# Effective Synchronization and Integration of Effects Through Cyberspace for the Joint Warfighter

*14 AUG 12*

BG George J. Franz, III

**Director of Current Operations**

**United States Cyber Command**

UNCLASSIFIED
Approved For Public Release

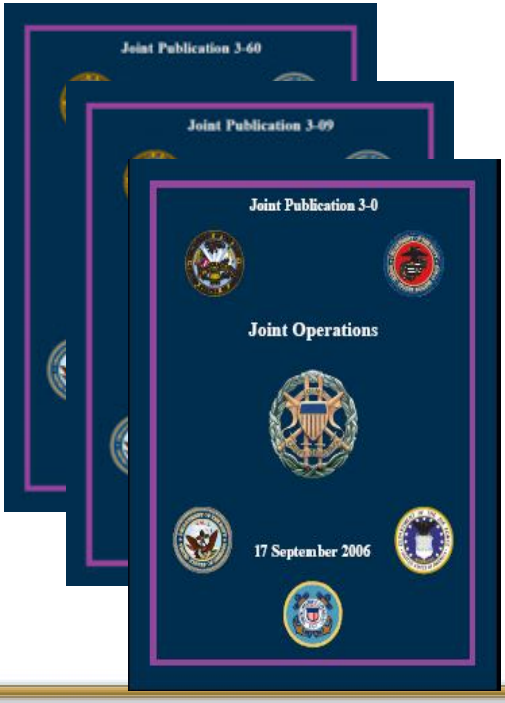
# Agenda

- Joint Operations
- Joint Cyberspace Doctrine
  - Joint Warfighting Functions
  - Cyberspace Domain
- Command and Control (C2)
  - Transitional C2 Model
- Planning to Execution
- Considerations/Thoughts

# Joint Operations

- "Joint operations doctrine is built on a sound base of warfighting philosophy, theory, and *practical experience*." - JP 3-0
- United States Cyber Command (USCYBERCOM) plans and executes operations in support of military objectives, and, in so doing, adheres to applicable Joint Doctrine, Execute Orders, and Presidential Directives."

  - Commander USCYBERCOM



Joint Publication 3-60

Joint Publication 3-09

Joint Publication 3-0

Joint Operations

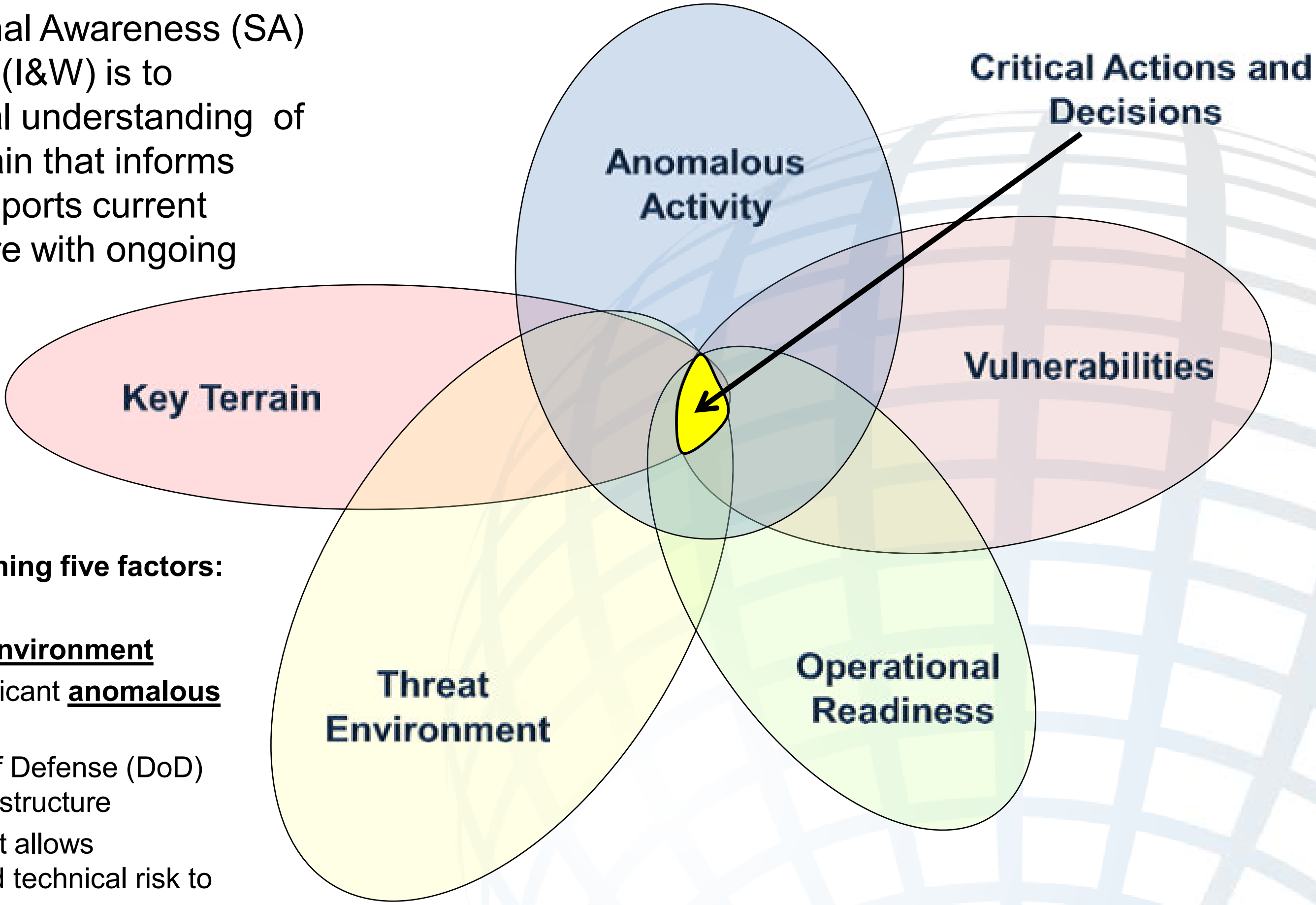
17 September 2006

***<u>Insights</u>***

- ***Effects must be synchronized to support the joint force commander's tactical objectives, operational goals, and strategic endstate***
- ***Cyber Support Elements integrated into the supported Joint Forces Components planning and execution (Battle Rhythm)***
  - ***"Acts as staff advisor to the Director of Operations"***
  - ***Clear agreement as to the effects desired (CERF) and how they are delivered (JCSR)***

# Ultimate Operational Goal

The ultimate goal of Situational Awareness (SA) and Indications and Warning (I&W) is to maintain strategic and tactical understanding  of the military cyberspace domain that informs operational risk decision, supports current actions, and does not interfere with ongoing operations.



