use Information

Move Information

Get Information

APPLICATIONS LAYER

Common Applications
File / Print / Share / E-Mail / Web / Office / AMHS /GPS / Voice / Video / Collaboration

Command & Control
GCCS / IWS / Chat
Callblast Telecon
WebARMS

Battlespace Awareness
IntelLink / Intelipedia / MIDB

Force Application
TBMCS / BMD / JADOCS

Logistics
GCSS / GDSS

Building Partnerships
Radiant Mercury
HARMONIEWEB/ APAN
CENTRIXS Tools

IAMD
TacView / C2BMC
Weapons & Authorities Dashboards

INFORMATION CONTENT LAYER

Information Retrieval
Content Discovery/People Discovery

Operational Logic
Business Rules

Data Sourcing
Timely, Accurate

Information Conditioning
Common formatting/Data Tagging

MISSION ASSURANCE BACKPLANE

Information Conditioning & Control

Identification & Authentication

Network Enclave Mgt.

Boundary Defense

Physical Enclave Mgt.

Continuity of Ops.

Personnel Education & Awareness

Agile Coalition Environment

Authorization & Privilege Mgt.

HBSS

Vulnerability Mgt.

Incident Mgt.

Shapes Vector

LiveAction

Virtual Secure Enclaves

NETWORKING & ENCLAVING LAYER

Tactical
Link 11 Link 16
TADIL-A TADIL-J

POTS

DSN

DVS-G

NIPRNET

SIPRNET

JWICS

NSANet

VPNs

CENTRIXSs

DMON / ARCNET

Internet

TELECOMMUNICATIONS LAYER

Commercial Space Military
INMARSAT DSCS AEHF EHF-LDR TSAT UHF
CWSP Iridium BBS WGS EHF-MDR GBS UHF JTRS

LOS/BLOS Radio
VHF HF TMR LMR WIMAX

Wireless Mobile Phone / IP Data
WiFi GSM EVDO

Terrestrial / Undersea
Undersea Cabling Area Cable Plants
Defense Data Transport Services
Commercial Data Transport Services

SENSORS, ACTUATORS & DATA LAYER

Mission Application Data

Readiness Data

Unattended Autonomous Vehicles

Weapon Platforms

Cyber Sensors

Undersea Sensors

Overhead Sensors

Backup / COOP Data

Ground Sensors

How do we C2 our C2?

USCYBERCOM Mission and Operations

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.*

Defend the Nation Against Strategic Cyber Attack

Operate and Defend DoD Information Networks (DoDIN)

