

# An Analytical Model For Characterizing Operations Centers

---

March 20 2012  
The Johns Hopkins University Applied Physics Laboratory (JHU/APL)

Contract HSSA01-09-C-0403

Version 2

## Table of Contents

<b>1</b>	<b>Introduction.....</b>	<b>3</b>
1.1	Purpose.....	4
1.2	Approach.....	4
1.3	Document Organization.....	7
<b>2</b>	<b>Operations Center Model Overview.....</b>	<b>8</b>
2.1	Scope.....	9
2.2	Activities.....	11
2.3	Organizational Dynamics.....	16
2.4	Facilities.....	18
2.5	Process Management.....	20
2.6	External Interactions.....	22
2.7	Environment.....	24
<b>3</b>	<b>Application of the Model.....</b>	<b>28</b>
3.1	Data Collection Questionnaire.....	29
3.2	Visual Representations of Collected Data and Comparative Analysis.....	30
3.3	Comparative Analysis Summary.....	47
<b>4</b>	<b>Conclusion.....</b>	<b>48</b>
<b>A</b>	<b>APPENDIX – Factor Details.....</b>	<b>49</b>
A.1	Scope Details.....	49
A.2	Activities Details.....	52
A.3	Organizational Dynamics Details.....	59
A.4	Facilities Details.....	61
A.5	Process Management Details.....	64
A.6	External Interactions Details.....	66
A.7	Environment Details.....	67
<b>B</b>	<b>APPENDIX B: Questionnaire Used for online and paper-based Data Collection.....</b>	<b>70</b>
<b>C</b>	<b>APPENDIX C: Changes to the Model.....</b>	<b>80</b>

## 1 Introduction

Emergency and routine operations performed by local, regional, national and international organizations in public and private sectors provide and ensure protection, search and rescue, safety and security. Some common examples include ensuring our roadways are passable during a major snowstorm, monitoring the safety and security of a casino, and detecting and responding to the next computer network attack by an organized crime ring. These organizations, while performing a variety of distinct functions, also have many commonalities that provide a basis for collaboration, including sharing information and tradecraft.

The need for a comparative model was identified and developed during review and analysis of operations center site visits, community events, interviews, and a document review conducted during 2009 and 2010. During the course of the data collection activities, the team recognized that a carefully thought-out and developed operations center model would be useful in organizing discussion points for future visits and for structuring data in a common framework to support focused or comprehensive analyses. A literature review conducted in 2010 and 2011 further clarified the need for a general analytical model for comparing and categorizing operations centers.

The Johns Hopkins University Applied Physics Laboratory (JHU/APL) developed a comparative model for operational organizations for structuring non-sensitive information to characterize an individual or grouping of operations centers. The comparative model enabled an analytic foundation to study and understand how these organizations operate, and how they may further their effectiveness and efficiencies through collaboration and partnership with other related operations centers.

The model was intended to focused on organizations performing defensive cyber operations; however, its design allows it to be generally applicable to operational organizations with non cyber defense focus. The model enables systematic examination of the foundational characteristics of an organization to better understand the current state of the organization, analyze its spectrum of operations, and identify potential crossover concepts between various operational entities in its community. As the model is populated with information from more and more centers, the catalogue of collected data will enable development of standardized views of operations, models for coordinated operations, and methods to test coordinated operational concepts prior to execution.

This paper presents a revised version of the operations center model based on socialization of the model within the community, especially at GFIRST Conference 2011. In addition, this paper replaces hypothetical examples with visuals and analysis from actual data collected from the community. The analysis provided in

this paper draws from data collected from four out of twelve centers during 2011 and 2012.

### 1.1 Purpose

The analytical model for operations center was intended to help operational organizations to:

- Better understand how their operations related or aligned to those of other operations centers;
- Better understand effective and efficient tailoring of information exchanges and products matched with distinct categories of operation center;
- Better understand their processes, practices, and daily routines in the context of similar centers;
- Determine which approaches/practices were applicable to a specific operations center;
- Determine where load sharing would be effective; and
- Determine where collaboration would be beneficial.

The model is used was a means to compare operations centers to each other in order to find opportunities for collaboration or complementary activities. It was designed to be easily populated using readily available information and short discussions, and was not intended to be sufficiently precise or detailed to enable an assessment of quality for a particular center. Instead, it was intended to characterize and categorize operations centers to more efficiently identify applicable tailored products, best practices, areas for collaboration, and other areas for follow-on discussion.

### 1.2 Approach

The approach used for the development of the operations center model consisted of data collection and analysis. Visits to readily accessible operations centers with sufficient diversity of functional role and size laid the foundation for the analysis. These visits included interviews with staff at those centers and covered such varied topics as scope, mission, best practices, size, and areas of specialization. Subsequent analysis of the data collected during the visits established the need for an analytical model to help structure the data to facilitate understanding of commonalities, uniqueness and interdependencies among operations centers.

#### 1.2.1 Data Collection

Data to develop and populate the model was collected from operations centers through interviews, observations, document reviews and questionnaires. The team visited about half-dozen such sites in the defense/intelligence, federal/civilian and commercial sectors.

Subject centers were selected based on accessibility, functional or mission diversity and size. The intent was to have the data collections team quickly obtain a broad overview of cyber defensive operations.

### *Interviews*

Interviews were conducted with center staff in order to understand the organization's mission, interactions, and products. The interviews were performed in addition to, or in lieu of, a formal site visit. Interviews were appropriate in cases where more detailed or specific information is needed about an operations center or formal role within the center.

### *Observations*

Observations of ongoing operations provided a sense of how the organization operated on a daily basis. Each site visit to an operations center included a semi-formal discussion with the center's executive management and technical leadership. After the discussion, a more informal tour of the center permitted observation of the facility and the activities performed. This tour also provided an ideal opportunity for discussions with operational staff. In order to foster candid and insightful conversations, the visits were conducted in an informal atmosphere and were driven by discussion rather than formal elicitation. The visits were designed to be non-intrusive so as to not interrupt operations and were not meant to perform an assessment of the organization for quality or effectiveness, but rather to collect data for the benefit of all operations organizations. Due to the informal and non-intrusive nature of the visits, much of the data and information processed in the model were qualitative in nature, though quantitative data was recorded when available.

Observation at exercises and other community events were also used as a source of information to develop the analytical foundation when available. Exercises highlighted operational use of tools, analytics, functions and inter-organizational interactions and were valuable for understanding "real time" constraints and requirements of a center.

### *Questionnaires*

A questionnaire was developed based on the model, and carefully designed to guide a recipient through quick overview and rapid data entry. The objectives were to (a) be administered through paper or online means; (b) be completed in about 15 minutes; (c) be easily understood by a new staff person at an operations center; and (d) also be appropriate for a seasoned expert at an operations center. The questionnaire was initially administered through paper and online means at GFIRST 2011, and subsequently using online media to invited staff from community operations centers. Data was collected from a dozen centers using this method.

### *Document Review*

A document review of relevant materials illustrates how others view, define and categorize operational centers, and specifically, activities associated with cyber defense operations. The following documents were reviewed to develop this model:

- Akamai. "Akamai Security Capabilities: Protecting Your Online Channels and Web Applications", 2010.

- Alberts, C. and Dorofee, A. "Mission Assurance Analysis Protocol (MAAP): Assessing Risk in Complex Environments", Technical Note CMU/SEI-2005-TN-032, September 2005.
- AT&T. "AT&T Information & Network Security Customer Reference Guide", January 2010.
- AT&T Business Service Guide. "AT&T Enterprise Hosting Services", November 29, 2010.
- Committee on National Security Systems, "National Information Assurance (IA) Glossary", CNSS Instruction No. 4009, 26 April 2010.
- DHS, "National Cyber Incident Response Plan", Interim Version, September 2010.
- Duggan, D. and Michalski, J. "Threat Analysis Framework", SANDIA Report, 2007.
- Jung, J. "Real-Time Detection of Malicious Network Activity Using Stochastic Models", Ph.D. Thesis, MIT, June 2006.
- Nagengast, J. C. "Cyber Security in the 21st Century - Building a National Cyber Defense Capability", AT&T Brief, 2010.
- National Cyber Security Center Policy Capture, Chart. [www.whitehouse.gov](http://www.whitehouse.gov).
- National Science and Technology Council, "Federal Plan for Cyber Security and Information Assurance Research and Development", April 2006.
- NIST IR 7497, "Security Architecture Design Process for Health Information Exchanges", September 2010.
- NIST SP 800-94, "Guide to Intrusion Detection and Prevention Systems", February 2007.
- NIST SP 800-83, "Guide to Malware Incident Prevention and Handling", November 2005.
- NIST SP 800-53, Revision 2, "Information Security", December 2007.
- NIST SP 800-61, Revision 1, "Computer Security Incident Handling Guide", March 2008.
- Sunita Sarawagi, "Information Extraction", Foundations and Trends in Databases, Vol 1, No. 3, 2007, pages 261-377.
- Symantec White Paper, "Symantec Cyber Threat Analysis Program", 2009.
- United Kingdom's Centre for the Protection of National Infrastructure (CPNI) Information Exchange classification scheme, <http://www.cpni.gov.uk/Docs/ie-membership-guidelines.pdf>.
- USAF, "Cyberspace Operations", Air Force Doctrine Document 3-12, 15 July 2010.
- Ye, N. "Automatic Extraction and Coordination of Audit Data and Features for Intrusion and Damage Assessment", Final Project Report to AFRL, March 31, 2006.
- Zimmerman, A. "A socio-technical framework for cyber infrastructure design", e-Social Science Conference, October 2007.

### 1.2.2 Analysis

The collected information was analyzed to identify the discerning characteristics between operations centers. Patterns and themes were identified in the data and then grouped into seven dimensions of like information. These dimensions are the foundation of the model: Scope, Activities, Organizational Dynamics, Facilities, Process Management, External Interactions, and Environment. The analysis team attached significance to the themes and patterns to draw conclusions from the data. The model output is a set of visualizations showcasing the pertinent characteristics of operations centers and their significance. These visualizations, and the information they contain, enable straightforward analysis of the organized data to answer a variety of questions that a center may ask about itself or its community.

### 1.3 Document Organization

An initial version of the model was developed based on data collected through document reviews, site visits, interviews, and community events during 2009 and 2010. The initial version was submitted to DHS/US-CERT in May 2010. The revised model is documented in this paper.

The operations center model is presented in detail in section 2. Each subsection within section 2 addresses additional details - an overview, definitions, and visualization - for each model dimension. In section 3, applications and audiences for this model are presented along with four actual examples. Finally, section 4 presents a summary of the model and its uses.

## 2 Operations Center Model Overview

The model is composed of seven dimensions that should be analyzed as a collection of information in their entirety and not as individual characterizations of a center since they are interrelated. The dimensions are:

- Scope – The scope dimension captures the scale, reach, primary role and mission timeline associated with the operations center;
- Activities – The activities dimension enumerates and organizes actions performed at operations centers into three areas – protection, incident management, and analysis;
- Organizational Dynamics – The organizational dynamics dimension captures the growth, change, and development of an operations center;
- Facilities – The facility dimension characterizes the physical space, orientation, continuity of operations and surge capabilities of an operations center;
- Process Management – The process management dimension describes an operations center’s experience, strength, and improvements in processes;
- External Interactions – The external organizational interactions dimension captures the nature and extent of internal and external interactions of an operations center; and
- Environment – The environment dimension describes physical or social factors outside the control of the operations center and the impact of those factors on a center’s ability to understand, respond to, influence, or collaborate with other operations centers.

Each dimension is further described by factors, attributes, and values. The diagram below, Figure 1, illustrates the relationships between each of these groups.

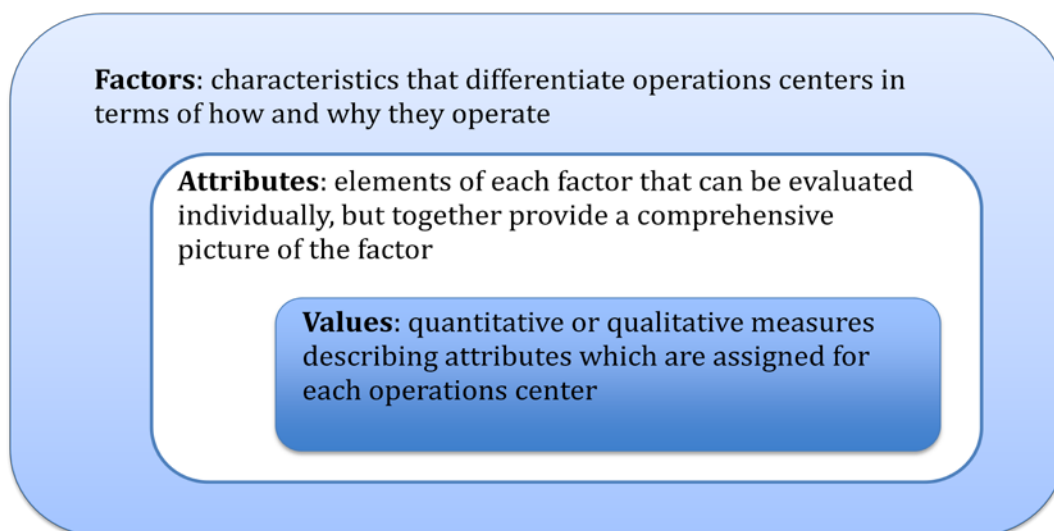


Figure 1 Factor, Attribute, and Value Relationships



Each dimension is characterized by multiple factors that capture relevant information pertaining to the dimension. Attributes decompose each factor into measurable or describable elements. These measures or descriptions associated with an attribute are called values, and the values recorded in the model are collected through site surveys, community activities and interviews. The attributes and values will be used to analyze and illustrate the information collected from each center in the context of other centers.

The model illustrates similarities between centers so that commonalities and differences can be identified for collaboration and awareness. It does not determine best practices or top performing centers, but the graphical representation of the model is used to rapidly compare one center or group of centers to another.

The following sections describe each dimension and its associated factors and attributes by first providing definitions and then presenting visualizations. The values are presented in detail in Appendix A.

## 2.1 Scope

The scope dimension focuses on the complexity, breadth, mission focus and responsibilities of an operations center. A center's scope influences how it obtains and responds to information, what types of organizations it partners with (captured in the external interactions dimension), and its ability to react during various stages of an event.

### 2.1.1 Scope Definitions

The scope dimension describes an operations center in terms of its span of influence, economic or government sector, functional role, functional activities pace and size. The key factors that comprise the scope model are divided into those that describe operational reach and those that describe function. A center is assigned a single primary attribute within this factor, but additional attributes may be deemed appropriate and documented accordingly.

- *Operational Reach*
  - *Impact Focus* – The types of incidents that fit an organization's mission focus.
  - *Sector* – The specialization or primary focus of the operations center's mission – commercial sector, government sector, or non-profit.
  - *Influence* – The geographical span of the infrastructure over which the organization's mission depends.
  - *Scale* – A characterization of the extent of the organizational responsibility based on a quantitative characterization of the infrastructure.
- *Function*
  - *Roles* – The significant roles performed by an operations organization for operating and defending its infrastructure.

- *Functional Abstraction* – The primary operational role or mission of an organization. Functional Abstraction will capture the purview of the center within its operational scope.
- *Type of Response* – The authority bestowed upon an organization to operate in a response capacity.
- *Timeline of Response* – The typical operating time interval that an organization needs to execute its functions as part of overall incident management.

Figure 2 shows the scope factors and their respective attributes. For ease of organization, the factors have been divided into those relating to the operational reach and function of an operations center. The values associated with each attribute are provided in detail in Appendix A.

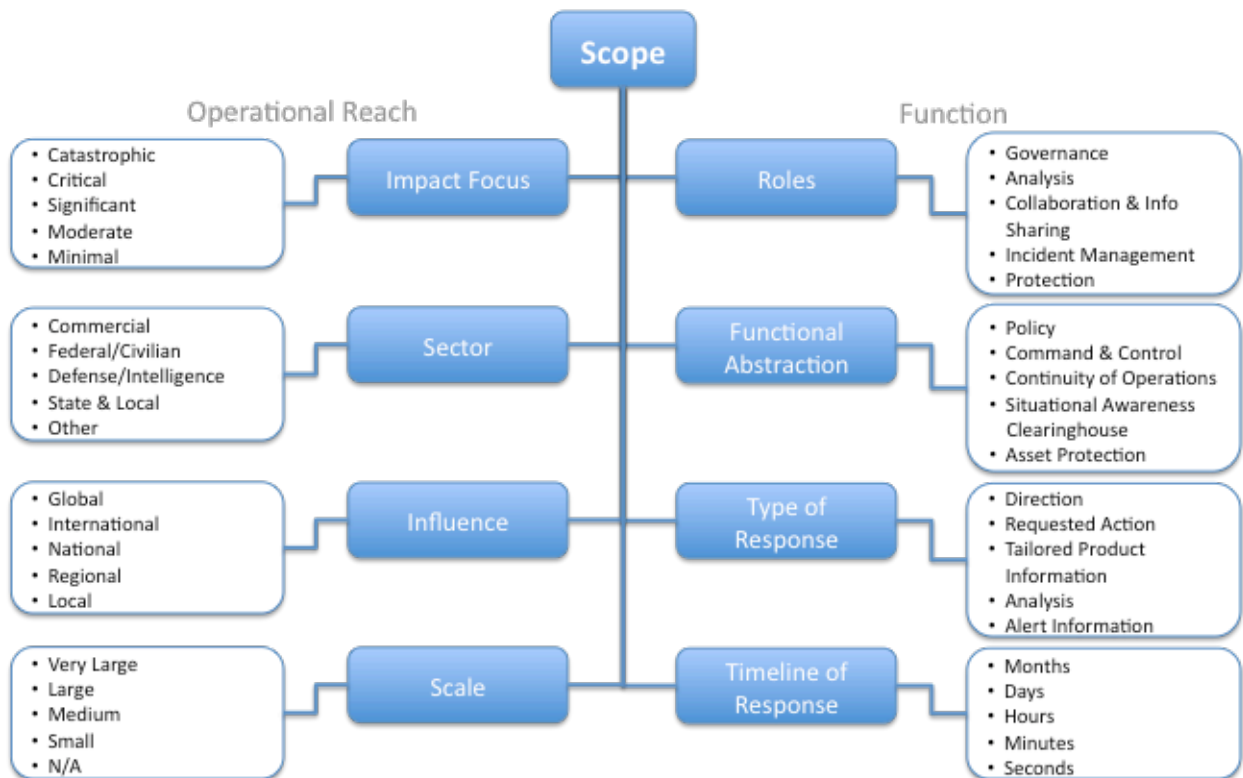


Figure 2.1-1: Scope Factors and Attributes

### 2.1.2 Scope Visualization

The octagon web illustration below, in Figure 2.1-2, depicts the eight factors that make up the scope dimension. The factors are organized into two areas – operational reach and function.

This chart is used to visually describe the operational reach and functions of a subject operations center by coloring appropriate values of the eight factors. The chart is also used to visually highlight commonalities and differences among selected centers by applying gradient colors or solid colors. The visual rendering

identifies areas of collaboration for different operations centers and identifies how they align and complement each other to advance their mission objectives.