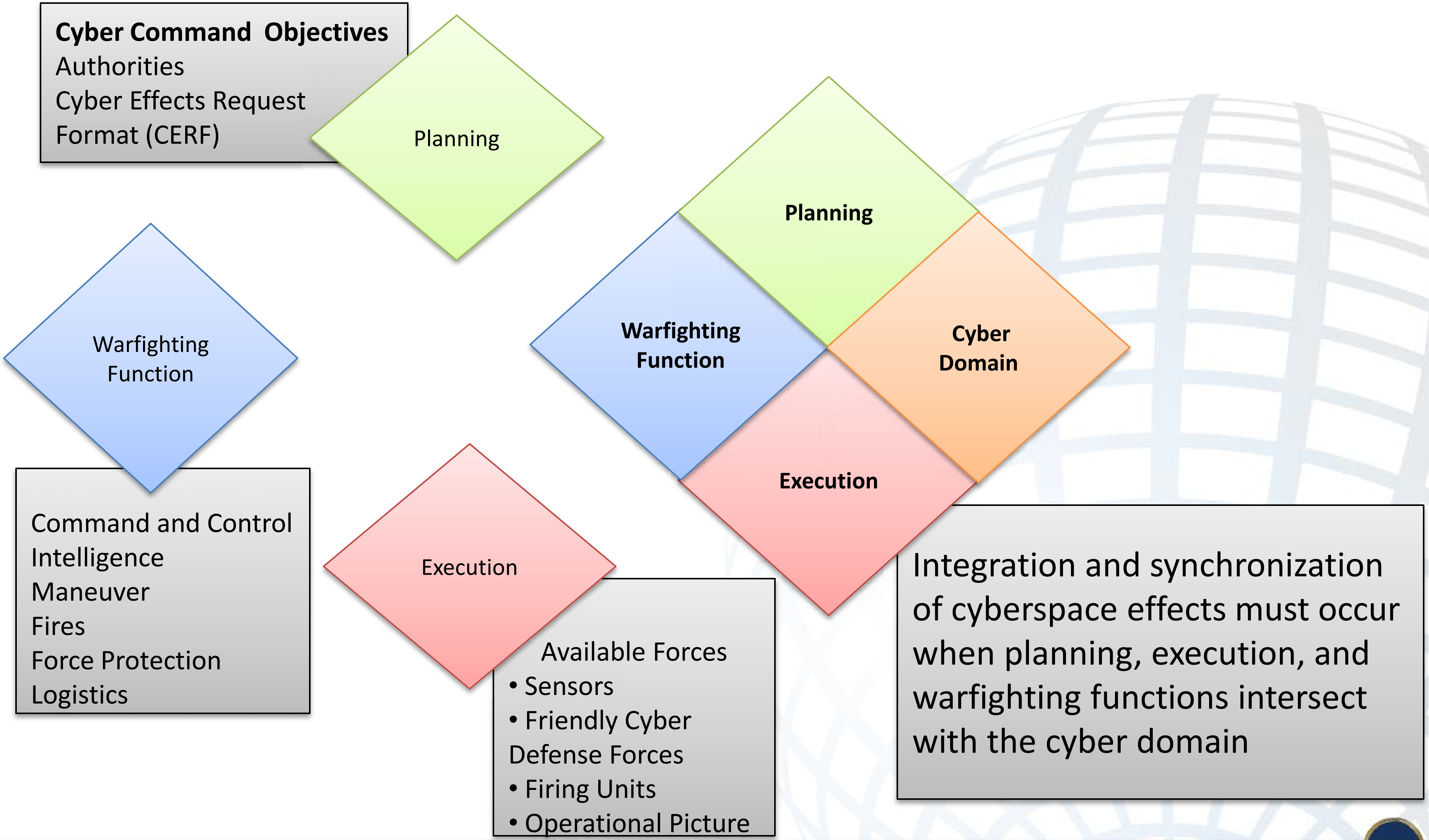
Continuous SA/IW enables informed, decisive actions

**Goal is reached by holistically examining five factors:**

1. Current and near-future **threat environment**
2. Identified global threat and significant **anomalous activity**
3. **Vulnerabilities** of Department of Defense (DoD) systems and the underlying infrastructure
4. Prioritized **key cyber terrain** that allows understanding of operational and technical risk to DoD operations and networks
5. Current **operational readiness** and capability of cyber forces and sensors

