Castles in the Clouds: Do we have the right battlement? (Cyber Situational Awareness)

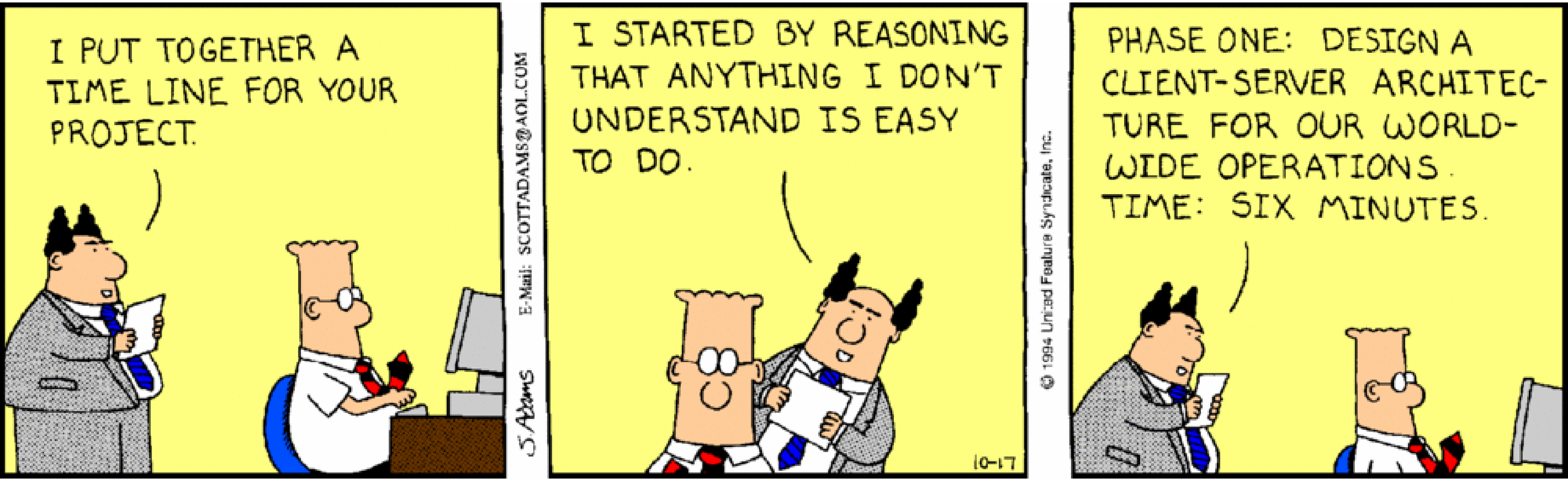
US Army Cyber Command and Second Army

COL Mark Schonberg, ARCYBER G6 (CIO)
11 March 2016

The Nation's Army in Cyberspace

OVERALL CLASSIFICATION:
UNCLASSIFIED

DOD Cyber Security Planning Process

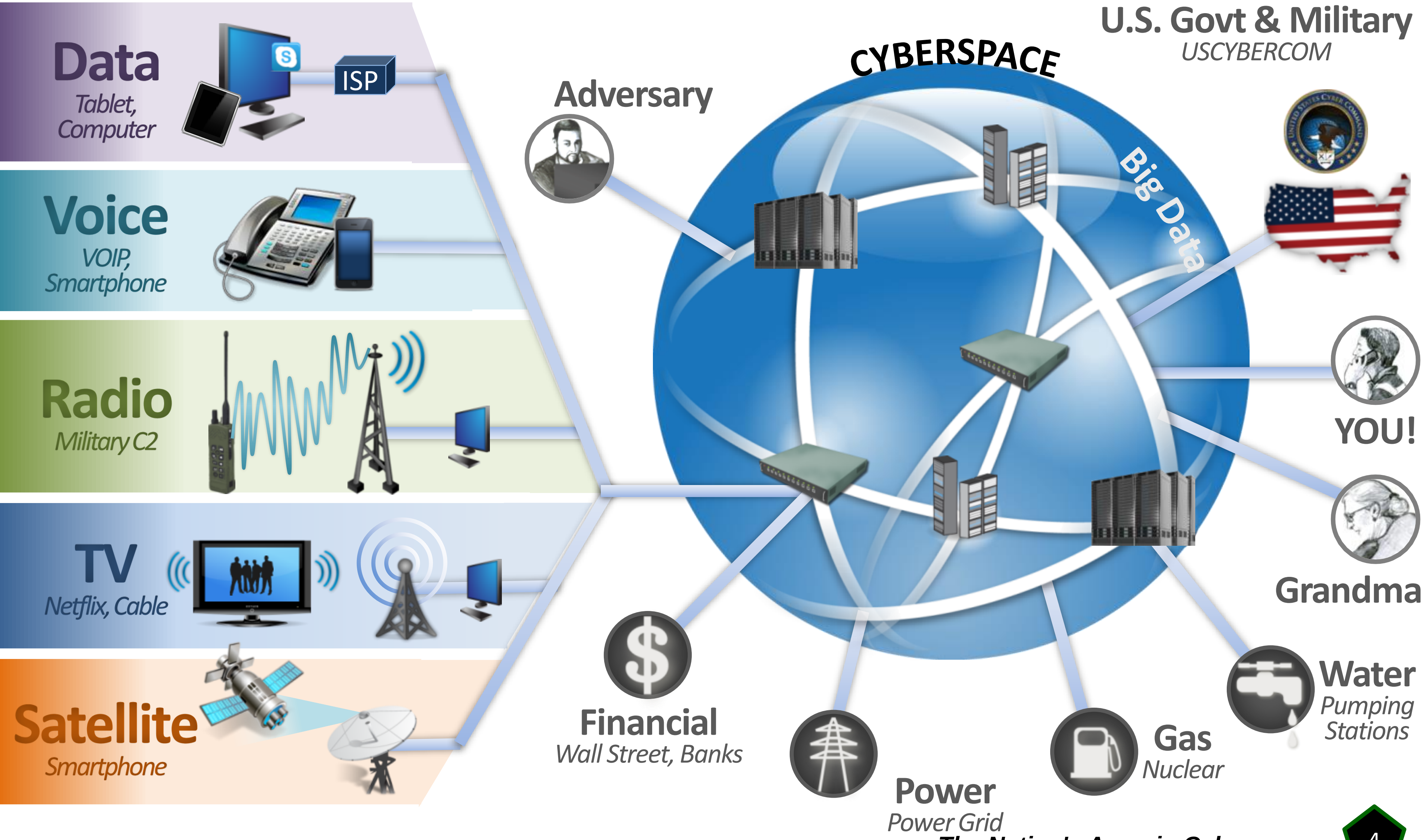

I PUT TOGETHER A TIME LINE FOR YOUR PROJECT.
E-Mail: SCOTTADAMS@AOL.COM
S. Adams
I STARTED BY REASONING THAT ANYTHING I DON'T UNDERSTAND IS EASY TO DO.
