

Cyber Situational Awareness: The NetOps Perspective

Operational Characteristics of the Enterprise Infrastructure – NetOps Implications

Always On

NetOps is a non-stop, all-day/everyday, real-time mission.

End-to-End Service

All tiers; all layers; all levels; from providers to consumers and back -- all enabling resources (network, spectrum, SATCOM, computing, applications, data, etc.) must be managed (monitored and controlled, operated and defended) as a reliable, efficient, and secure service-oriented fabric.

Full Spectrum Ops

NetOps must ensure resiliency in the face of adversaries, systemic flaws, human error, entropy, and natural events.

Contested Battlespace

NetOps must accommodate the resource diversity, user and mission customization, and rapid pace of change intrinsic to Cyberspace capabilities and essential for success in Cyberspace operations.

Interoperable

NetOps must provide assured availability, delivery, and protection of information and supporting infrastructure anywhere and everywhere required for DoD missions.

Global Mission

Topics to be Addressed

- **What is Cyber Situational Awareness?**
- **Who (Persons and NPEs) Consumes Cyber SA?**
- **What is Cyber SA Used For?**
- **Who (Persons and NPEs) Provides Cyber SA?**
- **How is Cyber SA Constructed?**
- **How is Cyber SA Delivered?**
- **How is Cyber SA Consumed?**
- **What Cyber SA Capabilities is the DISA NetOps PMO Delivering?**
- **When Will Those Capabilities be Delivered?**