# Joint Cyberspace Doctrine

## Joint Warfighting Function



**Cyber Command Objectives**
Authorities
Cyber Effects Request Format (CERF)

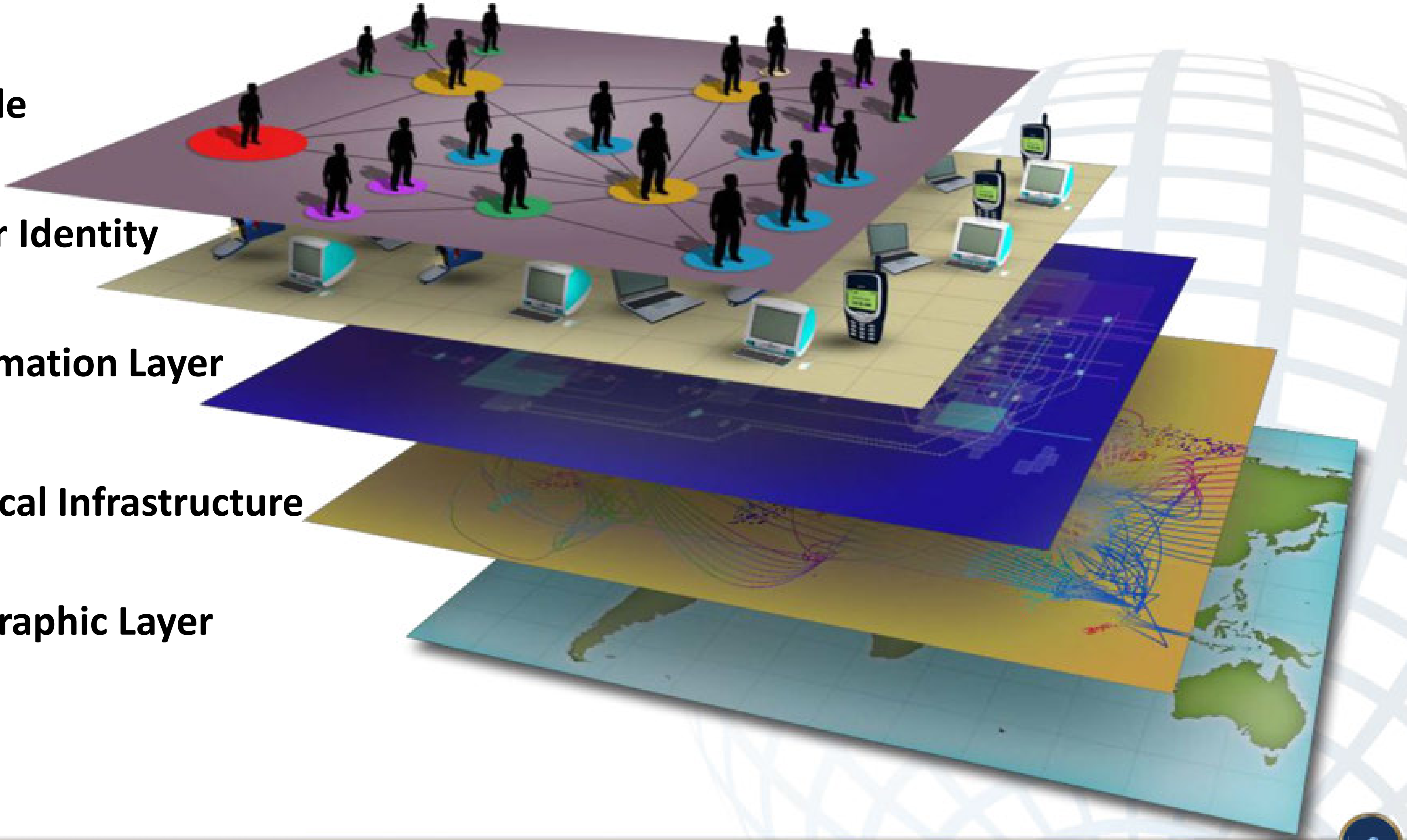
Command and Control
Intelligence
Maneuver
Fires
Force Protection
Logistics

Available Forces
- Sensors
- Friendly Cyber Defense Forces
- Firing Units
- Operational Picture

Integration and synchronization of cyberspace effects must occur when planning, execution, and warfighting functions intersect with the cyber domain

# Joint Cyberspace Doctrine

## Joint Cyberspace Domain



People

Cyber Identity

Information Layer

Physical Infrastructure

Geographic Layer

# Key Terrain

- Key Terrain – Any locality, or area, the seizure or retention of which affords a marked advantage to either combatant. (JP 1-02)
- What does this mean in the cyber domain?
  - Key terrain applies to those physical and logical elements of the domain that enable mission essential warfighting functions.
  - Key terrain is temporal. It changes with the mission and adversary. In the absence of either, these elements may be critical infrastructure or a key resource, but not key terrain.
  - Key terrain can be decomposed into personal, logical, informational, and physical layers.
  - Key terrain is applicable across the strategic, operational, and tactical levels of war.
  - Key terrain may be fiber optic cable, satellite communication (SATCOM) uplink/downlink, subnets, databases with usernames and passwords, even technicians themselves.

# Joint Cyberspace Domain

**Battle executed in minutes or seconds**

Response must be immediate or mission failure (similar response for accident)

**Attribution not required for a successful response**

Retaliation is not a condition of successful defense

**Crippling strategic effects if defensive preps are inadequate**

Preparations (access & development) take years, effects take moments

**Threats are inherently global and cross theaters**

Effects are globally dispersed and 2nd & 3rd order effects may not be predictable

**Challengers have the advantage**

The architecture of the networks significantly give the aggressor the advantage

# Command and Control

## United States Cyber Command (USCYBERCOM)

USCYBERCOM is US Strategic Command's (USSTRATCOM) execution arm for cyberspace operations, and directs offensive cyberspace operations. USCYBERCOM is directed by USSTRATCOM as the focal point for military cyberspace operations, and is delegated Operational Control (OPCON) or Tactical Control (TACON) of designated forces