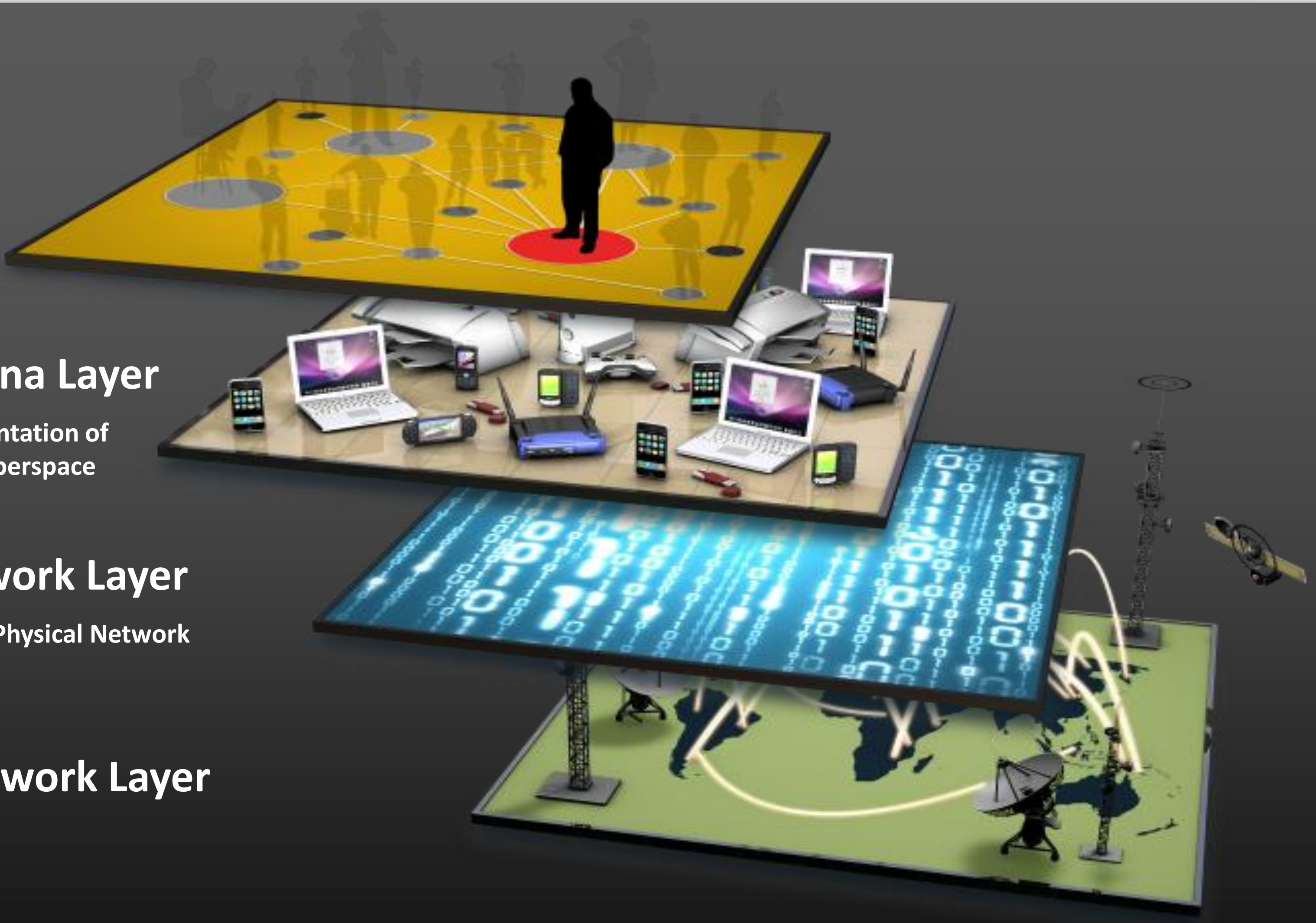
Combatant Command Support

National Mission Teams

DISA/Services Cyber Protection Teams

Combat Mission Teams

The Three Layers of Cyberspace



People

Cyber-Persona Layer

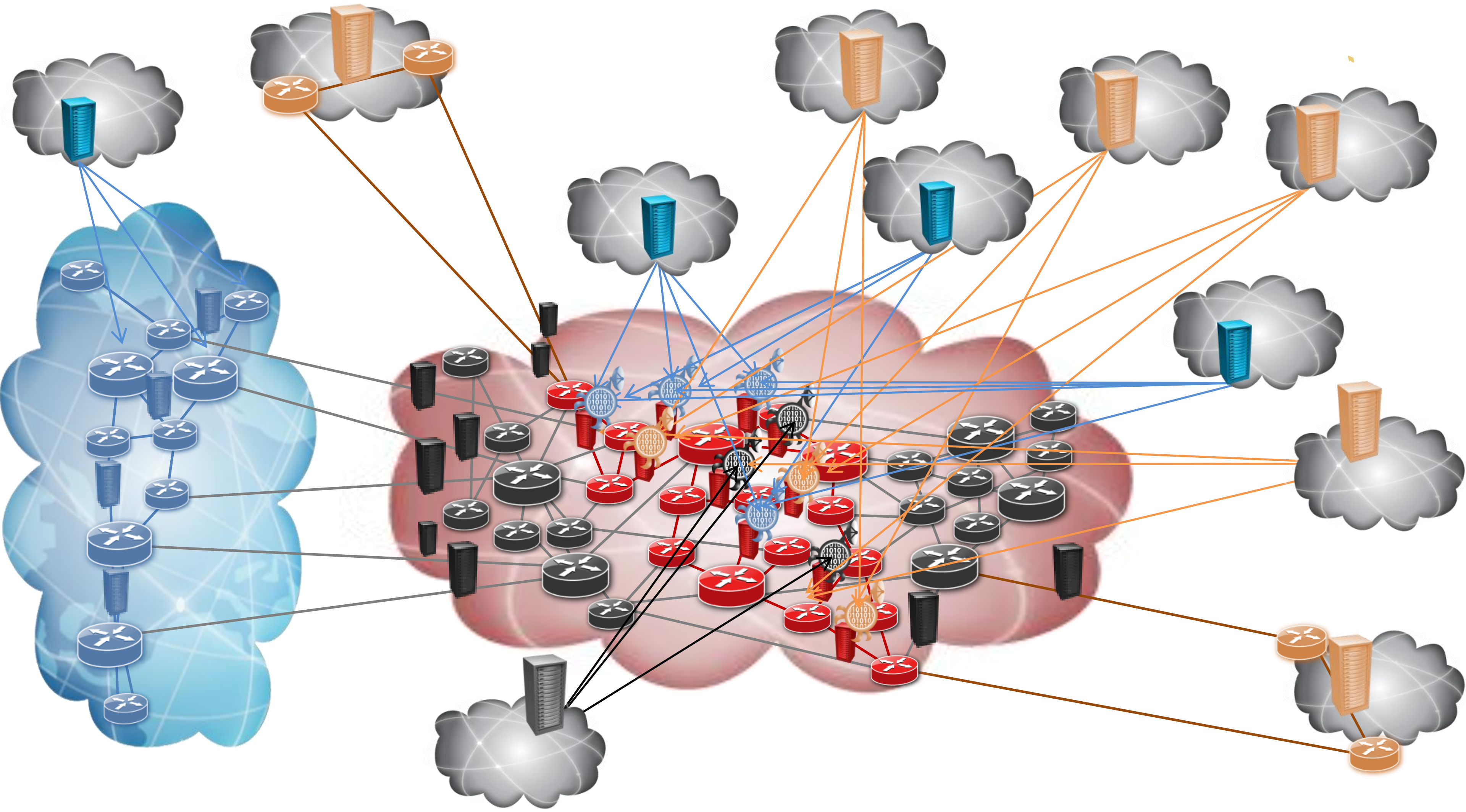
- Digital representation of an entity in cyberspace