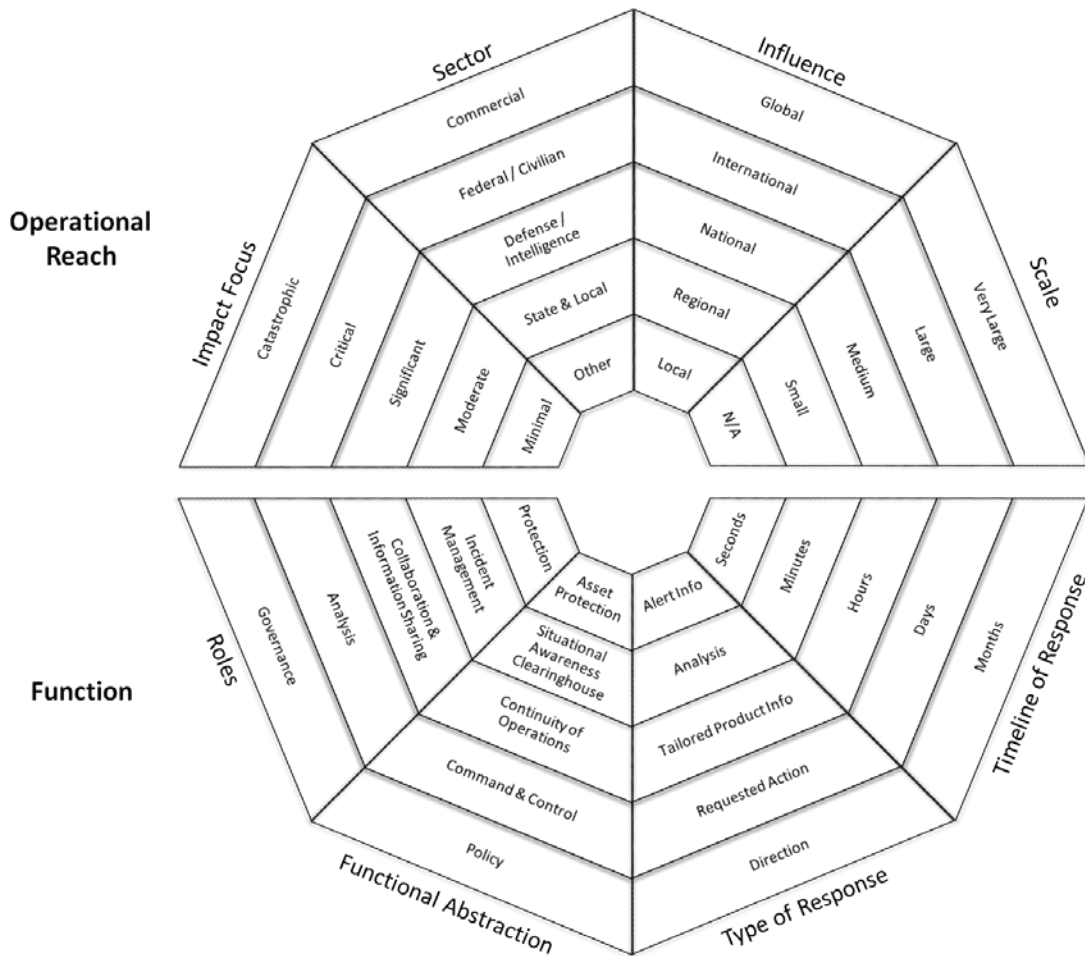


Figure 2.1-2: Scope Visualization

## 2.2 Activities

Activities are the sets of actions taken by an operations center, consistent with its operational processes, designed to meet its mission objectives. The activities model primarily applies to cyber operations; an analogous model can be developed for other types of operations. Activities broadly fall into three areas in cyber defense operations – protection, incident management, and analysis. A center’s activities identify the areas in which a center collaborates, interacts, and partners with peers.

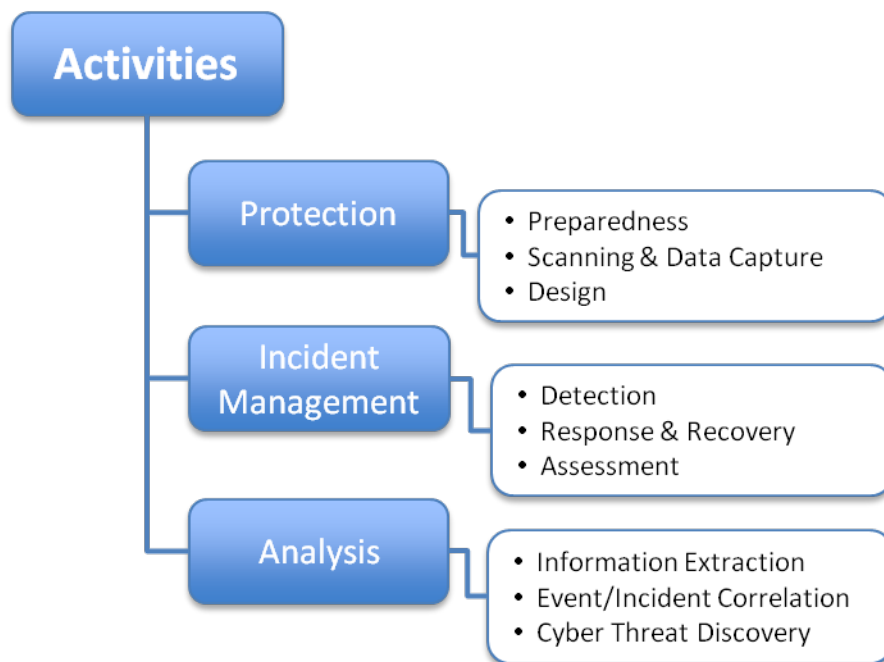
### 2.2.1 Activities Definitions

The activities model is built around three major types of activities – protection, incident management, and analysis. These three activities are divided into factors and attributes as shown in Figure 2.2-1. The associated values are defined in detail in Appendix A. The factors, attributes, and values were developed through direct reference or derivation from pedigree documentation, as noted in Appendix A. An

operations center can be assigned multiple attributes and values as it may perform several activities to meet operational needs.

The Activities factors are:

- *Protection* – Composed of a set of routine procedures, including oversight and/or performance of systems administration, maintenance and configuration management; formal training; monitoring; planning and design activities to secure and actively protect cyber infrastructure. A center could be assigned multiple factors and/or attributes in this activity.
- *Incident Management* – Includes procedures, actions and activities designed to detect, report, analyze, inform, coordinate and respond to incidents in the cyber infrastructure. A center could be assigned multiple factors and/or attributes within Incident Management.
- *Analysis* – Composed of a set of procedures, actions and activities designed to conduct in-depth assessment of information pertaining to missions, mission impacts, user activities, usage, traffic, performance incidents, threats, vulnerabilities, protection schemes, and incident management across cyber infrastructure. A center could be assigned multiple factors and/or attributes within the Analysis activity.



**Figure 2.2-1: Activities Factors and Attributes**

Figure 2.2-1b show the next level of details associated with the activities. These details pertain to activities associated with cyber defense operations.

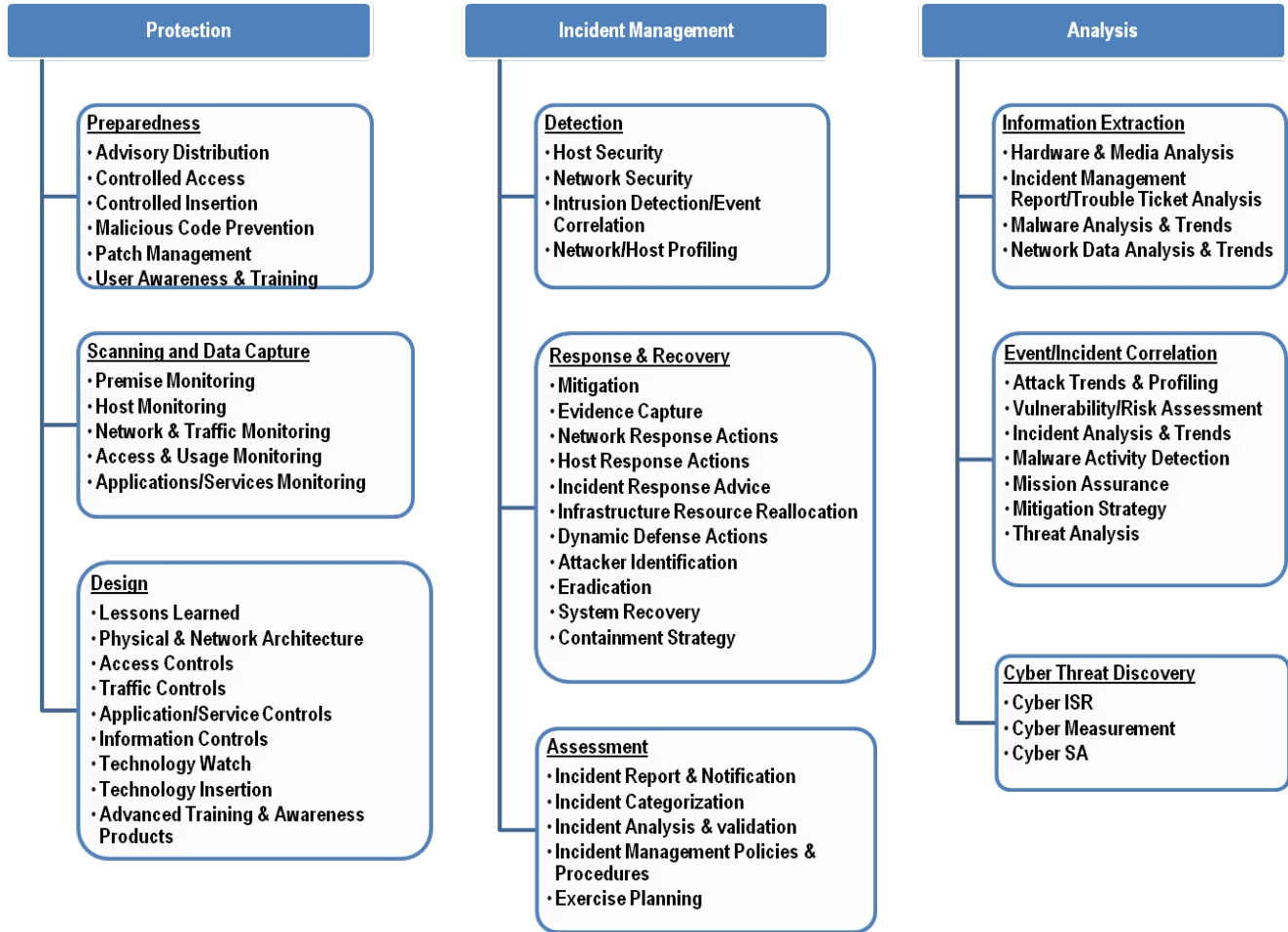
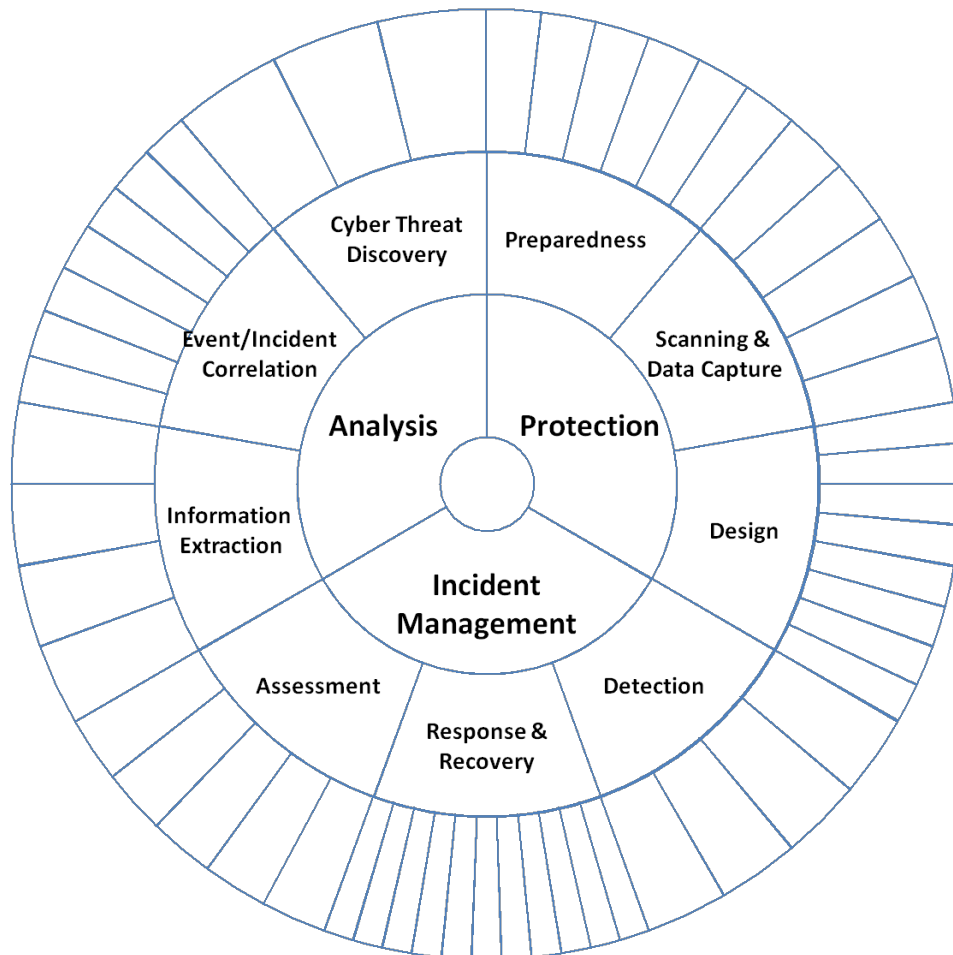


Figure 2.2-1b: Next level of details associated with Activity factors and attributes

### 2.2.2 Activities Visualization

The activities visualization shown in Figure 2.2-2 is a 3-layer doughnut chart used to organize the detailed breakout of the main factors and attributes of an operations center. The inner ring shows the breakout into the primary activities. The middle ring breakout is aligned with the inner chart to show how the three main activities are further defined. Finally, the outer ring shows the next level of details for the activities (figure 2.2-1b), and is aligned with the activity breakouts in the two inner rings.



**Figure 2.2-2: Activities Visualization**

The activities visualization chart is used to highlight key focus and specializations in activities at different operations centers, by highlighting the appropriate blocks in the outer ring. The highlights help contrast where two operations centers share common focus and where they complement each other. The focus and specialization is also useful in focusing on the tools and technologies, as well as best practices, adopted by a given operations center for its areas of specialization in accomplishing its objectives. A complete Activities visualization is shown in Figure 2.2-3.

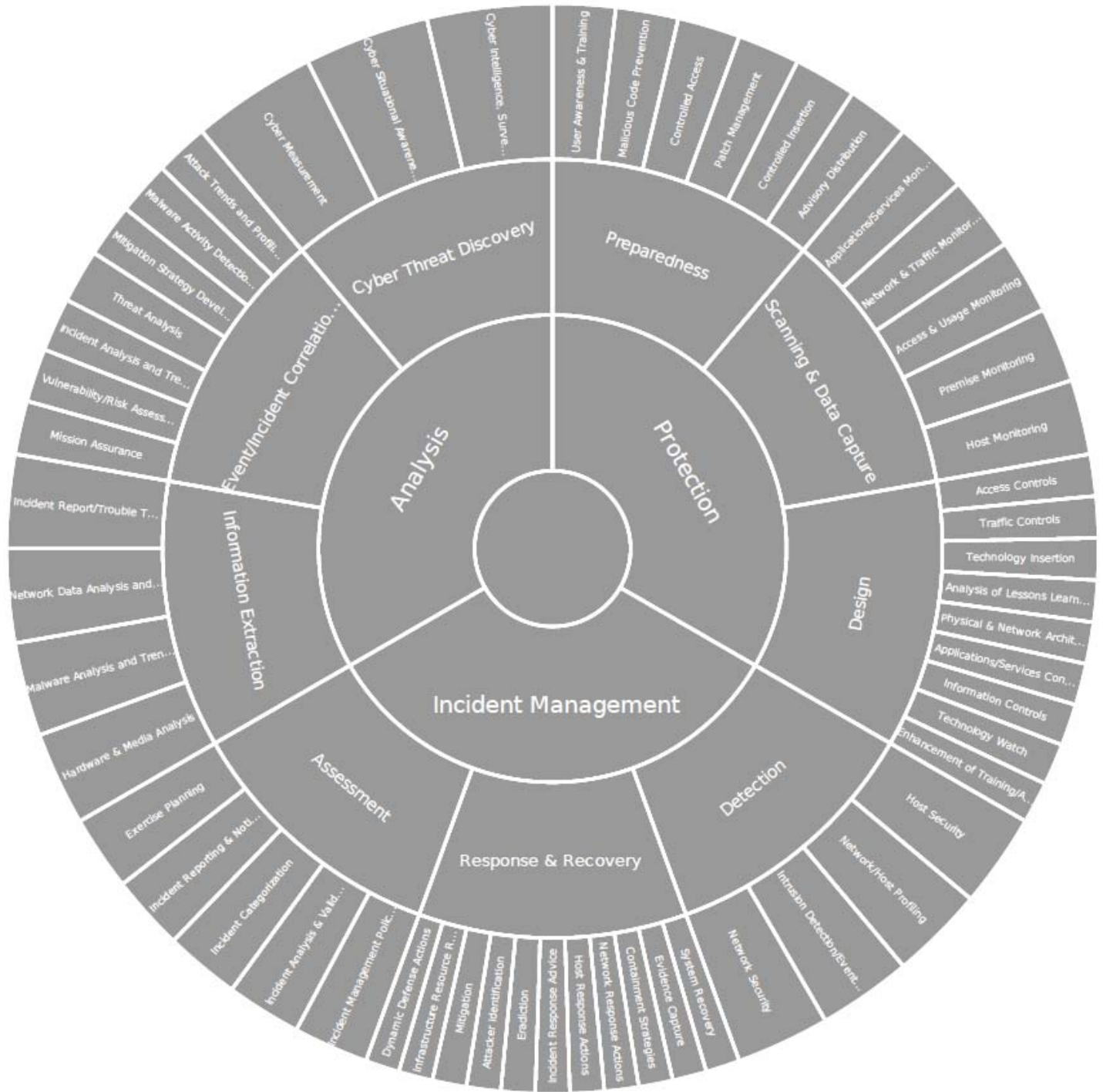


Figure 2.2-3: Activities Visualization with values.

## 2.3 Organizational Dynamics

The organizational dynamics dimension defines an organization's pattern of growth, change, or development over time. This dimension is described by five factors and coordinating attributes. A center's dynamics affects its internal operations and clarity in the context of its larger external mission and intent.

### 2.3.1 Organizational Dynamics Definitions

Organizational dynamics characterizes an organization's change over time with respect to its operating metrics. The following factors describe organizational dynamics:

- *Growth Rate* – The rate of growth of staff size at a center over time. Growth rate will be described based on the solicited response or research conducted about an operations center.
- *Organizational Longevity* – The amount of time an operations center has been in existence is measured by organizational longevity. Organizational longevity will be assigned based on interviews and research.
- *Organizational Change* – The transformations that occur in an operations center's executive level of organization structure and employee turnover rate. Operations centers will be solicited for information regarding changes in their organization chart over the life of the center to determine the number of times that executive management has changed over time. In addition, the operations centers will also be asked about their employee turnover rate. Both inputs combine to determine Organizational Change.
- *Mission Transformation* – The number of times an organization's mission changes or is significantly updated. This information will be captured during site surveys or interviews.
- *Funding Source* – The consistency and predictability of available funding for a center. Information for this factor will be solicited when possible, but can also be identified through open source research.