## Joint Operations Center (JOC)

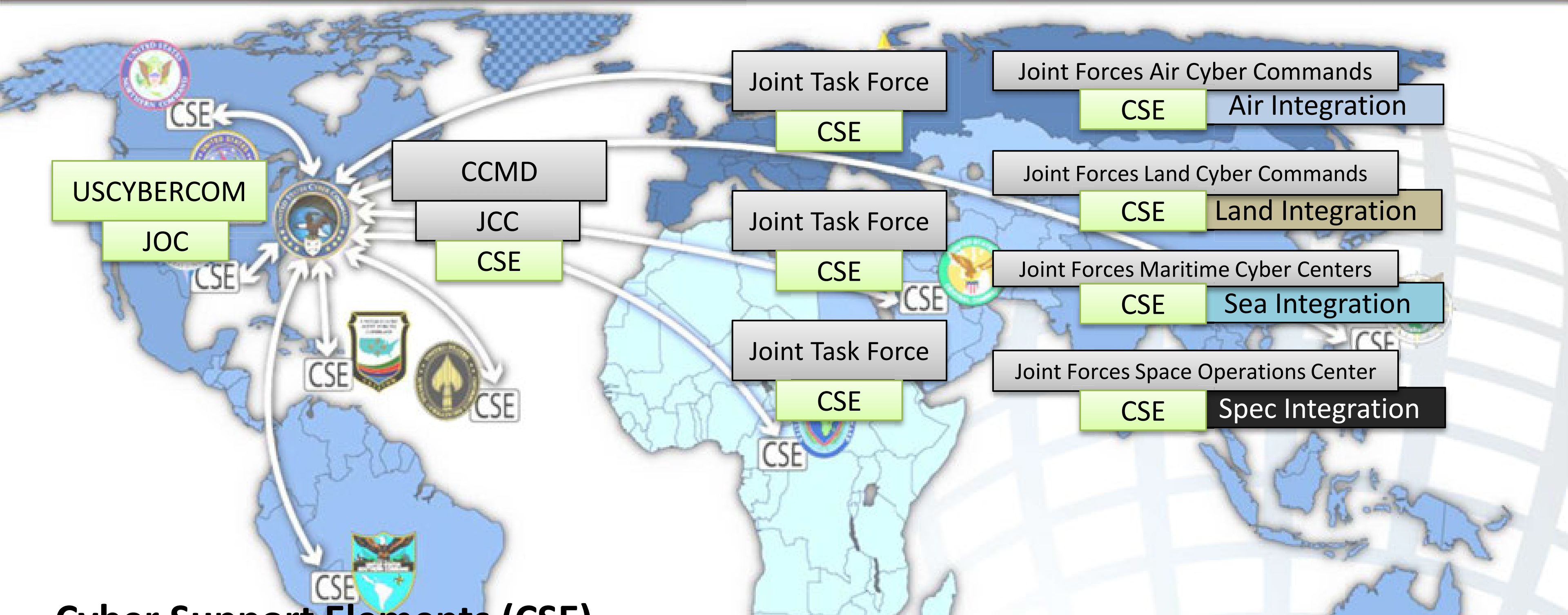
USCYBERCOM JOC coordinates, synchronizes, and directs operations, to include: (a) health and status of networks, (b) vulnerabilities and detected adversary activity, (c) priority event related tipping and cuing, (d) dissemination of orders, (e) adjusting countermeasures, (f) interface with external organizations/agencies.

## Joint Cyber Center (JCC)

Functions as the nexus for the Combatant Command cyberspace enterprise. The JCC supported by USCYBERCOM serves as the staff/component for planning and oversight of Combatant Command Defensive Cyber Operations (DCO), DoD Global Information Grid Operations (DGO), and Offensive Cyber Operations (OCO).

***CDRUSCYBERCOM deconflicts fires delivered in and through cyberspace***

# Transitional C2 Model



## Cyber Support Elements (CSE)

Organized from USCYBERCOM forces and stationed with Combatant Commanders (CCDR) for full integration with their staff. Provide subject matter experts for cyberspace operations, planning, and other related functions. Includes a forward-deployed element of USCYBERCOM (or service cyber component) personnel temporarily augmenting the CSE in CCDR designated locations during an operation