10-17
© 1994 United Feature Syndicate, Inc.
PHASE ONE: DESIGN A CLIENT-SERVER ARCHITECTURE FOR OUR WORLD-WIDE OPERATIONS. TIME: SIX MINUTES.

- **This is a Hyper-Complex Environment**

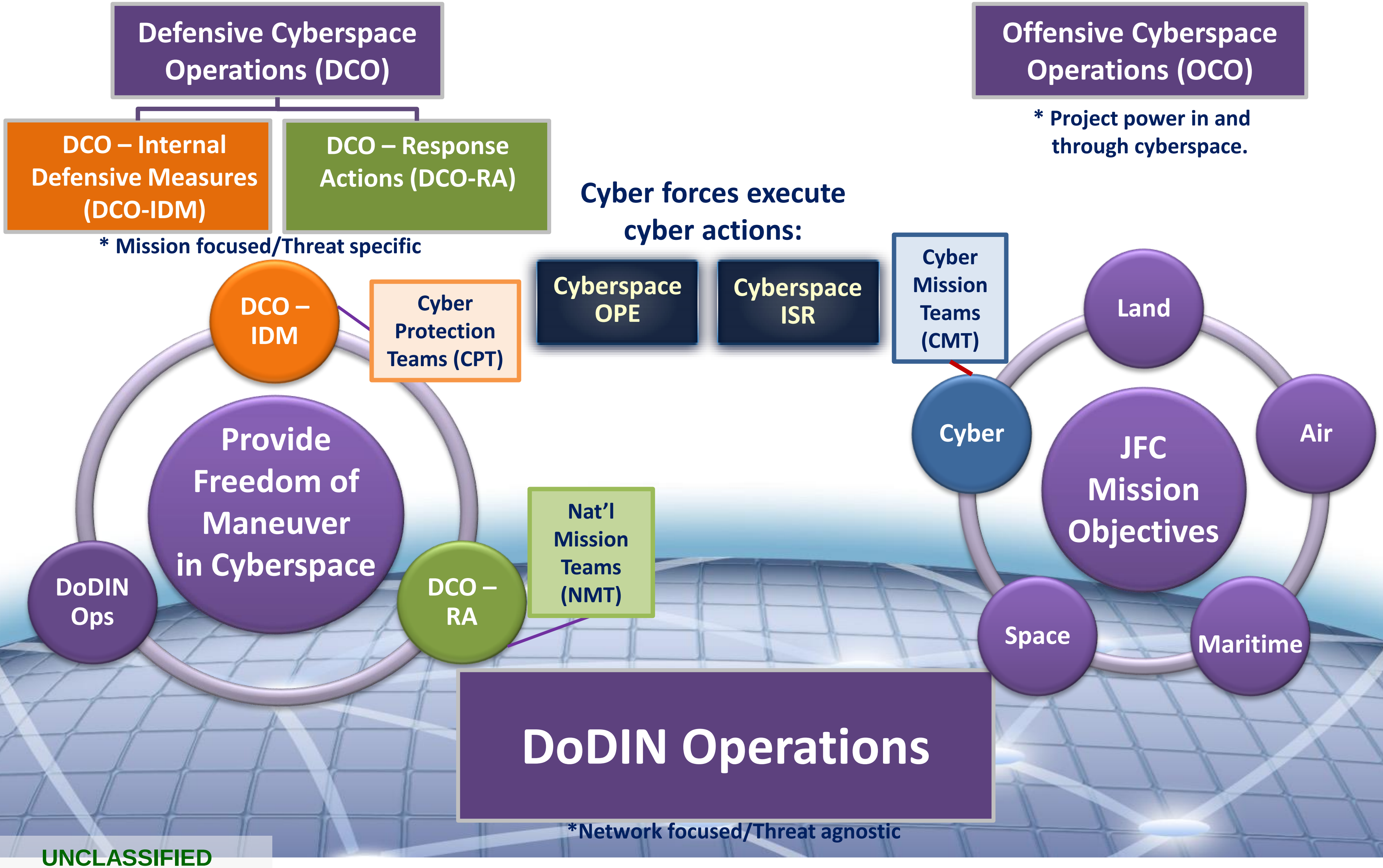
Agenda

- Convergence: A whole lot going on
- Lines of Effort
- Three Keys moving Forward
  - Design: Security Upfront gives you the right battlement
  - Data Management Strategy
  - Work Force Development (Training)
- Take Aways
- Questions?