Logical Network Layer

- Abstract from Physical Network

Physical Network Layer

Cyber Terrain



Cyberspace Operations

Per Joint Publication 3-12 (05 FEB 2013)

DoDIN Global Operations

*Network focused

Defensive Cyberspace Operations (DCO)

DCO – Internal Defensive Measures (DCO-IDM)

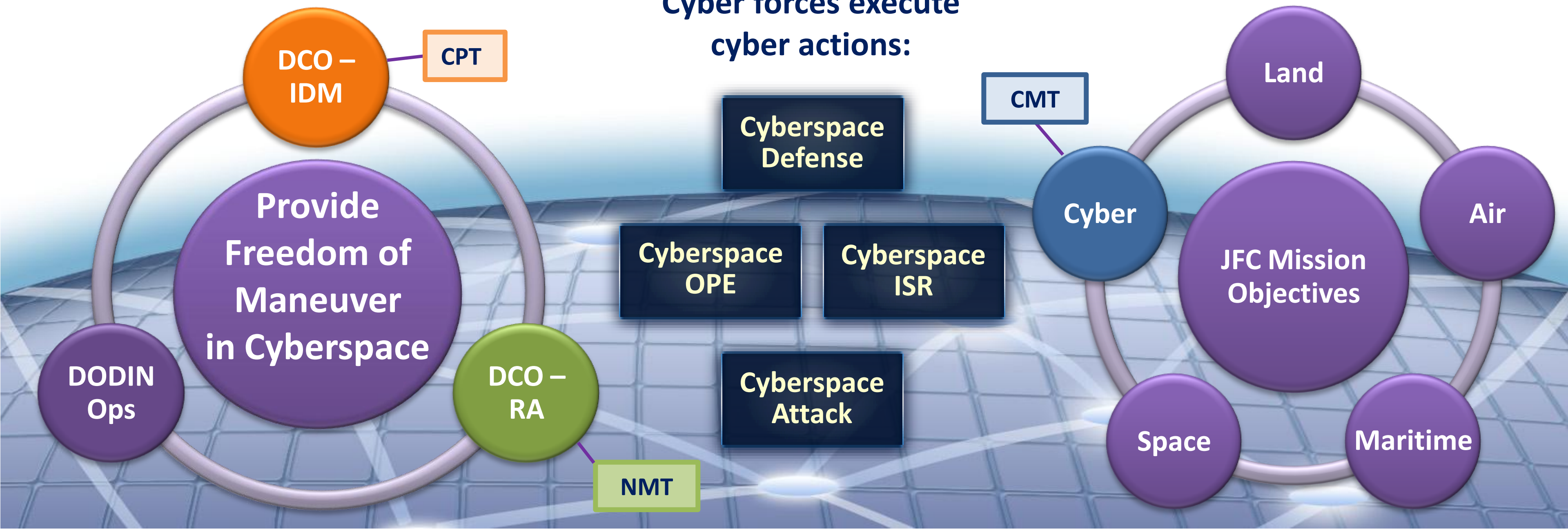
* Mission focused

DCO – Response Actions (DCO-RA)