Figure 2.3-1 depicts the relationship of the factors and attributes for organizational dynamics. For each factor, a center is assigned a single value. The attributes and values for each factor are defined in Appendix A.

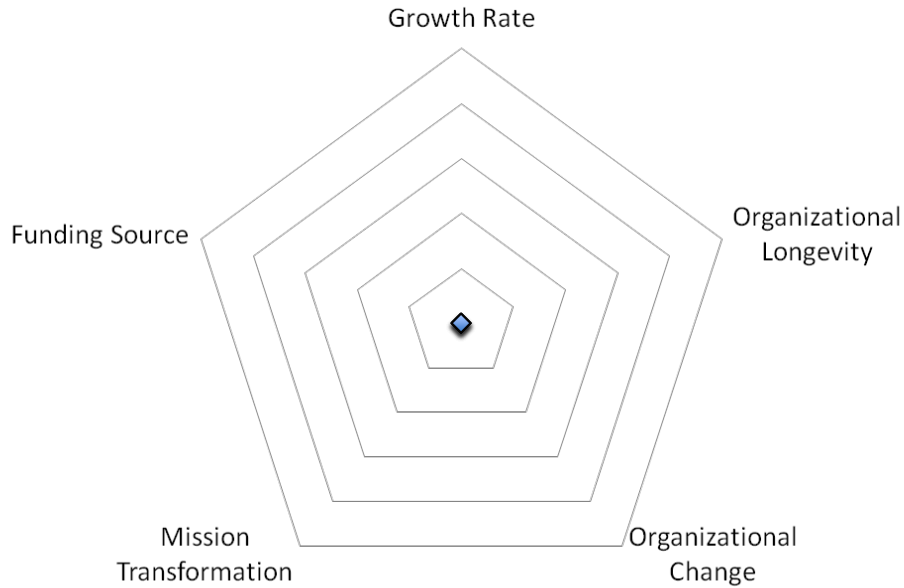




Figure 2.3-1: Organizational Dynamics Factors and Attributes

### 2.3.2 Organizational Dynamics Visualization

The output of this portion of the model is a five-sided “spider diagram”. Each side of the diagram represents a factor within the dimension and the attributes are converted to numerical values, zero to three. A representation of the diagram with a single organization is shown in Figure 2.3.2 below. The outer ring represents a low growth rate, high longevity, no organizational change, minimal mission transformation and full funding sources. Points on the outer ring identify well-established, steady organizations, while points on the inner ring identify dynamic, new or significantly evolving organizations.



**Figure 2.3-2: Organizational Dynamics Visualization**

Multiple organizations are represented on this diagram by overlaying additional lines onto the spider diagram. By using this diagram, a center finds other centers that are similar in a factor such as size or longevity. Organizations use this comparison to share information regarding organizational development or other internal dynamics.

The organizational dynamics chart is used to compare growth, changes and longevity of subject operations centers. Together, with the scope chart and activities chart, organizational dynamics helps identify operations centers that are very similar or vastly different in terms of their responsibilities and areas of focus. Another use of the chart is in conjunction with process management, where it is possible to look for best practices, and where newly formed operations centers look for collaboration or partnerships.

## 2.4 Facilities

The facilities dimension describes the physical space allocated to the operations center. It is characterized by eight factors and their associated attributes. A center's facilities affect how it communicates internally, externally and during a critical event.

### 2.4.1 Facilities Definitions

Facilities are characterized using space size, number of desks, surge capability, Continuity of Operations (COOP) capability and layout type. The following factors describe Facilities:

- *Space Size* – The physical contiguous or non-contiguous space (in square footage) used or owned by a center.

- *Number of Desks* – The number of physical seats available for operations center staff.
- *Surge Capability* – The operations centers ability to expand (as needed) during an event.
- *Center Hours* – The hours an operations center maintains to fulfill its role and mission.
- *Layout Type* – The physical configuration of furniture, equipment, and staff in the operations center.
- *COOP Scope* – The percentage of operations center resources (facilities, systems, staff, and decision making) targeted for continuity.
- *COOP Readiness* – How quickly the redundant Operations Center capabilities can be brought online and operational when a primary center is lost or degraded.
- *Coordination Methods* – The methods used by an operations center to coordinate activities with its peers/partners, i.e., periodic reports, conferencing, etc.

The factors and attributes for Facilities are shown in Figure. Details for the attributes and values are presented in Appendix A.

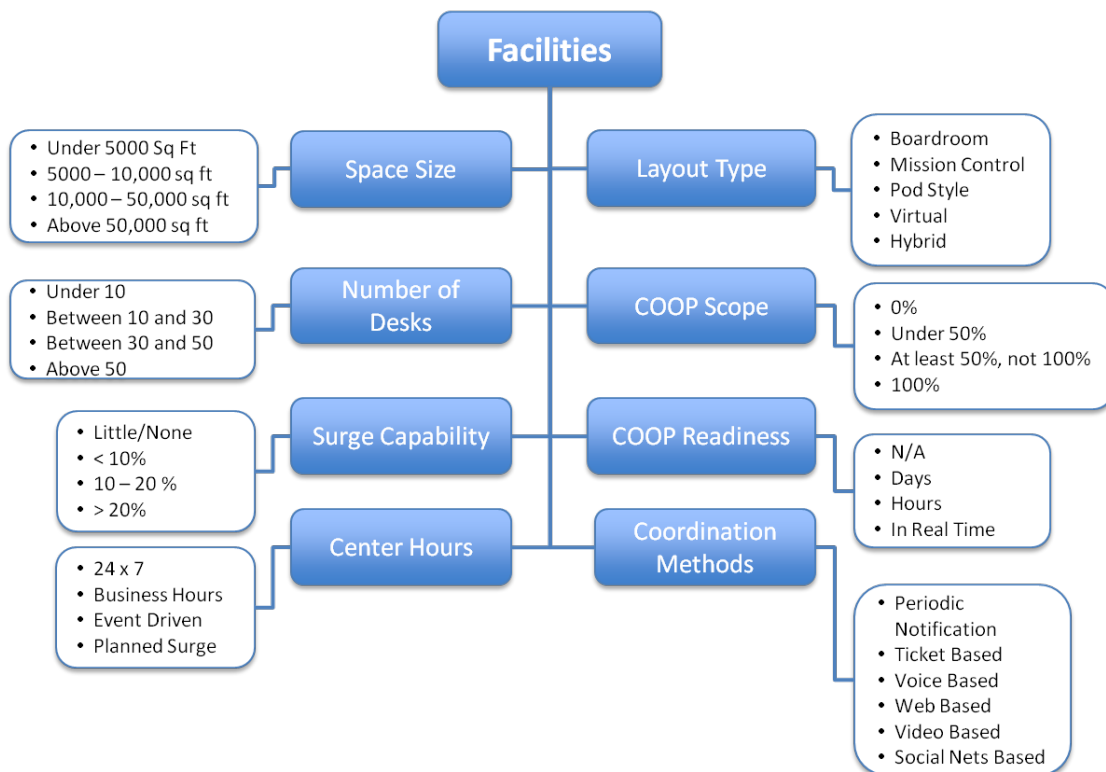


Figure 2.4-1: Facilities Factors and Attributes

### 2.4.2 Facilities Visualization

Visualization of the Facilities dimension is shown in Figure, below. Multiple operations centers are represented by their physical layout and associated physical

statistics. Items are catalogued in a visualization that allows for quick comparison and contrast of multiple centers.

The facilities chart renders a quick look of the characteristics of an operation center’s facilities. A side-by-side comparison of two facilities’ charts representing two operations centers is used to understand the facilities and how they relate to the scope and activities charts. The chart is also used to understand how one operations center may collaborate or partner with another.

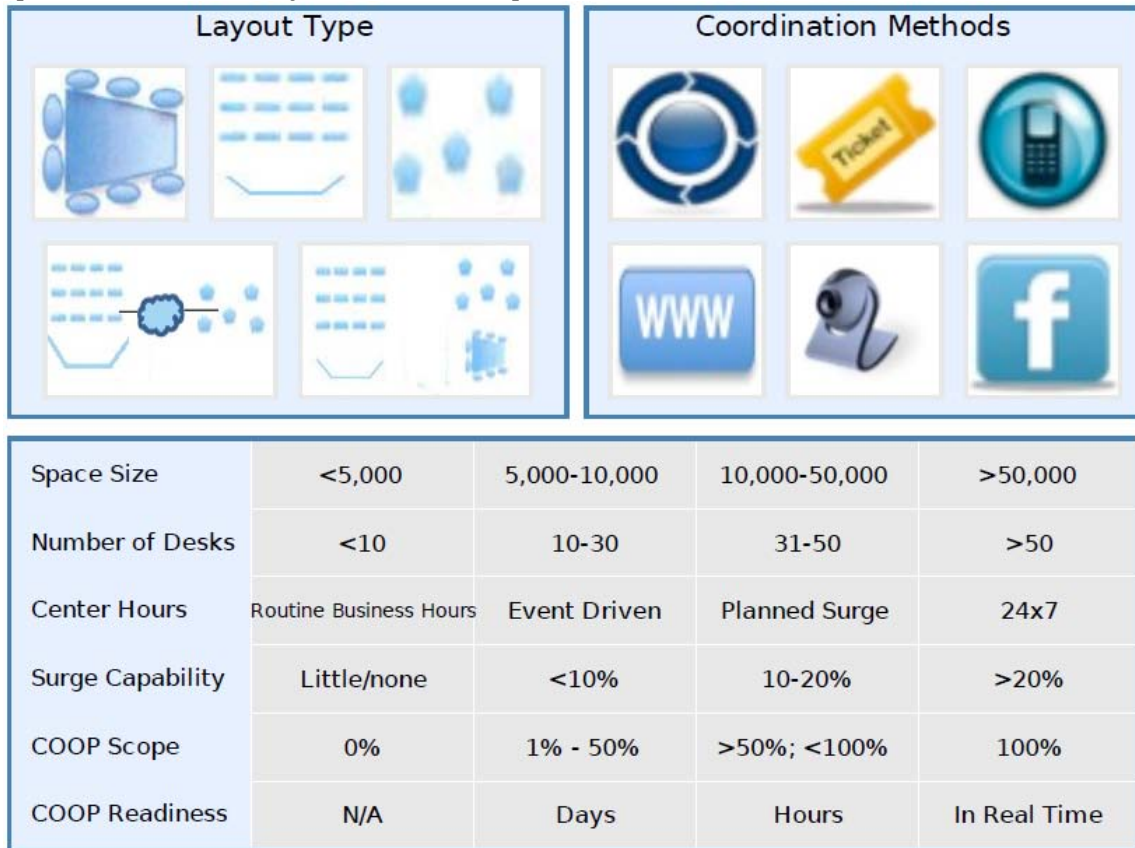


Figure2.4-2: Facilities Visualization

## 2.5 Process Management

Process Management defines an organization’s level of experience derived from observations of its standard practices. This dimension is based on community-accepted maturity models but does not require quantitative ratings on an organization’s maturity. Process Management highlights areas of internal strength or improvement that affect how a center fits into its external community.

### 2.5.1 Process Management Definitions

Process Management is articulated using four factors:

- *Training and Certification* – Formal, well defined regime for ensuring skills and training of staff for specific job functions.
- *Active Use of SOPs* – Well established, comprehensive, standardized set of process steps (standard operating procedures or SOPs), and their active use.

- *Production* – Well established, consistent and regularity of offerings of alerts, tailored information products, other services.
- *Analytics* – Establishment, collection, fusion and use of metrics to measure and refine processes.

A center is assigned a single attribute for each factor. Each factor in the Process Management model is rated using the following five attributes:

- *Initial* – An ad hoc or often inconsistent mode
- *Managed* – Individual functions are repeatable and consistent, but different functions not integrated
- *Defined* – Structured and integrated
- *Quantitatively Managed* – Disciplined and predictable
- *Optimizing* – Proactive and agile

The Process Management factors and attributes are depicted in Figure .



**Figure 2.5-1: Process Management Factors and Attributes**

### 2.5.2 Process Management Visualization

Process Management is illustrated using a matrix, as shown below in Figure 2-11. The matrix outlines each factor, attribute and value so that an operations center easily showcases applicable attributes.

	Initial: ad hoc	Managed: Repeatable in isolated functions	Defined: Structured and Integrated	Quantitatively Managed: Disciplined and predictable	Optimizing: Proactive and agile
Training and Certification	Initial: opportunistic, on the job training	Managed: training program for only a few specialized roles	Defined: all roles have defined requirements and training	Quantitatively Managed: training and certification metrics are available and used to predict needs	Optimizing: formal certification and re-certification is required for each role
Active Use of SOPs	Initial: individual techniques prevail	Managed: SOPs for each function exist without integration	Defined: SOPs integrated; trained on use of SOPs	Quantitatively Managed: metrics exist to monitor SOP use	Optimizing: metrics are used for planning and SOPs are agile and adaptable as needed
Production	Initial: opportunistic outputs with minimal impact	Managed: regular outputs with varied impact	Defined: defined outputs with confirmed usefulness	Quantitatively Managed: outputs in appropriate scope, but with variable quality; quality is measured and metrics exist	Optimizing: consistent institutionalized quality and impact
Analytics	Initial: negligible analytics use; get accurate data to improve operations	Managed: use analytics to improve one or more functional activities	Defined: use analytics to improve a distinctive capability	Quantitatively Managed: enterprise-wide perspective, able to use analytics for point advantage	Optimizing: enterprise-wide, big results, sustainable advantage

**Figure 3: Process Management Visualization**

The Process Management matrix is used to highlight growth and maturity of operational processes and analytics in use at an operations center. Two or more centers highlighted on the same chart, along with organizational dynamics and activities charts, helps identify where a center may look to grow and mature its processes.

## 2.6 External Interactions

External Interactions describe the formal and informal interactions supported by the operations center. These interactions affect the center’s ability to transmit and receive information and impact the center’s ability to react and respond to events.

### 2.6.1 External Interactions Definitions

This dimension describes a center’s relationships with six external organizations (see Figure 2.6-1).

- *Emergency Services* – The interactions pertain to collaboration and support services during emergencies, natural disasters or other catastrophic conditions.
- *Government* – The interactions pertain to government’s oversight role (such as export controls), government as a customer, sponsor or even a partner.
- *Law Enforcement* – The interactions pertain to working closely with Law enforcement as warranted for criminal, counter-terrorism or other critical investigations.
- *International* – The interactions pertain to awareness of and adherence to rules and laws of engagement in host countries, as well as complying with oversight requirements.
- *Commercial* – The interactions pertain to relationships with businesses that are suppliers, subscribers, peers or partners.
- *Intelligence* – The interactions pertain to working closely with defense and intelligence agencies of the government for counter-terrorism, counter-intelligence or other critical investigations.

For each organization, multiple attributes are assigned to characterize the type of interaction, as shown below. The attributes and values are described in detail in Appendix A.

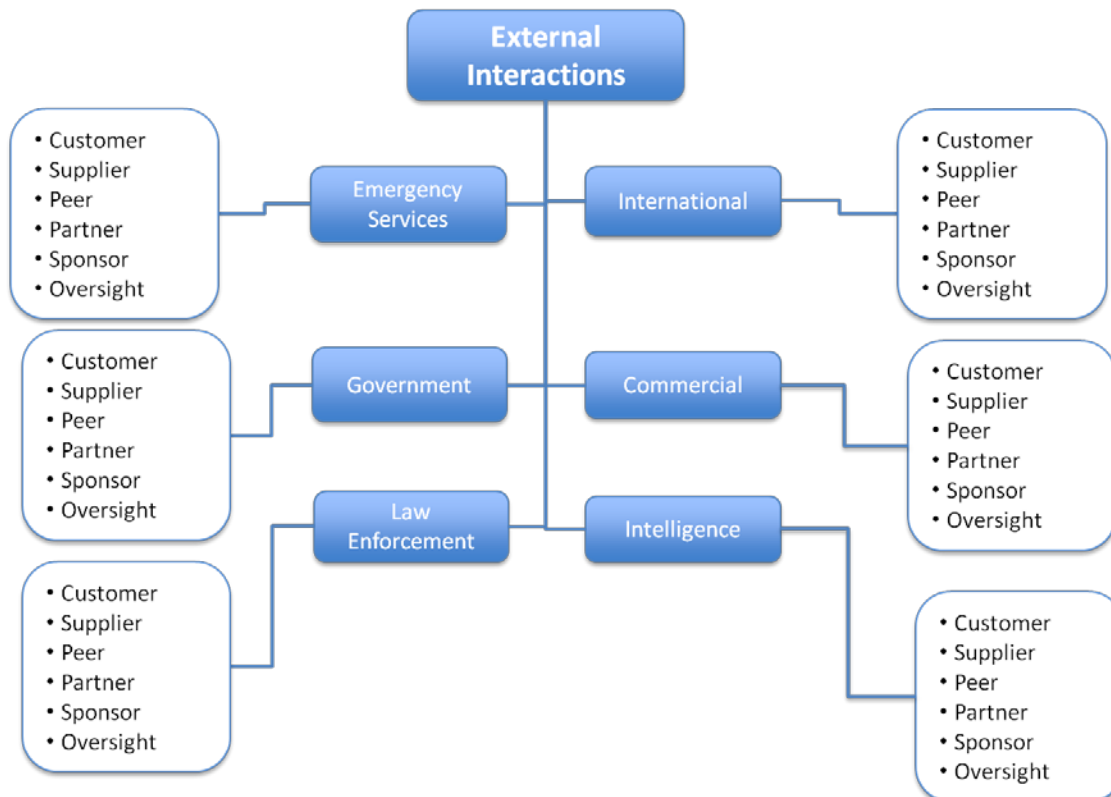


Figure 2.6-1: External Interactions Factors and Attributes

### 2.6.2 External Interactions Visualization

The external interactions visualization is shown in Figure 2. The relationship of the operations center to each organization is characterized by its type. The applicable attributes are color-coded for each center.

The chart is used to characterize interactions and dependencies of a subject operations center. Color-coding helps compare multiple organizations to derive similarities or uniqueness of interactions and dependencies. The chart is used to identify and augment partnerships and collaborations when combined with activities, organizational dynamics and scope charts.



Figure 2.6-2: External Interactions Visualization

### 2.7 Environment

Environment is the combination of social and physical conditions, outside a center's direct control, that affects its mission, development, and fortitude. The external



environment affects a center's ability to effectively collaborate, respond, interface, and influence its operational community. Environment is characterized by six factors with their corresponding attributes.

### 2.7.1 Environment Definitions

Environment is described by six factors as defined below. A center may be assigned multiple attributes within each factor.

- *Visibility* – The ability to observe within a center's operational environment. This factor attempts to answer the question, "What does the operations center *know*?"
- *Reach* – The ability of a center to influence areas within its operational environment. Reach describes the areas that an operations center can *affect*.
- *Data Handling* – The restrictions for handling and distribution of the data that a center uses.
- *Capability* – The external organizational considerations and policy considerations that may limit a center's ability to effectively respond to events and incidents.
- *External Stability* – The predictability of the domain in which the center operates, indicating the center's ability to respond to anticipated and unanticipated events.
- *Community Coordination* – The prevalent and common methods used in the community (regardless of what methods the specific center under study uses) for coordinating activities across peer, partner and oversight organizations.