Convergence



Cyberspace Lines of Effort



Defensive Cyberspace Operations (DCO)

DCO – Internal Defensive Measures (DCO-IDM)

DCO – Response Actions (DCO-RA)

* Mission focused/Threat specific

Offensive Cyberspace Operations (OCO)

* Project power in and through cyberspace.

Cyber forces execute cyber actions:

Cyberspace OPE

Cyberspace ISR

Cyber Mission Teams (CMT)

DCO – IDM

Cyber Protection Teams (CPT)

Provide Freedom of Maneuver in Cyberspace

DoDIN Ops

DCO – RA

Nat'l Mission Teams (NMT)

Land

Cyber

JFC Mission Objectives

Air

Space

Maritime

DoDIN Operations

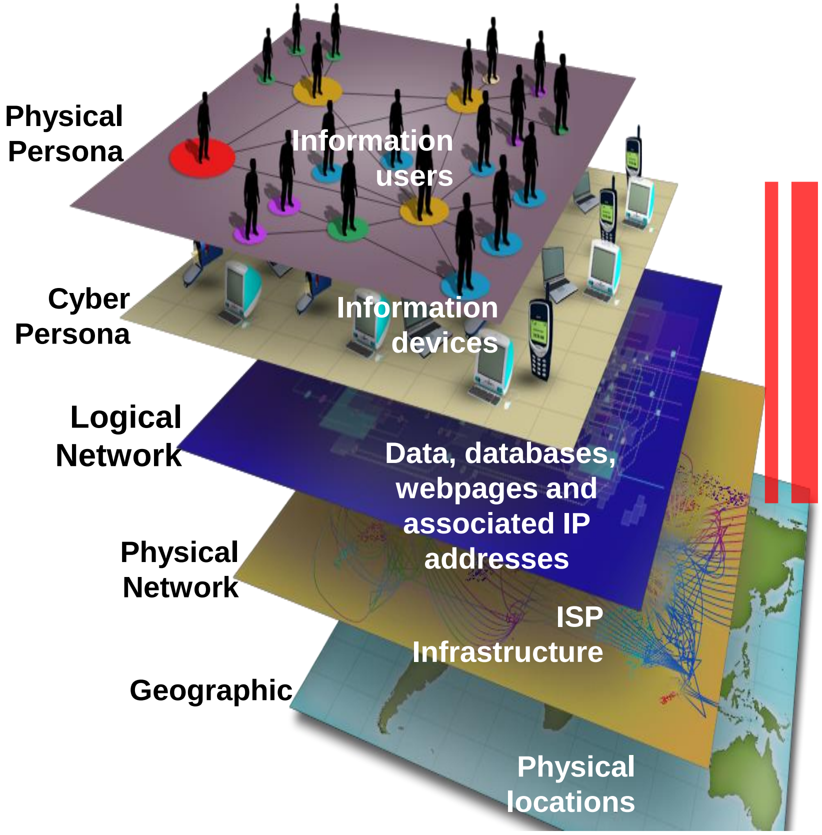
*Network focused/Threat agnostic

Cyberspace Environment

Each layer of Attacker’s Infrastructure and malware tools used can provide opportunities for mitigation.

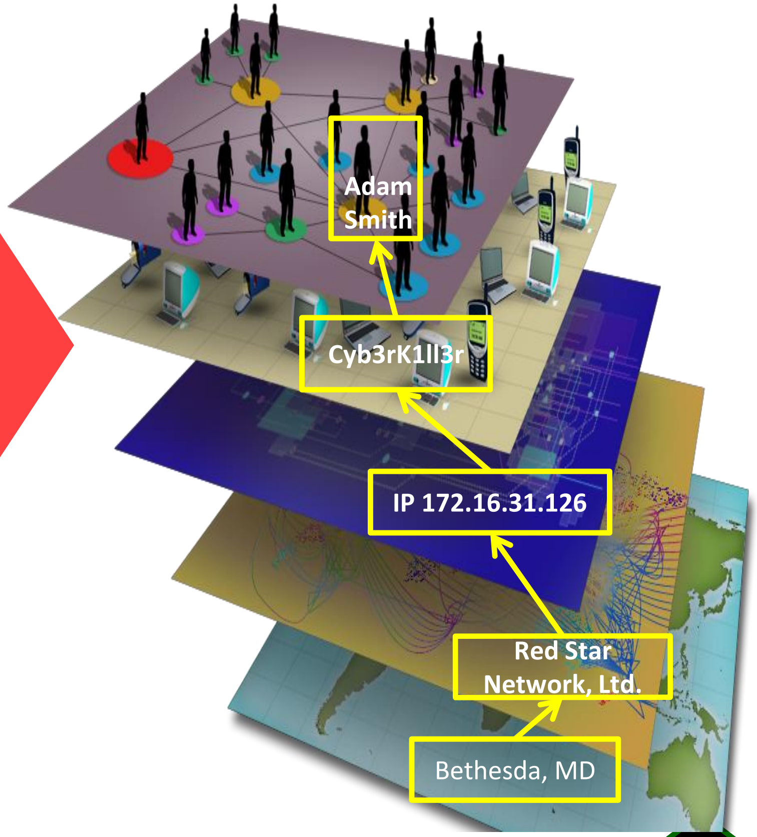
Every layer of the targeted victim’s organization (people and infrastructure) must be defended against attacks.