* Mission focused

Offensive Cyberspace Operations (OCO)

* Project power in and through cyberspace.



Cyber forces execute cyber actions:

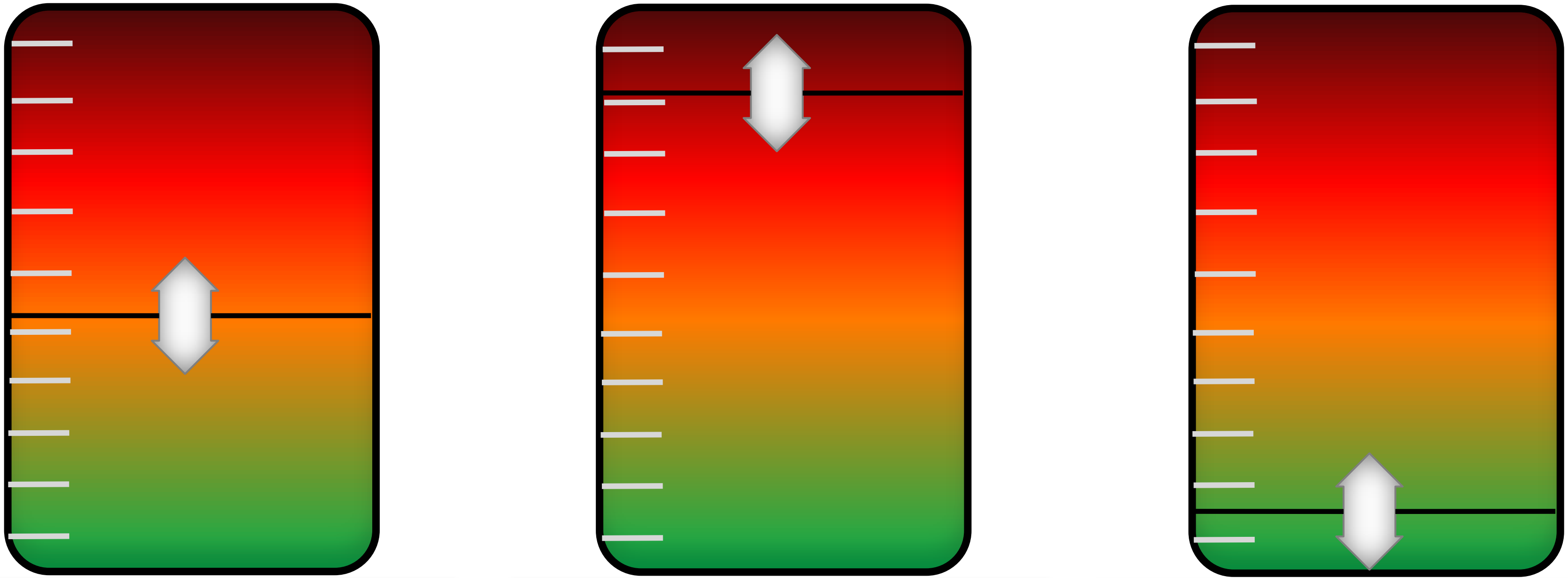
Cyberspace Defense

Cyberspace OPE

Cyberspace ISR

Cyberspace Attack

Preserve Friendly Freedom of Maneuver in Cyberspace



DoD Information Networks Global Operations (DoDIN Global Ops)

LIMITS

- Network performance

Defensive Cyberspace Operations – Internal Defensive Measures (DCO-IDM)

LIMITS

- Identify Key Cyber Terrain
- Link vulnerabilities to threat
- Capability and capacity
- Authorities