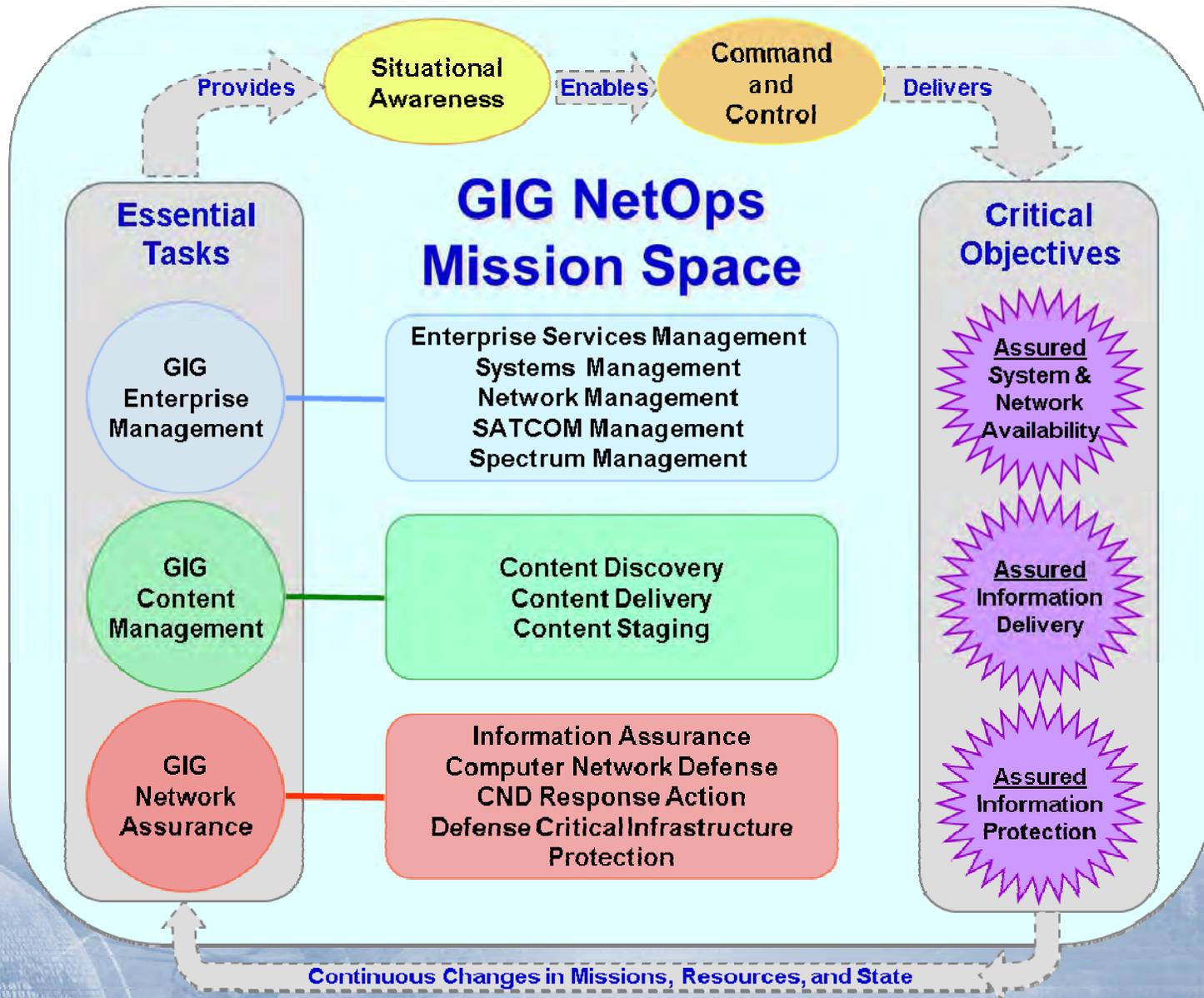
Bottom Line Up Front

- **Cyber Situational Awareness is a complex cyber capability**
- **Not a “one size fits all” problem or solution**
 - Must satisfy a wide spectrum of needs ... tactical, operational, strategic
- **Fundamental NetOps effectiveness across the complete service assurance mission is a prerequisite to trustable Cyber Situational Awareness**
 - Must balance with IT efficiency goals
- **Much more than monitoring, reporting, visualization**
- ***We can get there!***
 - With the right approach, the necessary resources, and sufficient time
 - Progress can be made in substantial increments
 - Scheduling based on consumer mission priorities, modulo technical and resource dependencies, can yield earlier and regular increments

