JFHQ-DODIN Update

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

Lt Col Patrick Daniel
JFHQ-DODIN J5
As of: 21 April 2016

Presentation Disclaimer

"The information provided in this briefing is for general information purposes only. It does not constitute a commitment on behalf of the United States Government to provide any of the capabilities, systems or equipment presented and in no way obligates the United States Government to enter into any future agreements with regard to the same. The information presented may not be disseminated without the express consent of the United States Government. This brief may also contain references to Unite States Government future plans and projected system capabilities. Mention of these plans or capabilities in no way guarantees that the U.S. Government will follow these plans or that any of the associated system capabilities will be available or releasable to foreign governments."

Cyberspace Ops Mission Alignment

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

Full Spectrum Cyberspace Operations

Core Mission Areas

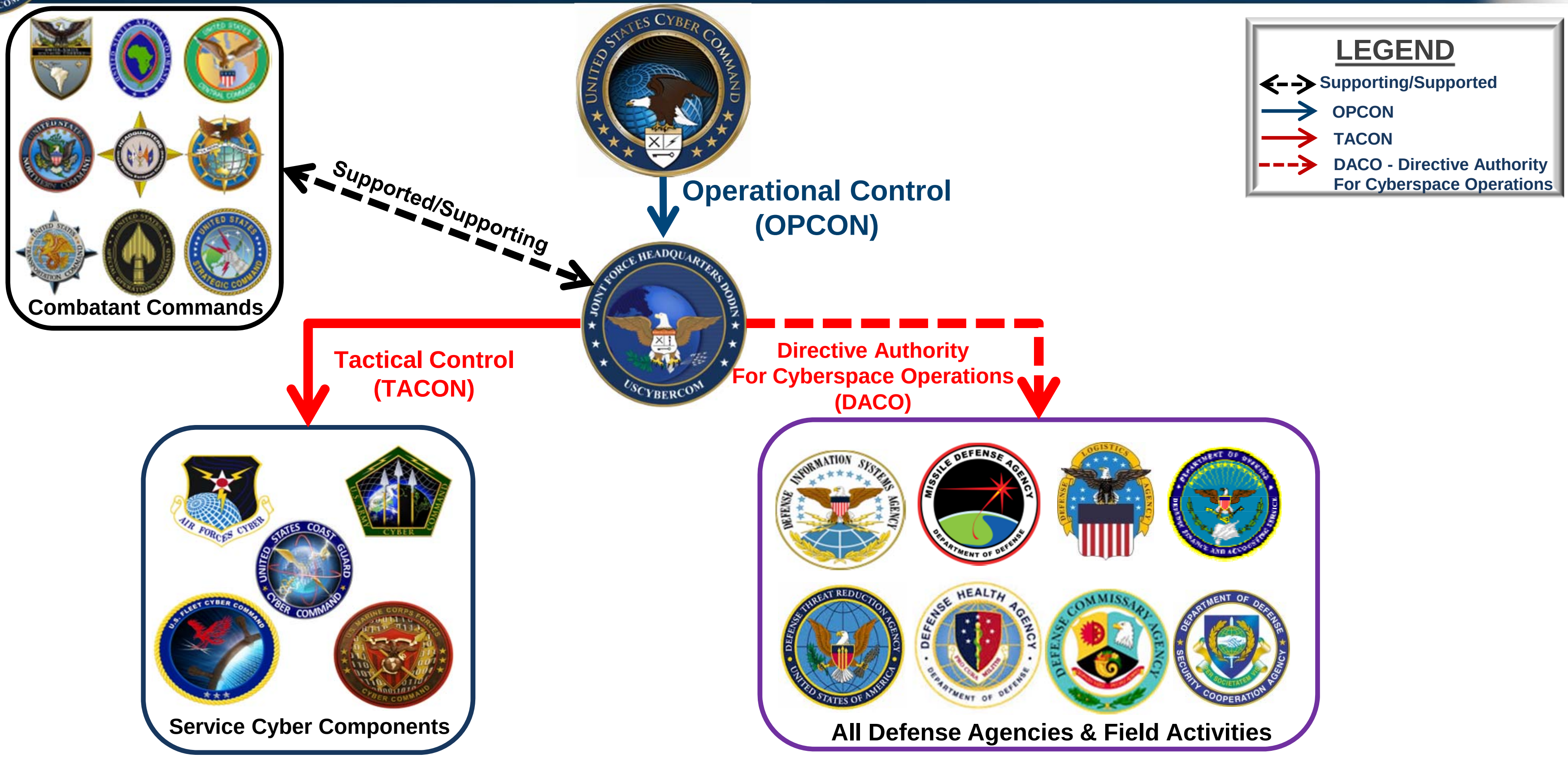
- Defend the Nation Against Strategic Cyber Attack
- Secure, Operate and Defend the DoD Information Networks (DODIN)
- Combatant Command Support

JFHQ-Cyber

Mission Statement

JFHQ-DODIN exercises command and control of DODIN operations & DCO-IDM globally in order to synchronize the protection of DOD component capabilities to enable power projection and freedom of action across all warfighting domains.