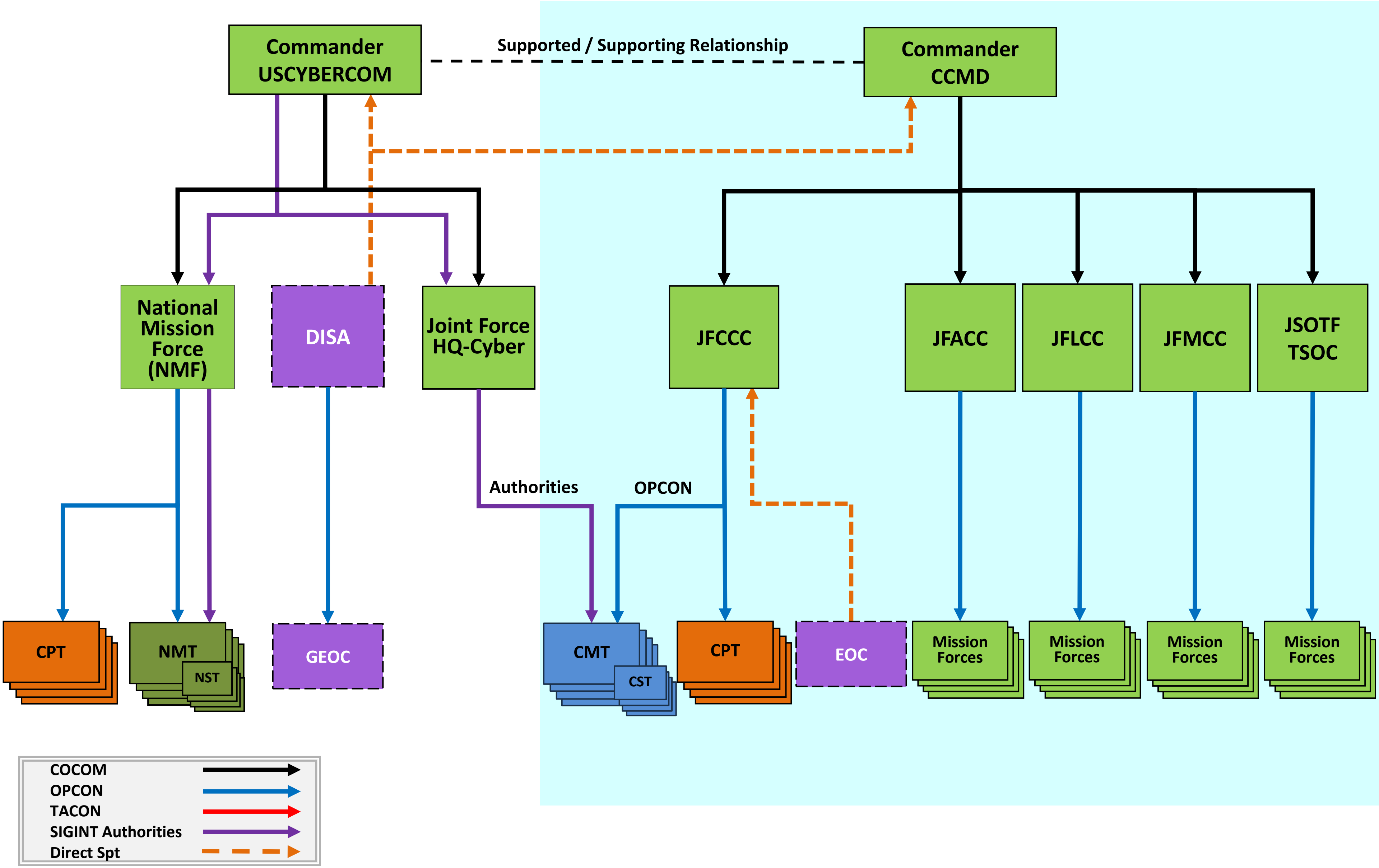
Defensive Cyberspace Operations – Response Actions (DCO-RA)