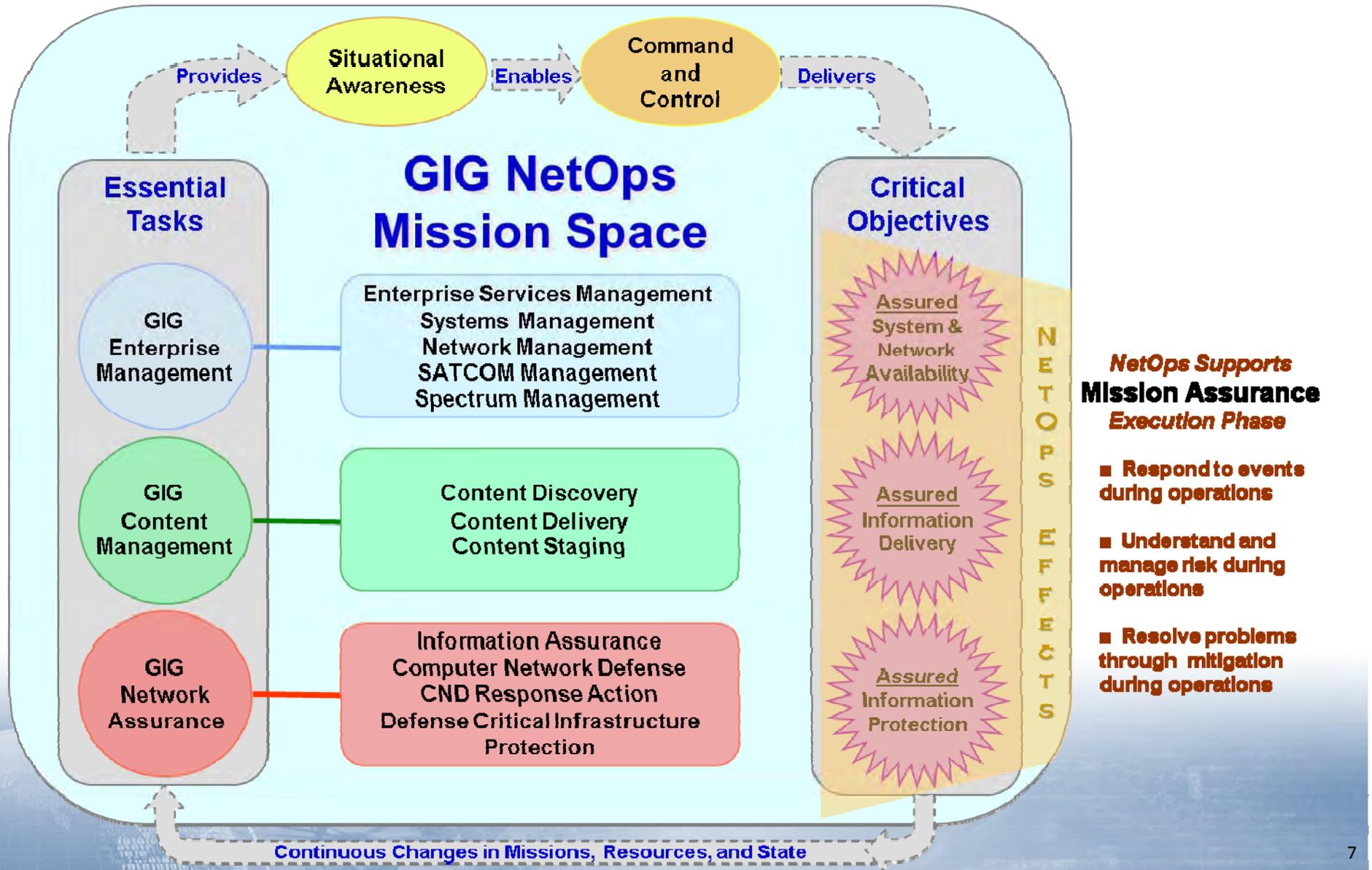
Premise and Foundations

- **Session premise: The “Cyber” in “Cyber Situational Awareness” is intentional ... specifically, it relates to the DoD concepts of “Cyberspace” and “Cyberspace Operations”, extending beyond the GIG alone.**
- **Cyberspace — A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (CJCS CM-0363-08)**
- **Cyberspace Operations — The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid. (JP 3-0)**