# USCC Workflow for Integrated Priorities

**JIPCL**
Joint Integrated Prioritized Collection List

**JIPL**
Joint Integrated Priority List

**JPG**
Joint Planning Groups (J5)

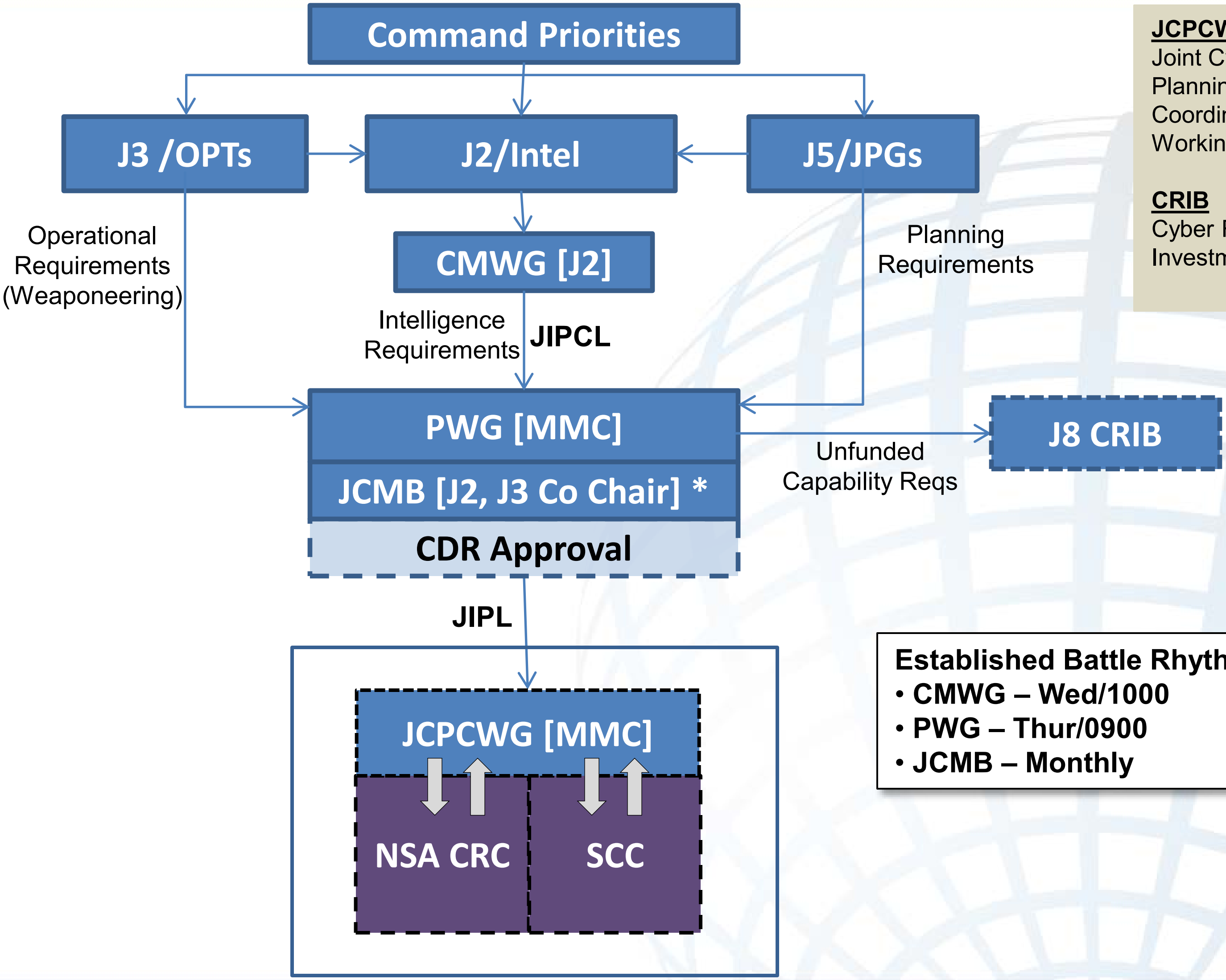
**OPTs**
Operations Planning Teams

**CMWG**
Collection Management Working Group

**JCMB**
Joint Collection Management Board

**MMC**
Mission Management Cell

**PWG**
Priorities Working Group



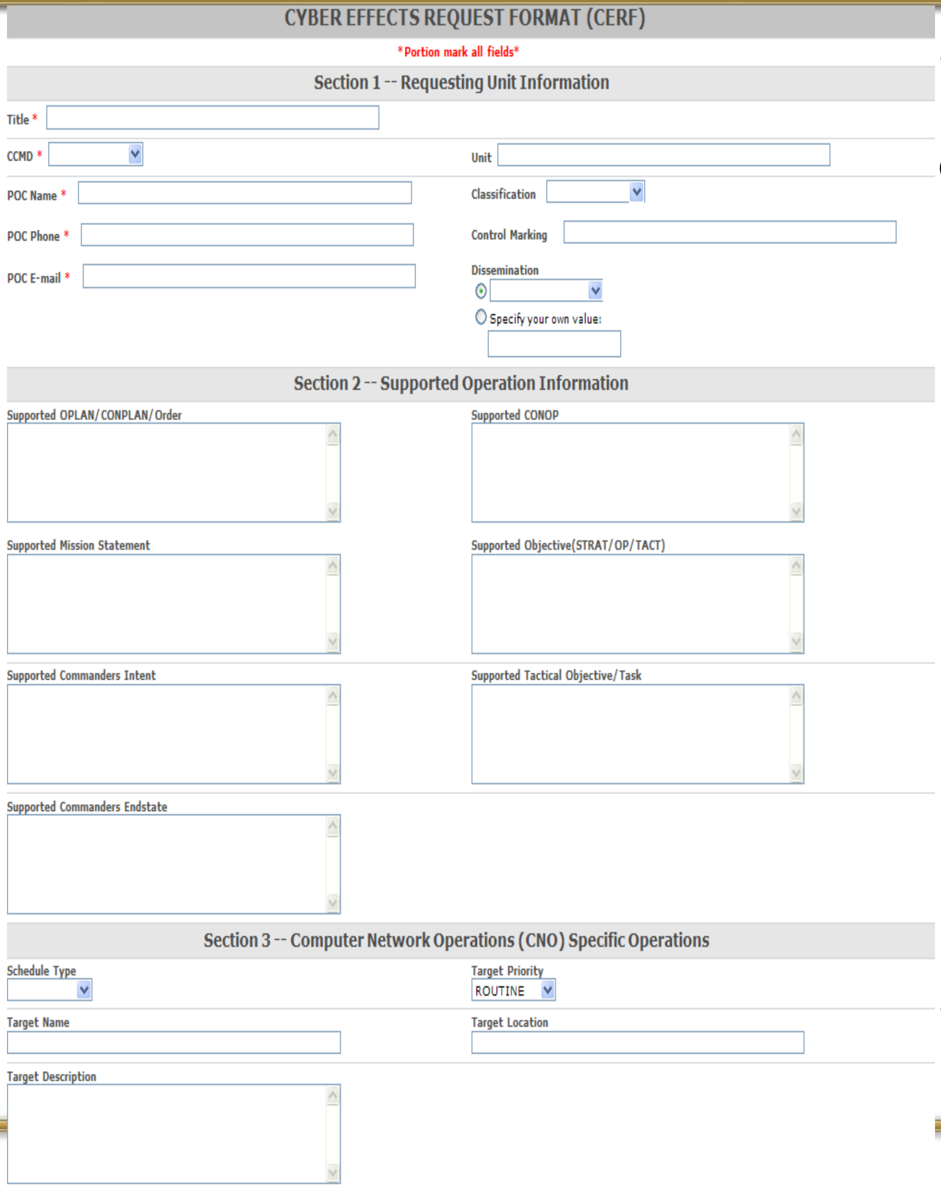
**JCPCWG**
Joint Cyber Planning and Coordination Working Group

**CRIB**
Cyber Reqs and Investment Board

**Established Battle Rhythm**
- CMWG – Wed/1000
- PWG – Thur/0900
- JCMB – Monthly

UNITED STATES CYBER COMMAND

CERF Portal



## CYBER EFFECTS REQUEST FORMAT (CERF)

*Portion mark all fields*

### Section 1 -- Requesting Unit Information

Title *

CCMD *

Unit

POC Name *

Classification

POC Phone *

Control Marking

POC E-mail *

Dissemination

●

○ Specify your own value:

### Section 2 -- Supported Operation Information

Supported OPLAN/CONPLAN/Order

Supported CONOP

Supported Mission Statement

Supported Objective(STRAT/OP/TACT)