The factors and their associated attributes are shown in Figure 2 and the details of their values are presented in Appendix A.

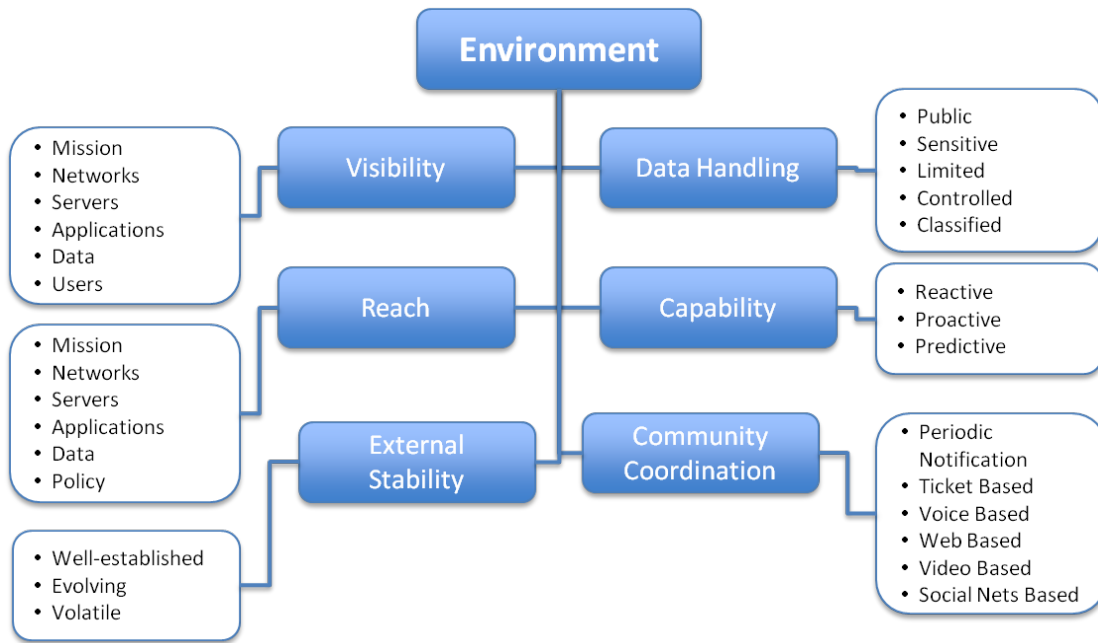
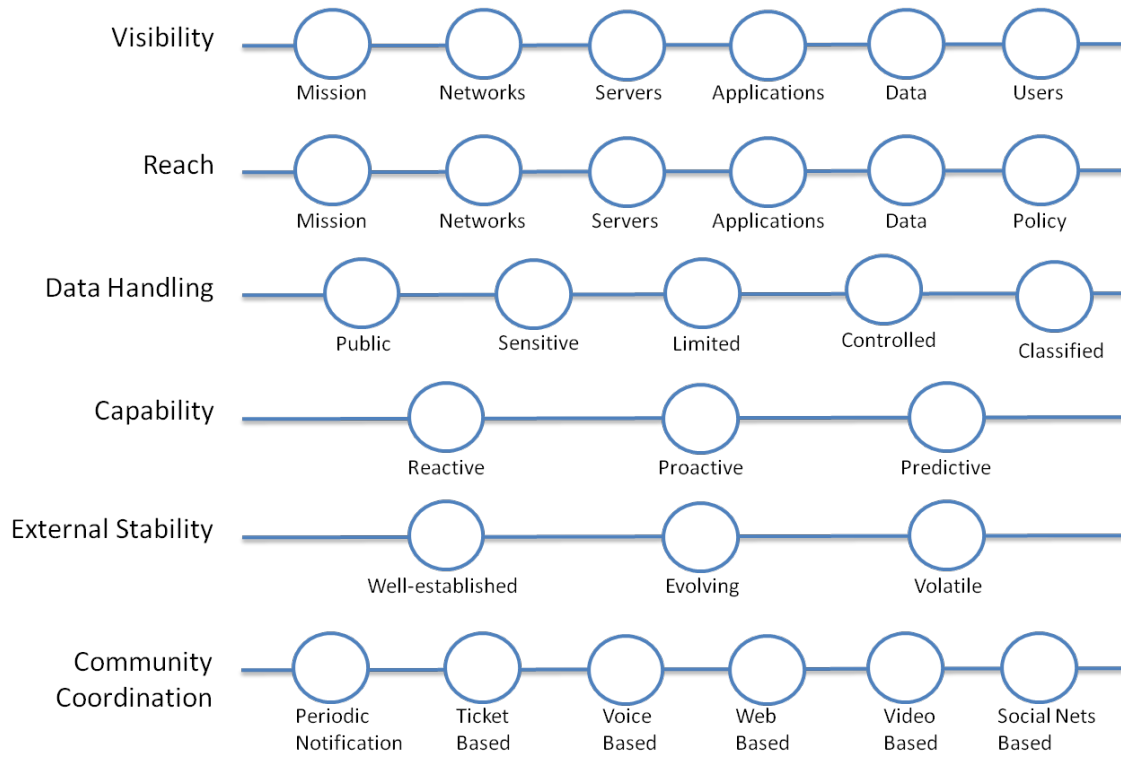


Figure 2.7-1: Environment Factors and Attributes

### 2.7.2 Environment Visualization

The environment visualization, shown in Figure 2, consists of six rows that each depicts a factor and its associated attributes. The attributes are filled in with color to show their assignments for a given center. Multiple centers are overlaid to show similarities and differences in their environment.

The environment chart is used to understand the external variables and constraints that influence how well an operations center is able to achieve its mission objectives, or is impeded in fully realizing its potential. When two or more operations centers are compared using the chart, it is possible to gauge the similarities and differences in environment factors that help or hinder them. This information along with the process management, organizational dynamics, activities, and scope charts help identify what an operations center may be able to do to improve or adapt to its environment through collaboration, partnership, or adoption of best practices.



**Figure 2.7-2: Environment Visualization**

### 3 Application of the Model

The operations center model described in section 2 assists individual organizations to (a) understand capabilities and specializations of different operations centers; (b) identify unique roles of each center to guide how it might align and fit with complementary missions of other organizations; and (c) tailor an appropriate partnership framework for collaboration and tailored information sharing among partner operations centers.

The following list enumerates possible applications of the model and value to respective audiences.

**Table 3-1 Applications of the Model**

Audience	Application	Result
I'm building a new watch floor...	<ul style="list-style-type: none"> <li>• How should we design the watch floor to maximize communication effectiveness?</li> <li>• What customers/partners/peers should we work with and how do we work with them?</li> </ul>	Benefits of various center layouts; structured method to identify organizational interactions; learn from mature centers in the same operations space
Our center is having trouble finding its niche...	<ul style="list-style-type: none"> <li>• What do our peers do well?</li> <li>• What portions of our work should be done in collaboration with partners instead of performing ourselves?</li> <li>• What part of our scope is different from our peers (what parts of the problem can only we do)?</li> </ul>	Comparison of activities and scope between peers and self; areas to collaborate with partners
Our center is doing well...	<ul style="list-style-type: none"> <li>• What does our center look like?</li> <li>• How do we compare to our peers?</li> <li>• Are there new techniques we could learn from our partners?</li> <li>• Where could we improve?</li> </ul>	Comparison to peers in terms of the six identified categories; areas to collaborate with partners; areas for improvement
We want to see what others are doing...	<ul style="list-style-type: none"> <li>• What types of information should we discuss with our peers?</li> <li>• What should we pay attention to during our site visits to other centers?</li> </ul>	Organized discussion points; relevant operational factors
We want to structure our partnerships better...	<ul style="list-style-type: none"> <li>• How should we customize our interactions with various partners, peers, and customers?</li> <li>• What special joint procedures should we establish?</li> <li>• How can we communicate what our center does to others?</li> </ul>	Identification of information exchanges between organizations; relevant information to develop joint surge and COOP procedures; test drive joint procedures using a common vocabulary

The following subsection presents visual representations of actual data collected from a few cyber defense operations centers, and provides analysis of the data being observed. The analysis focuses on structuring the relationship to establish and improve partnerships – outlined in the last row of Table 3-1, above.

### 3.1 Data Collection Questionnaire

An Operations Center Questionnaire was developed as one of several tools to gather data from the staff representing various operations centers in the cyber-defense operations community. The questionnaire can be completed in either a paper based format or an online format to match the preferences of the individual staff member. The questionnaire was designed to be fairly intuitive for operations center staff. In addition, being mindful of the tempo of their center activities, the questionnaire was expected to be completed within fifteen minutes. A number of other considerations went into the design of the questionnaire – (a) self-scoring of confidence for answers given with respect to each dimension; (b) entry of single or multiple answers as appropriate; (c) ability to disassociate attribute information to enable data aggregation; and (d) ability to align responses with different staff positions, as each staff position may have a slightly different perspective on the characteristics of their operations center.

The paper version of the questionnaire is included in the appendix B

Some of the sample data presented in the next section was collected during GFIRST conference held in August 2011, and the rest was collected during December 2011 and January 2012.

## 3.2 Visual Representations of Collected Data and Comparative Analysis

In the following subsections, data collected from four organizations performing cyber defense operations are presented visually, dimension by dimension, followed by an analysis of what each visual is providing individually and comparatively. Each of the four organizations seeks to explore effective mechanisms for community collaboration to advance their individual missions. The choice of the centers selected is primarily to demonstrate both commonality and diversity among the representative centers. For the purposes of this discussion, the centers represented here will be named Center A, Center B, Center C and Center D. In the figures that follow, Center A is at top-left, Center B is at top-right; Center C is at bottom-left; and finally, Center D is at bottom-right.

### 3.2.1 Overall Analysis

Looking across all the dimensions, it is possible to consider two areas of focus, center categorization and tailored information sharing, or how any of the four organizations collaborate with the other three, as a member of the cyber defense operations community. The categorization helps each center tailor its relationships with each external organization, but optimize it by a category. The tailoring of information products will help identify what information is best shared with a specific external organization, the coordination methods to be used, and how rapidly they must be executed.

#### *Categorization*

- By sector factor in Scope dimension
  - Federal/Civilian (Centers A and D)
  - Defense/Intelligence (Center B)
  - State/Local (Center C)
- By highlighted factors of Activities dimension; coupled by primary and secondary functions as well as roles factor of Scope dimension; and augmented by maturity level of process management
  - Analysis (all four Centers)
  - Incident Management (all four Centers)
  - Protection (all four centers)

#### *Tailored Information Sharing and Appropriate Coordination Method*

- Type of Information (based on primary and secondary functions of scope dimension)
  - Continuity of Operations (all four Centers)
  - Cyber SA (Centers A and D)
  - IT Protection (all four Centers)
- Common coordination methods described in the Facilities dimension
  - Web and Ticket-based (all four Centers)

- Periodic Notification, Voice, Web and Ticket based (all but Center C)
  - Social-Nets based (Centers A and C)
- Match response times in Scope Dimension
  - Hours (Centers A, C and D)
  - Hours, Minutes and Days (Centers A and D)
  - Days (all four centers)
- Data Handling
  - All data sensitivity types, except 'controlled' and 'classified' (All four centers)
  - Classified (Centers A, B and D)
  - Controlled (Centers A and D)

### 3.2.2 Scope Dimension

### 3.2.2.1 Scope Dimension Comparative Visualization

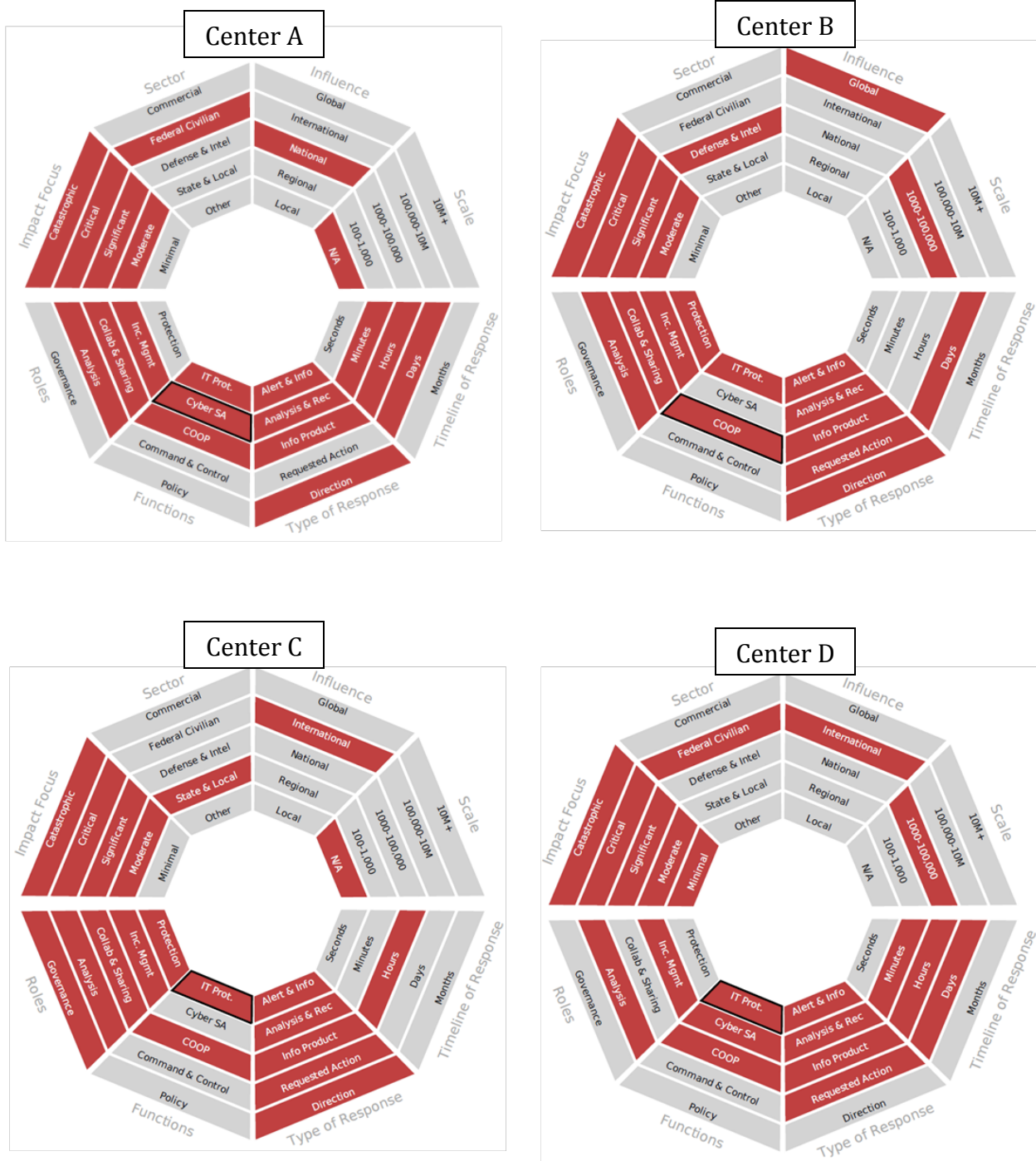


Figure 3-1: Scope for Centers A, B, C and D. Red colored boxes indicate areas of scope that apply to a given center. For functions, black bordered red box indicates primary function.



### 3.2.2.2 Scope Dimension Comparative Analysis

#### Summary

- The diversity of the organizations is evident not only in their primary functions, but also in the sector they operate – Center A and D are in Federal/Civilian space, Center B is in Defense/Intelligence and Center C is State/Local space.
- Three of the four organizations have identified ‘Direction’ as one of their response elements.
- Centers A and D have response times ranging from minutes to days. Center B has response time of days, but Center C has response time in hours.
- Scale is not a factor for Centers A and C; Centers B and D have identified medium scale
- Centers C and D have identified their influence spanning international relationships; Center B has influence spanning global operations; and Center A indicated national influence.
- Centers A and D have significant commonality, and may be candidates for aggregation into a common category.
- Centers B and C have a number of similarities, but the sectors are quite distinct. Thus, they may not candidates for aggregation into a common category.

#### Observations

- |  |
|--|
| <ul style="list-style-type: none"><li>• Organization C and D have identified IT Protection as the primary function of their centers, Organization A and B have identified Cyber Situational Awareness (Cyber SA) and Continuity of Operations (COOP) as their primary mission.</li><li>• IT protection and COOP is a common function for all of four centers</li><li>• Cyber SA is a common activity for center A and D.</li></ul> |
| <ul style="list-style-type: none"><li>• The operational roles associated with all four centers include analysis and incident management.</li><li>• Three of the four (all but Center D) indicated that their roles included collaboration and information sharing.</li><li>• Protection is a common role among Centers B and C.</li><li>• Governance is an additional role for Center C.</li></ul>                                 |

#### Finding(s)

All four organizations should collaborate on incident handling and analysis (collection, analysis methods and analysis products) in common cyber defense areas that impact all of them. Among the four centers, protection and collaboration have been identified either in the roles or in functions. Thus, they all should consider

sharing specific information pertaining to improving protection, and explore process methods and scope of that information sharing.