- **The Joint CONOPS for GIG NetOps says that “the primary purpose of [situational awareness] is to improve the quality and timeliness of collaborative decision-making regarding the employment, protection and defense of the GIG” and that “full situational awareness of the GIG [is produced] through common processes, standards and instrumentation, enabling near real time manipulation of any asset in order to optimize net-centric services.”**

The Role of Situational Awareness in the NetOps Mission



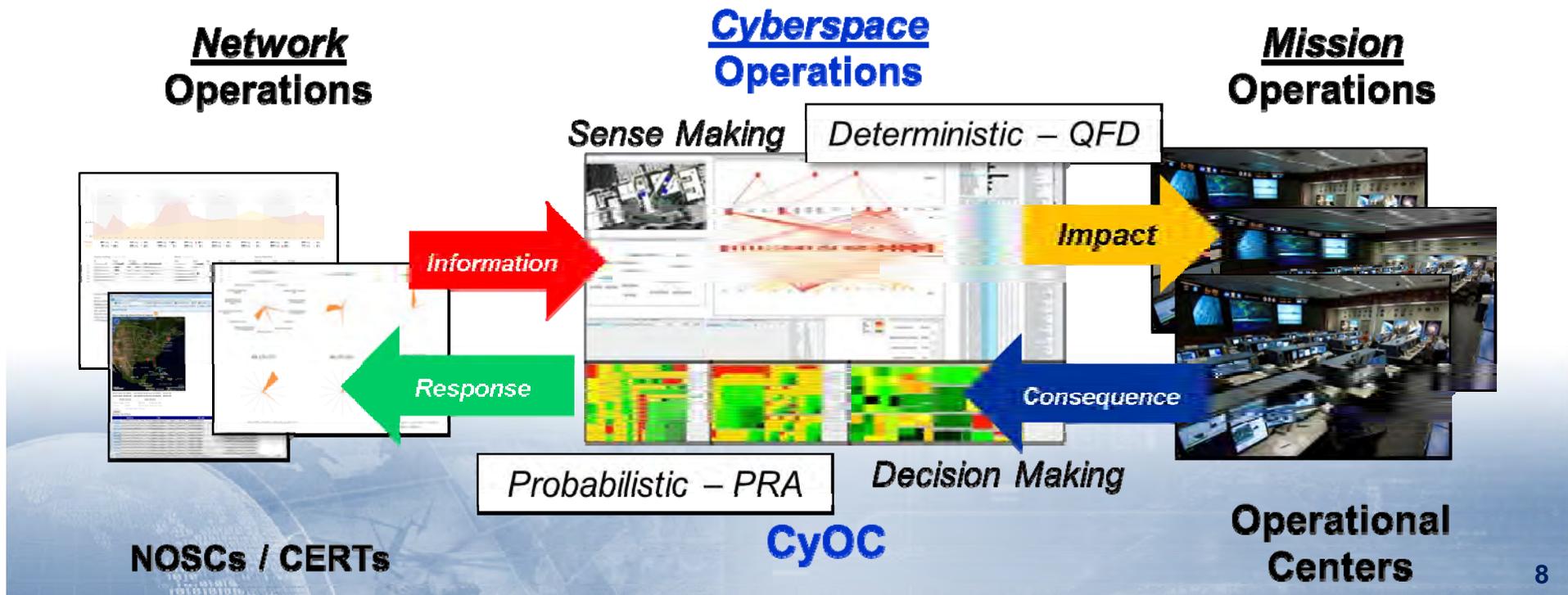
The NetOps SA Contribution to Overall Mission Assurance