Supported Commanders Intent

Supported Tactical Objective/Task

Supported Commanders Endstate

### Section 3 -- Computer Network Operations (CNO) Specific Operations

Schedule Type

Target Priority: ROUTINE

Target Name

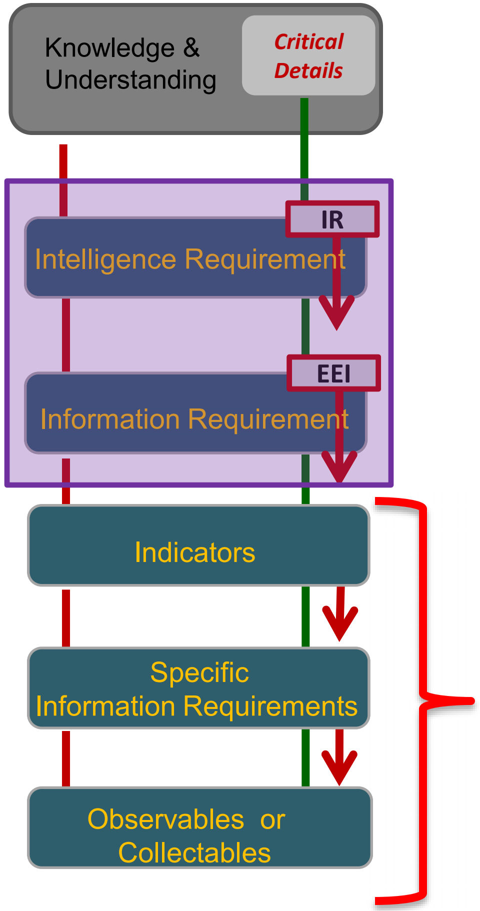
Target Location

Target Description

- Cyber Effects Request Format (CERF) Process initiates cyber effects planning across all lines of operation (LOOs)
  - Links the desired effect with the tactical objective, operational goal, and strategic endstate
  - Records, Tracks, and Manages requests from the supported Joint Forces Command (JFC)
  - 24/7, subsequently assigned in accordance with time horizon and function
  - Facilitates dialogue/Direct Line of Authority and transparency throughout the process
- Prioritizes requests and support through the MMC, reflects supported JFC prioritization

# Collection – Analytical Drilldown

**Requirements Development** → **Collaborative Steps and Processes**



Knowledge & Understanding

*Critical Details*

IR

Intelligence Requirement

EEI

Information Requirement

Indicators

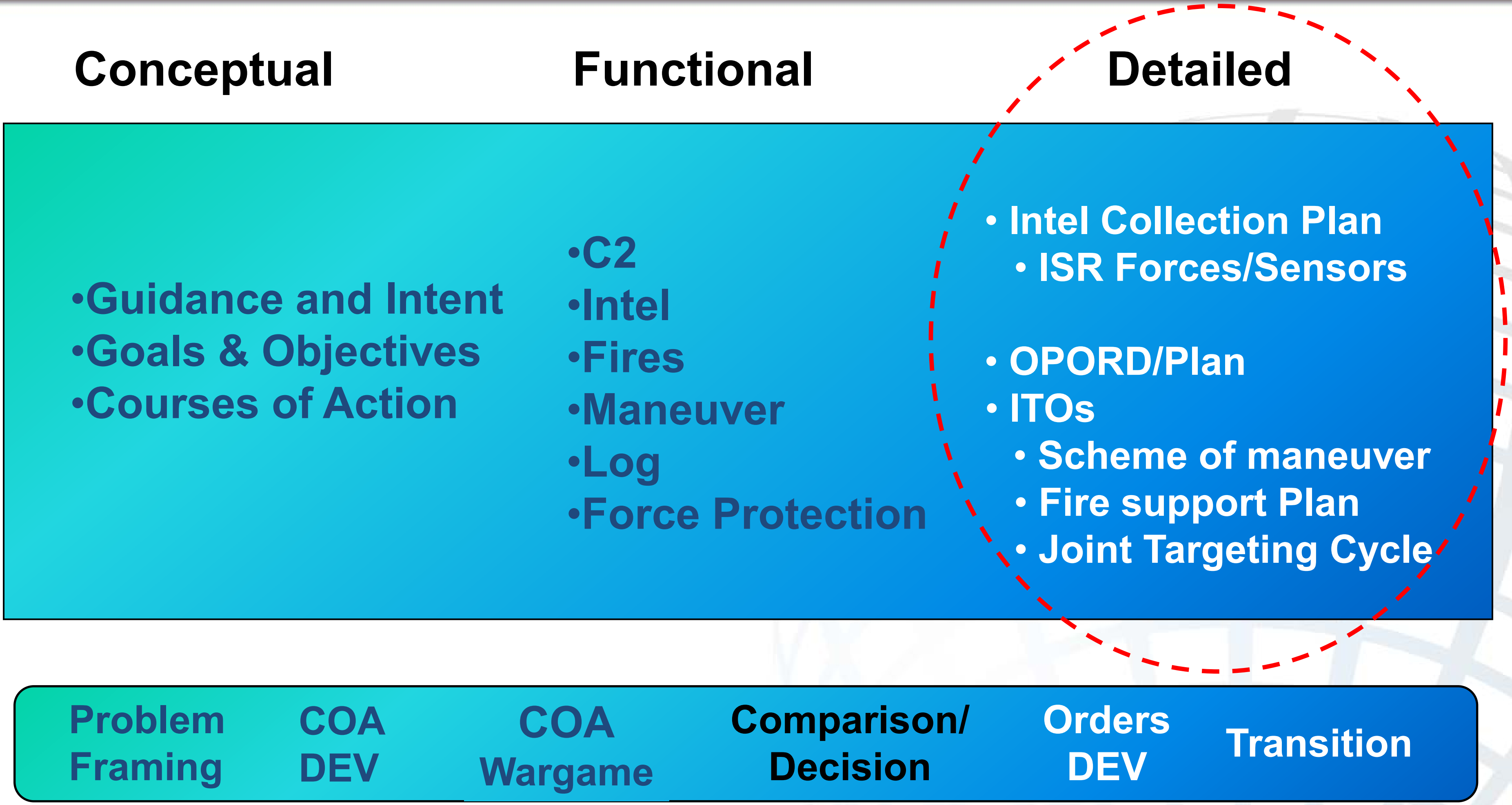
Specific Information Requirements

Observables or Collectables

| Step 1. Intelligence Priorities | Step 2. Intelligence Gaps | Step 3. EEIs "Drill Down" | Step 4. Collection Priorities | Step 5. Strategies & Assessments |
|---|---|---|---|---|
| *What do we need to focus on the most?* | *What do we need to know the most?* | *What are the important indicators ?* | *Where does the information reside?* | *How do we obtain answers?* |
| J2/J3/J5:<br>Establish intelligence priorities and focus areas | J2:<br>Identify critical intelligence gaps | J2:<br>Break down problem down to finest points | J2:<br>Identify Priority intelligence needs | J2:<br>Develop/ execute/ assess collection plans |