### 3.2.3 Activities Dimension

#### 3.2.3.1 Activities Comparative Visualization

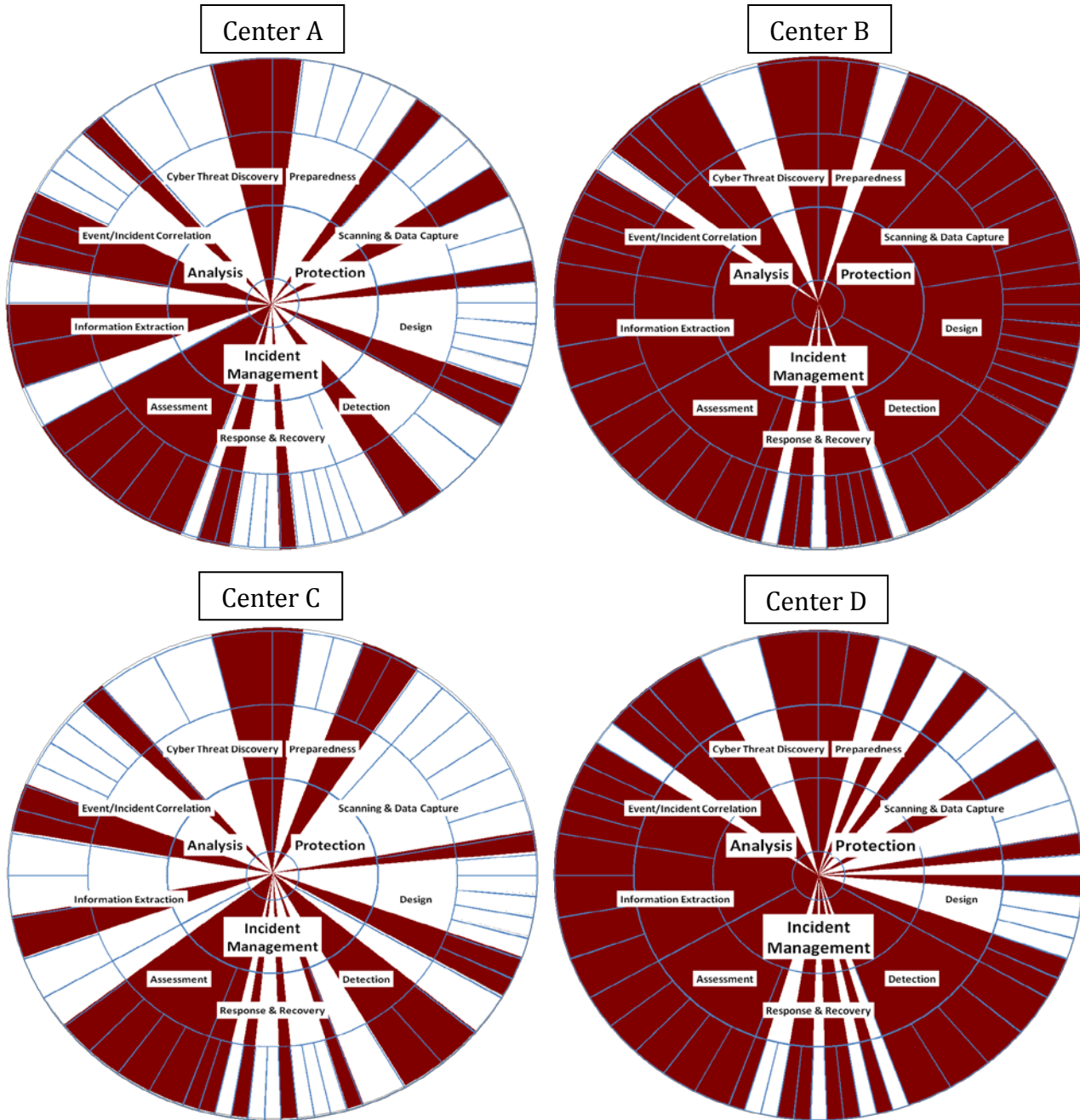


Figure 4: Activities for Centers A, B, C and D. Red colored areas in the chart indicate activities performed by the center.

### 3.2.3.2 Activities Comparative Analysis

#### Summary

From the activities perspective, the collaboration and information sharing among the four centers can be scoped to specific overlapping activities across the three areas. The range of such collaboration would be broader between Centers B and D, since they have a significant number of activities in common across all three areas. Center A and C appear to fall into a common category, since they both focus on incident management as the key activity area.

#### Observations

- The activities of Center B broadly cover all three areas – protection, incident management and analysis.
- While Center D also covers all three areas, it is mainly focused on incident management and analysis activities.
- Centers A and C touch all activity areas, but perform, specific and limited activities in them.

#### Finding(s)

Collaboration and information sharing among the operations centers should be tailored to commonality of specific cyber security activities. This tailoring can be the basis for categorization of operations centers. The information sharing should take such categorization into account to avoid having to manage unique, pair-wise relationships between any two centers in the community.

### 3.2.4 Facilities Dimension

#### 3.2.4.1 Facilities Comparative Visualization

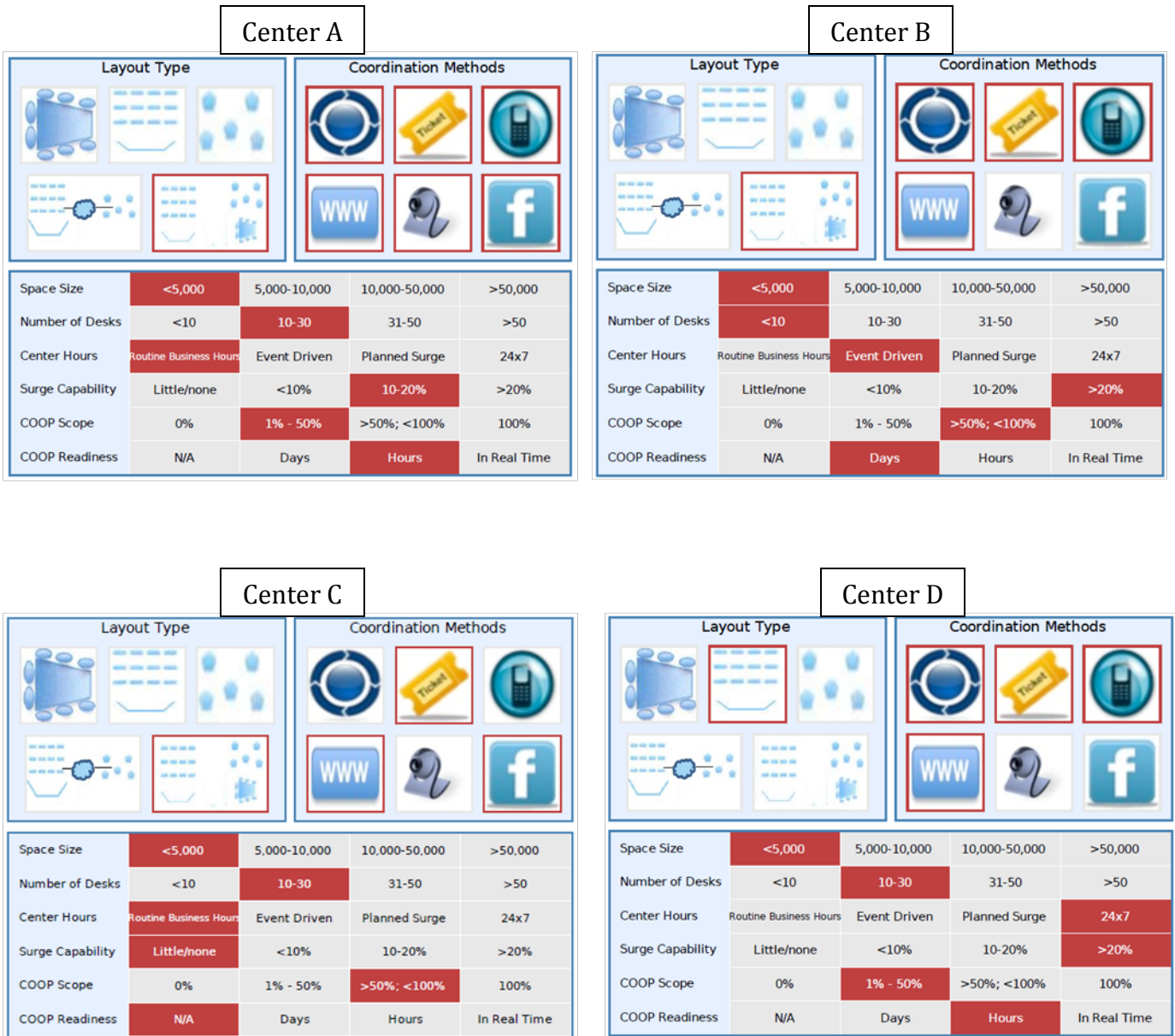


Figure 3-3: Facilities visualization for Centers A, B, C and D. Red-outlined boxes or red colored boxes indicate data points for each center.

### 3.2.4.2 Facilities Dimension Comparative Analysis

#### Summary

Trouble Ticketing, Web, periodic notification and voice appear to be common viable methods for collaboration. Center C can learn from the centers about defining and executing a COOP readiness strategy. Center D can explore transforming from a mission control layout to a hybrid layout to see if it better facilitates collaboration with other centers in the community.

#### Observations

- Three of centers have Hybrid Layout type, and Center D has mission control layout.
- All have relatively small areas dedicated for operational activities, but other than center B, all have desk spaces for 10-30 staff position. Center B has less than 10 desk spaces.
- Centers A and C operate during normal business hours, Center B operates on an event-driven basis and Center D has 24x7 operations.
- Center C has no surge capability. Center A has 10-20% surge capability. Centers B and D have above 20% surge capability.
- Center A uses all coordination methods; Center B uses all but video-based; Center D uses all but video and social-nets; and Center C only uses tickets-based, web-based and social-nets based.
- All centers have some accommodations for continuity of operations. Centers A and D are able to switch-over to back-up capabilities within hours. Center B switch-over may take days; and readiness of Center C is unclear.

#### Finding(s)

Centers A and C are likely candidates for being grouped into a common category as they share a number of common facilities attributes.

It is interesting that three of the four centers have adopted Hybrid layout. This layout may be most beneficial from the perspective of collaboration and information sharing among the centers, because it combines benefits of different layouts. Perhaps it is an indication that cyber defense operations are most effective in a collaborative environment, as opposed to command and control environment. Center D may consider reevaluating its facility layout by evaluating the effectiveness of the hybrid layout of the other three centers.

### 3.2.5 Organizational Dynamics

#### 3.2.5.1 Organizational Dynamics Comparative Visualization

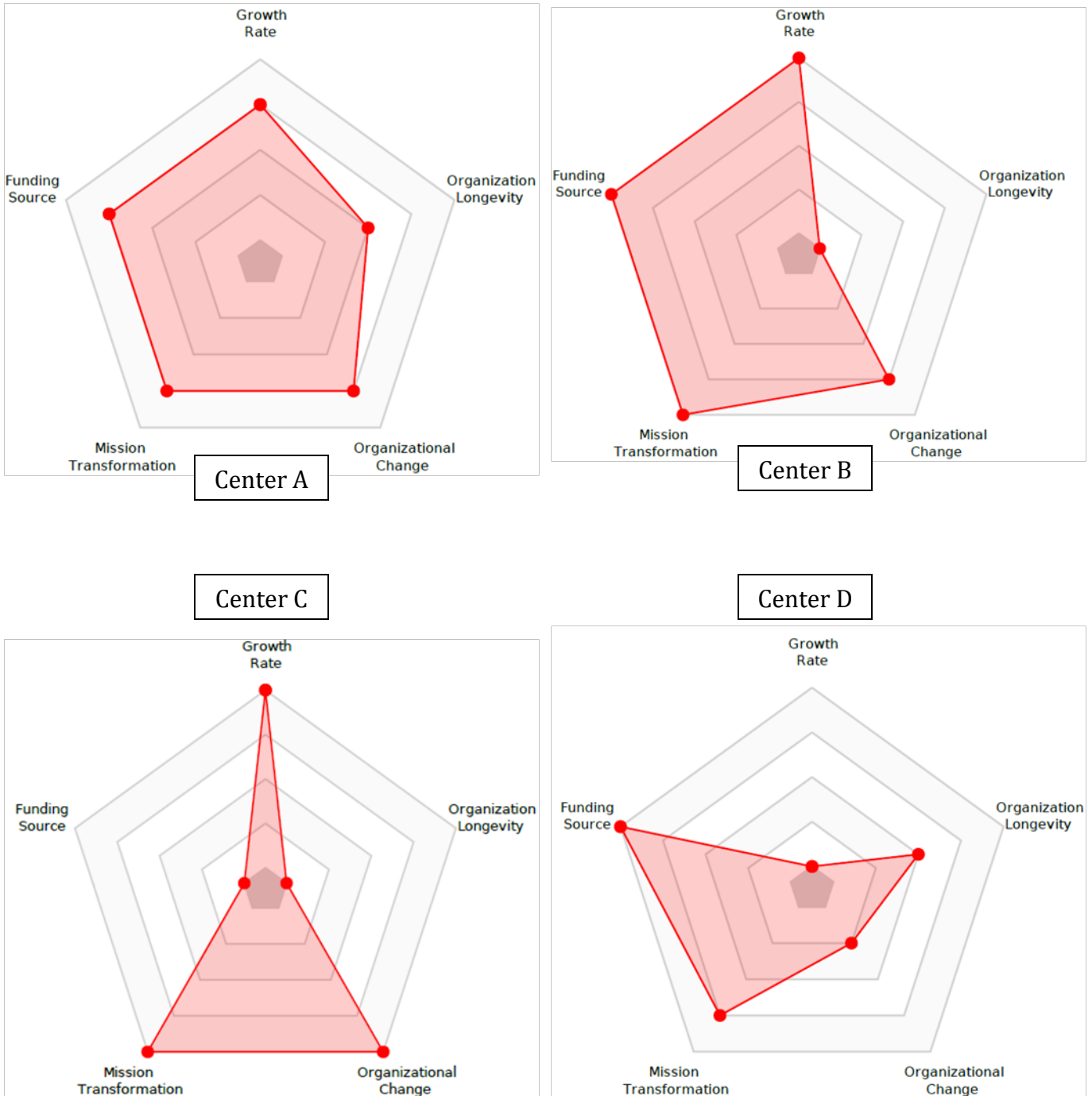


Figure 3-4: Organizational Dynamics for Centers A, B, C and D. The red data points indicate relative stability for each factor. Narrower colored surface indicates areas of dynamic change or transformation.

### *3.2.5.2 Organizational Dynamics Comparative Analysis*

#### *Summary*

Center B and C, being fairly new centers, will gain significantly by collaborating and learning from other centers

Centers B and C may be aggregated into a category based on organizational dynamics attribute of recently established centers.

#### *Observations*

- The Growth rate for three of the four centers is fairly stable, but the growth rate for Center D is very high.
- Centers B and C are fairly new. Centers A and D have been around longer, yet they are also fairly recently established.
- Centers A, B and C have minimal organizational changes, but Center D has been seeing significant organizational changes
- The mission for all four centers has been well established.
- All but Center C have well-established funding streams

#### *Finding(s)*

It may be appropriate to categorize Center C into an 'emerging center' category, since it is fairly new, and has unclear funding streams. Alternately, Centers B and C may be grouped into a broader category based on their recent establishment. Such categorization defers tailoring of information sharing and collaboration until such time as those organizations become better established. It also helps newer organizations collaborate with more mature organizations in defining appropriate set of activities, adopting best practices and establishing themselves more rapidly.



### 3.2.6 Process Management Dimension

#### 3.2.6.1 Process Management Comparative Visualization



Figure 3-5: Process Management indicators for Centers A, B, C and D. Red colored boxes indicate where each center sees itself in the process improvement chart.

### 3.2.6.2 Process Management Comparative Analysis

#### Summary

Centers A and C appear to be similar in the maturity of their process management. Center B has more mature processes in general, other than analytics. Center D has greater maturity with active use of SOPs.

#### Observations

- No data point on Centers C and D on training and certification. Center B indicates a quantitatively managed – a fairly well established process; and Center A indicates managed level of training and certification for some staff positions.
- Centers A and C report managed level process management for use of standard operating procedures (SOPs). Centers B and D report a more advanced level of Defined.
- Centers A and C indicate Defined level for the reports, analysis and other products they generate. Center D reports a managed level, and Center C reports a more advanced Quantified level.
- Centers A and C report managed level for analysis, whereas Centers B and D report an Initial or 'ad hoc' level. It is noteworthy that Center C characterizes its analytical processes as 'managed', even though it is a recently formed center.

#### Finding(s)

Centers A and C may be grouped into a common category based on the process management maturity. Centers A, C and D may collaborate with Center B to draw lessons learned, as they may seek to mature their own internal processes.

### 3.2.7 Environment Dimension

#### 3.2.7.1 Environment Comparative Visualization

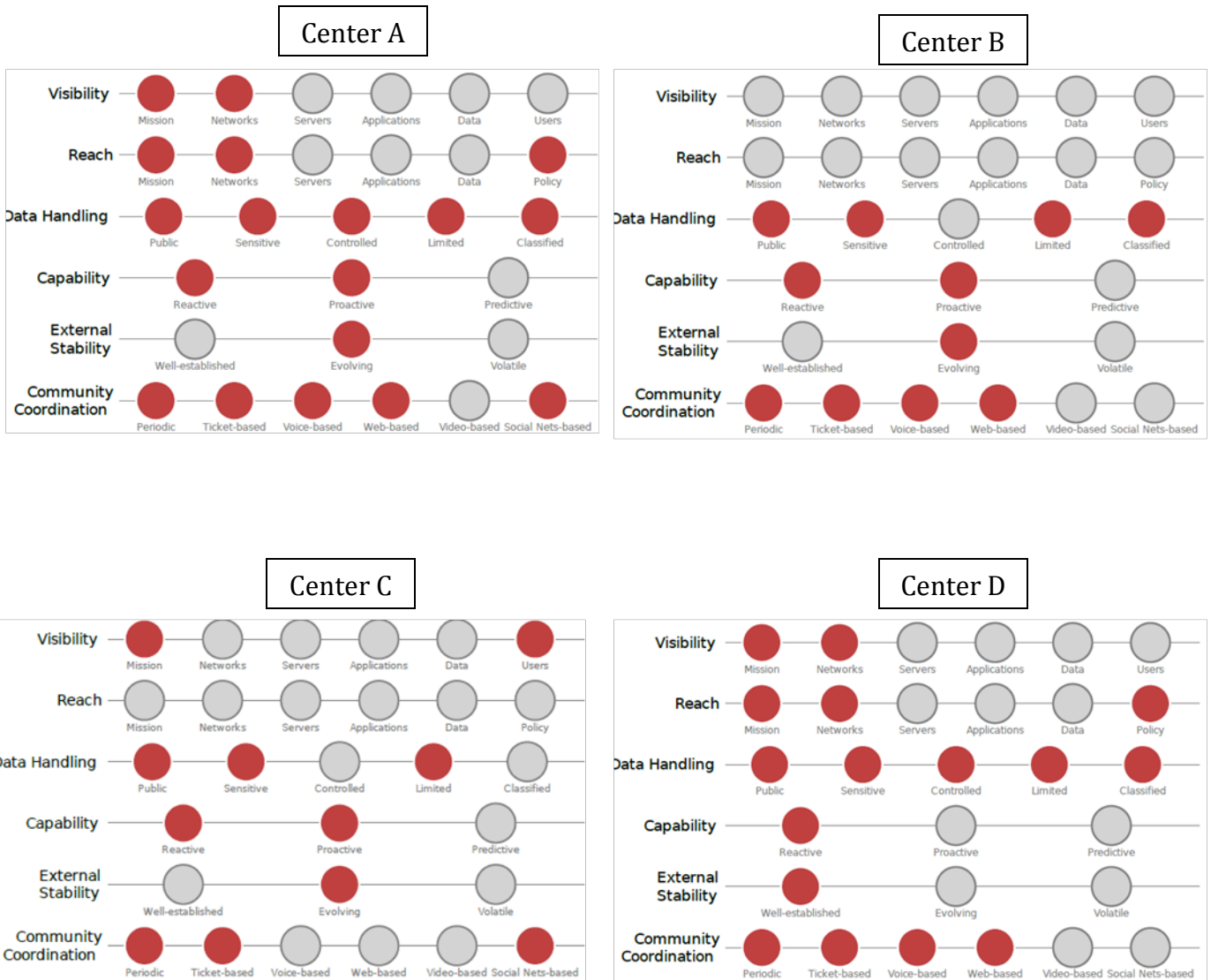


Figure 3-6: Environment of Centers A, B, C and D. Red colored circles describe the environment they operate in.

### 3.2.7.2 Environment Comparative Analysis

#### Summary

Centers A and D report similar environmental factors. Community coordination methods in general are periodic notification, ticket-based, web-based and voice-based. Centers A, B and C report proactive response capability, and that they operate in an 'evolving' stability environment.