The Needs/Solutions Spectrum for Cyber Situational Awareness

- Spectrum of challenges and needs for Cyber Situational Awareness
- Not all challenges or needs shared by all consumers
 - *One-size-fits-all solutions will not work!*
- Solution spectrum ranges from poles of Quantitative/Tactical on the left to Qualitative/Strategic on the right
- Nature of the mission and potential mission impact factor into where specific need sets appear on the spectrum

Notional

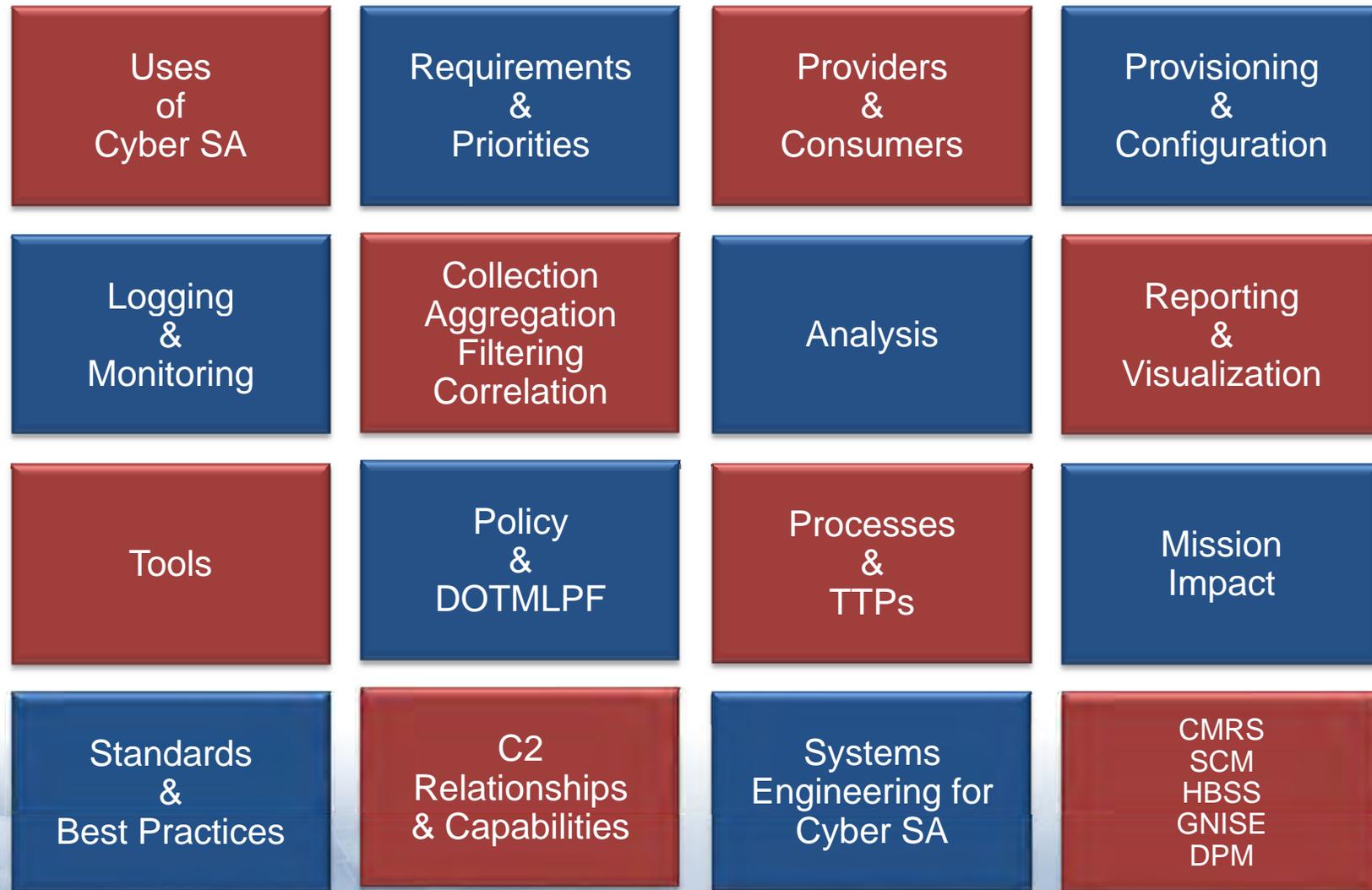


From Simple Views to Operational Reality ... Not a Simple Journey

- **WT¹: Why is automated reporting important?**
 - **STINE: If you can get the different tools and technologies operating in our environment to share data and then you can aggregate that data, you then have a larger set of information to correlate and make more informed decisions. A lot of our work is on the technical specifications that will let those tools communicate and allow greater analysis to take place.**
- **Yes, but ... that's a big "if ... and":**
 - **Must accomplish integration and interoperation across multiple tools and technologies, existing and future; and**
 - **Must share (expose, mediate, transport) and aggregate data; and**
 - **Must be able to perform correlation and other analytics across a "larger set of information" (storage, retention, staging ... on "Big Data"); and**
 - **Must present that processed information in a form suitable for decision-making (C2) based on situational awareness.**

1. "Inside NIST's cybersecurity strategy", <http://washingtontechnology.com/Articles/2012/03/12/TECH-TRENDS-Cyber.aspx>, 26-Mar-2012. Interview with Kevin Stine, manager of security outreach and integration, NIST.