**We would like to eventually incorporate Specific Information Requirements (SIRs) and Specific Observable Requirements (SORs)**

# Planning to Execution



Conceptual

- Guidance and Intent
- Goals & Objectives
- Courses of Action

Functional

- C2
- Intel
- Fires
- Maneuver
- Log
- Force Protection

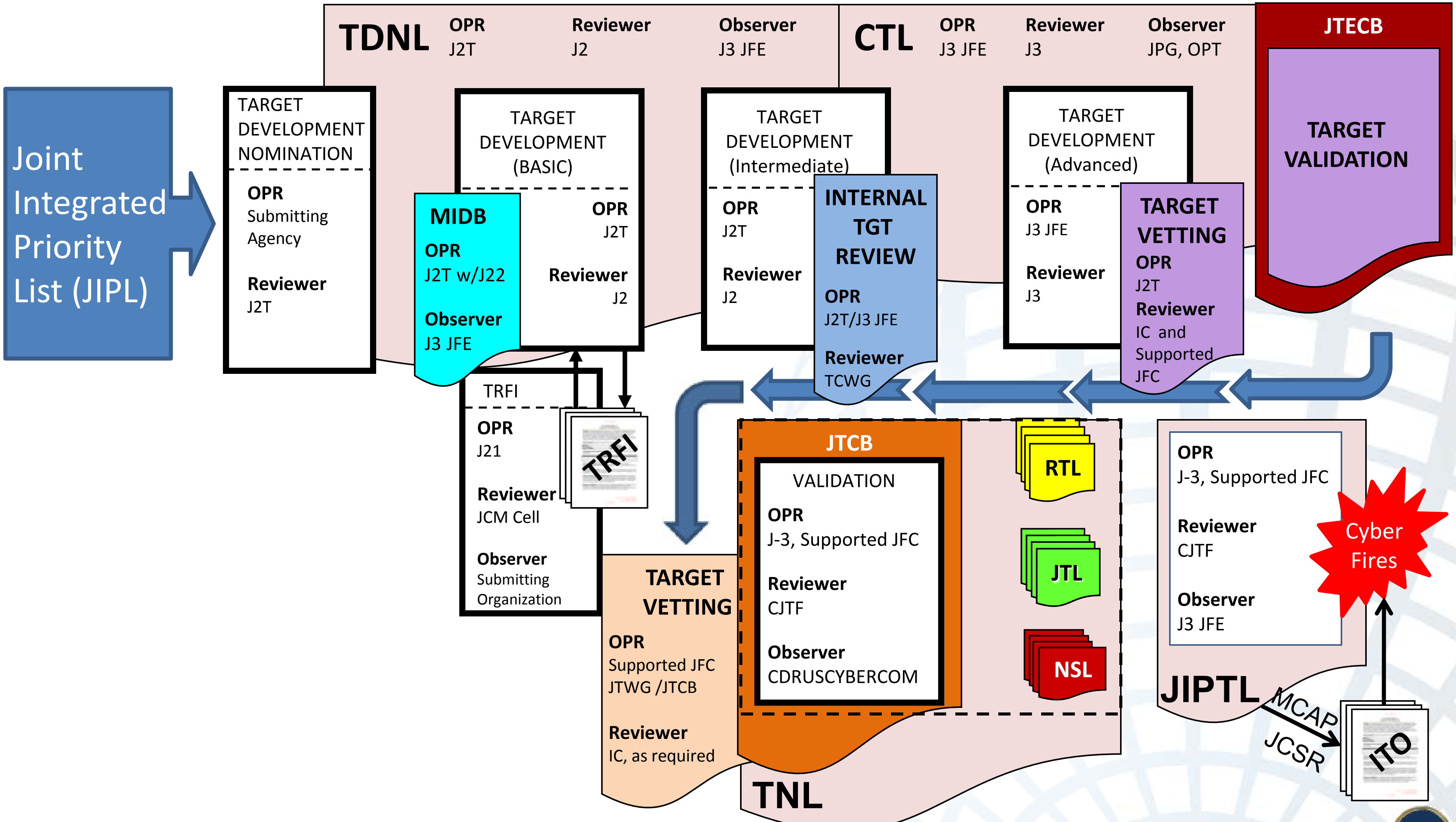
Detailed

- Intel Collection Plan
  - ISR Forces/Sensors
- OPORD/Plan
- ITOs
  - Scheme of maneuver
  - Fire support Plan
  - Joint Targeting Cycle

Problem Framing — COA DEV — COA Wargame — Comparison/ Decision — Orders DEV — Transition

| **ISR** | **OPORD** | **ITO** | **COA** | **DEV** |
|---|---|---|---|---|
| Intelligence, Surveillance, Reconnaissance | Operational Orders | Integrated Tasking Orders | Courses of Actions | Development |

# Targeting Process



Joint Integrated Priority List (JIPL)

TDNL OPR J2T Reviewer J2 Observer J3 JFE

TARGET DEVELOPMENT NOMINATION

OPR
Submitting Agency

Reviewer
J2T

TARGET DEVELOPMENT (BASIC)

OPR
J2T

Reviewer
J2

MIDB

OPR
J2T w/J22

Observer
J3 JFE

TRFI

OPR
J21

Reviewer
JCM Cell

Observer
Submitting Organization

TRFI

TARGET DEVELOPMENT (Intermediate)

OPR
J2T

Reviewer
J2

INTERNAL TGT REVIEW

OPR
J2T/J3 JFE

Reviewer
TCWG

CTL OPR J3 JFE Reviewer J3 Observer JPG, OPT

TARGET DEVELOPMENT (Advanced)