#### Observations

- Centers A and D have similar visibility reach characteristics in their environment; No data from Center B, Center C indicates visibility over mission and users, but no information on reach.
- Centers A and D have similar data handling characteristics covering all types. Centers B and C have similar characteristics except that Center B also handles classified data.
- Centers A, B and C indicate reactive and proactive response capability, whereas Center D indicates only reactive response.
- All centers report evolving external stability, except for Center D which reports well-established external stability.
- Periodic and Ticket-based coordination is common across all Centers. Voice and Web-based coordination is common for Centers A, B and D. Centers A and C also indicate social nets based coordination.

#### Finding(s)

Information sharing may be tailored by the data handling capabilities incumbent in a center, with awareness of that in the partnering centers. Center D may explore ways to add proactive response capability in collaboration with other three centers. Centers A and D may grouped into a common category based on the similarities of their environment profiles.

### 3.2.8 External Interactions Dimension

#### 3.2.8.1 External Interactions Comparative Visualization



Figure 3-7: Organizational Interactions for Centers A, B, C and D. Red colored boxes indicate the nature of external interactions.

### **3.2.8.2 External Interactions Comparative Analysis**

#### **Summary**

Centers A and D appear to have significant commonalities with external interactions, though Center A's interactions are not as broad as Center D's. Center C is an outlier.

#### **Observations**

- While all centers report partnering or peering interactions with external organizations, the ones for Centers A, B and D indicate interactions across a range of organizations. The interactions, especially for Centers A and D cover a variety of external organizations.
- Center C only indicates interactions with Emergency Services and International entities
- Center B indicates no interactions with Emergency Services
- Center D indicates a complete range of interactions with Government entities

#### **Finding(s)**

Centers A and D may be grouped into a common category based on their commonality of external interactions. Center C may collaborate with Centers A and D to explore any benefits it may derive by expanding its range of external interactions.

### 3.3 Comparative Analysis Summary

The Operations Center Analytical Model allows better understanding of the strengths, capabilities and focus areas of operations centers. Using the visualizations from actual data, it is clear that one can glean valuable insight into an individual center. Similarly, one can use the comparative visualizations to determine appropriate areas for mutually beneficial collaboration, and shape purposeful and targeted information sharing arrangements.

The information and analysis discussed in sections 3.1 and 3.2 have focused primarily on collaboration, information sharing and possible factors for grouping centers into categories for ease of managing community collaborations.

The model and visualizations may also be used in similar manner for analyzing the centers for other possible purposes, as illustrated in Table 3.1.

## 4 Conclusion

The development of the operations model has made it possible to characterize, categorize, compare, and generally understand operations centers of all types. The result is a multi-dimensional view of an individual operations center or a set of interdependent or collaborating operations centers through scope, activities, organization dynamics, facilities, process management, external interactions, and environment.

The model is able to support a number of uses, including better understanding of processes, determination of approaches and practices for operations, and identification of load sharing and collaboration opportunities; it is also able to serve as a basis for developing an analytical foundation for collaborative operations tradecraft. The comparative model specifically provides value to centers with a cyber defense operations mission, but is designed to be generally applicable to other types of centers as well.

The potential of the model is illustrated in Section 3, using actual data collected from four out of a dozen operations centers in the cyber defense operations community. A larger data collection would enable statistical analysis of the responses, aggregation and categorization of operations centers based on their scope, activities, community environment, interactions, process management, facilities and organizational dynamics.

The analytical model presented in this paper is a first of its kind designed for comparing and categorizing operations centers. Each operations organization will benefit from using the model and the questionnaire to collect information from their peers and partners in their community. This will improve their understanding of the other centers. In addition, they will be able to use the information to tailor, optimize and formalize collaboration, information sharing, load sharing (during surge operations) and trade-craft.



## A APPENDIX – Factor Details

### A.1 Scope Details

This section provides more detail about the Scope dimension described in section 2.1. Each table lists the attributes and values for the Scope factors as follows:

- A-1 – Impact Focus
- A-2 – Sector
- A-3 – Influence
- A-4 – Scale
- A-5 – Roles
- A-6 – Functional Abstraction
- A-7 – Type of Response
- A-8 – Timeline of Response

**Table A-1 Impact Focus Attributes and Values**

<b>Attributes</b>	<b>Values</b>
<i>Minimal</i>	Localized and non-critical impact on business continuity or mission assurance
<i>Moderate</i>	Broad and non-critical impact on business continuity or mission assurance
<i>Significant</i>	Broad and significant impact on business continuity or mission assurance
<i>Critical</i>	Broad and critical impact on business continuity or mission assurance
<i>Catastrophic</i>	Grave impact on business continuity or mission assurance

**Table A-2 Sector Attributes and Values**

<b>Attributes</b>	<b>Values</b>
<i>Commercial</i>	For Profit infrastructure encompassing economic sectors, such as banking, transportation, information technology, telecommunications, etc.
<i>Federal/Civilian</i>	Information Technology and telecommunications infrastructure covering one or more agencies or departments in the federal civilian government
<i>Defense/Intelligence</i>	IT and telecommunications infrastructure covering one or more agencies and departments with national security mission
<i>State &amp; Local</i>	IT and telecommunications infrastructure covering one or more county governments, one or more states/regional government

<i>Other</i>	IT and telecommunications infrastructure covering one or more sectors not included above – such as higher education, law enforcement, healthcare, non-profits, etc.
--------------	---

**Table A-1 Influence Attributes and Values**

<b>Attributes</b>	<b>Values</b>
<i>Global</i>	Includes direct or indirect functional purview over internally owned and managed or leased infrastructure enterprise across two or more continents
<i>International</i>	Includes collaboration and partnership in use and protection across independently managed infrastructure with two or more independent nations/states
<i>National</i>	Includes two or more regions, and possibly all regions of the United States
<i>Regional</i>	Includes two or more states within a contiguous area of the United States (example: National Capital Region, Mid-Atlantic States)
<i>Local</i>	Includes a localized area, such as a state, county or tri-state area

In the table below, scale values are defined as the size and composition of the infrastructure under the organizational purview, which includes the number of managed elements and number of distinct and significant technologies within the infrastructure.

**Table A-4 Scale Attributes and Values**

<b>Attributes</b>	<b>Values</b>
<i>Small</i>	Size: 100 to 1K (managed elements – infrastructure size, or assets or lives/property) units
<i>Medium</i>	Size: 1K to 100K
<i>Large</i>	Size: 100K to 10M
<i>Very Large</i>	Size: 10M+
<i>Not Applicable</i>	An organizational mission is independent of the size and composition of the infrastructure, assets, lives or property

**Table A-5 Roles Attributes and Values**

<b>Attributes</b>	<b>Values</b>
<i>Protection</i>	Includes all activities engaged in the protection of the cyber infrastructure

<i>Incident Management</i>	Includes all activities engaged in detection, alerting, escalation, analysis, mitigation and resolution of incidents in the cyber infrastructure
<i>Analysis</i>	Includes all activities engaged in the macro level understanding of the incidents, patterns, impacts, criticality, effective short-term and long-term mitigation, and the means and methods to improve protection and incident management
<i>Governance</i>	Includes all activities associated with governance of cyber security, and includes all activities that direct or mandate actions on participating organization in improving cyber protection and incident management
<i>Collaboration and Sharing</i>	Includes all activities that allow information sharing and collaboration among participating entities to include methods, means, threats, incidents, analysis and lessons learned

**Table A-6 Functional Abstraction Attributes and Values**

<b>Attributes</b>	<b>Values</b>
<i>Policy</i>	Involves developing and providing policy and guidance for operations. This in some cases involves governance of the operations across multiple business management levels.
<i>Command &amp; Control</i>	Involves identifying and managing critical mission capabilities within the overall business or mission of the organization, consistent with policy changes and/or impacts on the business or mission due to significant incidents in the underlying cyber infrastructure
<i>Continuity of Operations</i>	Involves ensuring continuity of critical business functions or services, or mission operations, in a degraded cyberspace
<i>Cyber SA Clearinghouse</i>	Involves receiving, processing and disseminating latest cyber space situational awareness information
<i>Asset Protection</i>	Involves coordination of protection and reporting activities of IT infrastructure by IT services providers, consistent with the latest policy guidance

**Table A-7 Type of Response Attributes and Values**

<b>Attributes</b>	<b>Values</b>
<i>Tailored Information Product</i>	Preparation and dissemination of targeted analytical and awareness information products, tailored to the needs and requirements of a specific partner/consumer
<i>General Alert &amp; Information</i>	Preparation and dissemination of general analytical and awareness information products targeted to satisfy common needs of the broadest set of partners/consumers

<i>Direction</i>	Dissemination of information products coupled with specific action requirements including compliance timelines and reporting requirements. In a hierarchical structure, the mandating authority is cited and that full compliance is expected. In federated or peer-peer structures, the mandates are bound to the contracts or memoranda of understanding among the collaborating entities
<i>Analysis &amp; Recommendation</i>	Dissemination of information products coupled with “best practices” and recommended actions to improve protection or mitigate incident impacts
<i>Requested Action</i>	Dissemination of information products coupled with “voluntary” mandates of compliance with recommended actions

**Table A-8 Timeline of Response Attributes and Values**

<b>Attributes</b>	<b>Values</b>
<i>Seconds (Automated)</i>	Pace of activities involve significant or exclusive employment of pre-planned and programmed automation, in order to satisfy operational response times under a minute
<i>Minutes (Automated, with minimal human intervention)</i>	Pace of activities involve a minimal degree of human analysis and intervention, combined with high degree of automation to provide rapid but deliberate operational responses, within minutes, but may take as much as one to two hours
<i>Hours (Coordination)</i>	Pace of activities involves some degree of automation, but is combined with human intervention, collaboration/coordination and analysis, to provide a deliberate and coordinated response, within 2-4 hours, but may take up to 10-12 hours
<i>Days (Planning and Coordination)</i>	Pace of activities involve analysis, planning, proposals, coordination and approvals, prior to response, and may take several days to weeks
<i>Months (Strategic Planning and Coordination)</i>	Pace of activities involve wide-ranging analysis, planning, proposals, coordination and approvals, prior to response, and may take one or more months

## A.2 Activities Details

Details about the Activities dimension, as described in section 2.2, are provided below. Each table lists the attributes and values for the Activities factors as follows:

- A-9 – Protection
  - Preparedness – Continuous Training, Procedures and Actions that apply and maintain up-to-date protection status of the infrastructure

- Scanning & Data Capture – Continuous data collection of activity and transactions ongoing in the infrastructure to support alerting, analysis and other investigations
- Design – Continual adjustments, modifications to infrastructure, preparedness and data capture to incorporate lessons learned, new thinking, new technologies
- **A-10 – Incident Management**
  - Detection – recording and maintaining network and host security, and their latest profiles, and to be able to recognize intrusions and other suspicious traffic/activities
  - Response and Recovery – understanding the nature of intrusions and other suspicious traffic/activities , developing and following through on mitigation strategies and actions, developing and following through on recovery strategies and actions
  - Assessment – categorization of incidents, assessing their impacts, developing or refining policies and procedures, notification of significant events and planning exercises to improve incident handling
- **A-11 – Analysis**
  - Information Extraction – search and retrieval of information associated with current and past similar and related incidents to be able to perform broad and deep incident analysis
  - Event/Incident Correlation – Perform analysis to profile specific attacks, specific vulnerabilities, incident impact, patterns of attack activity in seemingly routine traffic data, and the nature of threat posed by detected attack activity patterns
  - Cyber Threat Discovery - Gather routine, continuous awareness information on cyber space, fuse and quantify collected data to chart trends and statistics, and maintain general awareness of emerging threats, ongoing attacks and past incidents, impacts, and potential mitigation, protection or recovery responses to the same

**Table A-9 Protection Attributes and Values**

<b>Attributes</b>	<b>Values</b>	<b>Definitions</b>
<b>Preparedness</b>	<i>Advisory Distribution</i>	Preparation and dissemination of Vulnerability, threat alerts and related compliance guidelines
	<i>Controlled Access</i>	User or smart agent access to Network, application, information
	<i>Controlled Insertion</i>	Technology and new or enhanced applications and services
	<i>Malicious Code Prevention</i>	Planned and verified controls for detection, removal or blocking. Deployment of software to detect and stop malicious code at

		the host, application server and application client level. (NIST 800-61)
	<i>Patch Management</i>	Controlled and verified patch updates
	<i>User Awareness &amp; Training</i>	Users should be made aware of policies and procedures regarding appropriate use of networks, systems, and applications. Information technology (IT) staff should be trained so that they can maintain their networks, systems, and applications in accordance with the organization's security standards. (NIST 800-61)
<b>Scanning &amp; Data Capture</b>	<i>Premise Monitoring</i>	Baselines, Audits and Logs of significant premise security breaches, including environmental (power, temperature, flooding)
	<i>Host Monitoring</i>	Baselines, Audits, Logs and Reporting of host configurations and unexpected configuration changes
	<i>Network &amp; Traffic Monitoring</i>	Baseline, Audits, Logs and Reporting of network configurations, unexpected configuration changes, network traffic and usage patterns, and unusual network traffic and usage patterns
	<i>Access and Usage Monitoring</i>	Baseline, Audits, Logs and Reporting of user and IT staff access and privileges, access and usage patterns, and unusual access and usage patterns
	<i>Applications/Services Monitoring</i>	Baseline, Audits, Logs and Reporting of application configurations, service configurations, unexpected configuration changes, application and service performance, traffic, application and service usage patterns, and unusual application and service traffic and usage patterns
<b>Design</b>	<i>Analysis of Lessons Learned</i>	Review of vulnerabilities in existing protection design and assessment of audits of preparedness and scanning to identify areas of design improvements
	<i>Physical &amp; Network Architecture</i>	Design of physical and network controls, processes, policies to deter unauthorized entry or use; design of sensors to monitor physical environment, and detect all entry and use of physical spaces and network; and design of reporting systems to continuously report health, performance, entry and usage

		of physical spaces and network
	<i>Access Controls</i>	To ensure that an entity can only access protected resources if they have the appropriate permissions based on the predefined access control policies(NIST 7497)
	<i>Traffic Controls</i>	To ensure that appropriate network and applications traffic based on predefined policies are allowed to enter or leave a host, system, network
	<i>Application/Services Controls</i>	To ensure that an entity can only access and consume applications/services based on predefined control policies covering users, their roles or privilege attributes
	<i>Information Controls</i>	To ensure that an entity can only access and consume or post information based on predefined control policies covering users, their roles or privilege attributes
	<i>Technology Watch and Insertion</i>	Continual analysis of ongoing advancements in technology, best practices or innovative methods for assessing methods for controlled insertion of highly relevant and valuable technologies into existing or planned designs
	<i>Advanced Training/Awareness Products</i>	Continual revisions or updates to training and advisories based on lessons learned

**Table A -10 Incident Management Attributes and Values**

<b>Attributes</b>	<b>Values</b>	<b>Definitions</b>
<b>Detection</b>	<i>Host Security</i>	Keeping hosts properly patched and configured to provide only the minimum services to the appropriate users and hosts. (NIST 800-61)
	<i>Network Security</i>	Network perimeter is configured to deny all activity that is not permitted; only necessary activity should be permitted. Secure all connection points. (NIST 800-61)
	<i>Intrusion Detection/Event Correlation</i>	Detection of unauthorized act of bypassing the security mechanism of a system (NCIRP) Correlate events among multiple indication sources to validate the existence of an incident and consolidate data. (NIST 800-61)

	<i>Network/Host Profiling</i>	Measure the characteristics of expected activity levels to better detect changes in patterns. (NIST 800-61)
<b>Response &amp; Recovery</b>	<i>Mitigation</i>	Ongoing and sustained action to reduce the probability of or lessen the impact of an adverse incident. (NCIRP)
	<i>Evidence Capture</i>	Gathering evidence during an incident to assist in resolution or legal proceedings includes computer forensics. (NIST 800-61)
	<i>Network Response Actions</i>	Configuration of network perimeter to deny all incoming traffic that is not explicitly permitted, secure all remote access methods, put all publicly accessible services on a DMZ, use private IP addresses for all hosts on internal networks. (NIST 800-61)
	<i>Host Response Actions</i>	Perform regular vulnerability assessments to identify serious risks, disable all unneeded services on hosts, run services with the least privileges possible, use host-based/personal firewalls, limit unauthorized physical access, regularly verify the permission settings for critical resources. (NIST (800-61)
	<i>Incident Response Advice</i>	Use of antivirus software, prevent installation of spyware, block suspicious files, filter spam, limited use of non-essential programs, educate users, eliminate open window shares, user web browser security, prevent open relaying of email, configure email clients.
	<i>Infrastructure Resource Reallocation</i>	Reallocate resources based on impact and criticality of affected infrastructure. (NIST 800-61)
	<i>Dynamic Defense Actions</i>	Employing a strong layered defense strategy to reduce incidents. (NIST 800-61)
	<i>Attacker Identification</i>	Identification of the attacker through validation of the attackers IP address, scanning the attackers system, use of incident databases and monitoring attacker's communications channels. (NIST 800-61)
	<i>Eradication</i>	Elimination of components of the incident. (NIST 800-61)
	<i>System Recovery</i>	Restoring systems to normal operation and harden systems to prevent similar incidents. (NIST 800-61)
	<i>Containment Strategy</i>	Contain incident before damage. (NIST 800-61)
<b>Assessment</b>	<i>Incident Reporting &amp;</i>	Record facts related to incidents and maintain records (NIST 800-61) Notify internal and external



	<i>Notification</i>	of incident status. (NIST 800-61)
	<i>Incident Categorization</i>	Categorizing incidents into potential negative impacts to information and information systems. (DoE Incident Mgt Guide)
	<i>Incident Analysis &amp; Validation</i>	Determination of an incidents scope, originator and occurrence by profiling networks and systems, understanding normal behaviors, maintain log files, perform event correlation, maintain data, filter data, collect information. (NIST 800-61)
	<i>Incident Mgt Policies &amp; Procedures</i>	Creating an incident response policy & plan, developing procedures for performing incident handling & reporting, set guidelines for communicating with outside parties, establish relationships, staffing. (NIST 800-61)
	<i>Exercise Planning</i>	Conduct exercises in which the incident management team reviews incident scenarios. (NIST 800-61)

**Table A-11 Analysis Attributes and Values**

<b>Attributes</b>	<b>Values</b>	<b>Definitions</b>
<b>Information Extraction</b>	<i>Hardware &amp; Media Analysis</i>	Monitoring malware advisories and alerts produced by technical controls (e.g., antivirus software, spyware detection and removal utilities, intrusion detection systems) to identify likely impending malware incidents. (NIST 800-83)
	<i>Incident Report/Trouble Ticket Analysis</i>	Monitoring and reviewing incident reports and information technology services trouble tickets to determine patterns suggesting impending large-scale threats
	<i>Malware Analysis and Trends</i>	Reviewing malware incident data from such primary sources as user reports, IT staff reports, and technical controls to identify malware-related activity. Constructing trusted toolkits on removable media that contain up-to-date tools for identifying malware, listing currently running processes, and performing other analysis actions. (NIST 800-83)
	<i>Network Data Analysis and Trends</i>	Reviewing and extracting network traffic data patterns against baseline to seek or identify possible malware, botnets or other malicious traffic patterns