Adversary Infrastructure



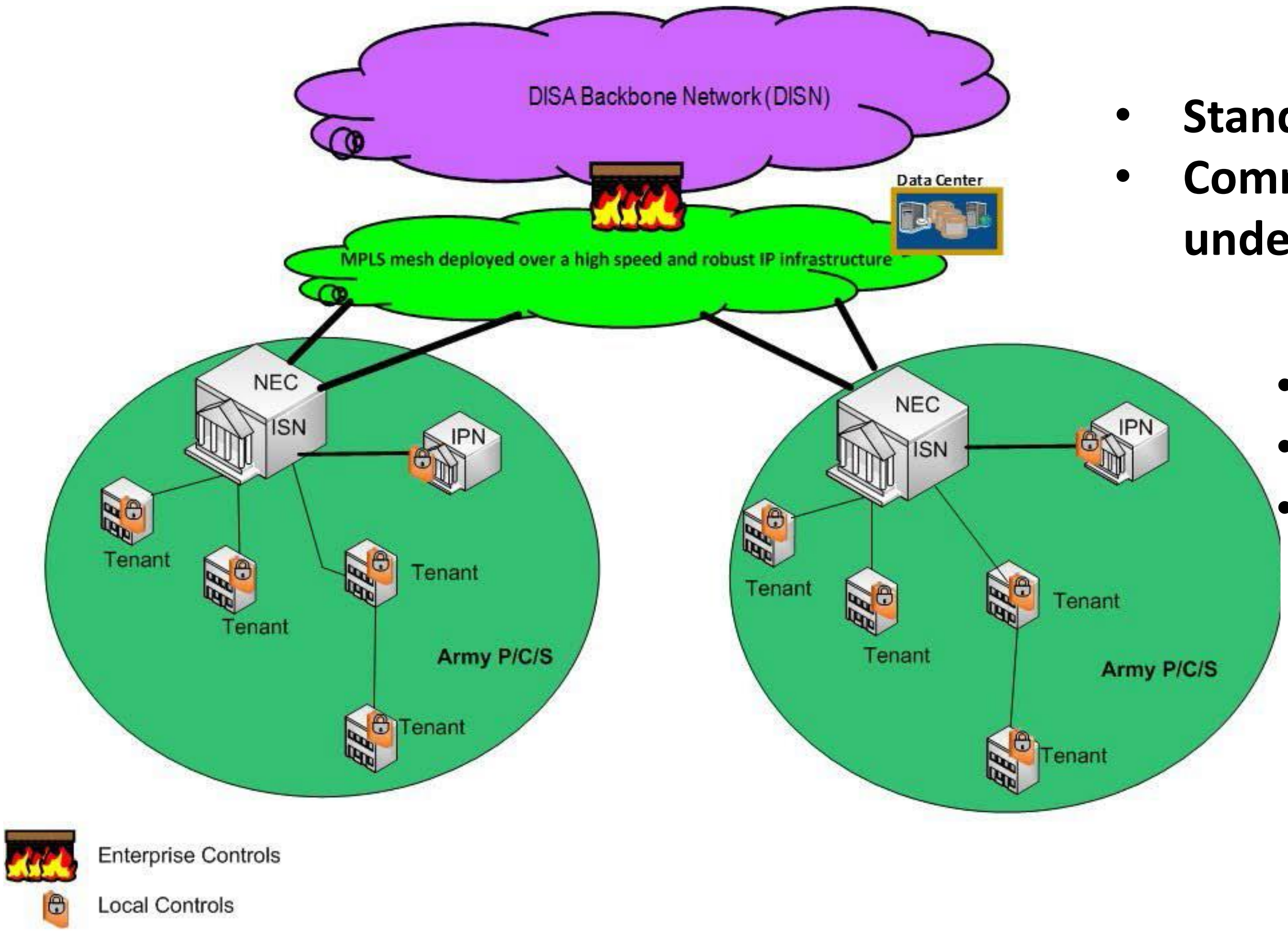
Attackers have the advantage since they need only succeed once. Defenders must succeed every time.

Victim’s Attack Surface



Security Upfront

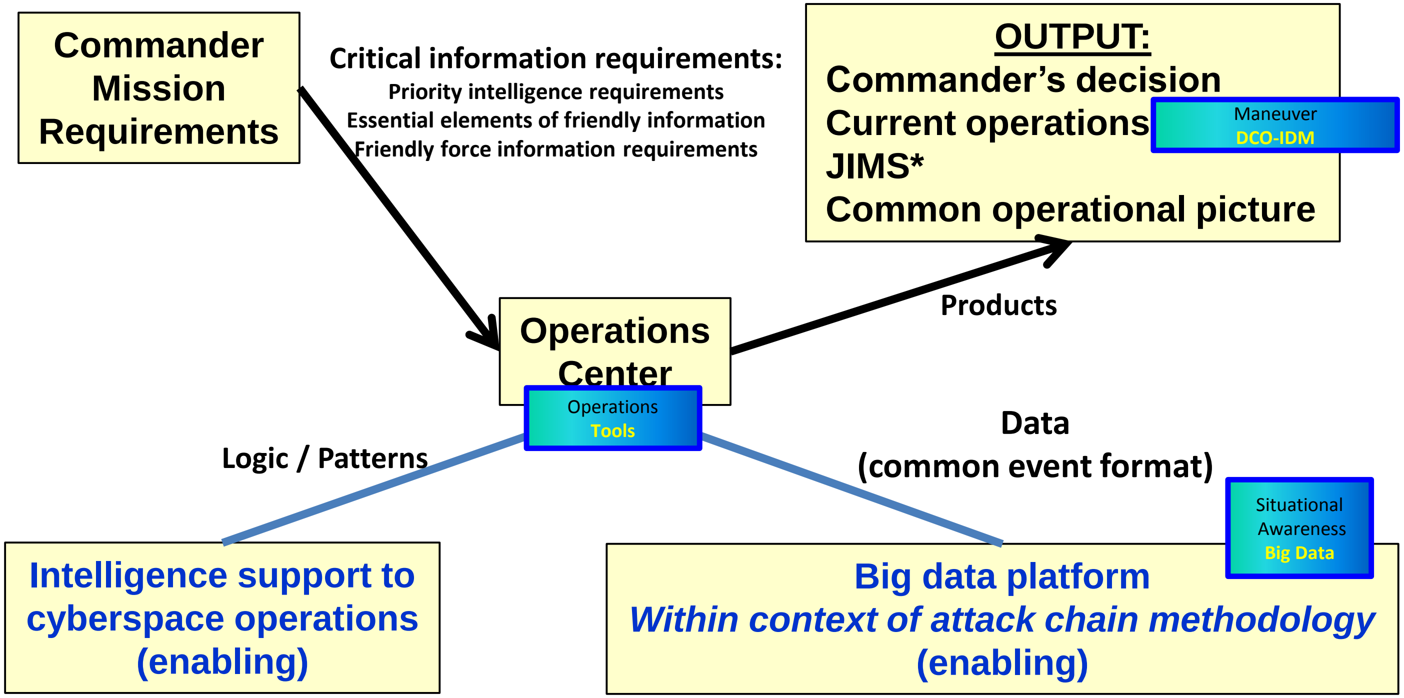
Joint Regional Security Stack (JRSS) Architecture