OPR
J3 JFE

Reviewer
J3

TARGET VETTING

OPR
J2T

Reviewer
IC and Supported JFC

JTECB

TARGET VALIDATION

TARGET VETTING

OPR
Supported JFC JTWG /JTCB

Reviewer
IC, as required

JTCB

VALIDATION

OPR
J-3, Supported JFC

Reviewer
CJTF

Observer
CDRUSCYBERCOM

RTL

JTL

NSL

TNL

OPR
J-3, Supported JFC

Reviewer
CJTF

Observer
J3 JFE

JIPTL

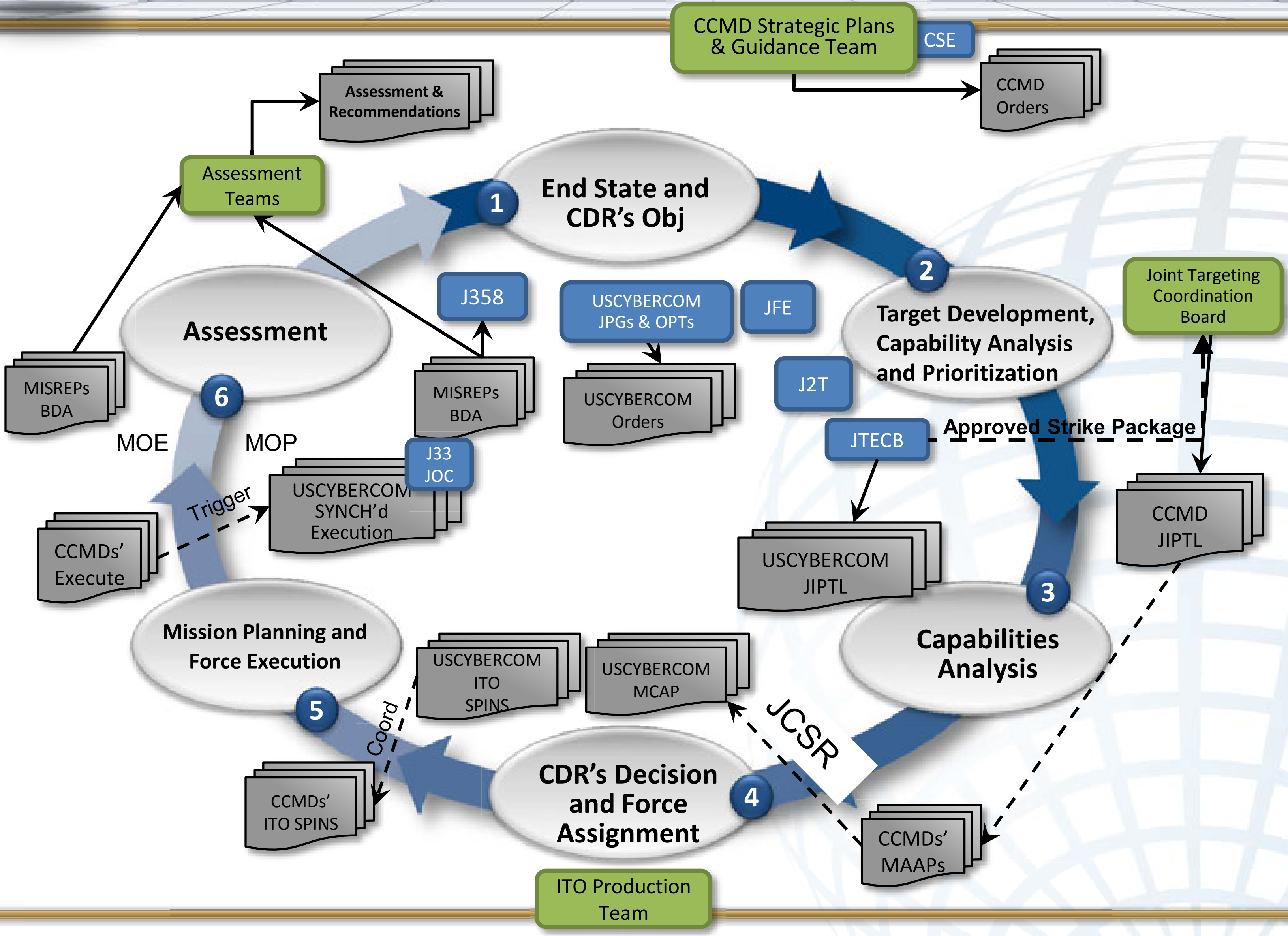
Cyber Fires

MCAP

JCSR

ITO

# Targeting Cycle In Support of a Joint Force Commander



# Cyber Support Package

- Strike package consists of:
  - Required items:
    - Contingency Operations / Tab-E
    - Intel Gain Loss Assessment (National Security Agency lead-Combined Military Planning and Access Strategies (CoMPAS))
    - Political Military Assessment (Defense Intelligence Agency lead)
    - Operational Law Review (USCYBERCOM Staff Judge Advocate (SJA))
    - Collateral Effects Estimation (USCYBERCOM J3F Fires)
    - Blowback Assessment (USCYBERCOM J34 Counter Measures)

- Under exigent circumstances only these items are required:
  - Collateral Effects Estimate (USCYBERCOM Combined J3F Fires)
  - Operational Law Review (USCYBERCOM SJA)

# Joint Cyber Strike Request

- Types of Fires
  - Scheduled
    - Planned targets against which cyber fires or other actions are scheduled for prosecution at a specific time
  - On-Call
    - Planned targets against which cyber fires or other actions are determined using deliberate targeting and are prosecuted based on a predetermined trigger

JCSR vs CERF

JCSR – Sets the timing and tempo to integrate cyber effects/fires with the supported Joint Force Commander's operation

CERF – Ensures desired effects meet the Combatant Commanders objectives

# Cyber Domain Essentials

- Cyberspace is a Contested Domain
- Cyber is Commander’s Business
- DoD Networks are a Warfighting Platform
- Unity of Effort and Unity of Command is Essential for Seamless Operations
  - Cyber Operations Must be Synchronized and De-conflicted Globally and Regionally
- Cyberspace Forces are High Demand/Low Density
- Highly trained people are the centerpiece of cyberspace operations

# Considerations/Thoughts ?