<b>Event/Incident Correlation</b>	<i>Attack Profiling and Trends</i>	Organization and characterization of the cause-effect chain of a cyber attacks, sorted into the categories: objective, propagation, attack origin, action, vulnerability, asset, operational state effects and performance effects. (Derived from AFOSR sponsored work – 2006: AFRL-SR-AR-TR-06-0118; Author Dr. Nong Ye, Arizona State University)
	<i>Vulnerability/Risk Assessment</i>	Organization and characterization of business/mission risks associated with vulnerabilities, and the potential for those vulnerabilities to be exploited for cyber attacks, based on past or potential threats
	<i>Incident Analysis and Trends</i>	Includes cyber incident monitoring, log management, detection, cyber incident triage, event scope and characteristics, incident investigation, impact and escalation and possible mitigation strategies.
	<i>Malicious Activity Detection</i>	Continuously monitor network traffic, determines whether the traffic from one or a set of sources reveals a certain malicious activity, and then triggers an alarm when it finds such traffic. (Intro section of 2006 PhD thesis of J.Jung, MIT)
	<i>Mission Assurance</i>	Mission assurance is establishing a reasonable degree of confidence in mission success. (CMU/SEI-2005-TN-032)
	<i>Mitigation Strategy Development</i>	Best practices associated with business or mission operations risk management, along with understanding of risks in a business/mission context, identifying business/mission impact, business/mission and risks, prioritizing business/mission and technical risks, and defining risk mitigation strategies. (Refined, based on risk management definition at <a href="https://buildsecurityin.us-cert.gov/bsi/articles/best-practices/risk.html">https://buildsecurityin.us-cert.gov/bsi/articles/best-practices/risk.html</a> )
	<i>Threat Analysis</i>	Extract and characterize threat information (adversary and intent); Identify potential targets of the threat, and vulnerabilities that adversary seeks to exploit; develop tailored threat information dissemination packages to alert and advise operators that may be impacted by the threat or the underlying vulnerabilities (based on SANDIA Threat Analysis Framework – SAND

		2007-5792)
<b>Cyber Threat Discovery</b>	<i>Cyber Intelligence, Surveillance &amp; Reconnaissance (ISR)</i>	Involves acquiring, fusing and analyzing information on specific targets or areas in the cyberspace, leveraging the sets of collection and processing systems, and associated information gathering operations (revised from a DoD definition of conventional ISR).
	<i>Cyber Measurement</i>	The collection of underlying information and calculating key metrics related to business or mission assurance. For example: measure the effects of IA investment, system security, cyber activity to allow: Investment decisions and tradeoffs; Assessment of performance; Operational soundness; and Readiness/preparedness
	<i>Cyber Situational Awareness</i>	The knowledge and understanding of the current operational status, risk posture, and threats to the cyber environment gained through instrumentation, reporting, assessments, research, investigation, and analysis, which are used to enable well-informed decisions and timely actions to pre-empt, deter, defend, defeat, or otherwise militate against those threats and vulnerabilities. (NCIRP)

### A.3 Organizational Dynamics Details

This section provides more detail about the Organizational Dynamics dimension described in section 2.3. Each table lists the attributes and values for the Scope factors as follows:

- A-12 – Growth Rate
- A-13 – Organizational Longevity
- A-14 – Organizational Change
- A-15 – Mission Transformation
- A-16 – Funding Source

**Table A-12 Growth Rate Attributes and Values**

<b>Attributes</b>	<b>Values</b>
<b>Negligible</b>	An organization’s growth rate is considered negligible if they grow less than 2% within a given year
<b>Minimal</b>	An organization’s growth rate is considered Minimal if they grow between 2 and 5% within a year
<b>Low</b>	An organization’s growth rate is considered Low if they grow between

	5 and 10% within a year
<b>Medium</b>	An organization's growth rate is considered Medium if they grow between 10 and 15% within a year
<b>High</b>	An organization's growth rate is considered High if they grow more than 15% within a year

**Table A-13 Organizational Longevity Attributes and Values**

<b>Attributes</b>	<b>Values</b>
<b>Negligible</b>	The organization has existed for 0-3 years
<b>Minimal</b>	The organization has existed for 4-6 years
<b>Low</b>	The organization has existed for 7-10 years
<b>Medium</b>	The organization has existed for 11-15 years
<b>High</b>	The organization has existed for more than 15 years

**Table A-14 Organizational Changes Attributes and Values**

<b>Attributes</b>	<b>Values</b>
<b>Negligible</b>	The operations center has had no executive management changes or major turnover events over the life of the center
<b>Minimal</b>	The operations center has undergone 1-3 executive management changes or major turnover events over the life of the center
<b>Low</b>	The operations center has undergone 4-6 executive management changes or major turnover events over the life of the center
<b>Moderate</b>	The operations center has undergone 7-9 executive management changes or major turnover events over the life of the center
<b>Significant</b>	The operations center has undergone more than 10 executive management changes or major turnover events over the life of the center

**Table A-15 Mission Transformation Attributes and Values**

<b>Attributes</b>	<b>Values</b>
<b>Negligible</b>	The mission has not been changed or significantly redirected (0 times) during the life of the center
<b>Minimal</b>	Minimal mission transformation means that the mission has been changed or significantly redirected 1-3 times during the life of the center
<b>Low</b>	Minimal mission transformation means that the mission has been changed or significantly redirected 4-6 times during the life of the center

<b>Medium</b>	Minimal mission transformation means that the mission has been changed or significantly redirected 7-9 times during the life of the center
<b>High</b>	Minimal mission transformation means that the mission has been changed or significantly redirected over 10 times during the life of the center

**Table A-16 Funding Source Attributes and Values**

<b>Attributes</b>	<b>Values</b>
<b>None</b>	No clear funding source
<b>Discontinued</b>	Funding is likely to be discontinued or significantly reallocated
<b>Partial</b>	A partial funding stream is identified
<b>Full (&lt; 5 years)</b>	A full funding stream is identified and sustained, but under a 5 year period
<b>Full (&gt; 5 Years)</b>	A full funding stream is identified and constant through a 5 year or more period

#### **A.4 Facilities Details**

The Facilities dimension, as described in section 2.4, is detailed below. Each table lists the attributes and values for the factors as follows:

- A-17 – Space Size
- A-18 – Number of Desks
- A-19 – Surge Capability
- A-20 – Center Hours
- A-21 – Layout Type
- A-22 – COOP Scope
- A-23 – COOP Readiness
- A-24 – Coordination Methods

**Table A-17 Space Size Attributes and Values**

<b>Attributes</b>	<b>Values</b>
<b>Very Small</b>	The physical space used by the operations center < 5000 sq ft
<b>Small</b>	The physical space used by the operations center is between 5000 and 10,000 sq ft
<b>Medium</b>	The physical space used by the operations center is between 10,000 and 50,000 sq ft
<b>Large</b>	The physical space used by the operations center is > 50,000 sq ft

**Table A-18 Number of Desks Attributes and Values**

<b>Attributes</b>	<b>Values</b>
-------------------	---------------

<b><i>Small</i></b>	The number of desks is considered small if less than 10 desk positions exist in the operations center
<b><i>Medium</i></b>	The number of desks is considered medium if 10-30 desk positions exist in the operations center
<b><i>Large</i></b>	The number of desks is considered large if over 31-50 desk positions exist in the operations center
<b><i>Very Large</i></b>	The number of desks is considered very large if over 50 desk positions exist in the operations center



**Table A-19 Surge Capability Attributes and Values**




<b><i>Attributes</i></b>	<b><i>Values</i></b>
<b><i>Minimal</i></b>	The operations center has little to no surge capacity.
<b><i>Low</i></b>	The operations center has less than 10% available space and equipment dedicated to surge
<b><i>Medium</i></b>	The operations center has between 10% and 20% available space and equipment dedicated to surge
<b><i>High</i></b>	The operations center has more than 20% available space and equipment dedicated to surge

**Table A-20 Center Hours Attributes and Values**

<b><i>Attributes</i></b>	<b><i>Values</i></b>
<b><i>24x7</i></b>	The Operations Center mission requires it be operations all day, every day
<b><i>Business Hours</i></b>	The Operations Center maintains normal business hours
<b><i>Event Driven</i></b>	An operations center is stood up on occurrence of a highly significant incident/event, operates continuously until rescue, recovery, restoration or mitigation is complete, and then ceases to exist
<b><i>Planned Surge</i></b>	An operations centers adds staff temporarily to prepare and respond to an anticipated significant incident/event

**Table A-21 Layout Type Attributes and Values**

<b><i>Attributes</i></b>	<b><i>Values</i></b>	<b><i>Visual</i></b>
<b><i>Boardroom</i></b>	Staff surrounds a single table	
<b><i>Mission Control</i></b>	Staff is in rows facing an operational picture	

<b>Pod Style</b>	Staff functions are grouped into “pods” or groups of desks to promote collaboration	
<b>Virtual</b>	Functions are distributed over non-contiguous space and collaboration occurs over virtual means	
<b>Hybrid</b>	Functions and staff are configured in a hybrid combination of pod, virtual, boardroom or mission	

Each of the various layout styles is useful for particular purposes. The boardroom is appropriate for directed responses managed by a coordinator. Mission control is often used when multiple teams perform independent functions while working towards a common goal. Pods are useful for dynamic and flexible teams requiring a collaborative communications atmosphere. Virtual centers are physically distributed but remain connected via technology such as data feeds, wikis, blogs, and video teleconferencing. Hybrid centers combine multiple types of layouts to accommodate various team dynamics within the same center.

**Table A-22 COOP Scope Attributes and Values**

<b>Attributes</b>	<b>Values</b>
<b>None</b>	No COOP Capability
<b>Minimal</b>	Between 1% and 50% COOP capability. COOP exists, with minimal capability. All equipment and vital files, records, databases, etc. for critical functions must be hand-carried to the alternate site. The alternate site has limited space/equipment and cannot perform critical functions.
<b>Some</b>	Above 50%, but not full COOP capability. COOP exists with some capability. Some staff positions, equipment and vital files, records, databases, etc. for critical functions exist at an alternate site or backed up at a third party location. The alternate site has the following characteristics: sufficient space /equipment, capability perform essential functions for less than 30 days, reliable logistical support, services and infrastructure systems, consideration for health, safety and emotional well-being for personnel, interoperable communications, computer equipment and software.
<b>Full</b>	100% COOP capability. COOP exists with full capability. All critical staff positions, equipment and vital files, records, databases, etc. for critical functions exist at an alternate site or backed up at a third party location. The alternate site has the following characteristics: sufficient space/equipment, capability perform essential functions up to 30 days, reliable logistical support, services and infrastructure

	systems, consideration for health, safety and emotional well-being for personnel, interoperable communications, computer equipment and software.
--	--

**Table A-23 COOP Readiness Attributes and Values**

<i>Attributes</i>	<i>Values</i>
<i>None</i>	Not Applicable
<i>Days</i>	COOP exists but may one or more days to be fully operational
<i>Hours</i>	COOP exists and may take one or more hours to be fully operational
<i>In Real-Time</i>	COOP exists and is fully operational at all times

**Table A-24 Coordination Methods Attributes and Values**

<i>Attributes</i>	<i>Values</i>
<i>Periodic Notification</i>	Coordination between peers, partners and oversight organizations is achieved through periodic (monthly, weekly, daily, hourly) reports disseminated either by paper or by electronic means
<i>Ticket Based</i>	Coordination between peers, partners and oversight organizations is achieved through trouble-ticketing systems and associated work-flows
<i>Voice Based</i>	Coordination between peers, partners and oversight organizations is achieved through use of telephony, audio-teleconferencing or voice based help-desks
<i>Video Based</i>	Coordination between peers, partners and oversight organizations is achieved through use of video conferencing or streaming video media
<i>Web Based</i>	Coordination between peers, partners and oversight organizations is achieved through use of web-based electronic means, such as web-conferencing, e-mails, chat, shared web-portals, etc. These may combine audio and video methods as well.
<i>Social Nets Based</i>	Coordination between peers, partners and oversight organizations is achieved through use of advanced web and social networking media. These may combine audio, video and web based methods as well.

**A.5 Process Management Details**

Process Management, as described in section 2.5, is detailed below. The tables list the attributes and values for the factors as follows:



- A-25 – Training and Certification
- A-26 – Active Use of SOPs
- A-27 – Production
- A-28 – Analytics

**Table A-25 Training and Certification Attributes and Values**

<b>Attributes</b>	<b>Values</b>
<b>Initial</b>	Consists solely of on-the-job training, when peers and colleagues train based on experience rather than a formal program
<b>Managed</b>	Training and certification occurs in disparate functions rather than an organization as a whole; for instance, when a training program exists for only a few specialized roles
<b>Defined</b>	Various roles and functions within a center have defined training and requirements. Usually, these are both documented and have existed in the organization for a number of years.
<b>Quantitatively Managed</b>	Defined training and certification programs are monitored and measured
<b>Optimizing</b>	Metrics are used to continually update and improve training programs. Additionally, certifications are required for staff in various functions and roles

**Table A-26 Active Use of SOPs Attributes and Values**

<b>Attributes</b>	<b>Values</b>
<b>Initial</b>	The operations centers do not actively use SOPs in their day-to-day operations and individual techniques and practices exist
<b>Managed</b>	The operations center has SOPs for each function, but they are individual and not cohesive across multiple operations in the center
<b>Defined</b>	An operations center has a cohesive set of SOPs used across multiple functions and staff are trained on the use of SOPs
<b>Quantitatively Managed</b>	Measures exist that monitor the use and effectiveness of SOPs
<b>Optimizing</b>	An operations center uses the measures to proactively plan future operations and can adapt operating procedures to a given situation or scenario

**Table A-27 Production Attributes and Values**

<b>Attributes</b>	<b>Values</b>
<b>Initial</b>	The operations center has inconsistent outputs with minimal impact to their customers, partners and community members
<b>Managed</b>	An operations center has regular outputs with variable impact to their community, partners and customers
<b>Defined</b>	The outputs of the operations center are defined and have an

	impact in the external community
<i>Quantitatively Managed</i>	An operations center has useful, measured outputs, but of variable quality
<i>Optimizing</i>	The operations center's output is consistent in both quality and impact and is institutionalized within the organization

**Table A-28 Analytics Attributes and Values**

<i>Attributes</i>	<i>Values</i>
<i>Initial</i>	The center does not use analytics to augment their operations
<i>Managed</i>	Analytics are used to improve one or more operational activities
<i>Defined</i>	Analytics augment multiple functions or a defined capability
<i>Quantitatively Managed</i>	An operations center has analytics that they measure with an enterprise-wide perspective, which gives them an operational advantage
<i>Optimizing</i>	Analytics are used to achieve operational efficiency and are adapted for all varieties of operational scenarios

## A.6 External Interactions Details

The attributes and values for factors associated with External organizational Interactions dimension, described in Section 2.6, are detailed below. The table for the factor is as follows:

- A-29 – Type

**Table A-29 Type Attributes and Values**

<i>Attributes</i>	<i>Values</i>
<i>Partner</i>	Includes activities with organizations focused on the same security customers, activities, provides non-commercial service, and enhances internal security operations
<i>Peer</i>	Includes activities with organizations that offer the same services and interact with like customers
<i>Sponsor</i>	Includes interactions with committees, groups, and other organizations, which may provide funding or drive the mission of the security operations
<i>Customer</i>	Includes interactions with organizations that receive services offered by the security operations
<i>Supplier</i>	Includes interactions with organizations that offer services in support of security operations
<i>Oversight</i>	Includes interactions with committees and other entities providing policy, guidance, direction or support of security operation activities

## A.7 Environment Details

The Environment dimension, as described in section 2.7, is detailed below. The tables list the attributes and values for the factors as follows:

- A-31 – Visibility
- A-32 – Reach
- A-33 – Data Handling
- A-34 – Capability
- A-35 – External Stability
- A-36 – Community Coordination

**Table A-31 Visibility Attributes and Values**

<i>Attributes</i>	<i>Values</i>
<i>Mission</i>	The ability to know the mission needs
<i>Networks</i>	The ability to view networks and network level information
<i>Servers</i>	The ability to view systems or servers on a given network
<i>Applications</i>	The ability to view application layer tools and techniques
<i>Data</i>	The ability to view data on a network, system or application
<i>Users</i>	The ability to view data regarding people and organizations within its environment

**Table A-32 Reach Attributes and Values**

<i>Attributes</i>	<i>Values</i>
<i>Mission</i>	The ability to affect the mission objectives
<i>Networks</i>	The ability to affect networks and network level information
<i>Servers</i>	The ability to affect systems or servers on a given network
<i>Applications</i>	The ability to affect application layer tools and techniques
<i>Data</i>	The ability to affect data on a network, system or application
<i>Policy</i>	The ability to affect policies governing the environment

The following Data Handling attributes are derived from the United Kingdom's Centre for the Protection of National Infrastructure (CPNI) Information Exchange classification scheme, <http://www.cpni.gov.uk/Docs/ie-membership-guidelines.pdf>.

**Table A-33 Data Handling Attributes and Values**

<i>Attributes</i>	<i>Values</i>
<i>Public</i>	Information that is for public, unrestricted dissemination, publication, web posting or broadcast. Any member may publish the information, subject to copyright [White in CPNI]
<i>Sensitive</i>	Information can be shared with other organizations, Information Exchanges or individuals in the community, but not published or

	posted on the web [Green in CPNI]
<b>Limited</b>	Limited disclosure and restricted to members of the Information Exchange; those within their organizations (whether direct employees, consultants, contractors or outsource-staff working in the organization) who have a need to know in order to take action [Amber in CPNI]
<b>Controlled</b>	Non-disclosable information and restricted to representatives present at the meeting themselves only. Representatives must not disseminate the information outside of the exchange. Information may be discussed during a meeting, where all representatives present have signed up to these rules. Guests & others such as visiting speakers who are not full members of the Exchange will be required to leave before such information is discussed. [Red in CPNI]
<b>Classified</b>	Highly restricted information with national security classification markings. Only those authorized for access to the appropriate classification level identified in the markings, and have established/verifiable need to know may publish or subscribe to this information.

**Table A-34 Capability Attributes and Values**

<b>Attributes</b>	<b>Values</b>
<b>Reactive</b>	The center has the ability to react in response to an event
<b>Proactive</b>	The center has the ability to proactively act in preparation for an event
<b>Predictive</b>	The center has the ability to analyze data to predict upcoming events

**Table A-35 External Stability Attributes and Values**

<b>Attributes</b>	<b>Values</b>
<b>Well-established</b>	The domain is well understood, with standardized vocabulary, processes and well-defined cause/effect relationships that operations personnel can rely on to produce predictable results
<b>Evolving</b>	The domain is mostly well defined, but may be moderately changing. The relationships between root causes and predictable effects are incomplete. Analysis relies on previously developed techniques, but often requires developing new approaches to address new circumstances
<b>Volatile</b>	The domain is ill defined and continuously changing, with new concerns and root causes still emerging. The ability to accurately predict the effects of actions taken is insufficient to meet the needs of operations personnel

**Table A-36 Community Coordination Attributes and Values**

<b><i>Attributes</i></b>	<b><i>Values</i></b>
<b><i>Periodic Notification</i></b>	Coordination between peers, partners and oversight organizations in the environment is achieved through periodic (monthly, weekly, daily, hourly) reports disseminated either by paper or by electronic means
<b><i>Ticket Based</i></b>	Coordination between peers, partners and oversight organizations in the environment is achieved through trouble-ticketing systems and associated work-flows
<b><i>Voice Based</i></b>	Coordination between peers, partners and oversight organizations in the environment is achieved through use of telephony, audio-teleconferencing or voice based help-desks
<b><i>Web Based</i></b>	Coordination between peers, partners and oversight organizations in the environment is achieved through use of web-based electronic means, such as web-conferencing, e-mails, chat, shared web-portals, etc. These may combine audio and video methods as well.
<b><i>Video Based</i></b>	Coordination between peers, partners and oversight organizations in the environment is achieved through use of video conferencing or streaming video media
<b><i>Social Nets Based</i></b>	Coordination between peers, partners and oversight organizations in the environment is achieved through use of advanced web and social networking media. These may combine audio, video and web based methods as well.