LIMITS

- Policy
- Rules of Engagement
- Authority

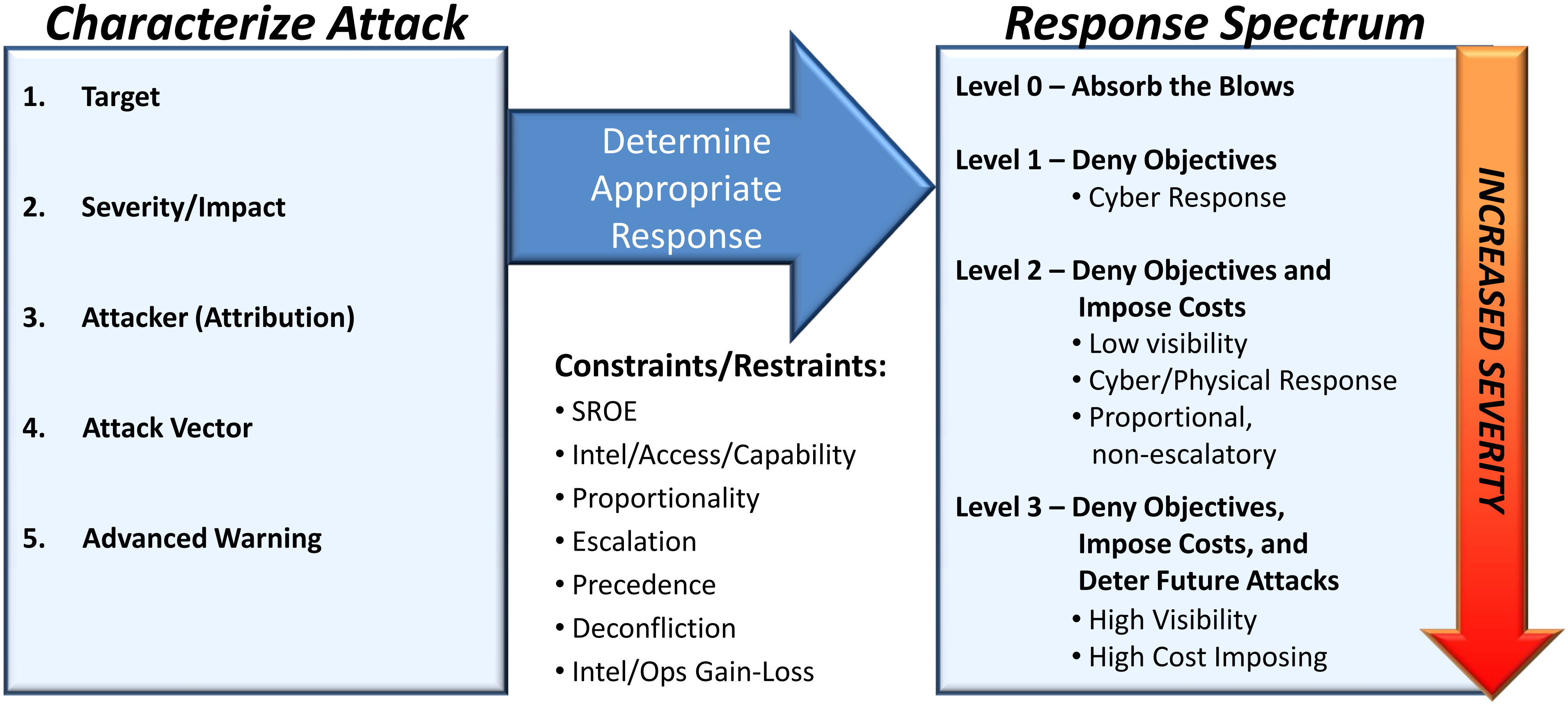
- Intelligence
- Access
- Capability

An Option for Cyber C2



Major General Brett T. Williams
Director of Operations (J3)
USCYBERCOM

Analytic Framework for Responding to Cyber Attack Against the U.S.



Characterize Attack

1. Target
2. Severity/Impact
3. Attacker (Attribution)
4. Attack Vector
5. Advanced Warning

Determine Appropriate Response

Constraints/Restraints:

- SROE
- Intel/Access/Capability
- Proportionality
- Escalation
- Precedence
- Deconfliction
- Intel/Ops Gain-Loss

Response Spectrum

Level 0 – Absorb the Blows

Level 1 – Deny Objectives

- Cyber Response

Level 2 – Deny Objectives and Impose Costs

- Low visibility
- Cyber/Physical Response
- Proportional, non-escalatory

Level 3 – Deny Objectives, Impose Costs, and Deter Future Attacks

- High Visibility
- High Cost Imposing

INCREASED SEVERITY

- ***Time (+target/severity) drives requirement for pre-approved, pre-planned actions.***
- ***Response execution by agency with capability and capacity, then align authorities.***