- Standardization (NIST)
- Common lexicon; shared understanding of definitions

- Globally Directed
- Regionally Aligned
- Locally Responsive

Data Management Concept



Commander Mission Requirements

Critical information requirements:
Priority intelligence requirements
Essential elements of friendly information
Friendly force information requirements

OUTPUT:
Commander’s decision
Current operations
JIMS*
Common operational picture

Maneuver
DCO-IDM

Products

Operations Center

Operations
Tools

Logic / Patterns

Data
(common event format)

Situational Awareness
Big Data

Intelligence support to cyberspace operations (enabling)

Big data platform
Within context of attack chain methodology
(enabling)

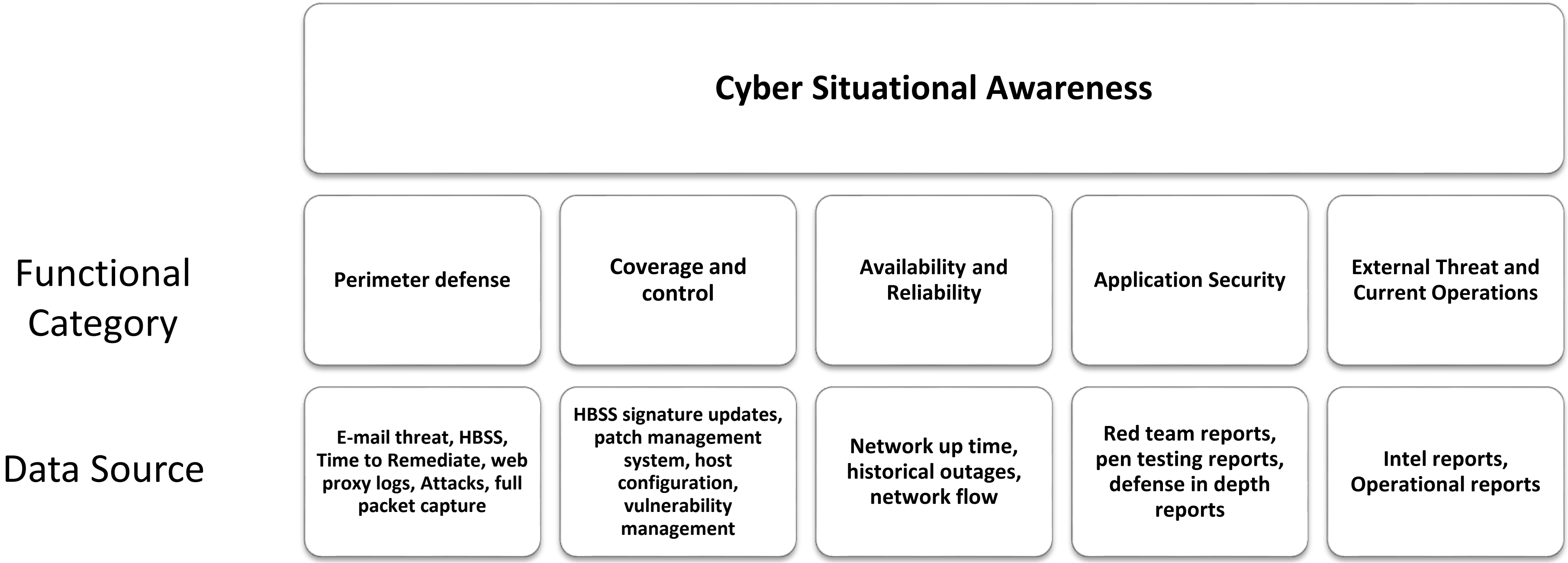
Data management strategy **critical non-materiel artifact,** ***what you collect determines your ability to see yourself***