## B APPENDIX B: Questionnaire Used for online and paper-based Data Collection

In the following pages, the questionnaire used for data collection is reproduced. The online version was enhanced with definitions for each area of data collection, including references to standard documents, where appropriate.

### *Tell us about yourself*

Date:

#### I. Contact Information

Name:

Email:

Phone:

#### II. About Your Role in Your Organization

Title:

Name of Organization:

Your Current Operations Role (if different from Title):

Your Specific Activities (check all that apply):

Protection			Incident Handling			Analysis		
<input type="checkbox"/> <i>Preparedness</i>	<input type="checkbox"/> <i>Scanning and Data Capture</i>	<input type="checkbox"/> <i>Design</i>	<input type="checkbox"/> <i>Detection</i>	<input type="checkbox"/> <i>Response &amp; Recovery</i>	<input type="checkbox"/> <i>Assessment</i>	<input type="checkbox"/> <i>Information Extraction</i>	<input type="checkbox"/> <i>Event or Incident Correlation</i>	<input type="checkbox"/> <i>Cyber Threat Discovery</i>

How many years in the current role:

III. Operations Center you are Describing:

Name or Type of Ops Center:

Single Center or Group of Centers:

Location(s):

## Questionnaire

### Scope

The mission, roles, scale and reach of the operations center

<b>Sector</b> (select 1)	primary focus area of the overall enterprise's mission <input type="checkbox"/> Commercial <input type="checkbox"/> Federal Civilian <input type="checkbox"/> Defense & Intelligence <input type="checkbox"/> State & Local <input type="checkbox"/> Other
<b>Roles</b>	significant roles performed by the operations center <input type="checkbox"/> Protection <input type="checkbox"/> Incident Management <input type="checkbox"/> Analysis <input type="checkbox"/> Governance <input type="checkbox"/> Collaboration & Sharing
<b>Primary Function</b> (select 1)	primary function of the operations center <input type="checkbox"/> Policy <input type="checkbox"/> Command & Control <input type="checkbox"/> Continuity of Operations <input type="checkbox"/> Cyber SA Clearing House <input type="checkbox"/> IT Protection
<b>Secondary Functions</b>	any additional functions of the operations center <input type="checkbox"/> Policy <input type="checkbox"/> Command & Control <input type="checkbox"/> Continuity of Operations <input type="checkbox"/> Cyber SA Clearing House <input type="checkbox"/> IT Protection
<b>Influence</b> (select 1)	geographic span of the infrastructure over which the operations center's mission depends <input type="checkbox"/> Local <input type="checkbox"/> Regional <input type="checkbox"/> National <input type="checkbox"/> International <input type="checkbox"/> Global
<b>Scale</b> (select 1)	number of managed elements or entities within the operations center's mission infrastructure (examples: for state/federal emergency management - # of people or size of property affected by a disaster; for network or IT – total # of computers, network systems, etc.; for IRS/US Treasury - # of individual or business tax records) <input type="checkbox"/> 100-1000 <input type="checkbox"/> 1000-100,000 <input type="checkbox"/> 100,000-10M <input type="checkbox"/> 10M+ <input type="checkbox"/> N/A
<b>Impact Focus</b>	types of incidents that fit the operations center's mission focus <input type="checkbox"/> Minimal <input type="checkbox"/> Moderate <input type="checkbox"/> Significant <input type="checkbox"/> Critical <input type="checkbox"/> Catastrophic
<b>Type of Response</b>	the operations center's response authority <input type="checkbox"/> Tailored Information Product <input type="checkbox"/> General Alert & Information <input type="checkbox"/> Direction <input type="checkbox"/> Analysis & Recommendation <input type="checkbox"/> Requested Action
<b>Timeline of Response</b>	the operations center's typical operating time intervals <input type="checkbox"/> Seconds <input type="checkbox"/> Minutes <input type="checkbox"/> Hours <input type="checkbox"/> Days <input type="checkbox"/> Months

Confidence in the responses provided in this section:

low     medium     high

Comments:



## Activities

Actions performed at the operations center organized into three areas – protection, incident management, and analysis

Protection	
<b>Preparedness</b>	<p>continuous training, procedures and actions that apply and maintain up-to-date protection status of the infrastructure</p> <p><input type="checkbox"/> Advisory Distribution      <input type="checkbox"/> Controlled Access      <input type="checkbox"/> Controlled Insertion      <input type="checkbox"/> Malicious Code Prevention      <input type="checkbox"/> Patch Management</p> <p><input type="checkbox"/> User Awareness &amp; Training</p>
<b>Scanning &amp; Data Capture</b>	<p>continuous data collection of activity and transactions ongoing in the infrastructure to support alerting, analysis and other investigations</p> <p><input type="checkbox"/> Premise Monitoring      <input type="checkbox"/> Host Monitoring      <input type="checkbox"/> Network &amp; Traffic Monitoring      <input type="checkbox"/> Access &amp; Usage Monitoring      <input type="checkbox"/> Applications / Services Monitoring</p>
<b>Design</b>	<p>continual adjustments, modifications to infrastructure, hygiene and data capture to incorporate lessons learned, new thinking, and new technologies</p> <p><input type="checkbox"/> Analysis of Lessons Learned      <input type="checkbox"/> Physical &amp; Network Architecture      <input type="checkbox"/> Access Controls      <input type="checkbox"/> Traffic Controls      <input type="checkbox"/> Applications / Services Controls</p> <p><input type="checkbox"/> Information Controls      <input type="checkbox"/> Technology Watch      <input type="checkbox"/> Technology Insertion      <input type="checkbox"/> Enhancement of Training / Awareness Products</p>
Incident Management	
<b>Detection</b>	<p>recording and maintaining network and host security as well as their latest profiles, and recognize intrusions and other suspicious traffic/activities</p> <p><input type="checkbox"/> Host Security      <input type="checkbox"/> Network Security      <input type="checkbox"/> Intrusion Detection / Event Correlation      <input type="checkbox"/> Network / Host Profiling</p>
<b>Response &amp; Recovery</b>	<p>understanding the nature of intrusions and other suspicious traffic/activities, developing and following through on mitigation strategies and actions, and developing and following through on recovery strategies and actions</p> <p><input type="checkbox"/> Containment Strategies      <input type="checkbox"/> System Recovery      <input type="checkbox"/> Eradication      <input type="checkbox"/> Attacker Identification      <input type="checkbox"/> Dynamic Defense Actions</p> <p><input type="checkbox"/> Infrastructure Resource Reallocation      <input type="checkbox"/> Incident Response Advice      <input type="checkbox"/> Host Response Actions      <input type="checkbox"/> Network Response Actions      <input type="checkbox"/> Evidence Capture</p> <p><input type="checkbox"/> Mitigation</p>
<b>Assessment</b>	<p>categorizing incidents, assessing their impacts, developing or refining policies and procedures, notification of significant events and planning exercises to improve incident handling</p> <p><input type="checkbox"/> Exercise Planning      <input type="checkbox"/> Incident Management Policies &amp; Procedures      <input type="checkbox"/> Incident Analysis &amp; Validation      <input type="checkbox"/> Incident Categorization      <input type="checkbox"/> Incident Reporting &amp; Notification</p>

<b>Analysis</b>	
<b>Information Extraction</b>	<p>search and retrieval of information associated with current and past similar and related incidents to be able to perform broad and deep incident analysis</p> <p> <input type="checkbox"/> Hardware &amp; Media Analysis           <input type="checkbox"/> Incident Report / Trouble Ticket Analysis           <input type="checkbox"/> Malware Analysis and Trends           <input type="checkbox"/> Network Data Analysis and Trends         </p>
<b>Event/Incident Correlation</b>	<p>perform analysis to profile specific attacks, specific vulnerabilities, incident impact, patterns of attack activity in seemingly routine traffic data, and the nature of threat posed by detected attack activity patterns</p> <p> <input type="checkbox"/> Threat Analysis           <input type="checkbox"/> Mitigation Strategy Development           <input type="checkbox"/> Mission Assurance           <input type="checkbox"/> Malware Activity Detection           <input type="checkbox"/> Incident Analysis and Trends         </p> <p> <input type="checkbox"/> Vulnerability /Risk Assessment           <input type="checkbox"/> Attack Trends and Profiling         </p>
<b>Cyber Threat Discovery</b>	<p>gather routine, continuous awareness information on cyber space, fuse and quantify collected data to chart trends and statistics, and maintain general awareness of emerging threats, ongoing attacks and past incidents, impacts, and potential mitigation, protection or recovery responses to the same</p> <p> <input type="checkbox"/> Cyber Intelligence, Surveillance, Reconnaissance           <input type="checkbox"/> Cyber Measurement           <input type="checkbox"/> Cyber Situational Awareness         </p>



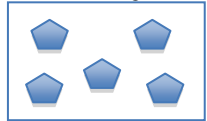

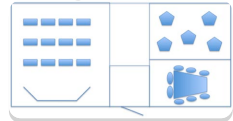
Confidence in the responses provided in this section:

low
  medium
  high

Comments:

## Facilities

The physical space, orientation, continuity of operations and surge capabilities of the operations center

<b>Space Size</b> (select 1)	total physical space used by the operations center (in sq. ft.) <input type="checkbox"/> <5,000 <input type="checkbox"/> 5,000-10,000 <input type="checkbox"/> 10,000 – 50,000 <input type="checkbox"/> > 50,000
<b>Number of Desks</b> (select 1)	number of physical seats available for the operations center's staff <input type="checkbox"/> <10 <input type="checkbox"/> 10-30 <input type="checkbox"/> 31-50 <input type="checkbox"/> > 50
<b>Center Hours</b> (select 1)	hours of operation <input type="checkbox"/> 24x7 <input type="checkbox"/> Planned Surge <input type="checkbox"/> Event Driven <input type="checkbox"/> Routine Business Hours
<b>Layout Type</b> (select 1)	physical configuration of furniture, equipment and staff <input type="checkbox"/> Boardroom  <input type="checkbox"/> Mission Control  <input type="checkbox"/> Pod Style  <input type="checkbox"/> Virtual  <input type="checkbox"/> Hybrid 
<b>Coordination Methods</b>	methods used by the operations center to coordinate with peers and partners <input type="checkbox"/> Periodic <input type="checkbox"/> Ticket-based <input type="checkbox"/> Voice-based <input type="checkbox"/> Web-based <input type="checkbox"/> Video-based <input type="checkbox"/> Social Nets-based
<b>Surge Capability</b> (select 1)	space and equipment available for a surge (# of Desks added during a crisis/emergency state) <input type="checkbox"/> Little/none <input type="checkbox"/> <10% <input type="checkbox"/> 10-20% <input type="checkbox"/> >20%
<b>COOP Scope</b> (select 1)	Percentage of continuity of normal/routine operations (facilities, systems, staff, decision making) <input type="checkbox"/> 0% <input type="checkbox"/> 1% - 50% <input type="checkbox"/> >50%; < 100% <input type="checkbox"/> 100%
<b>COOP Readiness</b> (select 1)	How quickly the switchover to COOP can occur <input type="checkbox"/> N/A <input type="checkbox"/> Days <input type="checkbox"/> Hours <input type="checkbox"/> In Real Time

Confidence in the responses provided in this section:

low       medium       high

Comments:

## Organizational Dynamics

The growth, change, and development of the operations center

<b>Organizational Longevity</b> (select 1)	number years the operations center has been in existence	<input type="checkbox"/> 0-3	<input type="checkbox"/> 4-6	<input type="checkbox"/> 7-10	<input type="checkbox"/> 11-15	<input type="checkbox"/> 16 or more
<b>Growth Rate</b> (select 1)	growth rate of the operations center staff, in the most recent year	<input type="checkbox"/> <2%	<input type="checkbox"/> 2.1-5%	<input type="checkbox"/> 5.1-10%	<input type="checkbox"/> 10.1-15. %	<input type="checkbox"/> >15%
<b>Funding Source</b> (select 1)	consistency and predictability of funding for the operations center	<input type="checkbox"/> None	<input type="checkbox"/> (to be) Discontinued	<input type="checkbox"/> Partial	<input type="checkbox"/> Full (<5 years)	<input type="checkbox"/> Full (>=5 years)
<b>Organizational Changes</b> (select 1)	number of executive management changes or major turnover events over the life of the operations center	<input type="checkbox"/> None	<input type="checkbox"/> 1-3	<input type="checkbox"/> 4-6	<input type="checkbox"/> 7-9	<input type="checkbox"/> 10 or more
<b>Mission Transformation</b> (select 1)	number of significant mission changes over the life of the operations center	<input type="checkbox"/> None	<input type="checkbox"/> 1-3	<input type="checkbox"/> 4-6	<input type="checkbox"/> 7-9	<input type="checkbox"/> 10 or more

Confidence in the responses provided in this section:

low     medium     high

Comments:

## Process Management

The operations center's experience, strength, and improvements in processes

<p><b>Training and Certification</b> (select 1)</p>	<p>planning and execution in training and certifying the operations center's staff for specific job functions</p>				
<p><b>Active Use of SOPs</b> (select 1)</p>	<p>how does the operations center use Standard Operating Procedures (SOPs) on a daily basis</p>				
<p><b>Production</b> (select 1)</p>	<p>ability to output products to the operations center's customers, partners and community members</p>				
<p><b>Analytics</b> (select 1)</p>	<p>maturity of the analytics used within the operations center's daily operations</p>				

Confidence in the responses provided in this section:

low     medium     high

Comments:

## Environment

Physical or social factors outside the control of the operations center and the impact of those factors on a center's ability to understand, respond, influence, or collaborate with other operations centers

<b>Visibility</b>	information available in the operations center <input type="checkbox"/> Mission <input type="checkbox"/> Networks <input type="checkbox"/> Servers <input type="checkbox"/> Applications <input type="checkbox"/> Data <input type="checkbox"/> Users
<b>Reach</b>	organizational areas that the operations center can directly influence/affect <input type="checkbox"/> Mission <input type="checkbox"/> Networks <input type="checkbox"/> Servers <input type="checkbox"/> Applications <input type="checkbox"/> Data <input type="checkbox"/> Policy
<b>Community Coordination</b>	methods used in the community (regardless of what methods the specific operations center uses) for coordinating activities across peer, partner and oversight organizations <input type="checkbox"/> Periodic <input type="checkbox"/> Ticket-based <input type="checkbox"/> Voice-based <input type="checkbox"/> Web-based <input type="checkbox"/> Video-based <input type="checkbox"/> Social Nets-based
<b>Data Handling</b>	Data handling and distribution types used in the community <input type="checkbox"/> Public <input type="checkbox"/> Sensitive <input type="checkbox"/> Limited <input type="checkbox"/> Controlled <input type="checkbox"/> Classified
<b>Capability</b>	the operations center's methods for responding to events/incidents <input type="checkbox"/> Reactive <input type="checkbox"/> Proactive <input type="checkbox"/> Predictive
<b>External Stability</b> (select 1)	stability of the operations center's operational domain (know-how, mature processes, effective coordination) <input type="checkbox"/> Well-established <input type="checkbox"/> Evolving <input type="checkbox"/> Volatile

Confidence in the responses provided in this section:

low       medium       high

Comments:

## External Interactions – relationships

Types of relationships the operations center has with external organizations

External Organizations	
<b>Emergency Services</b> Is my ...	collaboration and support services during emergencies, natural disasters or other catastrophic conditions <input type="checkbox"/> Customer <input type="checkbox"/> Supplier <input type="checkbox"/> Peer <input type="checkbox"/> Partner <input type="checkbox"/> Sponsor <input type="checkbox"/> Overseer
<b>International</b> Is my .....	awareness of and adherence to rules and laws of engagement in host countries <input type="checkbox"/> Customer <input type="checkbox"/> Supplier <input type="checkbox"/> Peer <input type="checkbox"/> Partner <input type="checkbox"/> Sponsor <input type="checkbox"/> Overseer
<b>Government</b> Is my ...	government's oversight role, government as a customer, sponsor, or partner <input type="checkbox"/> Customer <input type="checkbox"/> Supplier <input type="checkbox"/> Peer <input type="checkbox"/> Partner <input type="checkbox"/> Sponsor <input type="checkbox"/> Overseer
<b>Law Enforcement</b> Is my ...	interactions for criminal, counter-terrorism or other critical investigations <input type="checkbox"/> Customer <input type="checkbox"/> Supplier <input type="checkbox"/> Peer <input type="checkbox"/> Partner <input type="checkbox"/> Sponsor <input type="checkbox"/> Overseer
<b>Commercial</b> Is my ...	interactions with businesses that are suppliers, subscribers, peers or partners <input type="checkbox"/> Customer <input type="checkbox"/> Supplier <input type="checkbox"/> Peer <input type="checkbox"/> Partner <input type="checkbox"/> Sponsor <input type="checkbox"/> Overseer
<b>Intelligence</b> Is my ...	interactions with defense and intelligence agencies for counter-terrorism, counter-intelligence, etc. <input type="checkbox"/> Customer <input type="checkbox"/> Supplier <input type="checkbox"/> Peer <input type="checkbox"/> Partner <input type="checkbox"/> Sponsor <input type="checkbox"/> Overseer

Confidence in the responses provided in this section:

low     medium     high

Comments:

## C APPENDIX C: Changes to the Model

A number of changes were made to the document since the first version was delivered to U.S. CERT in April 2011.

The table below summarizes the key improvements and changes:

### Changes to the Model:

- Some of the names used in factors and attributes of Activities Dimension were changed to help clarify their purpose:
  - Hygiene was replaced with Preparedness
  - Directed Synthesis was replaced with Event/Incident Correlation
  - General Synthesis was replaced with Cyber Threat Discovery
- The visual for Facilities dimension was changed to allow easy comparison, and a few attributes and factors were changed as well:
  - A tabular form is used in the visual to show all possible values for each factor
  - Icons are used to show applicable coordination methods
  - COOP related attributes were renamed to COOP Scope and COOP Readiness, with values reflecting the new names
- The values for attributes associated with Organizational Dynamics were categorized into five possible sets. The visual now shows area covered by the selected values. Narrower areas indicate where an operations center is seeing dynamic changes
- The Subjective Maturity dimension has been renamed to Process Management
  - The definitions for this dimension were tweaked to improve clarity
- In the Environment dimension, the names for values – systems and humans, were replaced by servers and users, respectively
- Also, in the Environment dimension, ‘classified’ was added as a value for data handling
- Lastly, some improvements were made to the External organizational Interactions Dimension
  - Internal interactions were dropped from the dimension and visual
  - Types of interactions were retained, but Nature of interactions were dropped from the dimension and visuals
  - Supplier type value was added to the interactions
  - The definition of the types were reworded to clarify that ‘external organization is my type (customer, supplier, peer, etc.)’ to indicate interactions.