Cyber Situational Awareness Ecosystem of Capabilities and Dependencies



Cannot solve with tools alone

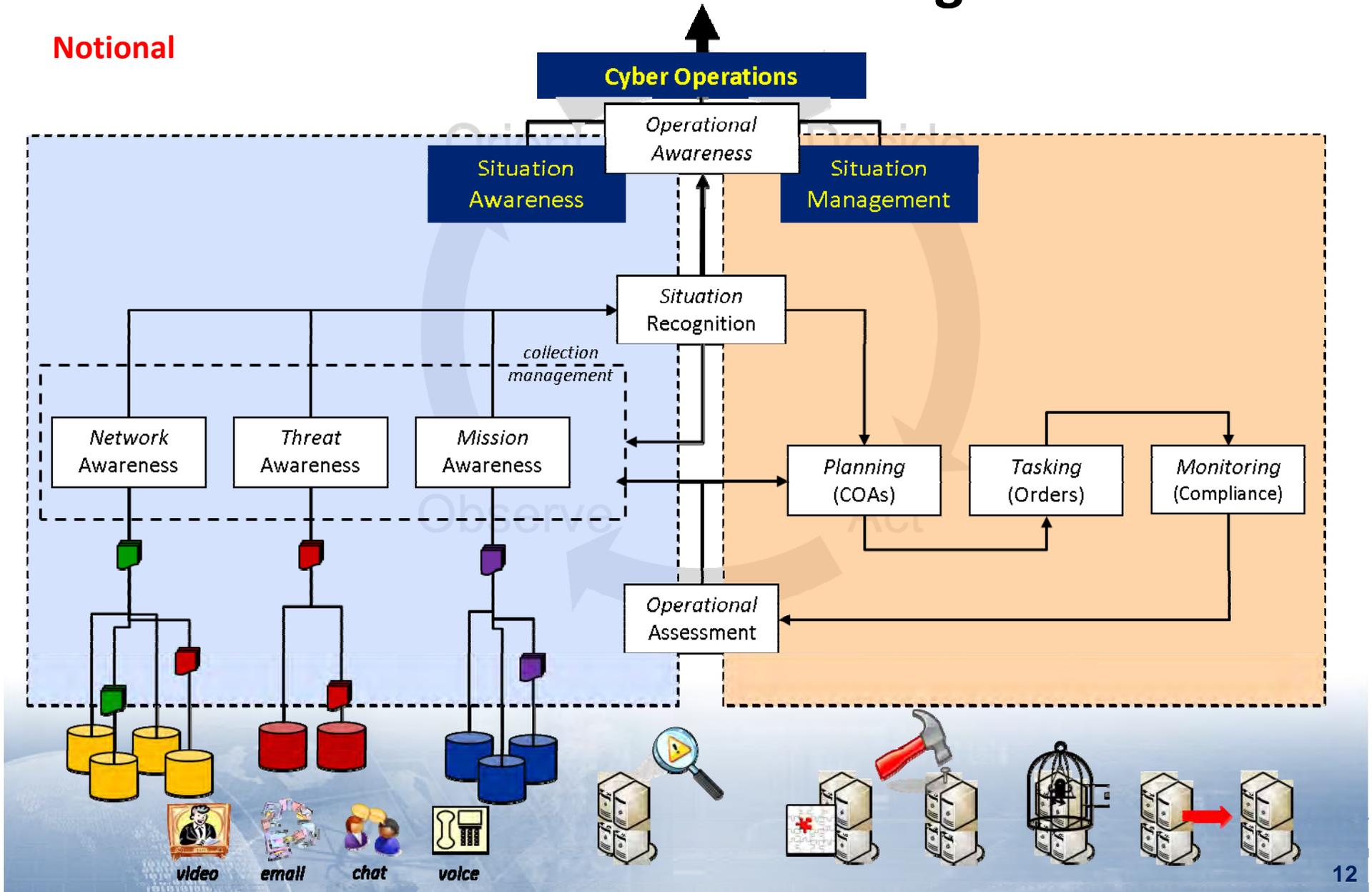
NRWG Cyber SA Groups

Reflects range of concerns noted on "Jeopardy" board

<p>Group 1</p>	<p>Provide visibility across the GIG current activities for shared awareness through both full public screen and personal views of cyber aspects within an operational environment to support leadership visibility and individual analysis specific to the role and span of responsibility of the cyber warrior at all tiers and all classification levels. This group provides the basic mission driven SA requirements.</p>
<p>Group 2</p>	<p>Provide assessment, analysis, and tracking support. This group provides the analysis and tracking SA requirements. These will support requirements in group 1 and provide analysis and tracking capabilities.</p>
<p>Group 3</p>	<p>Provide system functionality and presentation aspects, at all classification levels and all tiers. SA system interaction and presentation aspects that a capability must provide for integrated SA .</p>
<p>Group 4</p>	<p>Provide information sharing and collaboration horizontally and vertically between all tiers and CC/S/A enclaves and collected by various individual sources, provided at the appropriate classification level and the compilation of data at each higher level. Supports collaboration and sharing capabilities throughout the workflow.</p>
<p>Group 5</p>	<p>Provide mission support information/data. The data that must be available and interfaced (in as close to real-time as possible) to provide the SA basic requirements and analysis and tracking.</p>
<p>Group 6</p>	<p>Solution development guidelines, considerations, and embedded capabilities. Basic development requirements for an integrated SA capability.</p>
<p>Group 7</p>	<p>Provide net-centric, service-oriented, cross-domain information sharing solution(s) with guaranteed quality of service (QoS) for authorized users anywhere on the GIG with adjustable settings and system capabilities. Basic system and service capabilities and performance that must be provided for shared SA.</p>