*Joint Information Management System

Cyber Situational Awareness

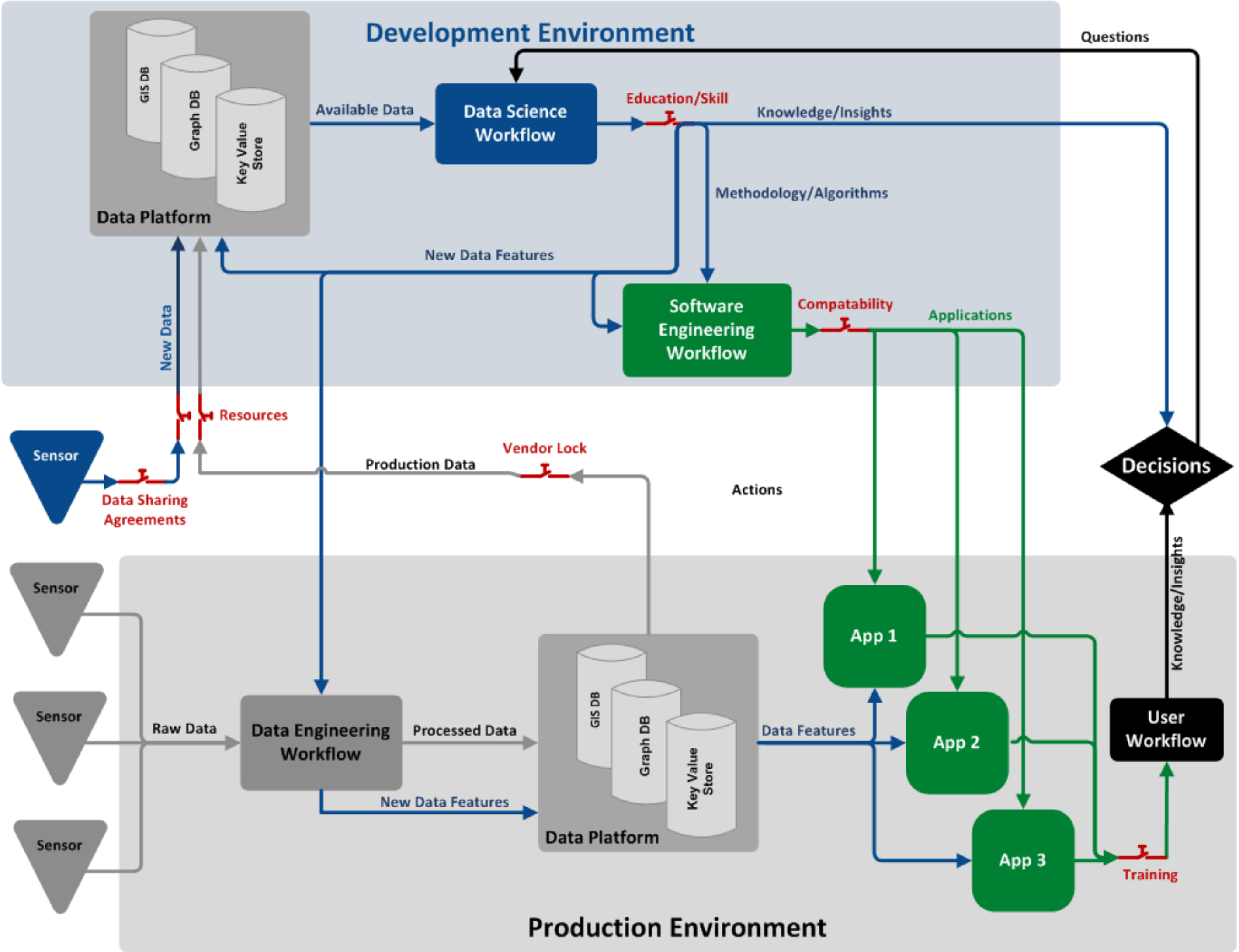
Situational Awareness: Knowledge and understanding of the current situation which promotes timely, relevant and accurate assessment of friendly, enemy and other operations within the battle space in order to facilitate decision making (Army FM 5.0)

Cyber Situational Awareness: The ability to aggregate and visualize specific **network and intelligence data** from key terrain in a manner that provides understanding of perimeter defense, coverage and control, availability/reliability, application security and mission context



	Cyber Situational Awareness				
Functional Category	Perimeter defense	Coverage and control	Availability and Reliability	Application Security	External Threat and Current Operations
Data Source	E-mail threat, HBSS, Time to Remediate, web proxy logs, Attacks, full packet capture	HBSS signature updates, patch management system, host configuration, vulnerability management	Network up time, historical outages, network flow	Red team reports, pen testing reports, defense in depth reports	Intel reports, Operational reports

Big Data Environment



Every data project has four components:

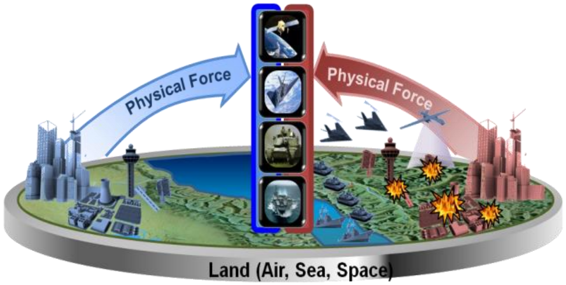
1. Understanding the business need. In our case it is threat detection.
2. Gathering, messaging and preparing the data.
3. Doing the modeling.
4. Operationalizing the outcome.