Secure, Operate & Defend the DODIN Command and Control Structure



Operational Control (OPCON)

Supported/Supporting

Combatant Commands

Tactical Control (TACON)

Directive Authority For Cyberspace Operations (DACO)

Service Cyber Components

All Defense Agencies & Field Activities

LEGEND

- <- -> Supporting/Supported
- → OPCON
- → TACON
- - - -> DACO - Directive Authority For Cyberspace Operations

JFHQ-DODIN – The Year in Review

- JFHQ-DODIN established 15 Jan 15
- Accomplishments
  - Led 17 named operations for DODIN defense
  - Produced 517 DODIN intelligence products
  - Assumed Operational Control (OPCON) of DODIN Cyber Protection Teams (CPTs)
  - Assumed control of Command Cyber Readiness Inspection (CCRI) process
  - Participated in 9 exercises and 2 war games
  - Began development of first-ever deliberate plan for DODIN defense
  - Established JTF in support of Combatant Command mission

DODIN Defined

Platform IT

Cloud Services

Agency Networks

CDCs

"The Department of Defense information network (DODIN) are a globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers and support personnel. The DODIN includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems." –JP 3-12

DODIN

Service Networks

Educational Institutions

Industrial Control Systems

Coalition & Multi-national Networks

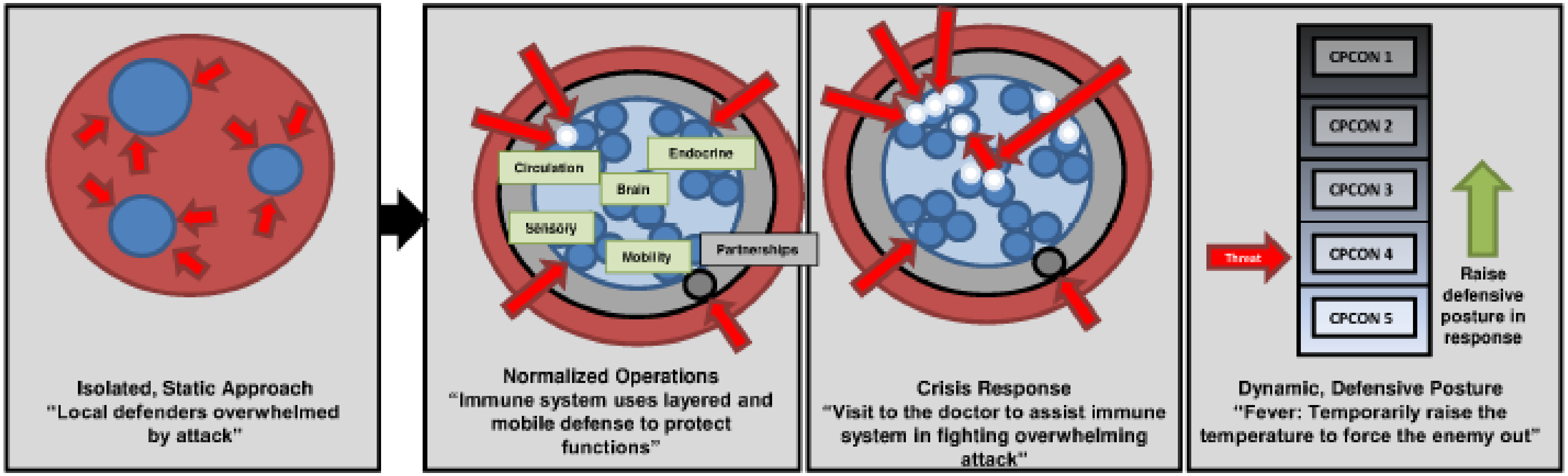
Tactical Communications Systems

Leased Telecom Services

Mobile Devices

Paradigm Shift within the DoD

Building an "immune system" for the DODIN



Isolated, Static Approach
"Local defenders overwhelmed by attack"

Normalized Operations
"Immune system uses layered and mobile defense to protect functions"

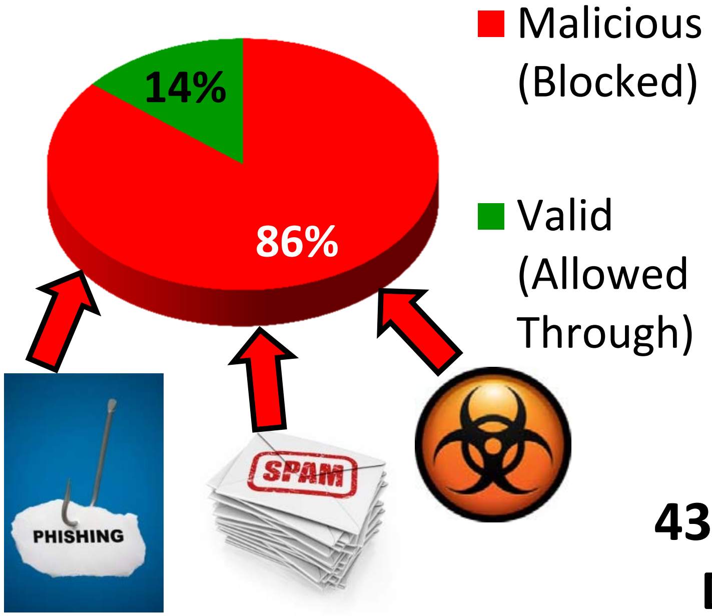
Crisis Response
"Visit to the doctor to assist immune system in fighting overwhelming attack"