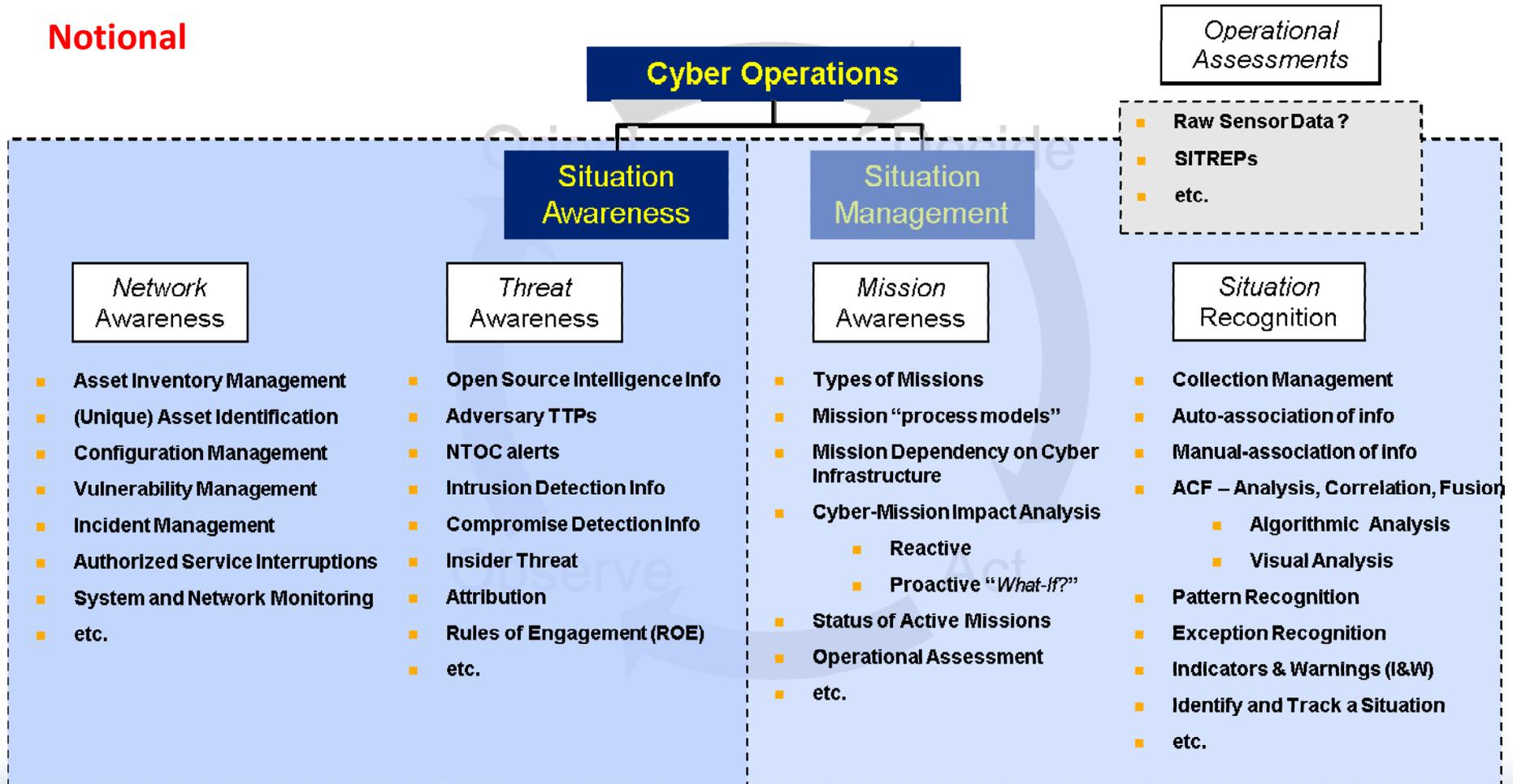
The Interaction of Situational Awareness and Situation Management

Notional



Functional Components of Cyber Operations for Cyber Situational Awareness

Notional



Criticality of NetOps Service Assurance for Trustable Cyber Situational Awareness

Assuring Effective Missions

Assess and control the cyber situation in **mission context**

Agile Operations

Dynamically reshape cyber systems as conditions/goals change, to escape harm



Source: Cyber S&T Priority Steering Council Research Roadmap (as of 8-Nov-2011): Four Major 10 Year Objectives

Resilient Infrastructure

Withstand cyber attacks, and sustain or recover critical functions

Trust

Establish known degree of assurance that devices, networks, and cyber-dependent functions perform as expected, despite attack or error

NetOps

The mission model is currently a missing link

NetOps

NetOps

Logically, a bottom-up process – Trust is the foundation ... service assurance is the trust objective for NetOps

Recap: The BLUF Reviewed

- **Cyber Situational Awareness is a complex cyber capability**
- **Not a “one size fits all” problem or solution**
 - Must satisfy a wide spectrum of needs ... tactical, operational, strategic
- **Fundamental NetOps effectiveness across the complete service assurance mission is a prerequisite to trustable Cyber Situational Awareness**
 - Must balance with IT efficiency goals
- **Much more than monitoring, reporting, visualization**
- ***We can get there!***
 - With the right approach, the necessary resources, and sufficient time
 - Progress can be made in substantial increments
 - Scheduling based on consumer mission priorities, modulo technical and resource dependencies, can yield earlier and regular increments

Questions?