- **Defined End-States**

Evolving Operational of the Environment (Emergence of Cyberspace Demands Training Evolution)

Past

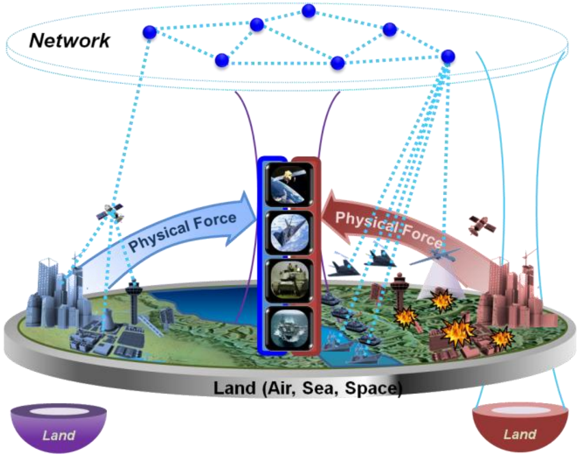
Classical – AirLand Battle



- WW II thru Vietnam

Today

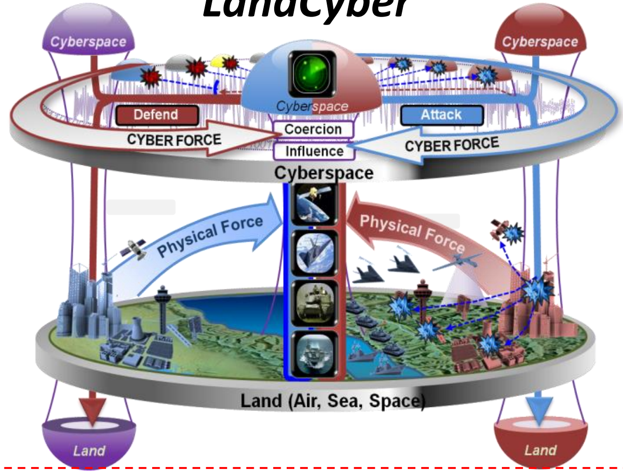
Classical–Network Enabled



- DS/DS thru OEF/OIF
- Network Enabled operations - PED from back in CONUS

Future

LandCyber



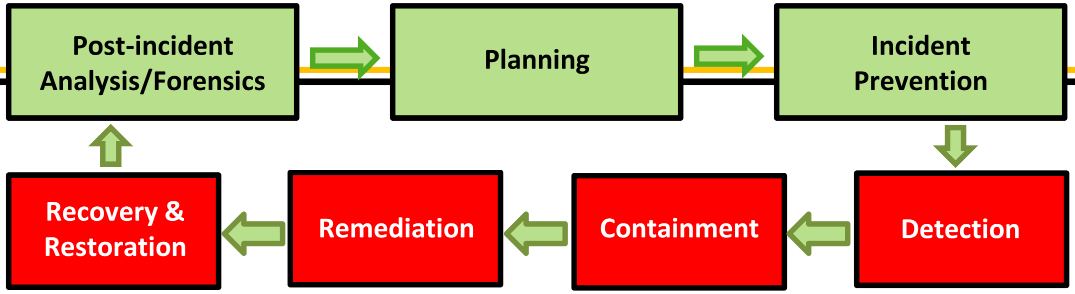
- Network Effects
- Force-on-force in Cyberspace operating in Phase 0
- No going back to grease pencils

Quantum Leap in the Mass, Velocity, and Non-Linear Interaction of Human Groups, their Machines, and their Information Objects

Our Adversaries have leveraged cyberspace to organize a new kind of force that leverages cyberspace as operational terrain and exploits the virtual dimension of human and machine behavior to revolutionize operations.