Dynamic, Defensive Posture
"Fever: Temporarily raise the temperature to force the enemy out"

JFHQ-DODIN provides unity of command to enable this new paradigm

A Day in the life of the DODIN

8.2M E-Mails Received



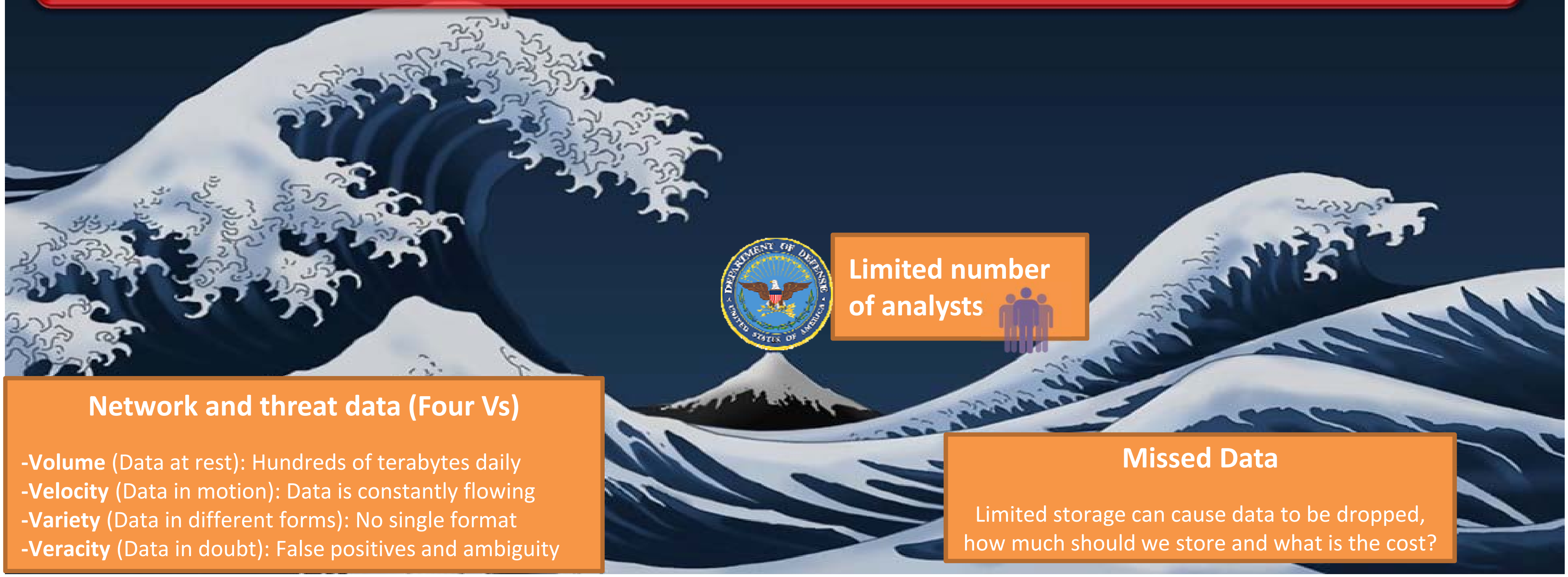
30 Suspicious Events
that require further analysis

43K Attempted Intrusions
Detected and Blocked

Each Year: 3B E-Mails Received, 16M Attempted Intrusions, 11K Events to be analyzed

The Big Data Tsunami

- We must transform data into information, then further refine that information into intelligence
- Better automation is critical



Limited number of analysts

Network and threat data (Four Vs)

-Volume (Data at rest): Hundreds of terabytes daily
-Velocity (Data in motion): Data is constantly flowing
-Variety (Data in different forms): No single format
-Veracity (Data in doubt): False positives and ambiguity

Missed Data

Limited storage can cause data to be dropped, how much should we store and what is the cost?

Takeaways

- JFHQ-DODIN leverages new command relationships to synchronize DODIN defense
- Technology-agnostic C2 framework helps us be flexible and responsive
- We must increase use of automation to solve the “big data tsunami” problem
  - How can industry help?
- Focus on “combined arms” approach to DODIN defense

Questions?