Incident Response Lifecycle

Best Practice



Post-incident Analysis/Forensics

Planning

Incident Prevention

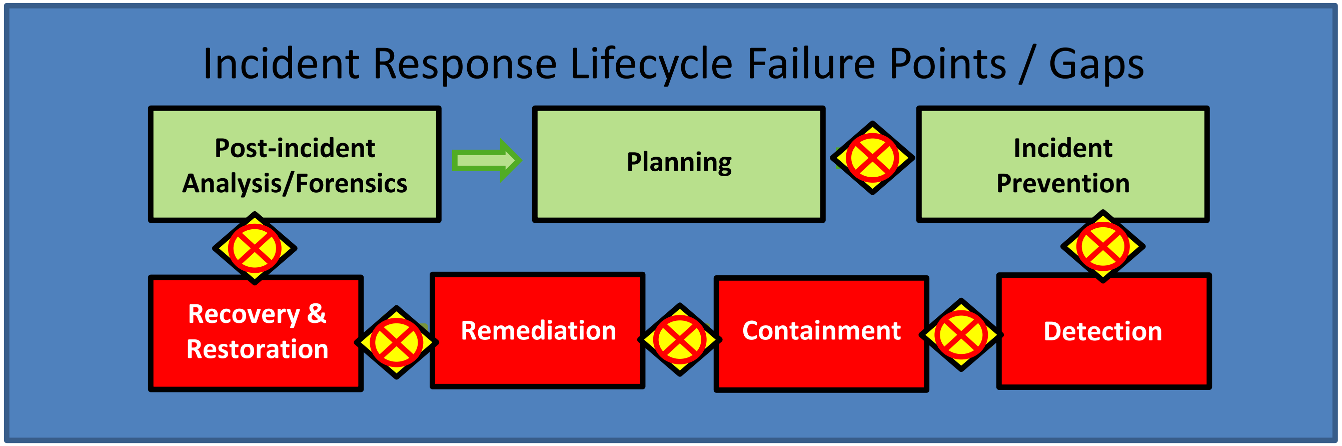
Detection

Containment

Remediation

Recovery & Restoration

Problem



Incident Response Lifecycle Failure Points / Gaps

Post-incident Analysis/Forensics

Planning

Incident Prevention

Detection

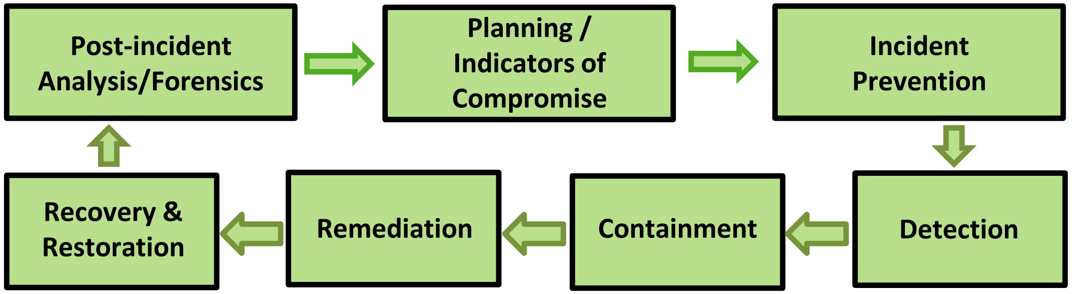
Containment

Remediation

Recovery & Restoration

Solution

Automated Failure Point / Gap **Remediation**



Post-incident Analysis/Forensics

Planning / Indicators of Compromise

Incident Prevention

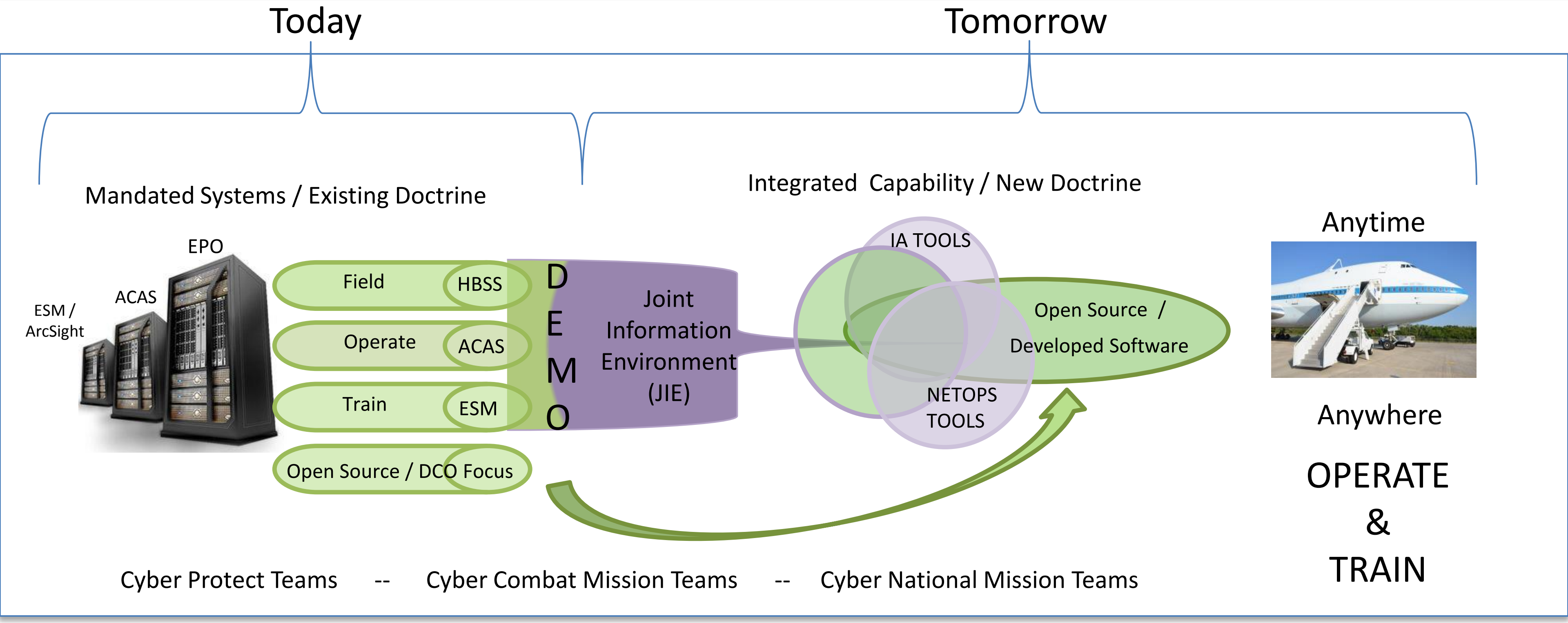
Detection

Containment

Remediation

Recovery & Restoration

Training Environment



Today

Tomorrow

Mandated Systems / Existing Doctrine

EPO

ESM / ArcSight

ACAS

Field — HBSS

Operate — ACAS

Train — ESM

Open Source / DCO Focus

DEMO

Joint Information Environment (JIE)

Integrated Capability / New Doctrine

IA TOOLS

Open Source / Developed Software

NETOPS TOOLS

Anytime

Anywhere

OPERATE & TRAIN

Cyber Protect Teams -- Cyber Combat Mission Teams -- Cyber National Mission Teams

Baseline Platform

Task Order (Requirement)

Integrate, Test, Field and Train =

Integrate in to the Army environment while fully automating manual incident response actions

OT Training Challenges

ICS

SCADA

DCS

PLC

APC

SIS

Turbo Machinery

PIT

- No Common Lexicon
- Cost prohibitive: function specific software
- Lack of Security tools
- Lack of Cyber Ranges for OT and associated systems
- Limited ability to execute operations

Take Aways …

- **Embrace Cyberspace as a contested domain; Design Security Upfront**
- **Understand your network and cyber key terrain; emplace sensors and monitor key reporting tools to create the right Cyber Situational Awareness (SIEM/BDP)**
- **Focus on Common standards; System Integration is key (OT - to - IT)**
- **Train your Cyber Workforce on processes do not get focused on tools; build the high-end engineering bench**
- **Don’t be afraid to take something off of the table; resources are limited**

Questions?